ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΥΛΛΗΨΗ ΠΑΚΕΤΩΝ (PACKET CAPTURING) ΣΕ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΩΝ:

ΔΕΛΕΓΚΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΑΠΑΡΙΣΤΕΙΔΗΣ ΓΕΩΡΓΙΟΣ

ΤΣΕΓΓΕΝΕΣ ΑΘΑΝΑΣΙΟΣ

ΕΙΣΗΓΗΤΗΣ:

ΔΑΡΣΙΝΟΣ ΒΑΣΙΛΕΙΟΣ

ΠΑΤΡΑ 2010

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1

ΣΥΛΛΗΨΗ ΠΑΚΕΤΩΝ (PACKET CAPTURING) ΣΕ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

1. Εισαγωγή

1.1 Διαδίκτυο και σύλληψη πακέτων

Ο παγκόσμιος ιστός δεν διαφέρει σε τίποτα από μια κοινωνία. Το Διαδίκτυο θα μπορούσε εύκολα να διεκδικήσει τον τίτλο ενός από τα θαύματα του σύγχρονου κόσμου. Πρόκειται για ένα μέσο που δίνει σε πραγματικό χρόνο πρόσβαση σε πληροφορία, γνώση αλλά και ψυχαγωγία. Οι ταχύτητες συνεχώς αυξάνονται κάνοντας την πληροφορία ακόμη πιο προσβάσιμη, ενώ και τα δίκτυα που χρησιμοποιούνται εξελίσσονται με γοργούς ρυθμούς ώστε η πληροφορία αυτή να είναι διαθέσιμη σε μεγαλύτερα τμήματα του πληθυσμού. Το πάτημα και μόνο του κουμπιού λειτουργίας ενός υπολογιστή συνδεδεμένου στο Διαδίκτυο, τον φέρνει σε άμεση σχεδόν επαφή με άλλους υπολογιστές, servers, υπηρεσίες, που θα ζητήσουν να λάβουν πληροφορίες για τα προγράμματα, το λειτουργικό ή θα θελήσουν να προμηθεύσουν στον υπολογιστή τις τελευταίες διαθέσιμες ενημερώσεις, μέσα από αυτοματοποιημένες διαδικασίες που ο χρήστης μπορεί να μην καταλάβει καν. Στην γενική του έννοια, διαδίκτυο είναι ένα δίκτυο ηλεκτρονικών υπολογιστών που (δια)συνδέει άλλα δίκτυα. Ο αντίστοιχος αγγλικός όρος internet προκύπτει από τη σύνθεση λέξεων inter-network.

Πολύ εύκολα μπορεί κάποιος να επικοινωνήσει με υπολογιστές σε όλο τον κόσμο, με σκοπό την ενημέρωση, την επικοινωνία με άλλα άτομα αλλά και για πολλούς ακόμη λόγους. Όμως τα πράγματα στο διαδίκτυο και ειδικότερα στα επιμέρους δίκτυα που δημιουργούνται, δεν είναι όσο απλά μπορεί να φαντάζουν στα μάτια ενός αρχάριου χρήστη. Συχνά δημιουργούνται προβλήματα επικοινωνίας μεταξύ των υπολογιστών ενός δικτύου ή ενός εξυπηρετητή με αποτέλεσμα η επικοινωνία να καθίσταται πολλές φορές αδύνατη. Αυτός είναι ένας από τους μεγαλύτερους πονοκεφάλους για τους διαχειριστές των δικτύων, δηλαδή η επίλυση προβλημάτων επικοινωνίας μεταξύ των

υπολογιστών. Για την επίλυση τέτοιων προβλημάτων έχει αναπτυχθεί μια μέθοδος παρακολούθησης των δικτύων η οποία λέγεται ***«σύλληψη πακέτων»***. Αυτή η τεχνική ονομάζεται έτσι διότι συλλέγει τα πακέτα δεδομένων που μεταδίδονται μέσω του δικτύου που μας ενδιαφέρει και με αυτόν τον τρόπο ο διαχειριστής ή ο μηχανικός του δικτύου βλέποντας τα πακέτα αυτά, είναι σε θέση να διαγνώσει το πρόβλημα και να το επιλύσει πιο εύκολα από ότι στο παρελθόν.

Στις επόμενες ενότητες θα παρουσιαστούν τα είδη των δικτύων και τα στοιχεία τους, ο τρόπος λειτουργίας τους με απλές έννοιες και η λεπτομερέστερη ανάπτυξη της έννοιας και της λειτουργίας της «σύλληψης πακέτων» ή όπως αναφέρεται της μεθόδου «Sniffing».

1.2 Ιστορία του Διαδικτύου

Τα θεμέλια του Διαδικτύου τα έθεσε ο Βάνεβαρ Μπους (Vannevar Bush) όταν στο κείμενό του “As We May Think” αναφέρθηκε σε ένα “γαλαξιακό δίκτυο” συνδεδεμένων υπολογιστών. Ο πυρήνας του Διαδικτύου ξεκίνησε το 1969 με την ονομασία ARPANET στην Υπηρεσία Προηγμένων Αμυντικών Ερευνών (Defense Advanced Research Projects Agency, DARPA) του Υπουργείου Άμυνας των ΗΠΑ. Ένα σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο έχτισε την πρώτη Διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet. Ωστόσο, η τεράστια ανάπτυξη του Διαδικτύου επήλθε όταν ο Σύμβουλος του CERN Τιμ Μπέρνερς-Λι δημιούργησε τις υποδομές για την υπηρεσία του Παγκόσμιου Ιστού. Στη δεκαετία του 1990 το Διαδίκτυο γνώρισε τρομακτική ανάπτυξη, απορροφώντας επιτυχώς την πλειοψηφία των παλιότερων δικτύων υπολογιστών. Αυτή η ανάπτυξη συχνά αποδίδεται στην έλλειψη κεντρικού ελέγχου για το Διαδίκτυο, η οποία επιτρέπει την οργανική ανάπτυξη του, όπως και στο μη ιδιοκτησιακό καθεστώς των πρωτοκόλλων του, τα οποία απέτρεψαν την άσκηση ελέγχου από μία και μόνο εταιρεία. Το πρώτο πράγμα που θα πρέπει να συνειδητοποιήσει κάθε χρήστης του Ίντερνετ, είναι ότι ο παγκόσμιος ιστός δε διαφέρει σε τίποτα από μια κοινωνία. Από αυτή την άποψη λοιπόν, κρύβει αντίστοιχους κινδύνους και απαιτεί αντίστοιχα μέτρα προστασίας από αυτούς. Η

σωστή και τακτική ενημέρωση σχετικά με τη φύση των κινδύνων αλλά και τον τρόπο αντιμετώπισης τους γίνεται έτσι απαραίτητη προκειμένου να ελαχιστοποιηθεί ο κίνδυνος έκθεσης του υπολογιστή στους βασικότερους τουλάχιστον κινδύνους. [1] [2]

Ένα δείγμα της εξάπλωσης του διαδικτύου μπορεί ν' αποτελέσουν τα σχετικά δημοσιεύματα όχι στον ειδικό τύπο, αλλά στα περιοδικά ποικίλης ύλης.

1.3 Διαδίκτυο - Δίκτυο υπολογιστών

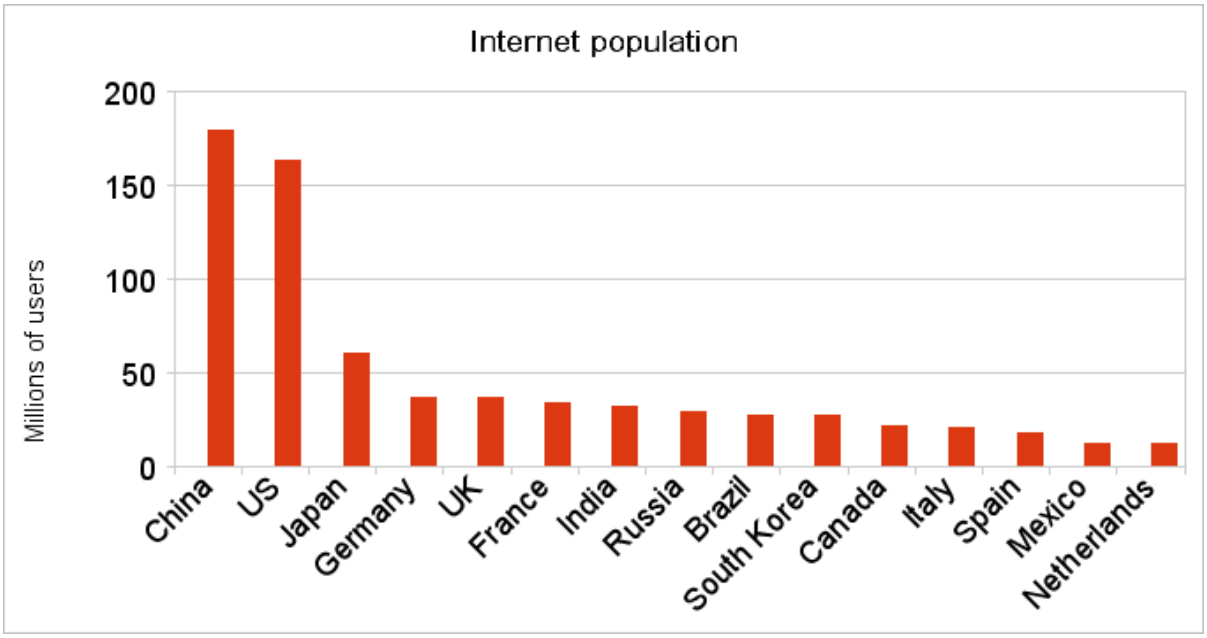
Στην γενική του έννοια, διαδίκτυο είναι ένα δίκτυο -ένα σύνολο- ηλεκτρονικών υπολογιστών που (δια)συνδέει άλλα δίκτυα. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη του μορφή, με τους όρους Διαδίκτυο, Ιντερνέτ ή Ίντερνετ (με κεφαλαίο το αρχικό γράμμα) περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του. Το Διαδίκτυο χρησιμοποιεί μετάδοση πακέτων δεδομένων (packet switching) και το πρωτόκολλο επικοινωνίας TCP/IP. Σήμερα, ο όρος διαδίκτυο κατέληξε να αναφέρεται στο παγκόσμιο αυτό δίκτυο. Η τεχνική της σύνδεσης δικτύων μέσω packet switching και TCP/IP ονομάζεται *internetworking*. Στους πίνακες 1 και 2 βλέπουμε τον αριθμό των χρηστών του διαδικτύου τα τελευταία χρόνια αλλά και στις μεγαλύτερες πληθυσμιακά χώρες.

Έτος	Αριθμός υπολογιστών
1977	111
1981	213
1983	562
1984	1.000
1986	5.000
1987	10.000
1989	100.000
1992	1.000.000
2001	150.000.000-175.000.000
2002	>200.000.000
2010	80% του πλανήτη θα είναι στο διαδίκτυο

Πίνακας 1: Αύξηση των χρηστών του διαδικτύου

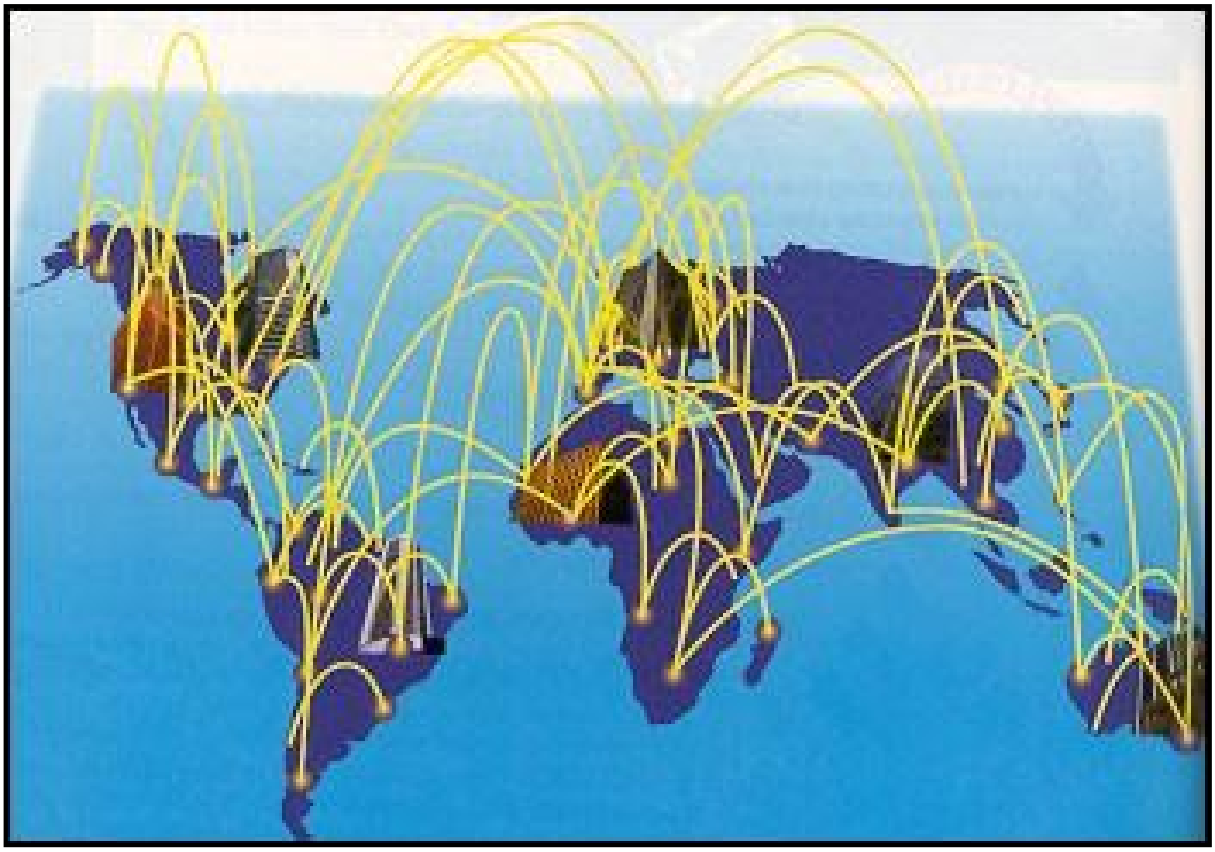
[1] "Άρθρο από Βικιπαιδεία" (http://en.wikipedia.org/wiki/History_of_the_Internet)

[2] "Άρθρο από Βικιπαιδεία" (http://el.wikipedia.org/wiki/BF)



Πίνακας 2: Αριθμός χρηστών στις μεγαλύτερες πληθυσμιακά χώρες του πλανήτη (σε εκατομμύρια)

Τα δίκτυα μπορούν να ταξινομηθούν με βάση το στρώμα δικτύων (network layer) με το οποίο λειτουργούν, σύμφωνα με τα βασικά πρότυπα αναφοράς που θεωρούνται ως πρότυπα στη βιομηχανία. Όπως το πρότυπο ακολουθίας πρωτοκόλλου Διαδικτύου Internet Protocol Suite (IP, 5 επίπεδα) ή το πρότυπο αναφοράς διασύνδεσης ανοικτών συστημάτων OSI (το πρότυπο με τα 7 επίπεδα -) το οποίο είναι περισσότερο γνωστό στον ακαδημαϊκό κόσμο. Η πλειοψηφία των δικτύων χρησιμοποιεί το πρωτόκολλο IP.



Εικόνα 1.1: Η εξάπλωση του διαδικτύου

1.4 Διάκριση Δικτύων

Τα Δίκτυα Ηλεκτρονικών Υπολογιστών φέρουν τους εξής χαρακτηρισμούς, που καθορίζουν και την κατηγορία τους :

Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως Ενσύρματα ή Ασύρματα. Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως Δημόσια ή Ιδιωτικά δίκτυα. Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως Τοπικά (LAN και WLAN), Μητροπολιτικά (**MAN** και **WMAN**), Ευρείας κάλυψης (**WAN** και **WWAN**) και Προσωπικά (**PAN** και **WPAN**).

1.4.1 Δίκτυο τοπικής περιοχής (τοπικό LAN)

Ένα δίκτυο που καλύπτει μια μικρή γεωγραφική περιοχή, όπως ένα σπίτι, ένα γραφείο, ή ένα κτήριο. Σύγχρονα LANs είναι πλέον πιθανά να βασιστούν στην τεχνολογία Ethernet. Παραδείγματος χάριν, μια βιβλιοθήκη θα έχει ενσύρματο ή

ασύρματο τοπικό LAN για την επικοινωνία των χρηστών, για να δια-συνδέσει τις τοπικές συσκευές (π.χ., εκτυπωτές και κεντρικοί υπολογιστές) και για να συνδέεται με το Διαδίκτυο. Όλοι οι Ηλεκτρονικοί Υπολογιστές στη βιβλιοθήκη συνδέονται με καλώδιο κατηγορίας 5 (Cat5), μέσω του οποίου περνά το πρωτόκολλο διασύνδεσης ieee 802,3 και συνδέεται τελικά με το Διαδίκτυο. Το καλώδιο στους κεντρικούς υπολογιστές είναι πιο ενισχυμένο (cat5), και μπορεί να υποστηρίξει το πρωτόκολλο ieee 802,3 σε ταχύτητες μέχρι και 1 Gbit/s.

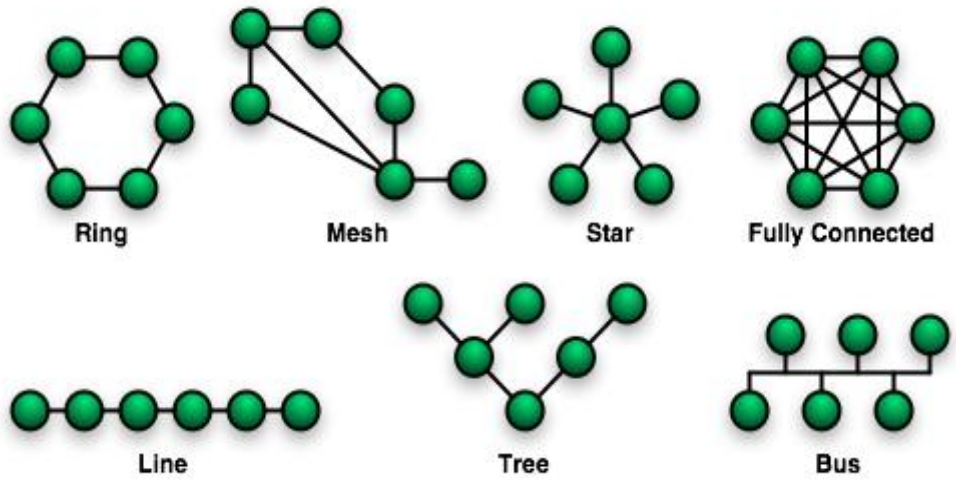
Το δίκτυο λειτουργεί ως εξής. Οι υπολογιστές προσωπικού μπορούν να φτάσουν σε όλους τους εκτυπωτές, στα αρχεία ελέγχου, στο ακαδημαϊκό δίκτυο και το Διαδίκτυο δηλαδή παντού μέσα στο δίκτυο. Οι υπολογιστές χρηστών μπορούν να φτάσουν στο Διαδίκτυο και τον κατάλογο εκτυπωτών για σύνδεση σε κάποιο κεντρικό εκτυπωτή. Κάθε ομάδα εργασίας μπορεί να φτάσει στον τοπικό εκτυπωτή της. Σημειώστε ότι οι εκτυπωτές δεν είναι προσιτοί από έξω από την ομάδα εργασίας τους.
Τα χαρακτηριστικά καθορισμού των LANs, σε αντίθεση με των WANs (δίκτυα ευρείας περιοχής), περιλαμβάνουν υψηλότερα ποσοστά επιτυχημένης μεταφοράς αρχείων, λόγω της μικρότερης γεωγραφικής απόστασης, και της έλλειψης ανάγκης για μισθωμένες γραμμές τηλεπικοινωνιών οι οποίες πολλές φορές παρουσιάζουν προβλήματα. Ένα LAN δίκτυο Ethernet λειτουργεί σε ταχύτητες έως και 10 Gbit/s. Αυτός είναι ο ρυθμός μεταφοράς δεδομένων. Τα Ethernet περιλαμβάνουν προγράμματα που πιάνουν ταχύτητες έως 100 Gbit/s.

1.4.2 Τοπολογία δικτύων (Network topology)

Η τοπολογία δικτύων είναι η μελέτη της ρύθμισης ή της χαρτογράφησης των στοιχείων (συνδέσεις, κόμβοι, κ.λπ....) ενός δικτύου, ιδιαίτερα των φυσικών (πραγματικών) και λογικών (ιδεατές) διασυνδέσεων μεταξύ των κόμβων.
Ένα δίκτυο τοπικής περιοχής (τοπικό LAN) είναι ένα παράδειγμα ενός δικτύου που έχει φυσική αλλά και λογική τοπολογία. Οποιοσδήποτε δεδομένος κόμβος στο τοπικό LAN θα έχει μια ή περισσότερες συνδέσεις με έναν ή περισσότερους άλλους κόμβους στο δίκτυο και η χαρτογράφηση αυτών των συνδέσεων και κόμβων επάνω σε μια γραφική παράσταση οδηγεί σε μια γεωμετρική μορφή που καθορίζει τη φυσική τοπολογία του δικτύου. Επιπλέον, η χαρτογράφηση της ροής των στοιχείων μεταξύ των κόμβων στο δίκτυο καθορίζει τη λογική τοπολογία του δικτύου. Είναι σημαντικό

να σημειωθεί ότι οι φυσικές και λογικές τοπολογίες μπορούν να είναι ίδιες σε οποιοδήποτε δίκτυο αλλά μπορούν επίσης να είναι διαφορετικές.

Οποιαδήποτε ιδιαίτερη τοπολογία δικτύων καθορίζεται μόνο από τη γραφική χαρτογράφηση της διαμόρφωσης των φυσικών ή λογικών συνδέσεων μεταξύ των κόμβων.. Οι αποστάσεις μεταξύ των κόμβων, των φυσικών διασυνδέσεων, των ποσοστών μετάδοσης, ή των τύπων σημάτων μπορούν να διαφέρουν σε δύο δίκτυα και όμως οι τοπολογίες τους μπορούν να είναι ίδιες. [3]



Εικόνα 1.2: Διάγραμμα των διαφορετικών τοπολογιών δικτύων.

Η ρύθμιση ή η χαρτογράφηση των στοιχείων ενός δικτύου προκαλεί ορισμένες βασικές τοπολογίες που μπορούν έπειτα να συνδυαστούν για να διαμορφώσουν τις πιο σύνθετες τοπολογίες (υβριδικές τοπολογίες).

Οι πιο κοινές τοπολογίες είναι:

- Bus (Linear, Linear Bus)
- Star-«αστέρας»
- Ring
- Mesh
- Partially connected mesh (or simply 'mesh')

[3] “Τοπολογίες Δικτύων από Βικιπαιδεία” (www.wikipedia.org/wiki/Network_topology)

- Fully connected mesh
- Tree
- Hybrid
- Point to Point

1.5 Πρωτόκολλα Δικτύων

Τα πιο βασικά πρωτόκολλα είναι:

1. Ethernet
2. Token Ring
3. ARCnet
4. Fiber Distributed Data Interconnect (FDDI)

Το βασικότερο πρωτόκολλο που χρησιμοποιείται ευρέως για μικρά δίκτυα είναι το Ethernet και αποτελεί την πλέον διαδεδομένη μέθοδο υλοποίησης τοπικών δικτύων (LAN) με τοπολογία αστέρα (Star) ή αρτηρίας (BUS), ενώ με βάση την αρχιτεκτονική που ακολουθούν τα δίκτυα χωρίζονται σε Ομότιμα (Peer-to-Peer) και στα δίκτυα πελάτη-διακομιστή (Server-based).

1.5.1 Ομότιμα - Peer to Peer (P2P)

Ένα τέτοιο δίκτυο επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Αυτό σημαίνει ότι όλοι οι κόμβοι του δικτύου έχουν τα ίδια δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο μπορούν να διαβαστούν από όλους τους υπόλοιπους και αντίστροφα. Υπάρχουν βέβαια και κάποιοι περιορισμοί οι οποίοι καθορίζονται πάντα από τον εκάστοτε κόμβο. Σε αυτού του τύπου το δίκτυο χρησιμοποιούνται συνήθως τοπολογίες αστέρα με Hub ή διαύλου. Τα πλεονεκτήματα ενός τέτοιου δικτύου είναι το χαμηλό κόστος και η ευκολία εγκατάστασης. Επίσης μπορεί ο καθένας κόμβος να σώζει τα αρχεία του σε οποιονδήποτε άλλο θέλει και έτσι να υπάρχουν πάντα αντίγραφα ασφαλείας. [4]

[4] “Peer to Peer” Από Βικιπαιδεία, (http://el.wikipedia.org/wiki/Peer-to-peer)

1.5.2 Πελάτη-Διακομιστή (Server-Based)

Εδώ δεν ισχύει πλέον η ισοτιμία μεταξύ των κόμβων, ένας ή περισσότεροι κεντρικοί ταχύτατοι υπολογιστές αναλαμβάνουν να κρατούν αποθηκευμένα όλα τα απαραίτητα αρχεία. Όλοι οι υπόλοιποι κόμβοι συνδέονται με τους κεντρικούς αυτούς υπολογιστές ή διακομιστές (servers), προκειμένου να αντλήσουν όποιες πληροφορίες χρειάζονται. Εντολές για εκτύπωση ή ηλεκτρονικό ταχυδρομείο(e-mail) περνούν πρώτα από το διακομιστή και στη συνέχεια εκτελούνται. Η αρχιτεκτονική αυτή καλείται Server-Client, όπου «πελάτες» χαρακτηρίζονται όλοι οι κόμβοι. Το πρότυπο Server- Client συναντάται σε μεγάλα δίκτυα δεκάδων ή και εκατοντάδων κόμβων-πελατών. Το κόστος είναι υψηλότερο από αυτό του Peer-to-Peer, αλλά προσφέρει περισσότερη ασφάλεια στα δεδομένα, αφού υπάρχει μεγαλύτερος έλεγχος των δικαιωμάτων κάθε κόμβου. [5]

1.5.3 Πρωτόκολλο Ethernet

Το Ethernet αναπτύχθηκε το 1960 από κοινού από τις Intel, Xerox και DEC και παρουσιάστηκε πρώτη φορά το 1973 στα εργαστήρια Xerox PARC, από τους Robert Metcalfe και David Boggs. [6] Το πρωτόκολλο Ethernet περιλαμβάνει δύο βασικές υποκατηγορίες, οι οποίες ξεχωρίζουν κυρίως για το ρυθμό μεταφοράς δεδομένων. Η μία είναι η απλή Ethernet και χαρακτηρίζεται από την ταχύτητα των 10Mbps και η άλλη είναι η Fast Ethernet που έχει αντίστοιχη ταχύτητα τα 100Mbps. Υπάρχει και μία ακόμα υποκατηγορία η οποία υποστηρίζει ταχύτητες 1000Mbps(1Gbps) και ονομάζεται Gigabit Ethernet, αλλά δεν είναι τόσο διαδεδομένη ακόμα λόγω του υψηλού κόστους. Το Ethernet επιτρέπει τη μετάδοση πακέτων δεδομένων (Frames ή Packets) μεταβλητού μεγέθους από 72 έως και 1518 Bytes με την χρήση της τεχνολογίας CSMA/CD1. Κάθε πακέτο περιέχει μία κεφαλίδα (Header) στην οποία περιλαμβάνονται πληροφορίες όπως η διεύθυνση του μηχανήματος-αποστολέα, καθώς και αυτή του παραλήπτη.

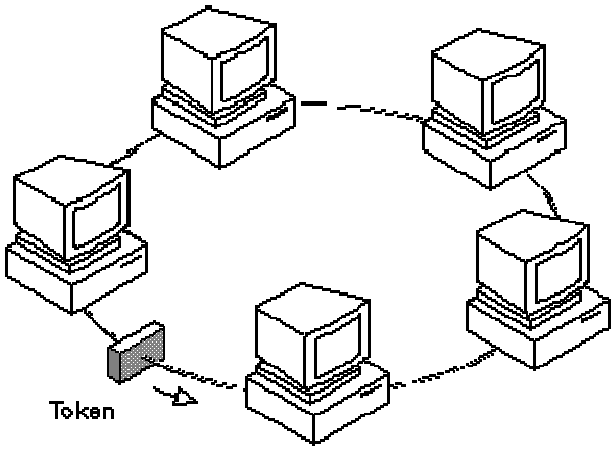
---

[5] “Server-Based Computing” (http://www.ericom.com/serverbased.asp)

[6] “Ethernet Protocol” Από Βικιπαιδεία, (http://en.wikipedia.org/wiki/Ethernet)

1.5.4 Πρωτόκολλο IBM Token Ring

Οι υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο δακτυλίου(Token Ring) χρησιμοποιούν ένα ειδικό σύντομο μήνυμα που λέγεται σκυτάλη(Token) για να συντονίζει τη χρήση του δακτυλίου. Μόνο μία σκυτάλη υπάρχει στο δακτύλιο οποιαδήποτε δεδομένη στιγμή. Για να στείλει δεδομένα ένας υπολογιστής, πρέπει να περιμένει να φτάσει σε αυτόν η σκυτάλη, να μεταδώσει ένα ακριβώς πλαίσιο, και μετά να μεταδώσει τη σκυτάλη στον επόμενο υπολογιστή. Όταν κανένας υπολογιστής δεν έχει δεδομένα να στείλει, η σκυτάλη κάνει κύκλους γύρω από το δακτύλιο με μεγάλη ταχύτητα. Ένα από τα κύρια μειονεκτήματα των δικτύων δακτυλίου με σκυτάλη είναι η ευπάθειά τους σε βλάβες . Επειδή ο κάθε υπολογιστής που είναι συνδεδεμένος στο δακτύλιο πρέπει να μεταβιβάζει τα bit ενός πλαισίου στον επόμενο υπολογιστή, μία βλάβη σε ένα μόνο υπολογιστή μπορεί να αχρηστεύσει όλο το δίκτυο. [7]



Εικόνα 1.3: Τοπολογία Δικτύου Token Ring

1.6 Μοντέλο αναφοράς OSI

Το Μοντέλο Αναφοράς ανοικτής διασύνδεσης συστημάτων ή Μοντέλο αναφοράς OSI (αγγλ. OSI reference model) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για σχεδίαση επικοινωνιών και δικτυακών πρωτοκόλλων για υπολογιστές, που

[7] "Token ring - Δακτύλιος με κουπόνι" Από Βικιπαιδεία (http://el.wikipedia.org/wiki/Token_ring)

δημιουργήθηκε από την πρωτοβουλία Ανοικτή διασύνδεση συστημάτων – OSI. Είναι γνωστό και ως Μοντέλο των επτά επιπέδων. [8]

1.6.1 Σκοπός του μοντέλου OSI

Το μοντέλο OSI διαιρεί τις λειτουργίες ενός δικτύου επικοινωνίας σε μια σειρά από επίπεδα. Κάθε επίπεδο χρησιμοποιεί μόνο τις λειτουργίες του κάτω επιπέδου και προσφέρει λειτουργικότητα στο πάνω επίπεδο. Ένα σύστημα είναι διαστρωματωμένο σε επίπεδα ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Οι στοίβες κατασκευάζονται με υλικό είτε με λογισμικό. Τυπικά, τα κατώτερα επίπεδα κατασκευάζονται με υλικό, ενώ τα ανώτερα επίπεδα είναι εφαρμογές λογισμικού.
Το μοντέλο OSI είναι βασικό κομμάτι στη δικτύωση μεταξύ των υπολογιστών. Το κύριο χαρακτηριστικό του είναι η διεπαφή μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασης αυτών των επιπέδων. Αυτό σημαίνει ότι ένα επίπεδο δημιουργημένο από έναν κατασκευαστή μπορεί να συνεργαστεί με το διπλανό επίπεδο που έχει κατασκευάσει άλλος (με την προϋπόθεση ότι έχει γίνει αντιληπτή η προδιαγραφή σωστά). Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments), και είναι πρότυπα για τον Διεθνή Οργανισμό Τυποποίησης ISO.
Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ την μελέτη της συμπεριφοράς των πρωτοκόλλων, και επιτρέπει να σχεδιάζουμε πολύπλοκες αλλά και πολύ αξιόπιστες στοίβες πρωτοκόλλων. Κάθε επίπεδο προσφέρει υπηρεσίες στο ανώτερό του και ζητά στοιχεία από το κατώτερό του.

Το μοντέλο OSI είναι μια ιεραρχική δομή επτά επιπέδων που καθορίζει τις απαιτήσεις για επικοινωνία δύο υπολογιστών μεταξύ τους και καθορίστηκε ως πρότυπο ISO 7498-1. Θεωρήθηκε ότι θα επέτρεπε την διαλειτουργικότητα μεταξύ διαφόρων συσκευών που προσέφεραν στην αγορά οι διάφοροι κατασκευαστές. Το μοντέλο επιτρέπει σε όλα τα στοιχεία ενός δικτύου να συλλειτουργούν ανεξάρτητα από το ποιος είναι ο κατασκευαστής τους. Περί τα τέλη της δεκαετίας 1980 ο ISO συνιστούσε την εφαρμογή του μοντέλου OSI ως δικτυακού προτύπου.

[8] "Μοντέλο αναφοράς OSI" από Βικιπαιδεία (http://el.wikipedia.org/wiki/OSI)

Βέβαια, εκείνη την εποχή, το πρωτόκολλο TCP/IP ήταν ήδη επί πολλά χρόνια σε χρήση. Το TCP/IP ήταν θεμελιώδες για το δίκτυο ARPANET και τα άλλα δίκτυα που εξελίχθηκαν στο σημερινό Διαδίκτυο. (Για σημαντικές διαφορές μεταξύ TCP/IP και ARPANET, δες το RFC 871.[9])

Μόνο ένα υποσύνολο του μοντέλου OSI χρησιμοποιείται σήμερα. Η γενική αντίληψη είναι ότι οι περισσότερες προδιαγραφές του είναι περίπλοκες και η πλήρης λειτουργικότητά του θα χρειαζόταν μεγάλο χρόνο κατασκευής, αν και υπάρχουν πολλοί άνθρωποι που υποστηρίζουν σθεναρά το μοντέλο OSI.

Μοντέλο OSI			
επίπεδα	**τι μεταφέρεται**	**επίπεδο**	**λειτουργίες**
επίπεδα λογισμικού	Χρήσιμα δεδομένα	7. Επίπεδο εφαρμογών (Application Layer)	Διαδικασίες δικτύου προς εφαρμογές
		6. Επίπεδο παρουσίασης (Presentation layer)	Παρουσίαση δεδομένων και κρυπτογράφηση
		5. Επίπεδο συνόδου (Session layer)	Επικοινωνία υπολογιστών, συγχρονισμός
	Τμήματα (Segments)	4. Επίπεδο μεταφοράς (Transport layer)	Διασφάλιση συνδέσεων, αξιοπιστία
επίπεδα υλικού	Πακέτα (Packets)	3. Επίπεδο δικτύου (Network layer)	Δρομολόγηση πακέτων, λογικές διευθύνσεις (IP)
	Πλαίσια (Frames)	2. Επίπεδο διασύνδεσης δεδομένων (Data link layer)	Φυσικές διευθύνσεις (MAC & LLC)
	Δυαδικά ψηφία (Bits)	1. Φυσικό επίπεδο (Physical layer)	Μετάδοση ψηφίων στο κανάλι επικοινωνίας

Πίνακας 3: Αναλυτική παρουσίαση του μοντέλου OSI

[9] Άρθρο από τον M. A. Padlipsky (www.rfc-archive.org)

1.6.2 Περιγραφή των επιπέδων OSI

Επίπεδο 7: Εφαρμογών

Το επίπεδο εφαρμογών είναι το ανώτατο επίπεδο του μοντέλου OSI, και παρέχει τη διεπαφή μεταξύ επιπέδου δικτύου και του λογισμικού που εκτελείται στον υπολογιστή. Το επίπεδο εφαρμογών παρέχει τις αναγκαίες υπηρεσίες που συνοδεύουν τις αιτήσεις

Επίπεδο 6: Παρουσίασης

Κατά την παρουσίαση επιπέδου παρουσίασης του μοντέλου OSI, τα δεδομένα που διαβιβάζονται είναι μεταφρασμένα. Αυτό το επίπεδο είναι υπεύθυνο για την απόδοση των αρχείων από το δίκτυο σε μορφή που ο υπολογιστής μπορεί να παρουσιάσει. Το επίπεδο παρουσίασης «μεταφράζει» τις μορφές αρχείων (format) που λαμβάνουμε, σε μια κοινή μορφή αρχείων που μπορεί να διαβάσει κάθε υπολογιστής.

Επίπεδο 5: Συνόδου

Το επίπεδο συνόδου ελέγχει τις συνόδους (δηλαδή τους διαλόγους) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει την σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης (remote) εφαρμογής.

Επίπεδο 4: Μεταφοράς

Το επίπεδο μεταφοράς διεκπεραιώνει την μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (flow control), τμηματοποίηση και αποτμηματοποίηση (segmentation / desegmentation), και έλεγχο σφαλμάτων (error control). Το καλύτερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης).

Επίπεδο 3: Δικτύου

Το επίπεδο δικτύου παρέχει τα λειτουργικά και διαδικαστικά μέσα για την μεταφορά στοιχειοσειρών δεδομένων μεταβλητού μήκους από μια προέλευση σε ένα προορισμό, μέσα από ένα ή περισσότερα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί

λειτουργίες δρομολόγησης, με πιθανές τμηματοποιήσεις / αποτμηματοποιήσεις, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (αγγλ. routers) λειτουργούν στο επίπεδο αυτό, και στέλνοντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Το καλύτερο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (αγγλ. Internet Protocol, IP).

Επίπεδο 2: Διασύνδεσης Δεδομένων

Το επίπεδο διασύνδεσης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για την μεταφορά δεδομένων από την μια συσκευή του δικτύου στην άλλη, και για τον έλεγχο και την πιθανή διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι ενσωματωμένες στις κάρτες δικτύου των συσκευών από το εργοστάσιο. Το πιο γνωστό παράδειγμα είναι το Ethernet.

Επίπεδο 1: Φυσικό

Το φυσικό επίπεδο ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές των συσκευών. Σ' αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων. Συσκευές φυσικού επιπέδου είναι οι διανεμητές (hub), οι αναμεταδότες (repeater), οι κάρτες δικτύου (card), οι προσαρμογείς (adaptor) αρτηρίας (bus).

Ο ευκολότερος τρόπος για την κατανόηση του μοντέλου OSI είναι να συνδέσουμε τα επίπεδα με τα κυριότερα πρωτόκολλα και πρότυπα με τα οποία σχετίζονται όπως βλέπουμε στον πίνακα 4. [10]

[10] "Μοντέλο αναφοράς OSI" από Βικιπαιδεία (http://el.wikipedia.org/wiki/OSI)

Επίπεδο	Όνομα	Κοινα πρωτόκολλα
7	Επίπεδο εφαρμογών	Telnet, FTP, SMTP, IMAP, POP, HTTP
6	Επίπεδο παρουσίασης	HTTP, SMTP, SNMP
5	Επίπεδο συνόδου	RPC, NetBIOS
4	Επίπεδο μεταφοράς	STCP, TCP, UDP
3	Επίπεδο δικτύου	IP
2	Επίπεδο διασύνδεσης δεδομένων	Ethernet, Token Ring,
1	Φυσικό επίπεδο	

Πίνακας 4: Τα 7 επίπεδα του μοντέλου OSI

1.7 Περίληψη

Το διαδίκτυο είναι η μεγαλύτερη και πιο σημαντική τεχνολογία του 21ου αιώνα. Η ανάπτυξή του είναι ραγδαία και σήμερα έχει περίπου 200.000.000 χρήστες σε όλο τον κόσμο. Η νέα γενιά Ιντερνετ (Internet2) είναι ήδη σε εφαρμογή. Όμως είναι ελεύθερη μόνο για τα πανεπιστήμια και νοσοκομεία. Σήμερα το διαδίκτυο είναι ανοιχτό σε όλους. Από τα ανώτερα μέχρι και τα κατώτερα κοινωνικά στρώματα.

Ένα υποσύνολο του διαδικτύου είναι τα δίκτυα υπολογιστών τα οποία είναι ένα σύνολο από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου.

Όλες οι κατηγορίες και τα είδη των δικτύων αντιμετωπίζουν τα ίδια προβλήματα. Τα προβλήματα αυτά εντοπίζονται κυρίως στην ασφάλεια των μεταφερόμενων δεδομένων και όχι τόσο στις τεχνολογίες υλοποίησης και στο λογισμικό που είναι ένας καθαρά τεχνικός τομέας. Στα παρακάτω κεφάλαια θα γίνει μια προσπάθεια να

απαντηθούν μερικά ερωτήματα που αφορούν την ασφάλεια των δεδομένων που μεταφέρονται δια μέσου των δικτύων. Πιο συγκεκριμένα θα γίνει αναφορά και ανάλυση της έννοιας και του τρόπου λειτουργίας της σύλληψης πακέτων δεδομένων (sniffing). Μια διαδικασία κατά την οποία «συλλαμβάνονται» τα δεδομένα που μεταφέρει το δίκτυο και ελέγχονται προσεχτικά για να καθοριστούν τυχόν πρόβλημα σε ένα δίκτυο.

Επίσης θα γίνει αναφορά στις δημοφιλέστερες εφαρμογές sniffing και παρακολούθησης δικτύων και ανάλυση των δυνατοτήτων του λογισμικού Wireshark (πρώην Ethereal), μια συσκευή ανάλυσης δικτύων που παρέχει πολλές δυνατότητες ελέγχου, έχει εύχρηστο περιβάλλον και είναι ανοιχτού κώδικα, χαρακτηριστικό το οποίο επιτρέπει στον προχωρημένο χρήστη να το προσαρμόσει στις ανάγκες και τις επιθυμίες του.

ΚΕΦΑΛΑΙΟ 2

2. Σύλληψη/Ανίχνευση πακέτων (Packet Sniffing)

2.1 Εισαγωγή στο sniffing

"Γιατί είναι το δίκτυο αργό;" "Γιατί δεν μπορώ να έχω πρόσβαση στο ηλεκτρονικό ταχυδρομείο μου;" "Γιατί δεν μπορώ να μπω στην κοινόχρηστη σύνδεση;" "Γιατί ο υπολογιστής μου ενεργεί περίεργα;" Εάν είστε διαχειριστής των υπολογιστικών δικτύων, ή μηχανικός δικτύων, ή μηχανικός ασφάλειας, θα έχετε ακούσει αυτά τα ερωτήματα αμέτρητες φορές. Κατά συνέπεια κάπως έτσι αρχίζει το κουραστικό και μερικές φορές επίπονο ταξίδι ανίχνευσης σφαλμάτων. Αρχίζετε με την προσπάθεια να επαναλάβετε το πρόβλημα από τον υπολογιστή σας, αλλά δεν μπορείτε να συνδεθείτε με το τοπικό δίκτυο ή το Διαδίκτυο. Αυτό που χρειάζεται να κάνουμε είναι να ελέγξουμε καθέναν από τους εξυπηρετητές ή κεντρικούς υπολογιστές (servers) και να σιγουρευτούμε ότι λειτουργούν κανονικά. Ελέγχουμε επίσης αν ο δρομολογητής (router) λειτουργεί κανονικά και τέλος ελέγχουμε την κάρτα δικτύου κάθε υπολογιστή ξεχωριστά.

Τώρα εξετάζουμε το παρακάτω σενάριο. Πηγαίνοντας στον κύριο μεταγωγέα (switch) δικτύου και ρυθμίζοντας μια από τις ελεύθερες δικτυακές πόρτες (ports) για την διαδικασία έλεγχου (port monitoring). Συνδέουμε το φορητό η/υ μας, λειτουργούμε τη συσκευή ανάλυσης δικτύων, και παρατηρούμε χιλιάδες πακέτα πρωτοκόλλου (TCP) (που προορίζονται για το port 25).
Κάνοντας αυτόν τον έλεγχο ανακαλύπτουμε ότι υπάρχει ένας ιός στο δίκτυο που διαδίδεται μέσω του ηλεκτρονικού ταχυδρομείου. Σαν λύση εφαρμόζουμε αμέσως φίλτρα πρόσβασης για να εμποδίζουν αυτά τα πακέτα κατά την είσοδο ή την έξοδο από το δίκτυό μας. Αυτά τα προβλήματα είναι συνήθη και πλέον με γνώσεις πάνω στις δικτυακές διαδικασίες διαγιγνώσκονται και αντιμετωπίζονται σχετικά εύκολα. [11]

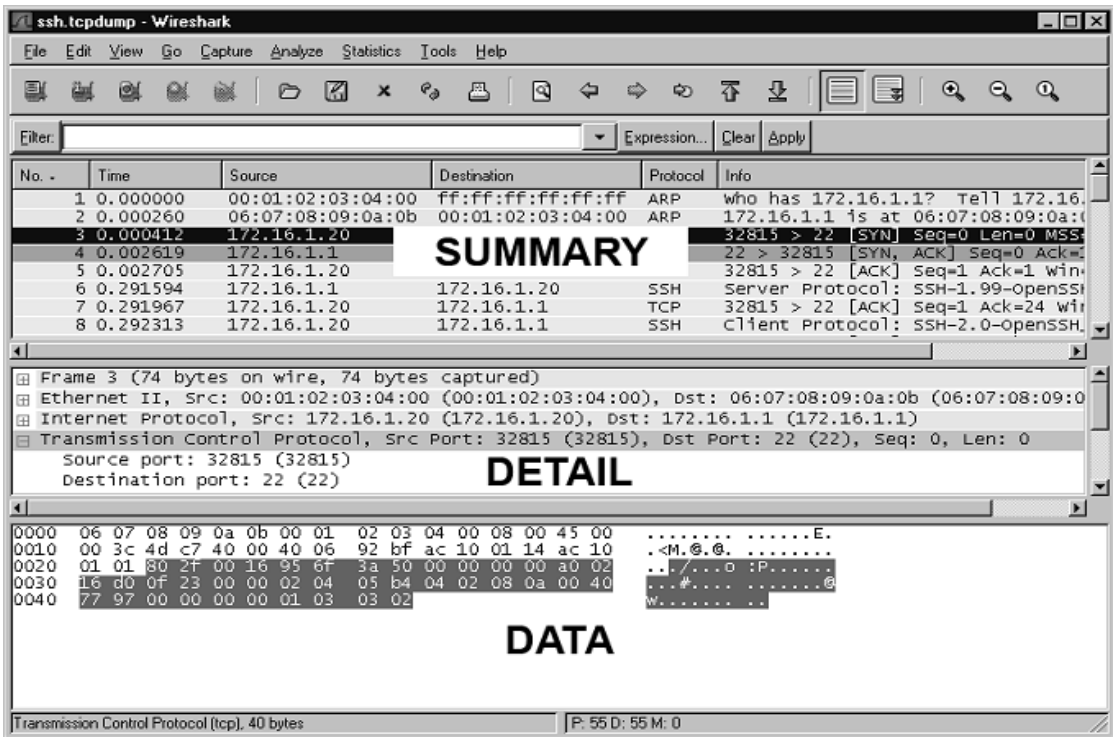
[11] "Packet sniffer" από Βικιπαιδεία (http://el.wikipedia.org/wiki/Packet_sniffer)

2.1.1 Τι είναι ανάλυση και ανίχνευση (Sniffing) στα δίκτυα

Η ανάλυση δικτύων (network analysis) ή αλλιώς Sniffing είναι η διαδικασία κατά την οποία «συλλαμβάνονται» τα δεδομένα που μεταφέρει το δίκτυο και ελέγχονται προσεχτικά για να καθοριστεί το τυχόν πρόβλημα σε αυτό το δίκτυο. Μια συσκευή ανάλυσης δικτύων αποκωδικοποιεί τα πακέτα δεδομένων των κοινών πρωτοκόλλων και εμφανίζει την κίνηση του δικτύου σε αναγνώσιμη μορφή. Ένα sniffer είναι ένα πρόγραμμα που ελέγχει τα στοιχεία που «ταξιδεύουν» στο δίκτυο. Τα μη εξουσιοδοτημένα sniffers είναι επικίνδυνα για ασφάλεια των δικτύων επειδή είναι δύσκολο να ανιχνευτούν και μπορούν να εγκατασταθούν οπουδήποτε, πράγμα το οποίο τα κάνει ένα από τα αγαπημένα όπλα των χάκερς. [12]

Μια συσκευή ανάλυσης δικτύων (Sniffer) μπορεί να είναι μια αυτόνομη συσκευή υλικού με το εξειδικευμένο λογισμικό, ή λογισμικό που εγκαθίστανται σε έναν επιτραπέζιο ή φορητό υπολογιστή. Οι διαφορές μεταξύ των συσκευών ανάλυσης εξαρτώνται από τα χαρακτηριστικά γνωρίσματα τους όπως ο αριθμός υποστηριζόμενων πρωτοκόλλων που μπορεί να αποκωδικοποιήσει, το περιβάλλον χρήσης, την δυνατότητα απεικόνισης με γραφική παράσταση και τις στατιστικές ικανότητές του. Άλλες διαφορές περιλαμβάνουν τις ικανότητες συμπεράσματος (π.χ., ειδικά χαρακτηριστικά γνωρίσματα ανάλυσης) και την ποιότητα του πακέτου που αποκωδικοποιεί. Αν και ποικίλες συσκευές ανάλυσης δικτύων αποκωδικοποιούν τα ίδια πρωτόκολλα, μερικές θα λειτουργήσουν καλύτερα από άλλες για το δικό σας σύστημα. Ένα παράδειγμα λογισμικού σύλληψης και ανάλυσης δικτύων φαίνεται στην εικόνα 2.1.

[12] “Packet sniffer” Από Βικιπαιδεία, (http//el.wikipedia.org/wiki/Packet_sniffer)



Εικόνα 2.1: Επίδειξη Περιβάλλοντος Συσκευής ανάλυσης δικτύων (Wireshark)

2.1.2 Ποια κομμάτια συνθέτουν μία συσκευή ανάλυσης Δικτύου

Αν και υπάρχουν διαφορές σε κάθε προϊόν, μια συσκευή ανάλυσης δικτύων αποτελείται από 5 βασικά μέρη:

Υλικό-Hardware.

Οι περισσότερες συσκευές ανάλυσης δικτύων είναι βασισμένες στο λογισμικό και λειτουργούν μέσω των λειτουργικών συστημάτων και των καρτών δικτύου (NICs). Εντούτοις, μερικές συσκευές ανάλυσης δικτύων υλικού προσφέρουν πρόσθετα πλεονεκτήματα όπως η ανάλυση των σφαλμάτων υλικού (π.χ., κυκλικά λάθη ελέγχου πλεονασμού-(CRC) errors, προβλήματα τάσης, προβλήματα καλωδίων, κ.α.). Κάποιοι αναλυτές δικτύων υποστηρίζουν μόνο τις Ethernet ή τις ασύρματες δικτυώσεις, ενώ άλλοι τις πολλαπλές συνδέσεις οι οποίες επιτρέπουν προσαρμοσμένες ρυθμίσεις. Ανάλογα με τις συνθήκες, μπορεί επίσης να χρειαστεί σύνδεση ενός δικτυακού κόμβου ή ενός καλωδίου στην υπάρχουσα σύνδεση.

Οδηγός προγράμματος σύλληψης-Capture Driver.

Αυτό είναι το μέρος της συσκευής δικτυακής ανάλυσης που είναι υπεύθυνο για την σύλληψη της «ωμής» δικτυακής κίνησης από το μέσο μεταφοράς που στην προκειμένη περίπτωση είναι το καλώδιο. Ο οδηγός του προγράμματος φιλτράρει την δικτυακή κίνηση που ο χρήστης επιλέγει να επεξεργαστεί και την αποθηκεύει σε ένα τμήμα της μνήμης. Είναι δηλαδή ο πυρήνας μιας συσκευής ανάλυσης δικτύου και δεν είναι δυνατή ή σύλληψη δεδομένων χωρίς αυτόν.

Ενδιάμεση μνήμη-Buffer.

Αυτό είναι το στοιχείο /μέρος του προγράμματος που αποθηκεύει τα συλληφθέντα στοιχεία της δικτυακής κίνησης. Τα στοιχεία μπορούν να αποθηκευτούν σε ένα μέρος της προσωρινής μνήμης ωσότου αυτή γεμίσει ή χρησιμοποιώντας μια μέθοδο κατά την οποία τα νεώτερα δεδομένα αντικαθιστούν τα παλαιοτέρα.

Ανάλυση σε πραγματικό χρόνο.

Αυτό το χαρακτηριστικό αναλύει τα δεδομένα που προέρχονται από το καλώδιο. Κάποιοι αναλυτές δικτύου το χρησιμοποιούν για να βρουν κάποιο πρόβλημα στην λειτουργία και στην απόδοση του δικτύου όπως επίσης και για την ανίχνευση συμπτωμάτων ενδεχόμενης εισβολής στο δίκτυο.

Αποκωδικοποίηση.

Αυτό το στοιχείο παρουσιάζει το περιεχόμενο (με περιγραφές) της κυκλοφορίας στο δίκτυο ώστε να είναι ευανάγνωστο. Οι αποκωδικοποιήσεις είναι εξειδικευμένες για κάθε πρωτόκολλο, άρα διαφέρουν ως προς τον αριθμό των δυνατών αποκωδικοποιήσεων που υποστηρίζονται. Ωστόσο, νέα στοιχεία συνεχώς προστίθεται στις συσκευές δικτυακής ανάλυσης.

2.1.3 Ποιος χρησιμοποιεί τις αναλύσεις ενός δικτύου;

Διαχειριστές συστημάτων, μηχανικοί δικτύων, μηχανικοί ασφάλειας, χειριστές συστημάτων, και προγραμματιστές, όλοι χρησιμοποιούν συσκευές ανάλυσης δικτύων, οι οποίες είναι ανεκτίμητα εργαλεία για την ανίχνευση λαθών και την λύση προβλημάτων ενός δικτύου, για ζητήματα ρυθμίσεων και για απλοποίηση δυσκολιών των εφαρμογών. Ιστορικά, οι συσκευές ανάλυσης δικτύων ήταν απλά και μόνο συσκευές υλικού που ήταν ακριβές και δύσκολες στη χρήση. Εντούτοις, οι νέες

πρόοδοι στην τεχνολογία έχουν επιτρέψει την ανάπτυξη των βασισμένων στο λογισμικό συσκευών ανάλυσης δικτύων, οι οποίες καθιστούν την χρήση τους καταλληλότερη και προσιτή για τους διαχειριστές ούτως ώστε να ανιχνεύουν αποτελεσματικά τα λάθη σε ένα δίκτυο.
Η τέχνη της ανάλυσης δικτύων είναι ένα δίκοπο ξίφος. Ενώ οι ειδικοί δικτύων, συστημάτων και ασφάλειας το χρησιμοποιούν για την ανίχνευση λαθών και τον έλεγχο του δικτύου, μερικοί εν δυνάμει εισβολείς χρησιμοποιούν την ανάλυση δικτύων για επιβλαβείς λόγους. Μια συσκευή ανάλυσης δικτύων είναι ένα εργαλείο, και όπως όλα τα εργαλεία, μπορεί να χρησιμοποιηθεί και για καλούς και κακούς λόγους.

Μια συσκευή ανάλυσης δικτύων χρησιμοποιείται για:

- Μετατροπή των δυαδικών στοιχείων σε δεδομένα με αναγνώσιμη μορφή
- Προβλήματα ανίχνευσης λαθών στο δίκτυο
- Ανάλυση της απόδοσης ενός δικτύου για να διαγνωστούν προβλήματα
- Ανίχνευση παραβίασης δικτύων
- Καταγραφή κίνησης δικτύου για διάγνωση και αποδείξεις
- Ανάλυση των διαδικασιών των εφαρμογών
- Ανακάλυψη των ελαττωματικών καρτών δικτύων
- Ανακάλυψη της προέλευσης των ιών ή της άρνησης των επιθέσεων υπηρεσιών (DOS)
- Ανίχνευση κατασκοπευτικού προγράμματος (spyware)
- Προγραμματισμός δικτύων για να διορθωθούν σφάλματα στο στάδιο της ανάπτυξης
- Ανίχνευση ενός υπολογιστή που έχει παραβιαστεί από χάκερ
- Επικύρωση της συμμόρφωσης με την πολιτική επιχείρησης
- Σαν εκπαιδευτικό πόρο κατά την εκμάθηση των πρωτοκόλλων

2.2 Ethernet και Sniffing

Το Ethernet είναι το δημοφιλέστερο πρότυπο πρωτοκόλλου που χρησιμοποιείται για να επιτρέψει στους υπολογιστές να επικοινωνήσουν. Ένα πρωτόκολλο είναι όπως η ομιλία μιας ιδιαίτερης γλώσσας. Το Ethernet χτίστηκε γύρω από την αρχή ενός

κοινού μέσου όπου όλοι οι υπολογιστές στο τοπικό τμήμα δικτύου μοιράζονται το ίδιο καλώδιο. Είναι γνωστό ως πρωτόκολλο μετάδοσης επειδή στέλνει τα στοιχεία σε όλους τους άλλους υπολογιστές στο ίδιο δίκτυο. Αυτές οι πληροφορίες διαιρούνται σε εύχρηστα μεγάλα κομμάτια αποκαλούμενα πακέτα, και κάθε πακέτο έχει μια επιγραφή που περιέχει τις διευθύνσεις και του προορισμού και των υπολογιστών της πηγής. Ακόμα κι αν οι πληροφορίες αυτές στέλνονται σε όλους τους υπολογιστές του δικτυακού τμήματος, μόνο ο υπολογιστής με την συγκεκριμένη διεύθυνση προορισμού αποκρίνεται. Όλοι οι άλλοι υπολογιστές στο δίκτυο βλέπουν το πακέτο, αλλά εάν δεν είναι οι προοριζόμενοι δεκτές του πακέτου αυτού το αγνοούν, εκτός αν κάποιος υπολογιστής λειτουργεί ένα sniffer. Κατά την λειτουργία ενός sniffer, ο οδηγός του προγράμματος βάζει τη NIC (κάρτα δικτύου) του υπολογιστή στην λειτουργία «promiscuous». Αυτό σημαίνει ότι ο sniffer υπολογιστής μπορεί να δει όλη την κίνηση του δικτυακού τμήματος ανεξάρτητα από ποιον στέλνεται. Κανονικά οι υπολογιστές τρέχουν στον μη-promiscious τρόπο, «ακούγοντας» τις πληροφορίες που προορίζονται μόνο για αυτούς. Εντούτοις, όταν η NIC είναι σε promiscuous mode, μπορεί να δει τις δικτυακές «συζητήσεις» όλων των υπολογιστών του δικτυακού τομέα.

Οι διευθύνσεις Ethernet είναι επίσης γνωστές ως διευθύνσεις ελέγχου πρόσβασης πολυμέσων (MAC) και διευθύνσεις υλικού. Επειδή πολλοί υπολογιστές μπορούν να μοιραστούν ένα ενιαίο Ethernet τομέα, κάθε ένας πρέπει να έχει ένα ατομικό αναγνωριστικό καλά-κωδικοποιημένο πάνω στην NIC. Η διεύθυνση MAC είναι ένας αριθμός 48-κομματιών, ο οποίος δηλώνεται επίσης ως 12-ψήφιος δεκαεξαδικός αριθμός που χωρίζεται σε δύο μισά: τα πρώτα 24 μπιτ προσδιορίζουν τον προμηθευτής της κάρτας Ethernet, και τα δεύτερα 24 μπιτ περιλαμβάνουν έναν αύξοντα αριθμό ορισμένο από τον προμηθευτή. [13]

[13] “Ethernet” Από Βικιπαιδεία, (http://en.wikipedia.org/wiki/Ethernet)

Τα ακόλουθα βήματα επιτρέπουν στο χρήστη να δει τις διευθύνσεις MAC και NIC:

■ στα Windows 9x/ME πηγαίνουμε στο μενού Start->Run πληκτρολογούμε winipcfg.exe. Η διεύθυνση MAC θα απαριθμηθεί ως "διεύθυνση προσαρμογέα."
■ στα Windows NT, 2000, XP και 2003 Πηγαίνουμε στη γραμμή εντολών και εισάγουμε τον τύπο εντολής ipconfig/all. Η διεύθυνση MAC θα απαριθμηθεί ως "φυσική διεύθυνση."

Μπορείτε επίσης να δούμε τις διευθύνσεις MAC άλλων υπολογιστών με τους οποίους έχουμε επικοινωνήσει πρόσφατα, με τη δακτυλογράφηση της εντολής arp –a.
Οι διευθύνσεις της MAC είναι μοναδικές, και κανένας υπολογιστής δεν έχει την ίδια με κάποιον άλλον. Εντούτοις, περιστασιακά ένα λάθος κατασκευής μπορεί να εμφανιστεί με αποτέλεσμα περισσότερες από μια NIC να έχουν την ίδια διεύθυνση MAC. Κατά συνέπεια, οι περισσότεροι άνθρωποι αλλάζουν τις MAC επίτηδες, κάτι το οποίο μπορεί να γίνει με ένα πρόγραμμα (π.χ., ifconfig) που επιτρέπει να δίνονται εικονικές MAC. Η απομίμηση της διεύθυνσης MAC (και άλλων τύπων διευθύνσεων) είναι επίσης γνωστή ως spoofing. Επίσης, μερικοί προσαρμογείς επιτρέπουν να χρησιμοποιήσουμε ένα πρόγραμμα για να επαναρυθμιστεί η διεύθυνση MAC, δηλαδή να επανέλθει μετά από μια διαδικασία.

2.2.1 Τρόπος λειτουργίας

Οι περισσότεροι προσωπικοί υπολογιστές συνδέονται σε ένα LAN (Local Area Network - Τοπικό Δίκτυο), που σημαίνει ότι μοιράζονται μία σύνδεση με άλλους υπολογιστές. Αν το δίκτυο δεν χρησιμοποιεί switch (διακόπτη) η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Επακόλουθα, κάθε υπολογιστής στην πραγματικότητα βλέπει τα δεδομένα που προέρχονται από ή προορίζονται για τους γειτονικούς υπολογιστές, αλλά τα αγνοεί.

Υπάρχουν πολλές δυνατότητες, που καθορίζουν την τύχη των πακέτων:

Τα πακέτα μετριούνται. Με αυτό τον τρόπο, προσθέτοντας στη συνέχεια το συνολικό μέγεθός τους για μία ορισμένη χρονική περίοδο (συμπεριλαμβάνοντας τις επικεφαλίδες των πακέτων), εξάγεται μια καλή ένδειξη για το πόσο φορτωμένο είναι

το δίκτυο. Το πρόγραμμα μπορεί να παρέχει γραφικές απεικονίσεις της σχετικής κίνησης του δικτύου.

Τα πακέτα μπορούν να εξετασθούν λεπτομερώς. Είναι δυνατόν να γίνει σύλληψη συγκεκριμένων πακέτων, ώστε να διαγνωσθεί και να αντιμετωπιστεί ένα πρόβλημα.

2.3 Χρησιμότητα διαδικασίας σύλληψης πακέτων

Τα προγράμματα σύλληψης πακέτων (sniffing) υπάρχουν για πολλά χρόνια στο περιβάλλον των υπολογιστών και χρησιμοποιούνται για να βοηθήσουν τους διαχειριστές δικτύων να διατηρήσουν τη σωστή λειτουργία τους. Ωστόσο υπάρχει και μια άλλη χρήση των sniffers, όταν αυτά χρησιμοποιούνται για να «διαρρήξουν» τους υπολογιστές.

2.3.1 Για ποιο σκοπό χρησιμοποιείται;

Οι χαρακτηριστικές χρήσεις τέτοιων παγίδων (wiretrap) προγραμμάτων περιλαμβάνουν:

- Αυτόματη ανακάλυψη των κωδικών πρόσβασης και των ονομάτων χρήστη από το δίκτυο. Χρησιμοποιούνται από χάκερς και κράκερς προκειμένου να μπουν στα συστήματα.
- Μετατροπή των στοιχείων σε αναγνώσιμη μορφή έτσι ώστε οι χρήστες υπολογιστών να μπορούν να διαβάσουν την κίνηση στο δίκτυο.
- Ανάλυση σφαλμάτων για να ανακαλυφθούν τα προβλήματα στο δίκτυο, όπως γιατί ο υπολογιστής Α δεν μπορεί να επικοινωνήσει με τον υπολογιστή Β.
- Ανάλυση απόδοσης για να ανακαλυφθούν τα προβλήματα κυκλοφορίας δεδομένων στα δίκτυα.
- Ανίχνευση εισβολής στα δίκτυα προκειμένου να ανακαλυφθούν οι χάκερς/ κράκερς.

2.3.2 Εξ' αποστάσεως πρόσβαση στο καλώδιο

Η εναλλακτική περίπτωση όπως αναφέρθηκε προηγουμένως είναι η διάρρηξη ενός δικτύου. Κάποιοι πραγματικά καλοί χάκερ, βρίσκουν διόδους για πρόσβαση σε

υπολογιστές ακόμα και από μεγάλη απόσταση. Αυτό μπορεί να γίνει με διάφορους τρόπους:

- Το «σπάσιμο» του υπολογιστή κάποιου και η εγκατάσταση λογισμικού που μπορεί να ελέγχει ο χάκερ εξ' αποστάσεως.
- «Σπάζοντας» τις ISPs (τις εταιρίες παροχής ιντερνετ και των δυο), και εγκαθιστώντας το λογισμικό σύλληψης πακέτων (sniffing) να μπορεί ο ίδιος να συλλάβει την κυκλοφορία ή και να την ελέγξει.
- Απλά δωροδοκώντας κάποιον σε μία τοποθεσία στόχο ώστε να μπει στις φυσικές εγκαταστάσεις και να εγκαταστήσει ένα sniffer, κ.λπ.

Φυσικά αυτές οι πληροφορίες δίνονται πληροφοριακά και με σκοπό την ενημέρωση και την προφύλαξη και όχι για επιβλαβή σκοπό.

2.3.3 Εναλλακτικός τρόπος λειτουργίας ενός Sniffer;

Η εναλλακτική περίπτωση καλείται «monitor mode». Αυτός ο τρόπος λειτουργίας των καρτών δικτύων ισχύει για τις ασύρματες κάρτες διεπαφών δικτύων (*network interface cards*-NICs). Λόγω των μοναδικών ιδιοτήτων ενός ασύρματου δικτύου, οποιοδήποτε στοιχείο που ταξιδεύει ασύρματα είναι δυνατό να αναγνωστεί από οποιαδήποτε συσκευή είναι ρυθμισμένη για να «ακούει». Αν μια κάρτα σε promiscuous mode λειτουργεί σε ασύρματα δίκτυα, τότε δεν υπάρχει καμία ανάγκη να είναι πραγματικά μέρος του δικτύου. Όμως μια κάρτα δικτύων σε promiscuous mode μπορεί να ανιχνευθεί λόγω του τρόπου που αλληλεπιδρά με το δίκτυο. Τότε σταματά όλη η διαδικασία «monitor mode» .

Κανονικά, το στρώμα δικτύων (Network layer) είναι υπεύθυνο για την έρευνα των πακέτων πληροφοριών και τη διεύθυνση προορισμού τους. Αυτή η διεύθυνση προορισμού είναι η διεύθυνση MAC ενός υπολογιστή. Υπάρχει μια μοναδική διεύθυνση της MAC για κάθε κάρτα δικτύου στον κόσμο. Αν και μπορείτε να αλλάξετε τη διεύθυνση, η διεύθυνση MAC εξασφαλίζει ότι το στοιχείο παραδίδεται στο σωστό υπολογιστή. Εάν η διεύθυνση ενός υπολογιστή δεν ταιριάζει με τη διεύθυνση στο πακέτο, το στοιχείο λογικά αγνοείται.

Ο λόγος που μια κάρτα δικτύων έχει αυτήν την επιλογή να τρέξει σε promiscuous mode είναι για λόγους ανίχνευσης λαθών (troubleshooting). Κανονικά, ένας

υπολογιστής δεν θέλει ή δεν χρειάζεται τις πληροφορίες που στέλνονται σε άλλους υπολογιστές στο δίκτυο. Εντούτοις, σε περίπτωση που κάτι πηγαίνει στραβά με την καλωδίωση ή το υλικό δικτύων, είναι σημαντικό για έναν τεχνικό δικτύων να κοιτάξει μέσα στα στοιχεία που ταξιδεύουν στο δίκτυο για να δει τι προκαλεί το πρόβλημα. Παραδείγματος χάριν, μια κοινή ένδειξη μια δυσλειτουργικής κάρτας δικτύων είναι όταν οι υπολογιστές δυσκολεύονται να μεταφέρουν δεδομένα. Αυτό θα μπορούσε να είναι το αποτέλεσμα της υπερφόρτωσης πληροφοριών στα καλώδια δικτύων. Η μεγάλη ροή των δεδομένων θα μπλόκαρε το δίκτυο και θα σταματούσε οποιαδήποτε παραγωγική επικοινωνία. Όταν ένας τεχνικός χρησιμοποιήσει έναν υπολογιστή με την ικανότητα να εξετάζει το δίκτυο, θα επισήμαινε γρήγορα την προέλευση των αλλοιωμένων στοιχείων, και έτσι τη θέση της δυσλειτουργικής κάρτας δικτύων. Θα μπορούσε έπειτα απλά να αντικαταστήσει την «κακή» κάρτα και όλα θα λειτουργούσαν ομαλά.

Ένας άλλος τρόπος να κατανοηθεί η λειτουργία ενός sniffer είναι να παρομοιάσουμε ένα δίκτυο με ένα κοκτέιλ πάρτι. Κάποιος συμμετέχων ακούει και απαντά στις συνομιλίες ενεργά. Έτσι ακριβώς μια κάρτα δικτύων πρέπει να λειτουργεί στο σύστημα σας. Υποτίθεται ότι πρέπει να ακούσει και να απαντήσει στις πληροφορίες που στέλνονται άμεσα σε αυτό. Επίσης υπάρχουν εκείνοι οι άνθρωποι στο πάρτι που στέκονται ήσυχα και ακούνε τις συνομιλίες. Αυτά τα πρόσωπα θα μπορούσαν να συγκριθούν με μια κάρτα δικτύων που τρέχει σε promiscuous mode. Επιπλέον, εάν αυτοί οι ακροατές άκουσαν ένα συγκεκριμένο θέμα μόνο, θα μπορούσαν να συγκριθούν με ένα sniffer που συλλαμβάνει όλα τα στοιχεία σχετικά με κωδικούς πρόσβασης μόνο.

2.3.4 Πώς οι χάκερς - κράκερς χρησιμοποιούν τα Sniffers

Όπως αναφέρθηκε προηγουμένως, τα sniffers χρησιμοποιούνται για να ανιχνεύσουν λάθη στην κυκλοφορία δικτύων. Οι χάκερς/ κράκερς μπορούν να χρησιμοποιήσουν αυτά ή παρόμοια εργαλεία για να κοιτάξουν αδιάκριτα μέσα σε ένα δίκτυο. Δεν τους χρησιμοποιούν για να ανιχνεύσουν λάθη, αλλά προσπαθούν να υποκλέψουν τους κωδικούς πρόσβασης και άλλα «μαργαριτάρια». Οι υπολογιστές μπορούν να στείλουν τις πληροφορίες είτε σε μορφή κειμένου, είτε σε μια κρυπτογραφημένη μορφή.

Η επικοινωνία Plaintext [14] είναι οποιεσδήποτε πληροφορίες που στέλνονται ακριβώς όπως αναγνωρίζει το ανθρώπινο μάτι. Για τις περισσότερες εφαρμογές, αυτό είναι ο τυποποιημένος τρόπος της μεταφοράς δεδομένων. Παραδείγματος χάριν, το Διαδίκτυο χρησιμοποιεί plaintext για τις περισσότερες από τις επικοινωνίες του. Αυτός είναι ο γρηγορότερος τρόπος να σταλούν τα δεδομένα. Τα προγράμματα συνομιλίας, το ηλεκτρονικό ταχυδρομείο, οι ιστοσελίδες και ένα πλήθος άλλων προγραμμάτων στέλνουν τις πληροφορίες τους σαν «plaintext». Αυτό είναι αποδεκτό για τις περισσότερες καταστάσεις, εντούτοις, γίνεται ένα πρόβλημα κατά τη διαβίβαση των ευαίσθητων πληροφοριών, όπως ένας αριθμός τραπεζικού λογαριασμού ή ένας κωδικός πρόσβασης.

Εάν εξετάζετε προσεχτικά το τμήμα plaintext, μπορείτε να δείτε ακριβώς πόσο επικίνδυνο ένα sniffer μπορεί να είναι όσον αφορά τις ευαίσθητες πληροφορίες. Για παράδειγμα αν κάποιος χάκερ υπέκλεπτε το e-mail μιας εταιρίας με τη χρήση ενός sniffer. Στο plaintext, μπορεί κάποιος να δει το εξής: «Η επιχείρησή μας θα συγχωνευθεί με μια άλλη επιχείρηση. Αυτό θα κάνει το απόθεμά μας 250.000 €. Μην το πείτε πουθενά». Εάν αυτό ήταν μια πραγματική συγχώνευση, ένας χάκερ θα μπορούσε να κερδίσει τα εκατομμύρια σε μια νύχτα.
Επιπλέον, οι πελάτες ηλεκτρονικού ταχυδρομείου και οι πελάτες «FTP» δεν κρυπτογραφούν κανονικά τους κωδικούς πρόσβασής τους, αυτό τους κάνει δύο από τα πιο συνηθέστερα «σνιφαρισμένα» θύματα σε ένα δίκτυο. Άλλα, συχνά χρησιμοποιημένα προγράμματα όπως το Telnet, οι φυλλομετρητές Ιστού (browsers όπως ο Internet explorer, firefox, opera κλπ.), και τα προγράμματα ειδήσεων στέλνουν επίσης τους κωδικούς πρόσβασής τους ως plaintext. Έτσι, εάν ένας χάκερ είχε εγκαταστήσει επιτυχώς ένα sniffer στο δίκτυό σας, θα είχε σύντομα έναν κατάλογο κωδικών πρόσβασης και ονομάτων χρηστών που θα μπορούσε να εκμεταλλευτεί.

Ακόμη και μερικοί κρυπτογραφημένοι κωδικοί πρόσβασης που χρησιμοποιούνται σε ένα δίκτυο των WINDOWS μπορούν να υποκλαπούν. Χάρη στο μάλλον γνωστό σχέδιο κρυπτογράφησης ενός κωδικού πρόσβασης, δεν χρειάζεται πολύ για να συλληφθούν και να αποκρυπτογραφηθούν οι κωδικοί πρόσβασης και να σπάσει ένα

[14] Βλέπε Λεξικό όρων (Τέλος Εργασίας)

δίκτυο ευρέως ανοικτό. Στην πραγματικότητα, υπάρχουν ακόμη και προγράμματα σνιφαρίσματος που έχουν ενσωματωμένο ένα αποκωδικοποιητή (κράκερ) κωδικών πρόσβασης NT στον κώδικα τους. Τα προγράμματα έχουν ως σκοπό να είναι πολύ φιλικά προς το χρήστη έτσι ώστε οι διαχειριστές δικτύων να μπορούν να εξετάσουν τα δίκτυά τους για τους αδύνατους κωδικούς πρόσβασης. Δυστυχώς, αυτά τα προγράμματα καταλήγουν συχνά στα χέρια ενός προγραμματιστή που μπορεί έτσι εύκολα να τα χρησιμοποιήσει για να προκαλέσει προβλήματα.

Αν και οι sniffers συνήθως λειτουργούν μέσα στα κλειστά επιχειρησιακά δίκτυα, μπορούν επίσης να χρησιμοποιηθούν και σε όλο το Διαδίκτυο. Όπως αναφέρεται προηγουμένως, το FBI έχει ένα πρόγραμμα που συλλαμβάνει όλες τις πληροφορίες, εισερχόμενες και εξερχόμενες από τους υπολογιστές που λειτουργούν στο δίκτυο. Αυτό το εργαλείο, προηγουμένως γνωστό ως carnivore, πρέπει απλά να συνδεθεί και να τεθεί σε λειτουργία. Αν και ο σκοπός του είναι να ξεχωρίζει οποιεσδήποτε πληροφορίες που δεν αφορούν τον χρήστη, αυτό το εργαλείο συλλαμβάνει πραγματικά όλα αυτά που ταξιδεύουν μέσω οποιουδήποτε καλωδίου με το οποίο συνδέεται και έπειτα το φιλτράρει σύμφωνα με τους κανόνες που ορίζονται στο πρόγραμμα. Κατά συνέπεια, το carnivore μπορεί ενδεχομένως να συλλάβει όλους εκείνους τους κωδικούς πρόσβασης, τα μηνύματα ηλεκτρονικού ταχυδρομείου, και τις συνομιλίες που περνούν μέσω της σύνδεσής του.

Εκτός από τα συνδεμένα με καλώδιο δίκτυα, τα sniffers μπορούν επίσης να χρησιμοποιηθούν και στα ασύρματα δίκτυα. Στην πραγματικότητα, ένα ασύρματο εταιρικό τοπικό δίκτυο LAN είναι μοναδικό από την προοπτική ενός χάκερ. Αυτό γιατί συνήθως είναι εύκολα ανιχνεύσιμο για να διευκολύνει την πρόσβαση των εργαζομένων στους κεντρικούς υπολογιστές αλλά και στο διαδίκτυο και έτσι το «ρουθούνισμα» (sniffing) είναι πιο εύκολο για κάποιον έμπειρο χάκερ. Εάν οι πληροφορίες στέλνονται ως plaintext στο δημόσιο τομέα, πώς μπορεί να είναι δύσκολο κάποιος να «ακούσει» απλά αυτές τις πληροφορίες;

2.4 Εισαγωγή στις μεθόδους σύλληψης πακέτων δεδομένων (sniffing)

2.4.1 Μέθοδοι sniffing

2.4.1.1 Ραδιοφωνικές μεταδόσεις (Broadcasts)

Ο ευκολότερος τρόπος να γίνει sniffing είναι να ελεγχθούν οι ραδιοφωνικές μεταδόσεις. Ένας κακόβουλος χρήστης μπορεί να εκμεταλλευθεί τα πρωτόκολλα δικτύων ραδιοφωνικής μετάδοσης όπως NetBIOS, SNMP, bootp/DHCP, κ.α.

2.4.1.2 Μπλοκάρισμα μεταγωγέων (Switch Jamming)

Σε μερικούς μεταγωγείς, συμβαίνει το απροσδόκητο αποτέλεσμα αποτυχίας των παροχών ασφάλειας από το δίκτυο. Αυτός ο μηχανισμός είναι γνωστός ως «αποτυχημένη ανοικτή συμπεριφορά» και συμβαίνει συνήθως σπάνια αλλά τελείως τυχαία. Οι κακόβουλοι χρήστες που παρακολουθούν συνεχώς εκμεταλλευόμενοι μια τέτοια τυχαία κατάσταση βάζουν τους μεταγωγείς σε promiscuous mode και λαμβάνουν όλα τα δεδομένα χωρίς να γίνουν αντιληπτοί έγκαιρα.

2.4.1.3 Επαναπροσανατολισμός ARP

Ένας υπολογιστής σε ένα δίκτυο Ethernet μπορεί να επικοινωνήσει με έναν άλλο, μόνο εάν ξέρει τη διεύθυνση Ethernet (MAC address) αυτού. Το ARP χρησιμοποιείται για να πάρει τη διεύθυνση Ethernet ενός υπολογιστή από τη διεύθυνση IP του. Το ARP χρησιμοποιείται εκτενώς από όλους τους οικοδεσπότες σε ένα δίκτυο Ethernet. Εξετάζοντας το μηχανισμό που περιγράφεται ανωτέρω, κάποιος μπορεί να φανταστεί τη μοιραία συνέπεια που θα μπορούσε να προκύψει από έναν κακόβουλο χρήστη που στέλνει πλαστά ARP πλαίσια. Παραδείγματος χάριν, κάποιος θα μπορούσε να μεταδώσει ραδιοφωνικά μία ARP υποστηρίζοντας ότι είναι κάποιος δρομολογητής δικτύων, οπότε σε αυτή την περίπτωση ο καθένας θα προσπαθούσε να καθοδηγήσει τα πακέτα του μέσω αυτού.

2.4.1.4 Επαναπροσανατολισμός ICMP [15]

Μία πύλη (gateway) στέλνει ένα μήνυμα σε έναν υπολογιστή (host) στην ακόλουθη κατάσταση:
Μια πύλη Π1 ενός δικτύου Α λαμβάνει ένα πακέτο από έναν κεντρικό υπολογιστή (host Β) ενός άλλου δικτύου Β στο οποίο η πύλη αφήνει ένα «σημάδι». Η πύλη Π1 ελέγχει τον πίνακα δρομολόγησης και αποκτά τη διεύθυνση της επόμενης πύλης Π2. Αν η Π2 και ο host Β, είναι στο ίδιο δίκτυο, ένα μήνυμα στέλνεται στον κεντρικό υπολογιστή του Α. Το μήνυμα αυτό συμβουλεύει τον host Β να στείλει την κίνηση για το δίκτυο Α απευθείας στην πύλη Π2 καθώς πρόκειται για συντομότερη διαδρομή προς τον προορισμό. Η πύλη των δεδομένων προωθεί το αρχικό διάγραμμα στον host Β. Ένας κακόβουλος χρήστης θα μπορούσε να ανατρέψει αυτό το μηχανισμό, στέλνοντας μια ανακατεύθυνση στο host Β υποστηρίζοντας ότι θα έπρεπε να στείλει τα πακέτα στον host Γ που είναι δικός του.

2.4.1.5 ICMP διαφημίσεις δρομολογητών (router advertisements)

Ένας δρομολογητής στέλνει μια περιοδική διαφήμιση δρομολογητών χρησιμοποιώντας ένα μήνυμα ICMP για να ειδοποιήσει τους οικοδεσπότες στο δίκτυο ότι ο δρομολογητής είναι ακόμα διαθέσιμος. Ένας κακόβουλος χρήστης θα μπορούσε να υποστηρίξει ότι είναι ο δρομολογητής με την αποστολή παρόμοιων μηνυμάτων και να χρησιμοποιήσει έπειτα το λογισμικό σύλληψης με σκοπό να κλέψει πληροφορίες.

2.4.1.6 MAC απομίμηση διευθύνσεων (address faking)

Χρησιμοποιώντας το χαρακτηριστικό γνώρισμα ενός μεταγωγέα, κάποιος μπορεί να στείλει τη διεύθυνση προέλευσης του θύματος για να αναγκάσει την αποστολή πακέτων προς τον ίδιο και όχι προς τον αληθινό παραλήπτη. Προφανώς, ένα τέτοιο τέχνασμα προκαλεί τα προβλήματα:

1. το θύμα θα συνεχίσει τη διαδικασία με το μεταγωγέα χωρίς να γνωρίζει τι γίνεται,
2. οι κακόβουλοι χρήστες μπορούν όχι μόνο να διακόψουν την επικοινωνία του θύματος χωρίς διακοπή του sniffing.

[15] Βλέπε Λεξικό όρων (Τέλος Εργασίας)

Διάφορες λύσεις είναι διαθέσιμες σε έναν επιτιθέμενο:

- Επαναπροσανατολισμός του διακόπτη και συνέχιση με τη σύνδεση σαν να μη έχει συμβεί τίποτα.
- Περιοδική αποστολή πακέτων χρησιμοποιώντας τη διεύθυνση MAC του θύματος χωρίς διακοπή της σύνδεσης του.

2.4.1.7 Cable-taps (συνδέσεις καλωδίου)

Τα Cable-taps είναι φυσικά προϊόντα, σχεδιασμένα να εφαρμόζουν στο καλώδιο Ethernet.

2.4.2 Application areas (περιοχές εφαρμογών)

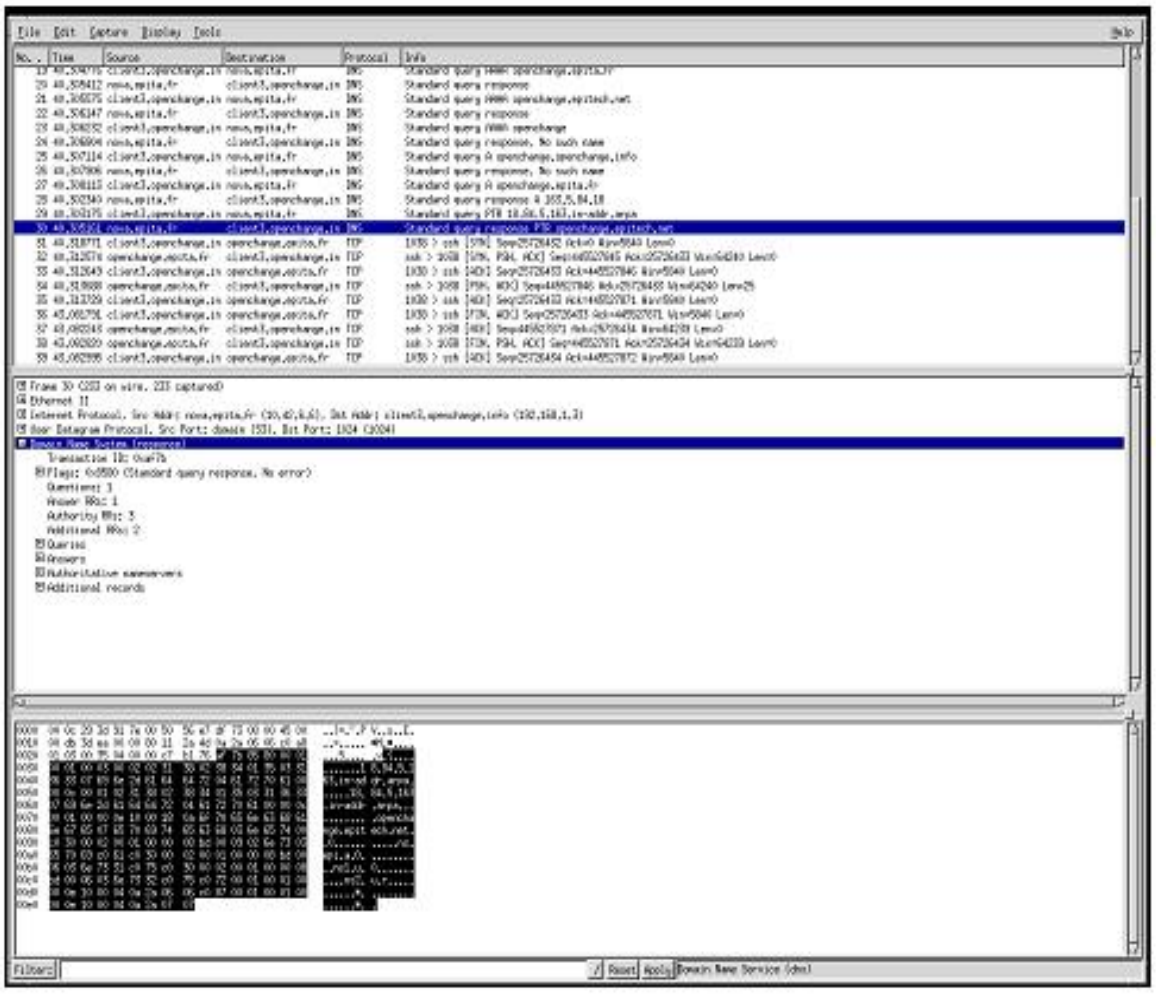
Μερικά πρωτόκολλα που είναι ιδιαίτερα ευάλωτα σε sniffing. Ακολουθεί ένας μη εξαντλητικός κατάλογος.

- **HTTP**: Χρήση του ελέγχου ταυτότητας κατά τον οποίο στέλνουν κωδικούς πρόσβασης σε όλο το δίκτυο σε μορφή απλού κειμένου. Τα δεδομένα που αποστέλλονται σε απλό κείμενο..
- **SNMP**: SNMP κωδικοί πρόσβασης - που ονομάζονται επίσης και community-strings - αποστέλλονται μέσω του δικτύου, με απλό κείμενο..
- **NNTP**: Κωδικός πρόσβασης αποστέλλονται σε απλά. Δεδομένα που αποστέλλονται σε απλή μορφή επίσης.
- **POP**: Κωδικός πρόσβασης αποστέλλονται σε απλά. Δεδομένα που αποστέλλονται σε απλή μορφή επίσης.
- **FTP**: Κωδικός πρόσβασης αποστέλλονται σε απλά. Δεδομένα που αποστέλλονται σε απλή μορφή επίσης.
- **IMAP**: Κωδικός πρόσβασης αποστέλλονται σε απλά. Δεδομένα που αποστέλλονται σε απλή μορφή επίσης.
- **TELNET**: Κωδικός πρόσβασης αποστέλλονται σε απλά. Δεδομένα που αποστέλλονται σε απλή μορφή επίσης.

2.4.3 Protocol analysis (Ανάλυση Πρωτοκόλλου)

Η ανάλυση του πρωτοκόλλου, συνίσταται στην καταγραφή της κίνησης του δικτύου, ώστε να αναληφθούμε την δραστηριότητα του δικτύου. Παρακάτω στην εικόνα 2.2

φαίνεται μια οθόνη σύλληψης πακέτων με την μέθοδο sniffing μέσω του προγράμματος Wireshark (πρώην Ethereal).



Εικόνα 2.2: Οθόνη χρήσης Wireshark

Το παράδειγμα στην Εικόνα 2.2 δείχνει πως το πρόγραμμα πάνω διαχωρίζει τα πλαίσια, σύμφωνα με τα στρώματα του πρωτοκόλλου. Πράγματι, το πλαίσιο 30 αποτελείται από δεδομένα Ethernet, IP δεδομένων, UDP δεδομένα και Domain Name System στοιχεία τα οποία αποδεικνύουν στρώματα με ενθυλάκωση των δεδομένων.

Σε γενικές γραμμές, η ανάλυση του πρωτοκόλλου είναι μακρά και σχολαστική. Απαιτεί επίσης ένα καλό πλαίσιο για δικτυακά πρωτόκολλα. Ωστόσο, οι περισσότεροι sniffers περιλαμβάνουν φίλτρα που επιτρέπουν να διακρίνουν εύκολα τα διάφορα στρώματα σε ένα ίδιο πλαίσιο.

2.5 Πώς να ανιχνεύσουμε έναν Sniffer

Υπάρχουν μερικοί τρόποι που ένας τεχνικός δικτύων μπορεί να ανιχνεύσει μια NIC που τρέχει σε promiscuous mode. Ένας τρόπος είναι να ελεγχθούν «φυσικά» όλοι οι τοπικοί υπολογιστές για οποιαδήποτε συσκευές ή προγράμματα sniffer. Υπάρχουν επίσης προγράμματα ανίχνευσης λογισμικού που μπορούν να ανιχνεύσουν τα δίκτυα για συσκευές που τρέχουν προγράμματα sniffer (παραδείγματος χάριν, AntiSniff). Αυτά τα προγράμματα ανιχνευτών χρησιμοποιούν διαφορετικές πτυχές της υπηρεσίας ονόματος περιοχών και των TCP/IP συστατικών ενός συστήματος δικτύων για να ανιχνεύσουν οποιαδήποτε κακόβουλα προγράμματα ή συσκευές που συλλαμβάνουν τα πακέτα (running in promiscuous mode). Εντούτοις, για το μέσο χρήστη, δεν υπάρχει πραγματικά κανένας τρόπος να ανιχνευθεί εάν ένας υπολογιστής έξω στο διαδίκτυο αντλεί τις πληροφορίες του. Γι' αυτό η κρυπτογράφηση συστήνεται έντονα.

2.6 Πώς μπορούμε να εμποδίσουμε τους Sniffers?

Υπάρχει πραγματικά μόνο ένας τρόπος να προστατευθούν οι πληροφορίες σας από το sniffing: αυτός είναι η χρήση κρυπτογράφησης. Χρησιμοποιώντας τα Secure Sockets Layer (SSL, προστατευόμενες τοποθεσίες Web) και άλλα εργαλεία προστασίας, μπορούμε να κρυπτογραφήσουμε κωδικούς πρόσβασης , τα μηνύματα email και τις συνεδρίες συνομιλίας. Υπάρχουν πολλά προγράμματα διαθέσιμα δωρεάν που είναι αρκετά εύχρηστα. Αν και δεν είναι πάντα απαραίτητο να προστατεύσετε τις πληροφορίες που περνούν κατά τη διάρκεια μιας συνομιλίας με τους φίλους σας, πρέπει τουλάχιστον να έχετε την επιλογή όταν χρειάζεται.

Λόγω της ιδιαίτερης φύσης ενός WLAN, η κρυπτογράφηση είναι σημαντική σε οποιαδήποτε κατάσταση. Ευτυχώς, τα ασύρματα δίκτυα έρχονται με την επιλογή της κρυπτογράφησης στο λογισμικό τους. Εντούτοις, λίγοι εκμεταλλεύονται αυτήν την ικανότητα, όπως και λίγοι γνωρίζουν ακόμα και ότι αυτή η επιλογή υπάρχει.

ΚΕΦΑΛΑΙΟ 3

3. Εφαρμογές για σύλληψη πακέτων

Πριν μερικά χρόνια, το hacking και η αντιμετώπισή του ήταν κάτι που σχεδόν απαιτούσε τη χρήση πλατφόρμων unix, αφού ελάχιστα προγράμματα κυκλοφορούσαν για windows. Όσο περνούν τα χρόνια όμως, εμφανίζονται όλο και περισσότερα πολλαπλών λειτουργικών (cross platform) εργαλεία. Τα πιο συνηθισμένα από αυτά θα αναφερθούν παρακάτω.

3.1 Tcpdump

Το tcpdump αναπτύχθηκε το 1987 στο εργαστήριο Lawrence Berkeley στο Πανεπιστήμιο του Berkeley της California, από τους Van Jacobson, Craig Leres, και Steven McCanne καθηγητών του πανεπιστημίου. Αναπτύχθηκε αρχικά για τα προβλήματα απόδοσης του πρωτοκόλλου TCP/IP. [16]

Διάφορα χαρακτηριστικά γνωρίσματα έχουν προστεθεί κατά τη διάρκεια του χρόνου αν και μερικές επιλογές μπορούν να μην είναι διαθέσιμες με κάθε εφαρμογή. Το πρόγραμμα αρχικά ήταν σε μια ευρεία ποικιλία των συστημάτων unix.

Για ποικίλους λόγους, το tcpdump είναι ένα ιδανικό εργαλείο για να αρχίσει κανείς. Είναι ελεύθερα διαθέσιμο, τρέχει σε πολλές πλατφόρμες Unix, ακόμη και σε Microsoft Windows. [17] Χαρακτηριστικά γνωρίσματα της σύνταξής του και το σύστημα αρχείων του έχει χρησιμοποιηθεί ή έχει υποστηριχθεί από έναν μεγάλο αριθμό προγραμμάτων. Ειδικότερα, περιλαμβάνει το λογισμικό σύλληψής libpcap, το οποίο χρησιμοποιείται συχνά και από άλλα προγράμματα σύλληψης. Παρά το ότι και άλλα προγράμματα με αρκετά πρόσθετα χαρακτηριστικά γνωρίσματα χρησιμοποιούνται ήδη ευρέως, η καθολικότητα του tcpdump το κάνει μια αναγκαία επιλογή. Εάν εργαζόμαστε με μια ευρεία ποικιλία πλατφορμών, πρέπει να είμαστε σε θέση να χρησιμοποιήσουμε το ίδιο πρόγραμμα για όλες ή τις περισσότερες από τις πλατφόρμες. Αυτό διευκολύνει ιδιαίτερα διότι είναι καλύτερο να γνωρίζουμε ένα

[16] Official site for tcpdump (and libpcap) (http://www.tcpdump.org/)

[17] “Tcpdump for Windows” (http://www.winpcap.org/windump/)

πρόγραμμα καλά παρά διάφορα προγράμματα επιφανειακά. Σε τέτοιες περιπτώσεις, συγκεκριμένα χαρακτηριστικά γνωρίσματα των προγραμμάτων πιθανώς δε θα χρησιμοποιηθούν ποτέ αφού μπορεί να μην έχουν το ίδιο επιθυμητό αποτέλεσμα.

3.1.1 Χρησιμοποιώντας το Πρόγραμμα

Ο απλούστερος τρόπος να τρέξει το tcpdump είναι πληκτρολογώντας το όνομα του προγράμματος στην επιλογή “run” του υπολογιστή μας. Το αποτέλεσμα θα εμφανιστεί στην οθόνη. Μπορούμε να κλείσουμε το πρόγραμμα πληκτρολογώντας Ctrl-C, εκτός αν έχουμε ένα idle network, δηλαδή ένα δίκτυο με πολλή μικρή και με διακοπές κυκλοφορία, οπότε είναι πιθανό να καθυστερούν ακόμα και οι λειτουργείς ανοίγματος – κλεισίματος του προγράμματος[18]. Η πρώτη σημαντική ερώτηση είναι πώς προγραμματίζουμε να χρησιμοποιήσετε το tcpdump.

3.1.2 Επιλογές

Ένα πλήθος εντολών είναι διαθέσιμες με το tcpdump. Κατά προσέγγιση, οι επιλογές μπορούν να χωριστούν σε τέσσερις ευρείες κατηγορίες

- εντολές που ελέγχουν τις διαδικασίες προγράμματος (excluding filtering),

- εντολές που ελέγχουν πώς εμφανίζεται η σύλληψη,

- εντολές που ελέγχουν ποια σύλληψη εμφανίζεται,

- και εντολές φιλτραρίσματος.

Παράδειγμα: [19]

Για να συλλέξουμε δεδομένα χρησιμοποιούμε την εντολή:

 # tcpdump -w raw file

[18] “Tcpdump for Windows” (http://www.winpcap.org/windump/)

[19] “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)

Τα στοιχεία θα μπορούσαν να μετατραπούν σε ένα αρχείο κειμένου για ευκολότερη μελέτη και ανάλυση με την εντολή:

 # tcpdump -r raw file > textile

3.1.3 Ελέγχοντας τη συμπεριφορά του προγράμματος

Αυτή η κατηγορία των επιλογών, έχει επιπτώσεις στη συμπεριφορά του προγράμματος, συμπεριλαμβανομένου του τρόπου που τα στοιχεία συλλέγονται. Έχουμε δει ήδη δύο παραδείγματα των εντολών ελέγχου, *-r* και *-w*. Η *-w* επιλογή επιτρέπει να επαναπροσανατολίσουμε (redirect) το αποτέλεσμα σε ένα αρχείο για ανάλυση, το οποίο μπορεί να είναι εξαιρετικά χρήσιμο. Μπορούμε να επαναλάβουμε διαφορετικές επιλογές επίδειξης ή να φιλτράρουμε τα δεδομένα μέχρι να βρούμε ακριβώς τις πληροφορίες που θέλουμε. Αυτές οι επιλογές είναι εξαιρετικά χρήσιμες στην εκμάθηση του tcpdump.

Εάν ξέρουμε πόσα πακέτα θέλουμε να συλλάβουμε ή εάν έχουμε ένα όριο στον αριθμό πακέτων, η επιλογή *-c* μας επιτρέπει να διευκρινίσουμε τον αριθμό αυτό. Το πρόγραμμα θα ολοκληρωθεί αυτόματα όταν επιτευχθεί ο αριθμός αυτός, εξαλείφοντας την ανάγκη να χρησιμοποιήσουμε μια εντολή κλεισίματος ή Ctrl-C.

Μπορούμε να προσδιορίσουμε κάποιες σημαντικές επιλογές που καθορίζουν τον τρόπο συλλογής πακέτων και είναι σημαντικές σε αρκετές περιπτώσεις. [20]

Στο επόμενο παράδειγμα, το tcpdump θα κλείσει αυτόματα αφότου συλλέξει 100 πακέτα:

 # tcpdump -c100

Η ακόλουθη εντολή θα συλλέξει τα πακέτα αν το μέγεθος είναι μικρότερο ή ίσο με 200 bytes.

 # tcpdump -s200

Τα πακέτα μεγαλύτερου μεγέθους θα περικοπούν σε 200 bytes.

[20] “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)

3.1.4 Φιλτράρισμα

Για να χρησιμοποιήσουμε αποτελεσματικά το tcpdump, είναι απαραίτητη η χρήση των φίλτρων. Τα φίλτρα επιτρέπουν σε εμάς να διευκρινίσουμε ποια κυκλοφορία θέλουμε να συλλάβουμε, επιτρέποντας μας να στραφούμε ακριβώς σε ότι μας είναι ενδιαφέρον. Αυτό μπορεί να είναι απολύτως ουσιαστικό εάν πρέπει να εξαγάγουμε ένα μικρό ποσό κυκλοφορίας από ένα ογκώδες αρχείο (trace file). Εργαλεία όπως το ethereal χρησιμοποιούν τον τρόπο σύνταξης φίλτρων του tcpdump για τη σύλληψη κυκλοφορίας, αυτό σημαίνει ότι πρέπει να μάθετε τη σύνταξη αυτή εάν προγραμματίζετε να χρησιμοποιήσετε λεπτομερώς αυτά τα εργαλεία.

Εάν είμαστε απολύτως σίγουροι ότι δεν ενδιαφερόμαστε για μερικά είδη κυκλοφορίας, μπορούμε να αποκλείσουμε την κυκλοφορία καθώς συλλαμβάνεται. Εάν είμαστε ασαφείς ποια κυκλοφορίας θέλουμε, μπορούμε να συλλέξουμε ακατέργαστα στοιχεία row data σε ένα αρχείο και να εφαρμόσουμε τα φίλτρα όταν διαβάσουμε πάλι το αρχείο. Στην πράξη, εναλλασσόμαστε συχνά μεταξύ αυτών των δύο προσεγγίσεων.

Τα φίλτρα στο απλούστερό τους είναι λέξεις κλειδιά που προστίθενται στο τέλος της γραμμής εντολής. Εντούτοις, οι εξαιρετικά σύνθετες εντολές μπορούν να κατασκευαστούν χρησιμοποιώντας τους λογικούς τελεστές. Στην τελευταία περίπτωση, είναι συνήθως καλύτερο να σωθεί το φίλτρο σε ένα αρχείο χρησιμοποιώντας την *-F* επιλογή. Παραδείγματος χάριν, εάν testfilter είναι ένα αρχείο κειμένων που περιέχει τον οικοδεσπότη ‘host 205.153.63.30’, η εντολή ‘tcpdump –Ftestfilter’ είναι ισοδύναμη με τη δακτυλογράφηση της εντολής *tcpdump host 205.153.63.30.* Γενικά, θα θελήσουμε να χρησιμοποιήσουμε αυτό το χαρακτηριστικό γνώρισμα με τα σύνθετα φίλτρα μόνο. Εντούτοις, δεν μπορούμε να συνδυάσουμε τα φίλτρα στη γραμμή εντολής με ένα αρχείο φίλτρων στην ίδια εντολή.

3.1.5 Φιλτράρισμα βάση διεύθυνσης

Δεν πρέπει να αποτελέσει έκπληξη ότι τα φίλτρα μπορούν να επιλέξουν την κυκλοφορία βασιζόμενα στις διευθύνσεις.

Παραδείγματος χάριν, εξετάζουμε την εντολή:

tcpdump host 205.153.63.30

Αυτή η εντολή συλλαμβάνει όλη την κυκλοφορία από και προς τον υπολογιστή με τη διεύθυνση IP 205.153.63.30. Ο υπολογιστής μπορεί να διευκρινιστεί από τον αριθμό ή το όνομα του. Ας υποθέσουμε ότι η κυκλοφορία που συλλαμβάνεται θα περιοριστεί στην κυκλοφορία της συγκεκριμένης IP διεύθυνσης. Στην πραγματικότητα και άλλη κυκλοφορία, όπως η ARP κυκλοφορία, θα συλλεχθεί επίσης από αυτό το φίλτρο. Ο περιορισμός που χρειάζεται για να συλληφθεί ένα ιδιαίτερο πρωτόκολλο απαιτεί ένα πιο σύνθετο φίλτρο. Αυτή η συμπεριφορά απαιτεί πρώτα μια λεπτομερή δοκιμή όλων των φίλτρων.

Υπάρχουν κάποια προγράμματα που συνοδεύουν το Tcpdump τα οποία μας διευκολύνουν είτε στην συλλογή είτε στην ανάγνωση των δεδομένων που συλλαμβάνονται. Τα πιο σημαντικά από αυτά είναι τα εξής: [21]

1. tcpdpriv

Το πρόγραμμα tcpdpriv είναι ένα άλλο πρόγραμμα για την απομάκρυνση ευαίσθητων πληροφοριών από τα αρχεία του tcpdump.

2. Tcp-flow

Ένα άλλο χρήσιμο εργαλείο είναι το tcpflow, το οποίο δημιούργησε ο Jeremy Elson. Αυτό το πρόγραμμα μας επιτρέπει να συλλάβουμε μεμονωμένες TCP ροές ή συνόδους. Εάν η κυκλοφορία που εξετάζουμε περιλαμβάνει, τρεις διαφορετικές συνόδους, το tcpflow θα χωρίσει την κυκλοφορία σε τρία διαφορετικά αρχεία έτσι ώστε να μπορούμε να εξετάσουμε κάθε ένα χωριστά. Το tcpflow αποθηκεύει κάθε ροή σε ένα χωριστό αρχείο με ένα όνομα βασισμένο στην πηγή και τη διεύθυνση προορισμού.

[21] “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)

3. tcpshow

Το πρόγραμμα tcpshow αποκωδικοποιεί ένα tcpdump αρχείο. Αντιπροσωπεύει μια εναλλακτική λύση στη χρησιμοποίηση του tcpdump για να αποκωδικοποιήσει τα στοιχεία που συλλέγονται. Το αρχικό πλεονέκτημα του tcpshow είναι ότι παρουσιάζει μια πιο εύχρηστη μορφοποίηση για την εμφάνιση αποτελεσμάτων.

Παραδείγματος χάριν, εδώ είναι η παραγωγή tcpdump για ένα πακέτο:

12:36:54.772066 sloan.lander.edu.1174 > 205.153.63.238.telnet: . ack

3259091394 win 8647 (DF) b

Εδώ είναι η αντίστοιχη παραγωγή από το tcpshow για το ίδιο πακέτο:

Packet 1

TIME: 12:36:54.772066

LINK: 00:10:5A:A1:E9:08 -> 00:10:5A:E3:37:0C type=IP

IP: sloan -> 205.153.63.238 hlen=20 TOS=00 dgramlen=40 id=B30C

MF/DF=0/1 frag=0 TTL=128 proto=TCP cksum=2D84

TCP: port 1174 -> telnet seq=0016775603 ack=3259091394

hlen=20 (data=0) UAPRSF=010000 wnd=8647 cksum=E869 urg=0

DATA: <No data>

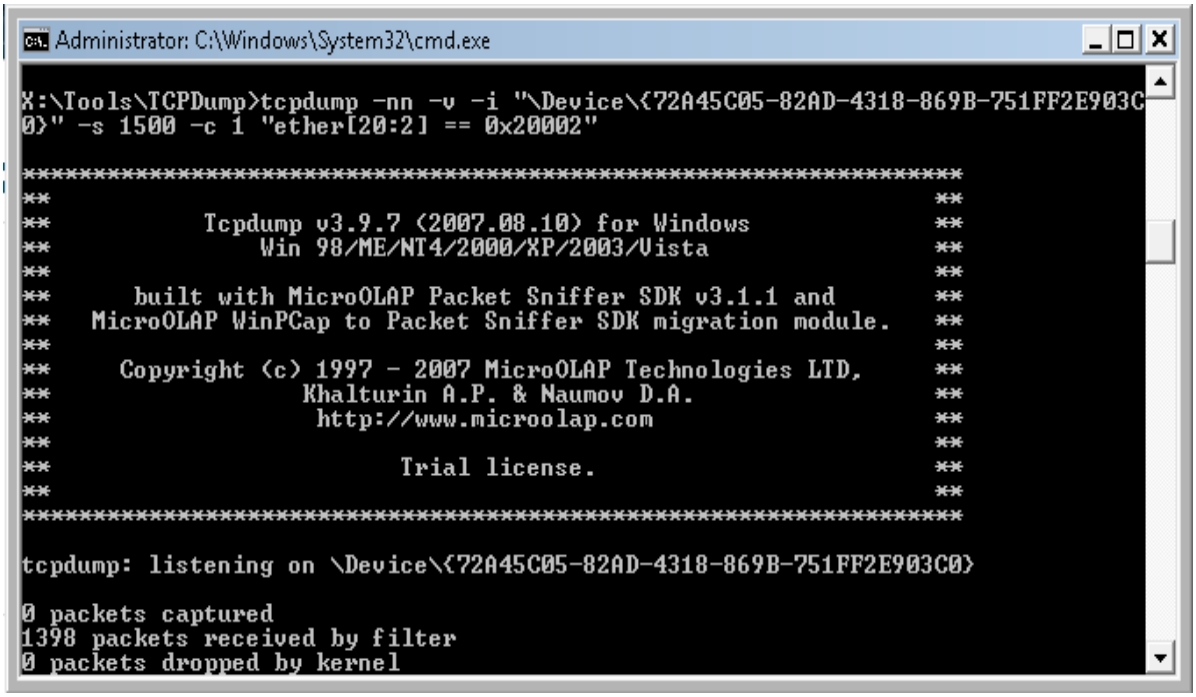
Η σύνταξη έχει ως εξής:

tcpshow < trace-file

4. trafshow

Το πρόγραμμα trafshow είναι ένα ακόμα πρόγραμμα σύλληψης πακέτων. Παρέχει μια συνεχή επίδειξη της κυκλοφορίας και πέρα από το δίκτυο, δίνοντας επαναλαμβανόμενα στιγμιότυπα της κυκλοφορίας. Επιδεικνύει τη διεύθυνση προέλευσης, τη διεύθυνση προορισμού, το πρωτόκολλο, και τον αριθμό των bytes. Αυτό το πρόγραμμα θα ήταν πιο χρήσιμο στην έρευνα της «ύποπτης» κυκλοφορίας, ή απλά να παίρνουμε μια γενική ιδέα της κυκλοφορίας του δικτύου μας.

Παρακάτω στην εικόνα 3.1 φαίνεται ο τρόπος που εκκινεί και τρέχει το tcpdump σε περιβάλλον DOS



Εικόνα 3.1: Το tcpdump σε περιβάλλον DOS

3.2 Cain and Abel

Υπάρχει όμως ένα πρόγραμμα, το Cain & Abel της oxid, που κυκλοφορεί από το 2001 (ελεύθερα), εξελίσσεται συνεχώς και κάνει τους χρήστες windows υπερήφανους. Δημιουργήθηκε από τον Massimiliano Montoro. Μιλάμε ίσως για το καλύτερο εργαλείο hacking για πλατφόρμα windows το οποίο ξεκίνησε κυρίως ως εργαλείο αποκατάστασης κωδικών, αλλά μπορεί να κάνει πολλά περισσότερα.

Το πρόγραμμα αποτελείται από δύο μέρη, τα οποία λειτουργούν αυτόνομα μεταξύ τους. Το Cain, το οποίο είναι και το βασικό πρόγραμμα, και το Abel το οποίο τρέχει σαν server στον υπολογιστή και δίνει τη δυνατότητα να τον ελέγξετε από απόσταση μέσω του Cain, χρησιμοποιώντας μια μακρινή εντολή (remote command prompt).[22]

Μερικές μόνο από της δυνατότητες του Cain είναι:

- Σνιφάρισμα δικτύου (network sniffing)
- Σπάσιμο κρυπτογραφημένων κωδικών με τη χρήση λεξικού (cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks)
- Εγγραφή συνομιλιών (recording VoIP conversations)
- Αποκατάσταση ασυρμάτων δικτύων (recovering wireless network keys)
- Αποκάλυψη κωδικών (revealing password boxes)
- Αποκάλυψη αποθηκευμένων κωδικών (uncovering cached passwords)
- Ανάλυση πρωτοκόλλων δρομολόγησης (analyzing routing protocols)
- APR (Arp Poison Routing)

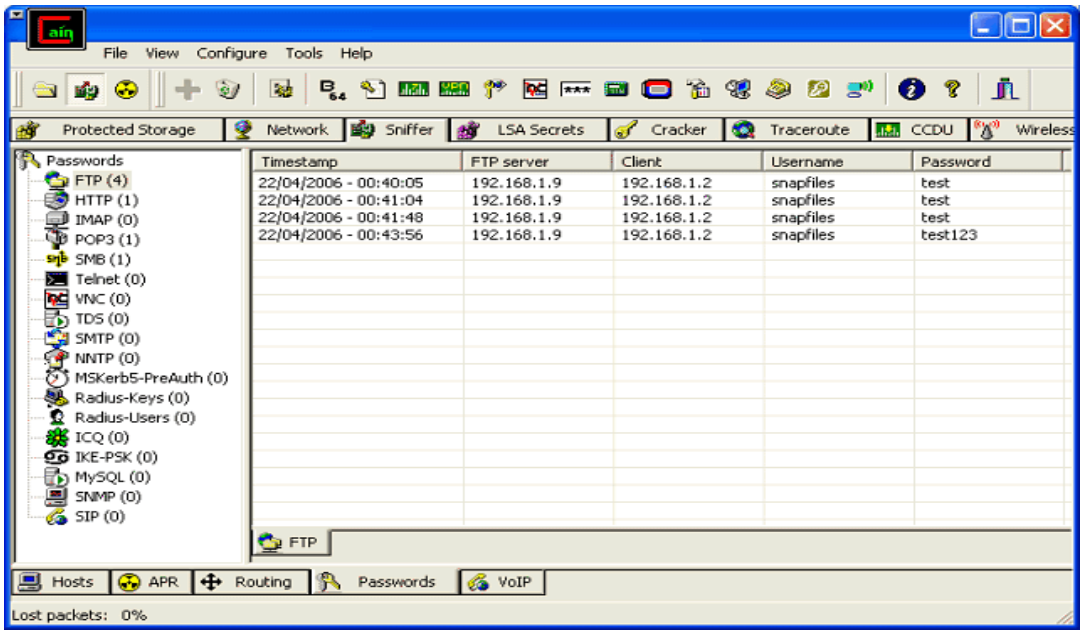
Το Cain & Abel είναι ένα εργαλείο ανάκτησης κωδικών πρόσβασης για τα λειτουργικά συστήματα της Microsoft. Επιτρέπει δικτυακό sniffing', σπάει κρυπτογραφημένους κωδικούς πρόσβασης χρησιμοποιώντας λεξικό και βοηθάει στην ανάκτηση κλειδιών ασύρματων δικτύων και στην ανάλυση των πρωτοκόλλων δρομολόγησης. [23]

Αναπτύχθηκε με σκοπό να χρησιμοποιηθεί από διαχειριστές δικτύων, καθηγητές, και συμβούλους ασφαλείας. Η πιο πρόσφατη έκδοση είναι γρηγορότερη και περιέχει πολλά νέα χαρακτηριστικά γνωρίσματα.

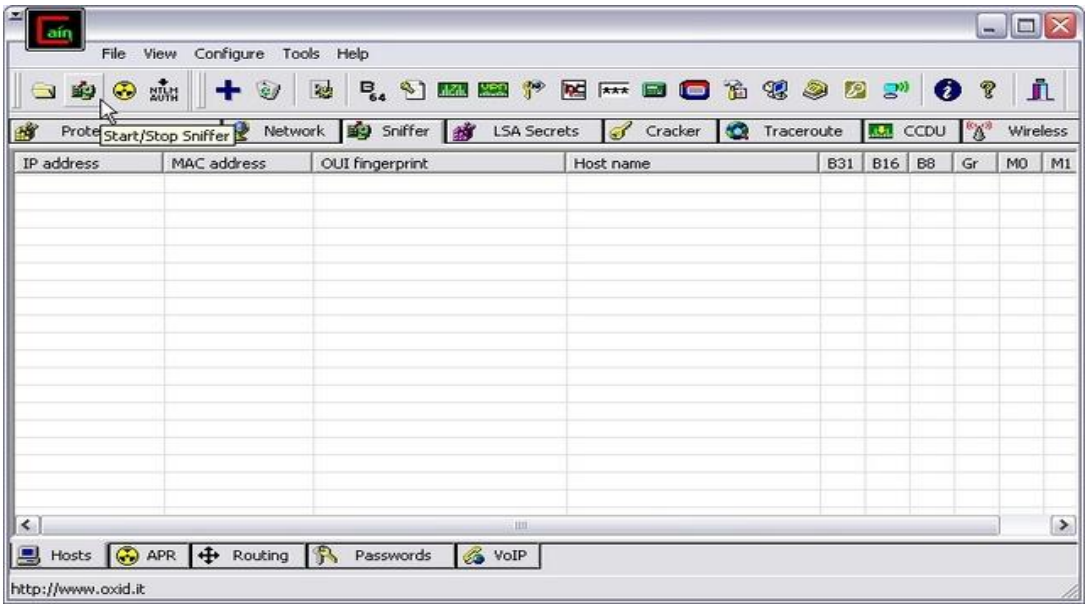
---

[22] Άρθρο, 5 Ιανουαρίου 2008 "Cain & Abel – το απόλυτο windows hacking tool" (http://mechanicshell.wordpress.com)

[23] http://www.oxid.it/cain.html



Εικόνα 3.2: Περιβάλλον του Cain and Avel

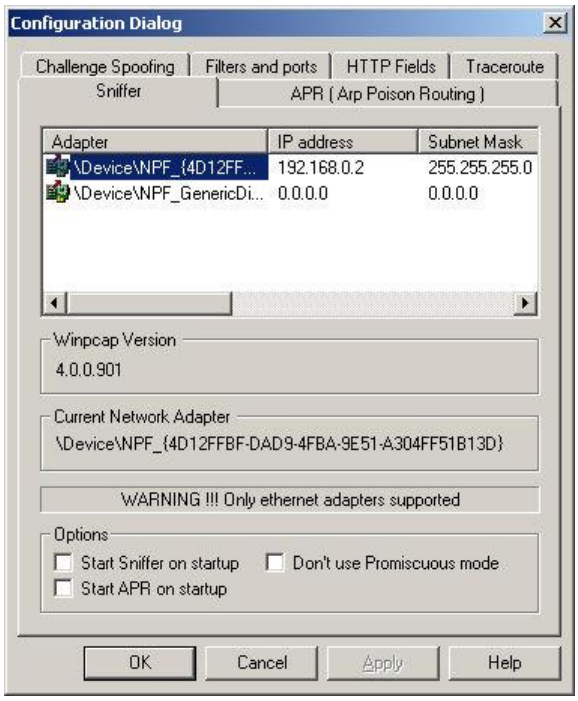


Εικόνα 3.3: Περιβάλλον του Cain and Avel

3.2.1 Διαμόρφωση Παραμέτρων

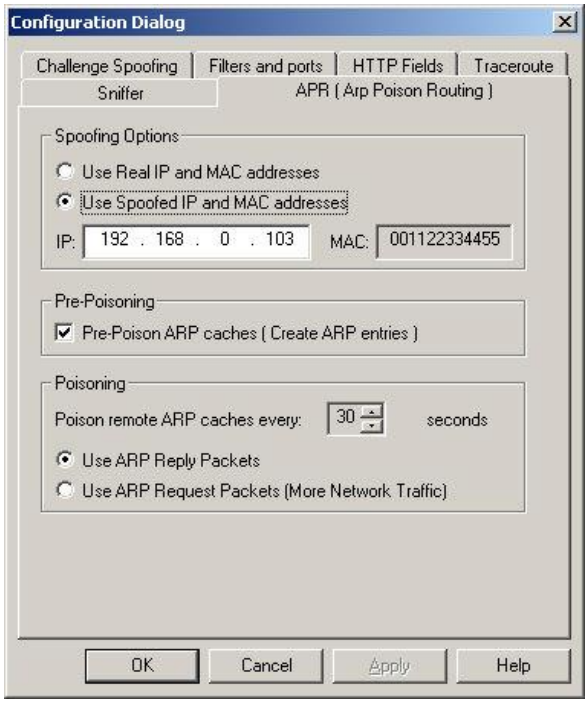
Το Cain & Abel απαιτεί τη διαμόρφωση μερικών παραμέτρων οι οποίες μπορούν να γίνουν από το κεντρικό παράθυρο διαλόγου (configuration dialog) όπως παρακάτω.[24]

[24] "Ηλεκτρονικό Εγχειρίδιο Cain and Abel" http://www.oxid.it/ca_um/



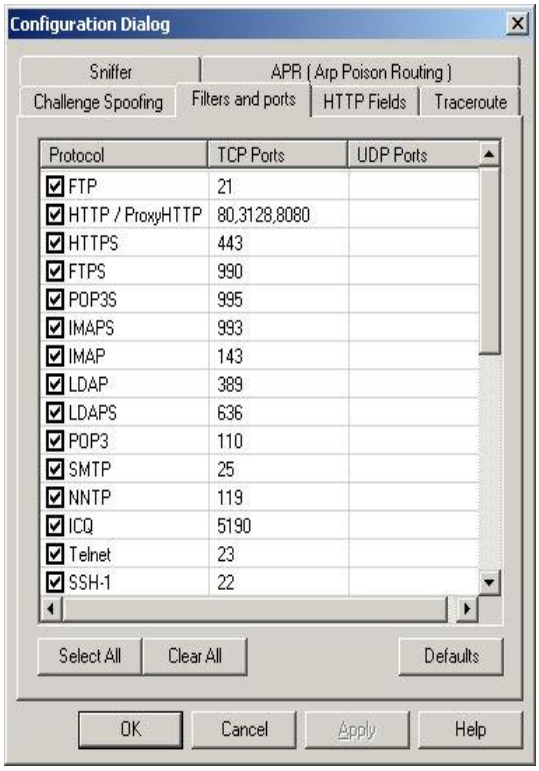
Εικόνα 3.4: Επιλογή κάρτας δικτύου

Εδώ μπορούμε να ρυθμίσουμε την κάρτα δικτύων που θα χρησιμοποιεί το Cain sniffer και χαρακτηριστικά γνωρίσματα του APR. Τα τελευταία δύο παράθυρα ελέγχου ενεργοποιούν/ απενεργοποιούν αυτές τις λειτουργίες στο ξεκίνημα του προγράμματος. Εάν «τσεκαριστεί», η επιλογή "Don't use Promiscuous mode" ενεργοποιείται η «APR Poisoning» *σε* ασύρματα δίκτυα. Διαμόρφωση που επιτρέπει να περάσει όλη η κυκλοφορία που θα λαμβάνει.



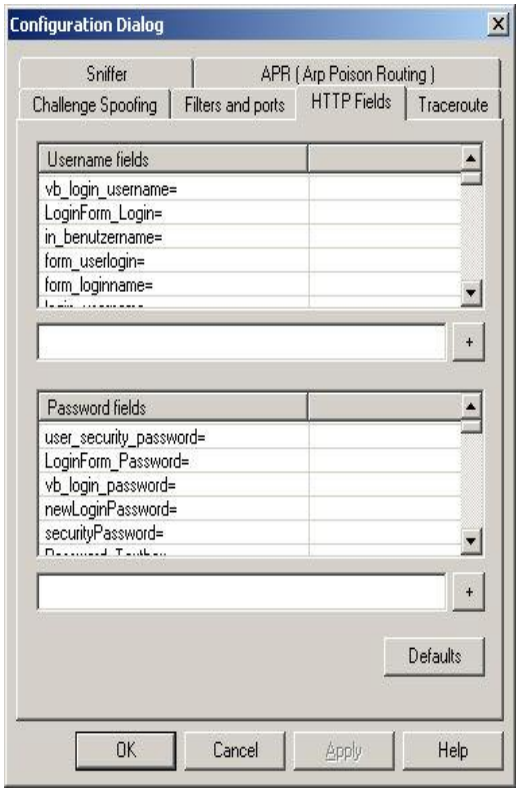
Εικόνα 3.5: Απόκρυψη διεύθυνσης

Οι επιλογές spoofing καθορίζουν τις διευθύνσεις που το Cain γράφει στο Ethernet, ARP επικεφαλίδες και επανακαθοδηγημένα πακέτα. Σε αυτήν την περίπτωση η ARP Poison επίθεση θα είναι απολύτως ανώνυμη επειδή η πραγματική MAC IP του επιτιθεμένου δεν στέλνεται ποτέ στο δίκτυο.



Εικόνα 3.6: Καρτέλα φίλτρων θυρών

Εδώ μπορείτε να επιτρέψουμε ή να θέσουμε εκτός λειτουργίας τα φίλτρα και τα πρωτόκολλα εφαρμογής των θυρών TCP/UDP. Το Cain συλλαμβάνει μόνο πληροφορίες επικύρωσης και όχι το ολόκληρο περιεχόμενο κάθε πακέτου, εντούτοις μπορούμε να χρησιμοποιήσουμε το φίλτρο Telnet για απόρριψη, ενός αρχείου, ή όλων των στοιχείων που είναι παρόντα σε μια σύνοδο πρωτοκόλλου TCP , τροποποιώντας το σχετικό φίλτρο θύρας.



Εικόνα 3.7: Καρτέλα τομέων http

Αυτή η καρτέλα περιέχει έναν κατάλογο ονομάτων και κωδικών πρόσβασης των πεδίων των οποίων χρησιμοποιούνται από το φίλτρο HTTP. Τα Cookies και οι HTML μορφές στα πακέτα HTTP εξετάζονται κατ' αυτό τον τρόπο: για κάθε τομέα ονόματος χρηστών όλοι οι τομείς κωδικού πρόσβασης ελέγχονται και εάν αυτές οι δύο παράμετροι βρίσκονται, τα πιστοποιητικά θα συλληφθούν και θα επιδειχθούν στην οθόνη.

3.3 Carnivore

Το Carnivore είναι ένας συνδυασμός από υλικό και λογισμικό που ανήκει στην κατηγορία των "packet sniffers" (από το αγγλικό sniff, ρουφώ με τη μύτη). Είναι, δηλαδή, ένα εργαλείο που επιτρέπει την παρακολούθηση και την καταγραφή των δεδομένων που μεταφέρονται μέσω ενός δικτύου. Είναι ένα σύστημα που εφαρμόζεται από το Ομοσπονδιακό γραφείο Έρευνας των Η.Π.Α. (F.B.I.) και ο τρόπος λειτουργίας του έχει να κάνει με την υποκλοπή τηλεφωνικών συνδιαλέξεων. Εκτός από αυτήν την περίπτωση, χρησιμοποιείται για να «τρυπάει» το ηλεκτρονικό ταχυδρομείο και άλλες επικοινωνίες όπως την υποκλοπή τηλεφωνικών συνδιαλέξεων μέσω Internet (VoIP, Voice Over IP). Το Carnivore είναι ένα εξατομικεύσιμο πακέτο sniffer το οποίο μπορεί να ελέγξει ενός ή πολλών χρηστών την διαδικτυακή κυκλοφορία μαζί. Το Carnivore εφαρμόστηκε κατά τη διάρκεια της Προεδρίας Clinton με την έγκριση της Γενικής εισαγγελέως Janet Reno των Η.Π.Α. Οι κυβερνητικοί ανώτεροι υπάλληλοι ούτε έχουν επιβεβαιώσει ούτε έχουν αρνηθεί τη χρήση του Carnivore.[25] αλλά υπάρχουν μερικά γεγονότα που είναι γενικώς αναγνωρισμένα.

Το Carnivore είναι βασισμένο στα Microsoft Windows. Ο υπολογιστής στον οποίο «τρέχει» πρέπει να εγκατασταθεί ως φυσικός Φορέας παροχής υπηρεσιών Διαδικτύου ISP (Internet Service Provider, η εταιρεία μέσω της οποίας αποκτούμε πρόσβαση στο Internet) ή απλά σε κάποια άλλη θέση όπου μπορεί «να υποκλέψει» την κυκλοφορία ενός Τοπικού LAN δικτύου για να ψάξει τα μηνύματα ηλεκτρονικού ταχυδρομείου κατά τη μεταφορά τους από τον έναν υπολογιστή σε έναν άλλο.

3.3.1 Τρόπος λειτουργίας

Ο τρόπος λειτουργίας του λογισμικού είναι απλός και έχει ως εξής:

Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ταιριάζει με τα κριτήρια φιλτραρίσματος που έχουν επιλεγεί εξ’ αρχής το μήνυμα καταγράφεται μαζί με τις πληροφορίες για την ημερομηνία, το χρόνο, την προέλευση και τον προορισμό. Το Carnivore "γαντζώνεται" στο ISP, στον οποίο είναι συνδρομητής ο εκάστοτε ‘στόχος’, με σκοπό να εξεταστούν τα e-mail καθώς και η εν γένει η χρήση του Internet από αυτόν. Το

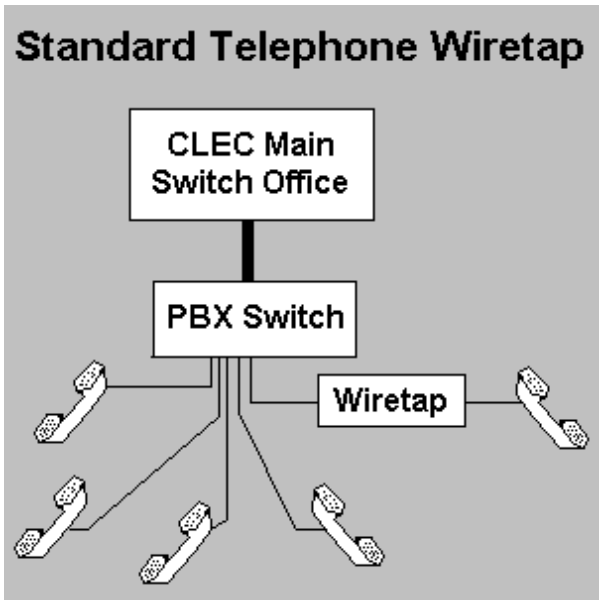
[25] http://www.worldlingo.com/ma/enwiki/el/Carnivore_(software)

"σαρκοφάγο" Carnivore, σύμφωνα με την "The Wall Street Journal", είναι σε θέση να αναλύσει εκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου κάθε δευτερόλεπτο.

Το Carnivore είναι ένα από τα προγράμματα ενός άλλου λογισμικού του ‘’Dragonware’’ από τα οποία είναι και το σημαντικότερο που χρησιμοποιείται αυτόνομα. Το Dragonware αποτελείται από τρία προγράμματα:

Το Carnivore, το πρόγραμμα σύλληψης Packeteer, το πρόγραμμα επανασύνδεσης των πακέτων σε χρήσιμα δεδομένα Coolminer, το Web-based πρόγραμμα ανάλυσης και επεξεργασίας των δεδομένων. [26]

Ενώ οι απλές τηλεφωνικές συνδέσεις εγγυώνται ότι η παρακολούθηση ενός συνδρομητή δεν εκθέτει άλλους ταυτόχρονα, δε συμβαίνει το ίδιο και με το Internet και όλες τις ψηφιακές επικοινωνίες. Πιο κάτω στις εικόνες φαίνεται με ποιον τρόπο το Carnivore εκμεταλλεύεται τις δυνατότητες του Internet. [27]

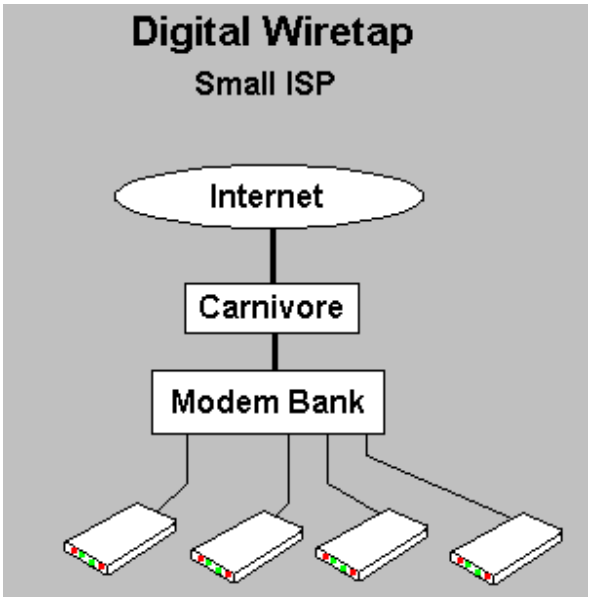


Εικόνα 3.8: Τυποποιημένη καλωδίωση

Η τυποποιημένη καλωδίωση εκθέτει μόνο μία γραμμή τη φορά

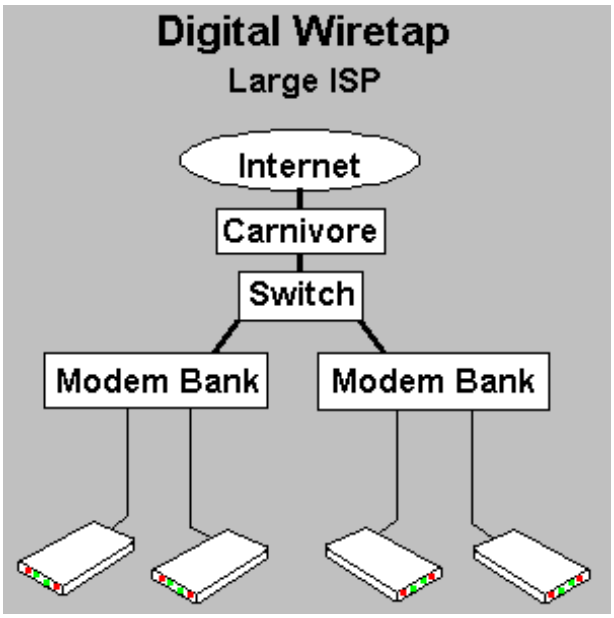
[26] “Άρθρο” Κυριακή 1 Δεκεμβρίου 2002 (http://athens.indymedia.org)

[27] Άρθρο από τον James McPherson 09 Ιαν 2001 (http://articles.techrepublic.com)



Εικόνα 3.9: Κεντρικός κατανεμητής τηλεπικοινωνιών

Όλες οι επικοινωνίες μαζεύονται σε ένα κεντρικό κατανεμητή και το λειτουργικό του προγράμματος μπορεί να τις επεξεργαστεί ταυτόχρονα



Εικόνα 3.10: Δίκτυο με περισσότερους κατανεμητές τηλεπικοινωνίας

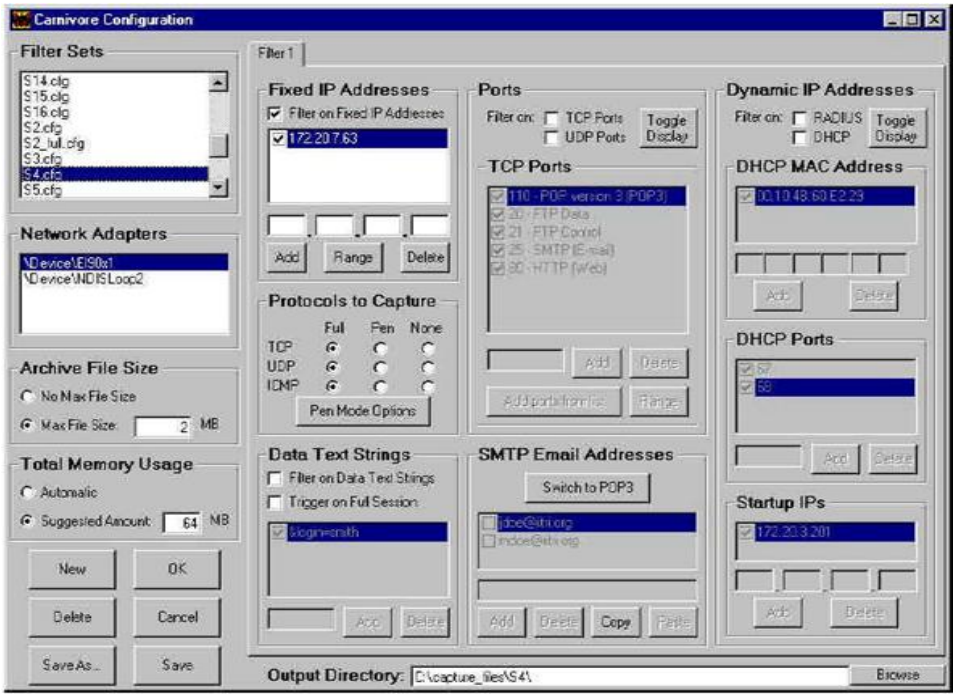
Ακόμα και για πολύ μεγάλα δίκτυα και παροχείς υπηρεσιών Internet με διακόπτες το Carnivore αν και εκτός τοπικού δικτύου μπορεί να κάνει όλες τις επικοινωνίες εύκολα προσπελάσιμες.

Λόγω της ευκολίας του προγράμματος στην υποκλοπή συνδιαλέξεων αναλογικών ή κυρίως ψηφιακών το EPIC (Electronic Privacy Information Center- Κέντρο Πληροφόρησης για το Ηλεκτρονικό Απόρρητο) των Η.Π.Α. επικαλέστηκε το νόμο περί της ελευθερίας των πληροφοριών (FOIA, Freedom of Information Act) και πέτυχε τη δημοσιοποίηση μιας σειράς εγγράφων σχετικά με το Carnivore που έχουν ως σκοπό να αποτρέψουν οποιονδήποτε οργανισμό -Δημόσιο και μη- να εκμεταλλεύεται προς όφελος του το λογισμικό αυτό. Εφόσον το Carnivore αναπτύχθηκε από το FBI εγκαθίσταται μόνο εντός των ΗΠΑ, ο υπόλοιπος κόσμος δεν θα έπρεπε να επηρεάζεται. Δυστυχώς όμως, τα πράγματα δεν είναι έτσι, καθώς τα πιο πολλά δεδομένα από και προς την Ελλάδα περνούν μέσα από αμερικάνικο έδαφος. Η βασική αιτία είναι το γεγονός ότι η επικοινωνία της πλειοψηφίας των ελληνικών ISPs με το υπόλοιπο Internet γίνεται κατά βάση μέσω ΗΠΑ.

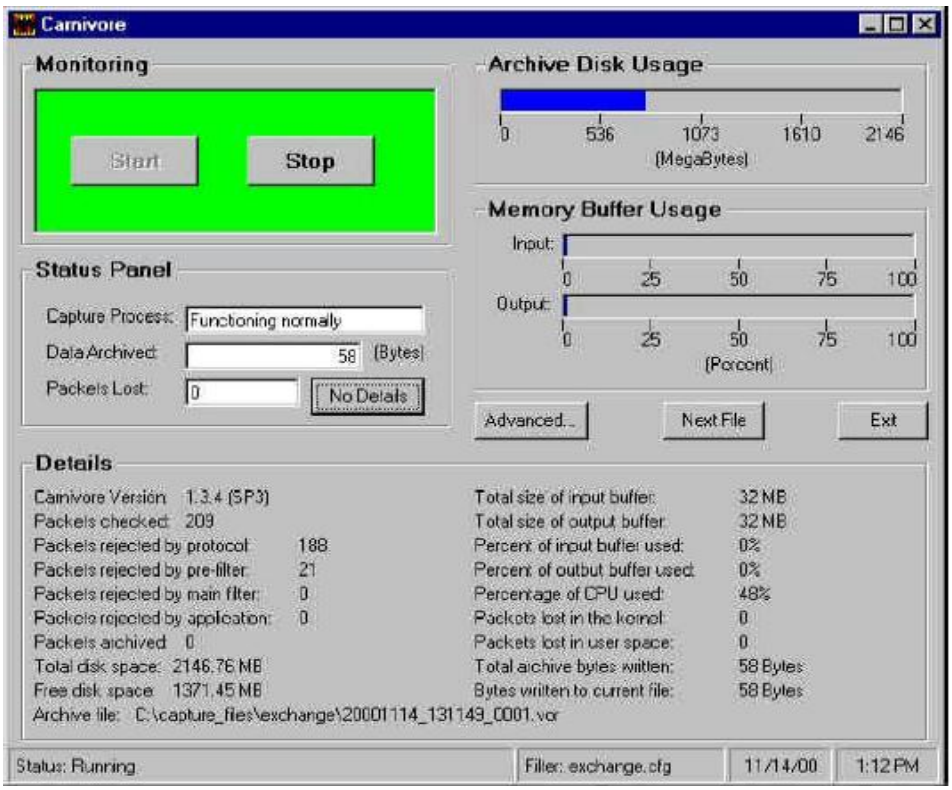
Ενας απλός τρόπος να εξακριβώσουμε εάν και τα δεδομένα από και προς τον δικό μας υπολογιστή μπορεί να είναι ορατά από το FBI, είναι το πρόγραμμα ‘’tracert.exe’’ που βρίσκεται στο directory των Windows και το οποίο εμφανίζει την πορεία των πακέτων των δεδομένων ανάμεσα σε εμάς και το επιθυμητό site. Ενώ είμαστε συνδεδεμένοι στο Internet, από ένα παράθυρο DOS μπορούμε να δώσουμε την εντολή «tracert + ‘όνομα site’ » (π.χ. tracert www.gchq.gov.uk) και αν στον πίνακα των ενδιάμεσων κόμβων εμφανιστούν και κάποια στις Η.Π.Α., τότε το Carnivore και η διαμάχη γι’ αυτό θα έπρεπε να μας ενδιαφέρει άμεσα. [28]

Το περιβάλλον του προγράμματος για λειτουργία και διαμόρφωση επιλογών αναζήτησης φαίνεται στις εικόνες 3.11 και 3.12 παρακάτω.

[28] Άρθρο από τον James McPherson 09 Ιαν 2001 (http://articles.techrepublic.com)



Εικόνα 3.11: Περιβάλλον του Carnivore



Εικόνα 3.12: Περιβάλλον του Carnivore

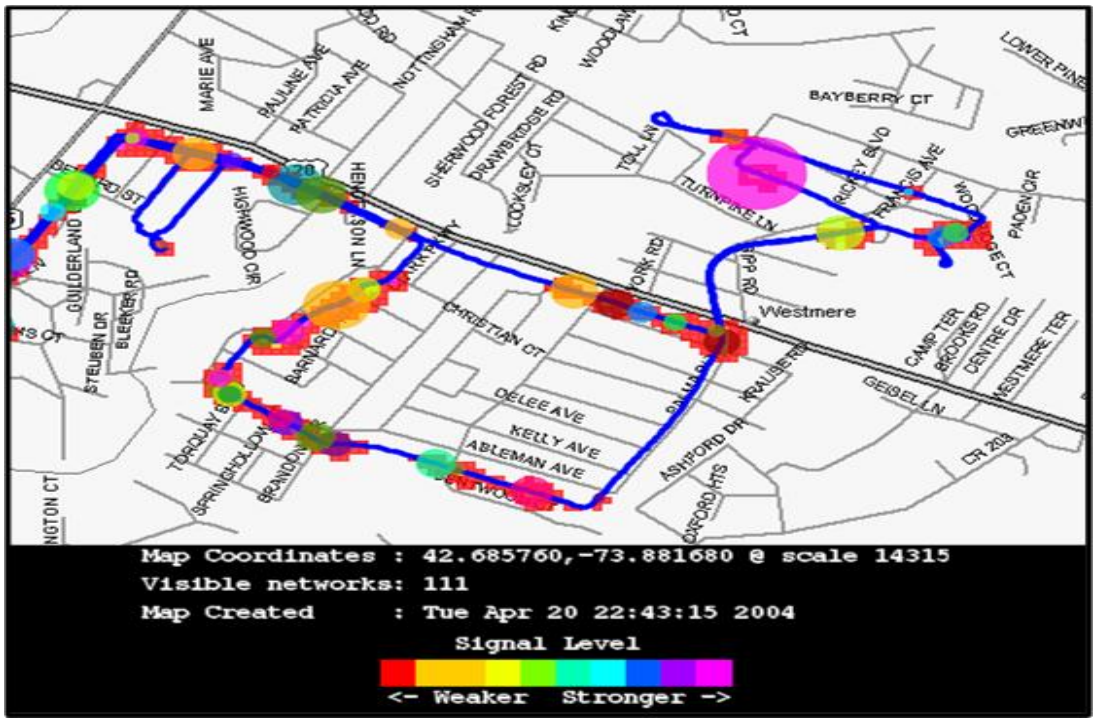
3.4 Kismet

Το όνομα Kismet σημαίνει ‘’μοίρα’’ , ‘’πεπρωμένο’’ . Αναπτύχθηκε από τον Άγγλο προγραμματιστή *Mike Kershaw* το 1999 και είναι ένα πρόγραμμα ηλεκτρονικού υπολογιστή το οποίο μπορεί να εντοπίζει δίκτυα (network detector), να υποκλέπτει πακέτα (packet sniffer) και επίσης μπορεί να εντοπίζει επιθέσεις σε 802.11 WLAN δίκτυα. Το Kismet δουλεύει με όλες τις ασύρματες κάρτες που υποστηρίζουν monitor mode, και μπορεί να ανιχνεύσει δίκτυα 802.11a, 802.11b, 802.11g. Το πρόγραμμα τρέχει σε όλες σχεδόν τις πλατφόρμες όπως Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, και Microsoft Windows μέχρι και την τελευταία έκδοση μέχρι σήμερα τα Windows 7. Αναπτύχθηκε στην τελική του κατάσταση γύρω στο 2005 παρά το ότι λειτουργεί από πιο παλιά και διατίθεται από την Γενική Άδεια Χρήσης GNU και είναι ελεύθερο λογισμικό. [29]

3.4.1 Τρόπος λειτουργίας / Δυνατότητες

Το Kismet σε αντίθεση με τα άλλα προγράμματα του είδους λειτουργεί παθητικά αυτό σημαίνει ότι μπορεί να ανιχνεύσει, χωρίς να στείλει κάποιο πακέτο, τα ασύρματα σημεία πρόσβασης και να τα συσχετίσει μεταξύ τους. Το Kismet δεν μπορεί να ξέρει την ακριβή θέση ενός δικτύου, μπορεί μόνο να ξέρει τη θέση όπου ανακάλυψε ένα σήμα κυκλώνοντας την πιθανή θέση. Εντούτοις αυτό δεν είναι απολύτως ακριβές. Για να αλλάξει αυτό μπορεί να γίνει κάτι διαφορετικό. Το Kismet μπορεί να ενσωματωθεί σε μία συσκευή GPS, η οποία με τη σειρά της θα παρέχει τις συντεταγμένες για το δίκτυο που ανιχνεύθηκε. Αυτό μπορεί να επιλεγεί από το φάκελο <pcap> όταν ενεργοποιείται η συσκευή η οποία διαθέτει επίσης το ‘Kismap’ που είναι «τρίτο» κομμάτι του Kismap. Η ανάγνωση του δικτύου μπορεί να γίνει είτε από ένα υπολογιστή συνδεδεμένο με τη συσκευή GPS είτε απευθείας από το GPS. Για τη σωστή διαδικασία θα πρέπει να οριστούν επακριβώς οι κατάλληλοι drivers του GPS.

[29] “Kismet Readme Manual” από τον Mike Kershaw 2010 (http://www.kismetwireless.net/documentation.shtml)

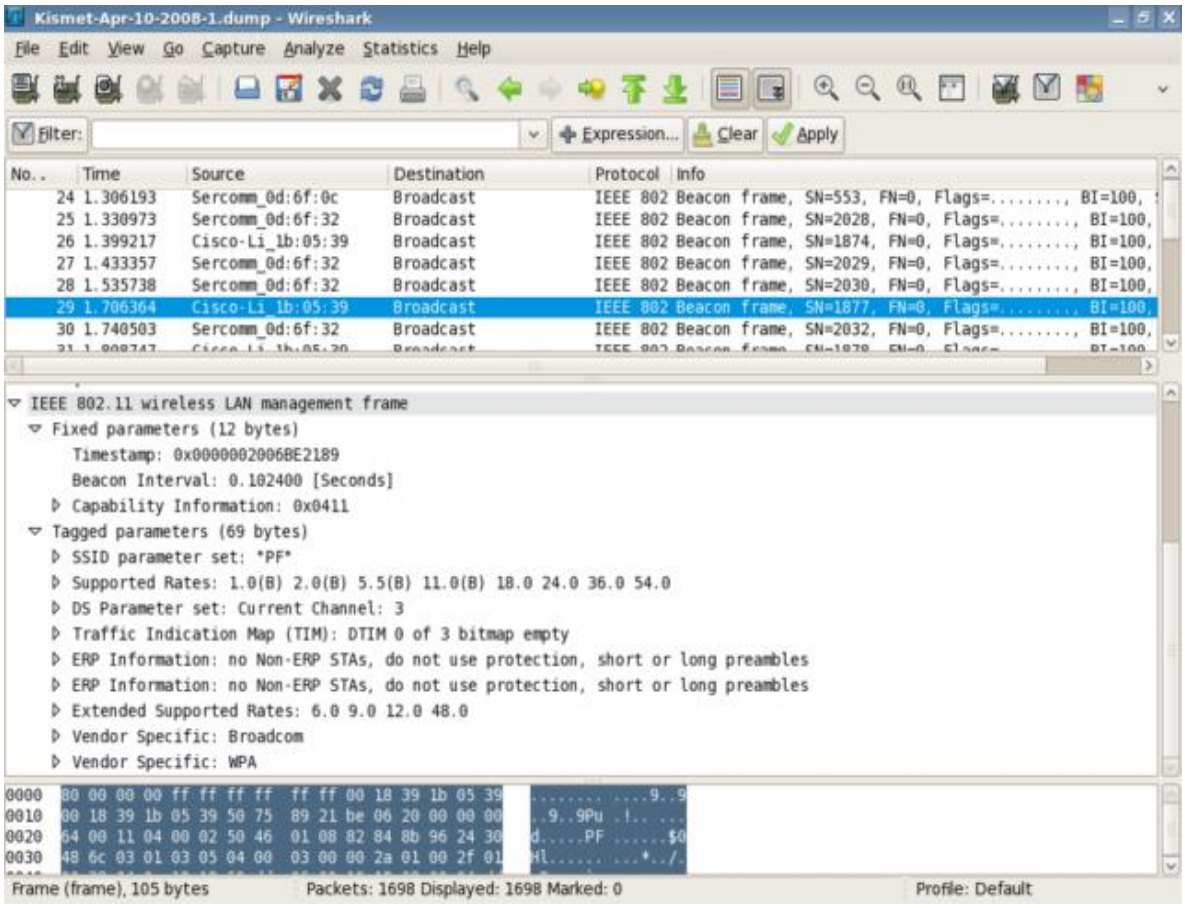


Εικόνα 3.13: Γραφική απεικόνιση ανάγνωσης από GPS

Είναι απαραίτητο να επιλέξουμε στο Kismet ποιο συγκεκριμένο τύπο κάρτας χρησιμοποιούμε επειδή διαφορετικοί drivers συχνά έχουν διαφορετικές μεθόδους χρήσης και τρόπους για να παρουσιάσουν τις πληροφορίες που λαμβάνει το λογισμικό του προγράμματος.

Είναι ένα λογισμικό με πάρα πολλές δυνατότητες και ικανότητες. Για παράδειγμα ακόμα και αν χάσει την ασύρματη σύνδεση για κάποιο χρονικό διάστημα λόγω κάποιου εξωτερικού παράγοντα, μπορεί να την ανακτήσει άμεσα όταν αυτή επανέλθει και να συνεχίσει την ανάγνωση των πακέτων που λαμβάνει.

Μπορεί να αποθηκεύσει τα δεδομένα που μαζεύει σε ειδικά αρχεία τα οποία αναγνωρίζονται και από άλλα προγράμματα στη συνέχεια. Το Kismet είναι απόλυτα συμβατό με το Wireshark (όπως φαίνεται από το screenshot στην εικόνα 3.14) για την ανάλυση των δεδομένων όπως και με το Tcpdump που αναφέρθηκε σε αυτό το κεφάλαιο.

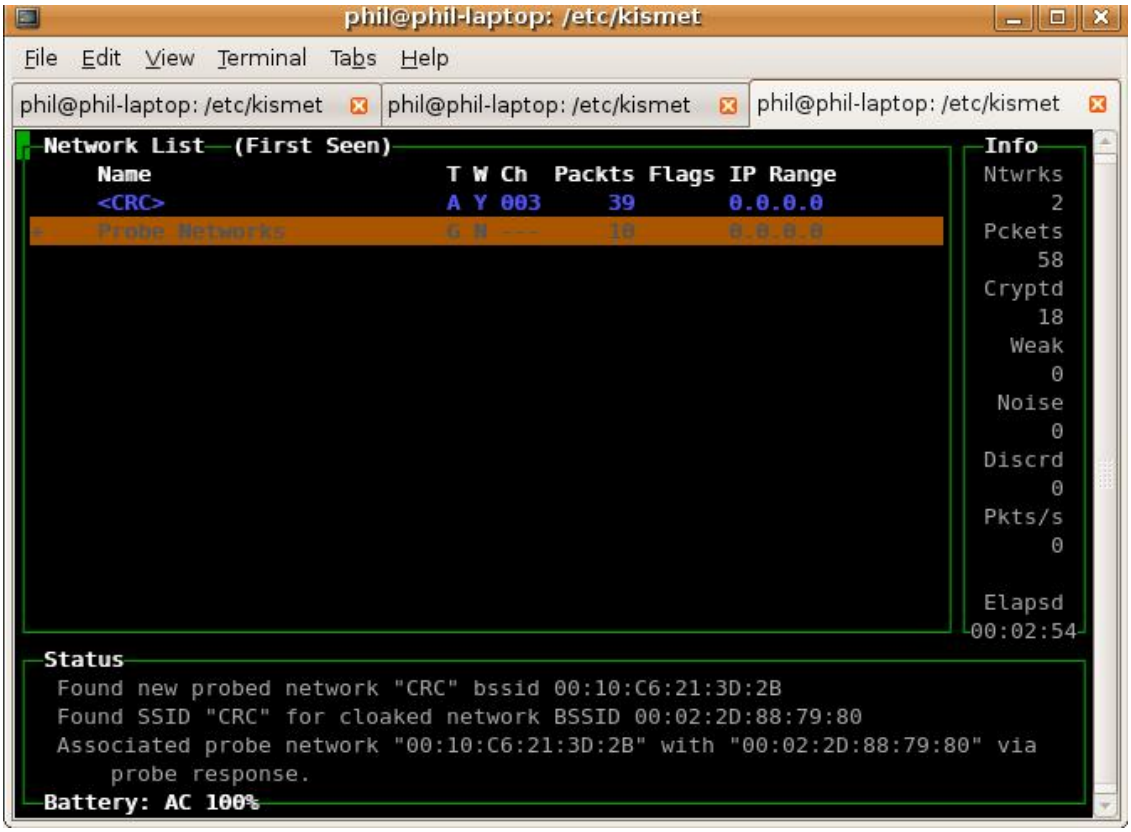


Εικόνα 3.14: Συμβατότητα του Kismet με το Wireshark

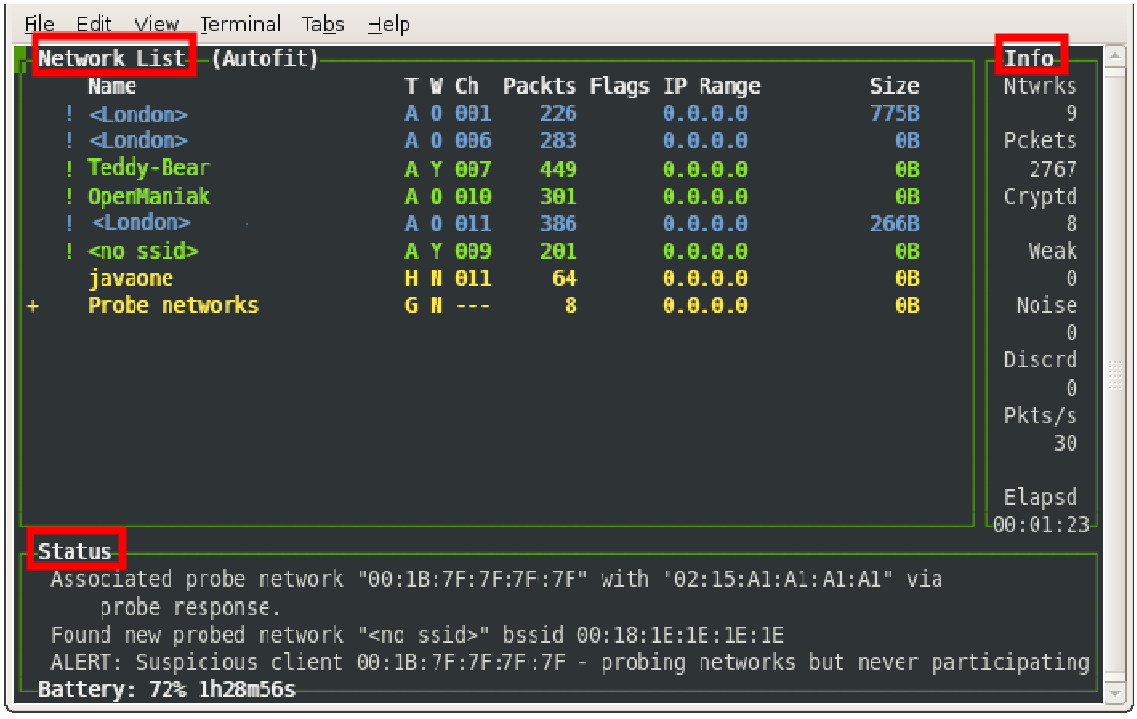
Το Kismet είναι αυτόνομο όσον αφορά τα περιεχόμενα του, όμως σε κάποιες περιπτώσεις απαιτούνται κάποιες συγκεκριμένες εφαρμογές που υποβοηθούν το πρόγραμμα. Για παράδειγμα μία από αυτές είναι το LibPcap (σε έκδοση 0.9 ή μεταγενέστερη) το οποίο είναι απαραίτητο και για πολλά άλλα προγράμματα Σύλληψης Πακέτων. Χωρίς αυτό το Kismet θα ήταν ουσιαστικά άχρηστο. [30]

Το περιβάλλον του προγράμματος φαίνεται στις εικόνες 3.15 και 3.16.

[30] "Kismet Readme Manual" από τον Mike Kershaw 2010 (http://www.kismetwireless.net/documentation.shtml)



Εικόνα 3.15: Περιβάλλον του Kismet



Εικόνα 3.16: Περιβάλλον του Kismet

3.5 Microsoft Network Monitor

Ένας πιο εύκολος και άμεσος τρόπος να γίνει καταγραφή της κίνησης αλλά και εποπτεία του δικτύου είναι με το εργαλείο των Windows, το “Microsoft Network Monitor”. [31] Η Εποπτεία δικτύου (Network Monitor) είναι ένα διαγνωστικό εργαλείο δικτύου το οποίο παρακολουθεί τα τοπικά δίκτυα και παρέχει γραφική παρουσίαση των στατιστικών του δικτύου. Οι διαχειριστές δικτύων μπορούν να χρησιμοποιούν αυτές τις στατιστικές για την εκτέλεση συνηθισμένων εργασιών αντιμετώπισης προβλημάτων, όπως είναι ο εντοπισμός ενός διακομιστή που βρίσκεται εκτός λειτουργίας ή που λαμβάνει δυσανάλογο αριθμό αιτήσεων εργασίας. Κατά τη συγκέντρωση πληροφοριών από τη ροή δεδομένων δικτύου, η Εποπτεία δικτύου εμφανίζει τους ακόλουθους τύπους πληροφοριών:

- Τη διεύθυνση προέλευσης του υπολογιστή ο οποίος έστειλε ένα πλαίσιο στο δίκτυο. (Η διεύθυνση αυτή αποτελείται από έναν μοναδικό δεκαεξαδικό (ή base-16) αριθμό ο οποίος προσδιορίζει το συγκεκριμένο υπολογιστή στο δίκτυο.)
- Τη διεύθυνση προορισμού του υπολογιστή που έλαβε το πλαίσιο.
- Τα πρωτόκολλα που χρησιμοποιήθηκαν για την αποστολή του πλαισίου.
- Τα δεδομένα ή ένα μέρος του μηνύματος που στάλθηκε.

Η διαδικασία με την οποία η Εποπτεία δικτύου συγκεντρώνει αυτές τις πληροφορίες ονομάζεται "καταγραφή" (capturing). Από προεπιλογή, η Εποπτεία δικτύου εξάγει δεδομένα και παρατηρήσεις από όλα τα πλαίσια που ανιχνεύει στο δίκτυο σε ένα buffer καταγραφής, το οποίο είναι ένας δεσμευμένος χώρος αποθήκευσης στη μνήμη. Για την καταγραφή στατιστικών μόνο σε ένα συγκεκριμένο υποσύνολο πλαισίων, μπορούμε να απομονώσουμε αυτά τα πλαίσια σχεδιάζοντας ένα φίλτρο

[31] “Κεντρική σελίδα Υποστήριξης Microsoft” (http://support.microsoft.com/kb/148942/el)

καταγραφής. Αφού τελειώσουμε με την καταγραφή των πληροφοριών, μπορούμε να σχεδιάσουμε ένα φίλτρο εμφάνισης για να καθορίσουμε το πλήθος των πληροφοριών που θα εμφανίζονται στο παράθυρο "Πρόγραμμα προβολής πλαισίου" (Frame Viewer) της Εποπτείας δικτύου, από αυτές που έχουν καταγραφεί.

Για να χρησιμοποιήσουμε την Εποπτεία δικτύου (Network Monitor), ο υπολογιστής μας πρέπει να διαθέτει μια κάρτα δικτύου που να υποστηρίζει ετερόκλητη λειτουργία.[32] Εάν χρησιμοποιούμε την Εποπτεία δικτύου σε έναν απομακρυσμένο υπολογιστή, ο τοπικός σταθμός εργασίας δεν χρειάζεται κάρτα δικτύου που να υποστηρίζει ετερόκλητη λειτουργία, ο απομακρυσμένος υπολογιστής όμως την χρειάζεται.

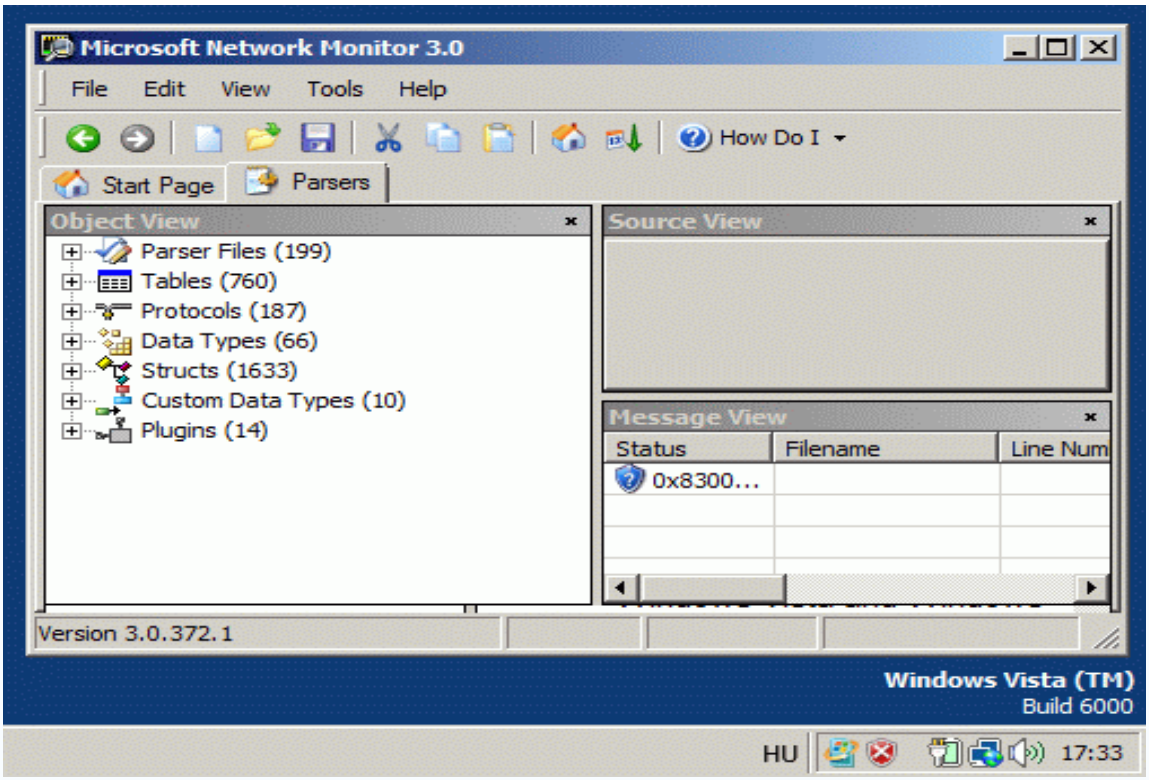
Αφού γίνει καταγραφή των δεδομένων είτε από τοπικό είτε από απομακρυσμένο υπολογιστή, τα δεδομένα μπορούν να αποθηκευτούν σε ένα αρχείο κειμένου ή καταγραφής και να τα ανοίξουμε και να τα εξετάσουμε αργότερα.

Σημείωση:

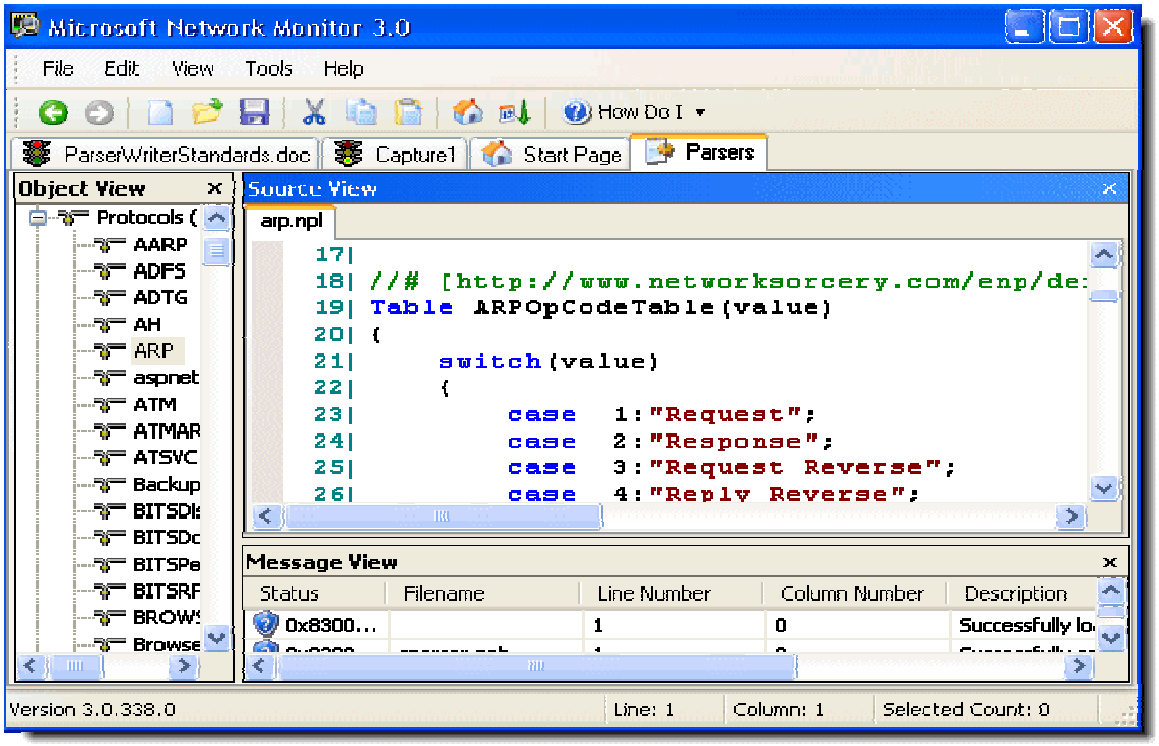
Η βασική λειτουργικότητα της Εποπτείας δικτύου, υποστηρίζεται από τις Υπηρεσίες Τεχνικής Υποστήριξης της Microsoft (Microsoft Product Support Services). Οι εργασίες που βασίζονται σε δίκτυο, όπως η ερμηνεία δεδομένων που έχουν καταγραφεί από το δίκτυό μας, δεν υποστηρίζονται. Ο Παράγοντας Εποπτείας δικτύου υποστηρίζεται από τα Windows NT, δεν υποστηρίζεται όμως από σταθμούς εργασίας Windows 3.1 και Windows for Workgroups.

Οι εικόνες 3.17 και 3.18 δείχνουν το περιβάλλον εργασίας του Microsoft Network Monitor.

[32] "Ετερόκλητη Λειτουργία" (http://en.wikipedia.org/wiki/Promiscuous_mode)



Εικόνα 3.17: περιβάλλον εργασίας του Microsoft Network Monitor.



Εικόνα 3.18: περιβάλλον εργασίας του Microsoft Network Monitor.

3.6 Wireshark: Network Protocol Analyzer

Το Wireshark είναι το καλύτερο ‘open-source’ λογισμικό ανάλυσης δικτύων που είναι διαθέσιμο αυτή τη στιγμή. Συσκευάζεται με αρκετά χαρακτηριστικά γνωρίσματα συγκρίσιμα με τα περισσότερα εμπορικά λογισμικά ανάλυσης δικτύων (κάποια από τα οποία αναφέραμε προηγουμένως).

Το Wireshark είναι ένα σταθερό και χρήσιμο συστατικό για όλα τα δίκτυα, και για το οποίο νέα χαρακτηριστικά γνωρίσματα αναπτύσσονται συνεχώς. Πολλή πρόοδος έχει σημειωθεί από την αρχή των ημερών του Wireshark (όταν ονομαζόταν ακόμα ethereal) και η εφαρμογή αποδίδει τώρα ανάλογα ή και καλύτερα από αρχικά πιο γνωστά λογισμικά.

Σε αυτό το κεφάλαιο θα μάθουμε λίγα για την ιστορία του Wireshark, πώς κατέληξε να είναι μια τόσο δημοφιλής συσκευή ανάλυσης δικτύων, και γιατί παραμένει μια κορυφαία επιλογή για τη διοίκηση συστημάτων και ασφάλειας. Θα προσπαθήσουμε να αντιληφθούμε καλύτερα αυτό που είναι το Wireshark, ποια είναι τα κύρια χαρακτηριστικά γνωρίσματά του, και πώς μπορούμε να το χρησιμοποιήσουμε στην αρχιτεκτονική του δικτύου μας.

3.6.1 Η Ιστορία του Wireshark

Ο Gerald Combs πρώτος ανέπτυξε το Ethereal το 1997, επειδή προσπαθούσε να επεκτείνει τις γνώσεις του σχετικά με τη δικτύωση και χρειαζόταν ένα εργαλείο για την ανίχνευση λαθών και την αντιμετώπιση προβλημάτων στα δίκτύα. Η πρώτη έκδοση (v0.2.0) βγήκε τον Ιούλιο του 1998. Μια ομάδα ανάπτυξης, στην οποία ήταν και οι: Gilbert Ramirez, Guy Harris, και Richard Sharpe, στη συνέχεια δούλεψαν με στόχο διορθώσεις (patches) και τον εμπλουτισμό του προγράμματος (enhancements). Όπως επίσης και ‘’Dissectors’’ που είναι αυτά που επιτρέπουν στο Wireshark να αποκωδικοποιήσει τα μεμονωμένα πρωτόκολλα και να τα παρουσιάσει με έναν εύκολα αναγνώσιμο τρόπο-μορφή.

Από τότε, ένας μεγάλος αριθμός ατόμων έχει συμβάλει στη δημιουργία συγκεκριμένων dissectors πρωτοκόλλου και σε άλλες αυξήσεις και βελτιώσεις στο Wireshark. [33]

[33] “Λίστα συγγραφέων Wireshark” (www.wireshark.org/about.html#authors)

Λόγω της συντριπτικής ανάπτυξης υποστήριξης και της μεγάλης βάσης χρηστών, οι ικανότητες του Wireshark και η δημοτικότητα του συνεχίζουν να αυξάνονται κάθε ημέρα.

3.6.2 Τι είναι το Wireshark

Το Wireshark είναι ένα λογισμικό ανάλυσης δικτύων. Διαβάζει τα πακέτα από το δίκτυο, τα αποκωδικοποιεί, και τα παρουσιάζει με έναν πιο εύκολο τρόπο σε εμάς. Μερικές από τις σημαντικότερες πτυχές του Wireshark είναι ότι είναι open source, ελεύθερα διαθέσιμο, και δωρεάν. Οι ακόλουθες είναι μερικές από τις άλλες σημαντικές πτυχές του Wireshark:

■ Λειτουργεί με ανοιχτό (promiscuous) και μη ανοιχτό (non-promiscuous) mode.
■ Μπορεί να συλλάβει τα στοιχεία από το δίκτυο ή να διαβάσει από ένα αρχείο αποθηκευμένο.
■ Έχει εύκολο εγχειρίδιο.
■ Έχει πλούσιες ικανότητες φιλτραρίσματος.
■ Υποστηρίζει τη μορφή αρχείων του tcpdump. Έχει ένα χαρακτηριστικό γνώρισμα που αναδημιουργεί ένα αρχείο TCP σε αρχείο του κώδικα ASCII,.
■ Τρέχει σε πάνω από 20 πλατφόρμες, συμπεριλαμβανομένων των «Uniplexed Information and Computing System» (UNIX) σε συστήματα OS, και στα Windows, και υπάρχει και διαθέσιμο για Mac OS X.
■ Υποστηρίζει πάνω από 750 πρωτόκολλα, και, επειδή είναι open source, νέα συστήματα προστίθενται συνέχεια.
■ Μπορεί να διαβάσει αρχεία που έχουν συλληφθεί από πάνω από 25 διαφορετικά προϊόντα.
■ Μπορεί να σώσει τα αρχεία σύλληψης με ποικίλα σχήματα (e.g., libpcap, Network Associates Sniffer, Microsoft Network Monitor (NetMon), και Sun snoop).
■ Μπορεί να συλλάβει τα στοιχεία από ποικίλα μέσα (e.g., Ethernet,Token-Ring, 802.11 Wireless).
■ Περιλαμβάνει μία έκδοση ‘εντολή-γραμμή’ από τη συσκευή ανάλυσης δικτύων η οποία λέγεται *tshark*.

■ Περιλαμβάνει ποικίλα ενισχυτικά προγράμματα όπως τα: *editcap*, *mergecap*, και *text2pcap*.

■ Το αποτέλεσμα μπορεί να σωθεί ή να τυπωθεί σαν plaintext ή PostScript.

3.6.3 Συμβατότητα

Όπως προαναφέρθηκε, το Wireshark μπορεί να διαβάσει και να επεξεργαστεί τα αρχεία σύλληψης από αρκετά διαφορετικά προϊόντα, συμπεριλαμβανομένων άλλων sniffers, routers, και network utilities. Επειδή το Wireshark χρησιμοποιεί το δημοφιλή Promiscuous Capture Library (libpcap)-based capture format, διασυνδέεται εύκολα με άλλα προϊόντα που χρησιμοποιούν libpcap. Έχει επίσης τη δυνατότητα να διαβάσει τις συλλήψεις με ποικίλα άλλα σχήματα (formats). Με το Wireshark μπορείτε αυτόματα να καθορίσετε τον τύπο αρχείου που διαβάζετε και μπορείτε να αποσυμπιέσετε GNU Zip (gzip) files. Ο ακόλουθος κατάλογος παρουσιάζει τα προϊόντα από τα οποία το Wireshark μπορεί να διαβάσει αρχεία σύλληψης:

■ Tcpdump
■ Sun snoop και atmsnoop
■ Microsoft NetMon
■ Network Associates Sniffer (compressed or uncompressed) και Sniffer Pro
■ Shomiti/Finisar Surveyor
■ Novell LANalyzer
■ Cinco Networks NetXRay
■ AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek
■ RADCOM’s wide area network (WAN)/local area network (LAN) analyzer
■ Visual Networks’ Visual UpTime
■ Lucent/Ascend router debug output
■ Toshiba’s Integrated Services Digital Network (ISDN) routers dump output
■ Cisco Secure intrusion detection systems (IDS) iplog
■ AIX’s iptrace
■ HP-UX nettl
■ ISDN4BSD project’s i4btrace output
■ Point-To-point Protocol Daemon (PPPD) logs (pppdump-format)
■ VMS’s TCPIPtrace utility

■ DBS Etherwatch Virtual Memory System (VMS) utility
■ CoSine L2 debug
■ Accellent's 5Views LAN agent output
■ Endace Measurement Systems' Electronic Remote Fill (ERF) capture format
■ Linux Bluez Bluetooth stack "hcidump –w" traces
■ Catapult DCT2000
■ Network Instruments Observer version 9
■ EyeSDN Universal Serial Bus (USB) S0 traces

3.6.4 Υποστηριζόμενα πρωτόκολλα

Όταν μια συσκευή ανάλυσης δικτύων διαβάζει τα στοιχεία από το δίκτυο πρέπει να ξέρει πώς να ερμηνεύσει αυτό που βλέπει και έπειτα να παρουσιάσει το αποτέλεσμα με έναν εύκολα αναγνώσιμο τρόπο. Αυτό είναι γνωστό ως: Αποκωδικοποίηση πρωτοκόλλου (protocol decoding). Συχνά, ο αριθμός πρωτοκόλλων που ένα sniffer μπορεί να διαβάσει και να παρουσιάσει καθορίζει τη δύναμή του, κατά συνέπεια τα περισσότερα εμπορικά sniffers μπορούν να υποστηρίξουν αρκετές εκατοντάδες πρωτόκολλα. Το Wireshark είναι πολύ ανταγωνιστικό σε αυτήν την διαδικασία, με την τρέχουσα υποστήριξή του που περιλαμβάνει πάνω από 750 πρωτόκολλα,[34] ενώ συνεχώς νέα πρωτόκολλα προστίθενται από διάφορους συνεισφέροντες στο πρόγραμμα Wireshark. Το πρωτόκολλο αποκωδικοποιεί επίσης τα γνωστά και ως dissectors, τα οποία μπορούν να προστίθενται άμεσα στον κώδικα ή να συμπεριλαμβάνονται ως plug-ins.

[34] "Λίστα με τα 752 πρωτόκολλα που υποστηρίζονται" (Online Wireshark User's Manual, www.syngress.com)

3.6.5 Διεπαφή χρήστη του Wireshark (Wireshark's User Interface)

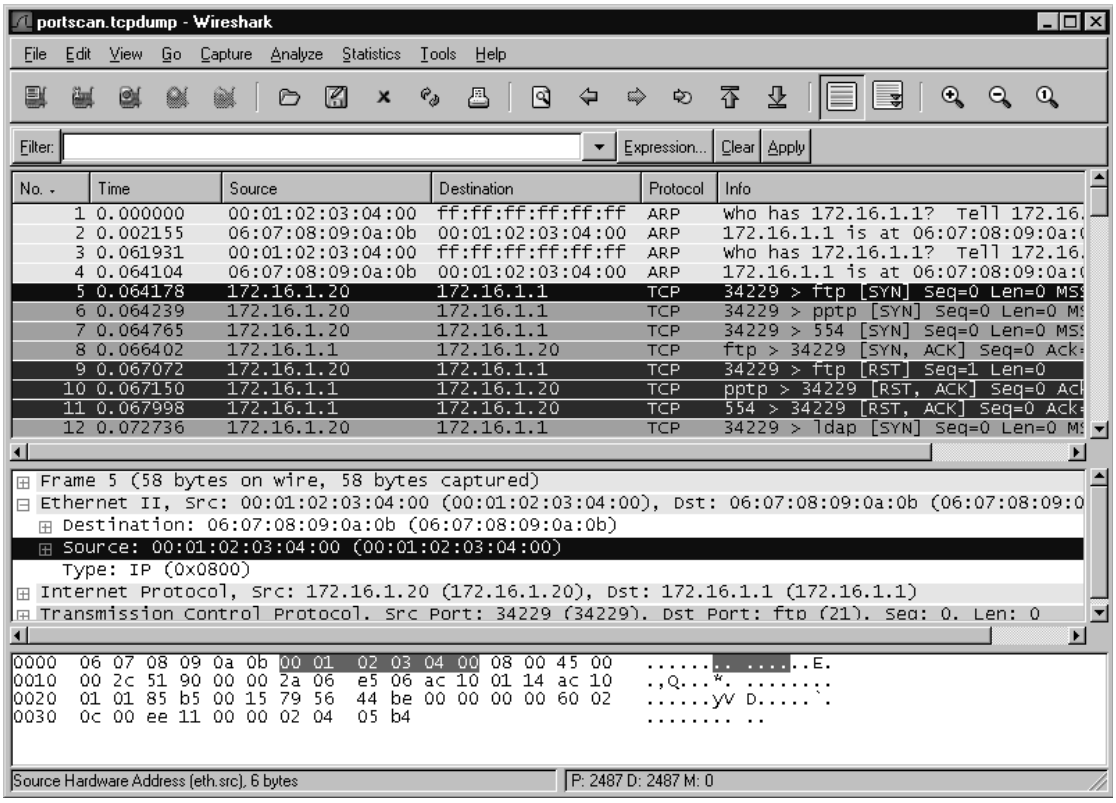
Το περιβάλλον του Wireshark είναι διαμορφώσιμο και εύχρηστο. Και όπως άλλες συσκευές ανάλυσης δικτύων, το Wireshark συλλαμβάνει τις πληροφορίες σε τρία κύρια παράθυρα (panes).

Η Εικόνα 3.19 παρουσιάζει μία σύλληψη από το Wireshark.
Κάθε παράθυρο είναι διαμορφώσιμο σε μέγεθος πατώντας τη σειρά μεταξύ των μικρότερων παραθύρων και σέρνοντας πάνω η κάτω. Το ανώτερο παράθυρο είναι το παράθυρο περίληψης, το οποίο δείχνει μία περίληψη της σύλληψης σε μία γραμμή.

Οι βασικοί τομείς του Wireshark είναι οι εξής:

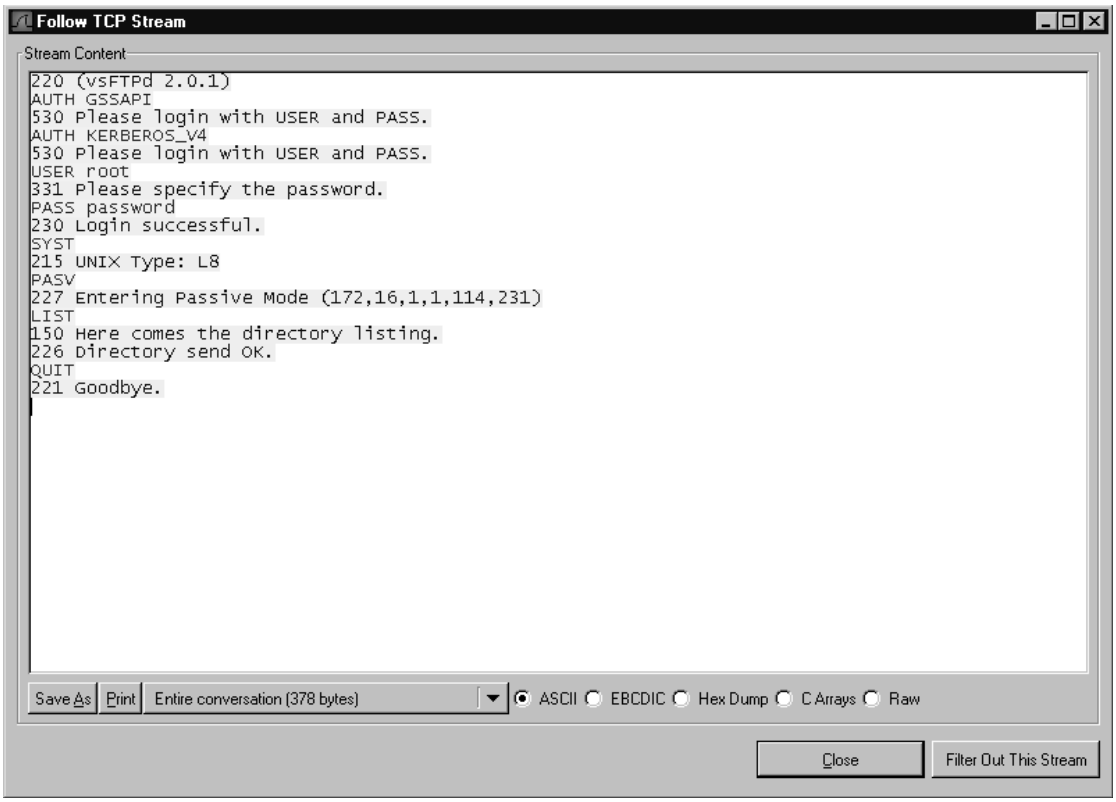
- Αριθμός Πακέτου (Packet number)
- Χρόνος (Time)
- Διεύθυνση Πηγής (Source address)
- Διεύθυνση Προορισμού (Destination address)
- Όνομα Πρωτοκόλλου και διάφορες πληροφορίες.

Αυτές οι στήλες διαμορφώνονται εύκολα, και νέες μπορούν να προστεθούν από την επιλογή Διαμόρφωση. Μπορείτε επίσης να ταξινομήσετε τις στήλες με μια ανιούσα ή κατιούσα σειρά κατά τομέα, και μπορείτε να ρυθμίσετε εκ νέου τα παράθυρα.
Το μεσαίο παράθυρο είναι το παράθυρο που μας δίνει τις λεπτομέρειες του πρωτοκόλλου (protocol detail pane),το οποίο παρέχει τις λεπτομέρειες (σε μια μορφή δέντρου) από κάθε «στρώμα» που περιλαμβάνεται στο πακέτο που έχει συλληφθεί. Πατώντας στα διάφορα μέρη του δέντρου φαίνεται αντίστοιχα σε δεκαεξαδικό σύστημα (hex) αλλά και σε κώδικα ASCII στο κατώτατο παράθυρο.
Η Εικόνα 3.19 παρουσιάζει το περιβάλλον του Wireshark και ένα παράδειγμα σύλληψης πακέτων. Παρατηρούμε ότι τονίζοντας τη διεύθυνση MAC της πηγής στο μέσο πλακάκι εμφάνισης πρωτοκόλλου αυτομάτως τονίζεται το κομμάτι του δεκαεξαδικού κώδικα στο χαμηλότερο παράθυρο.



Εικόνα 3.19 Περιβάλλον του Wireshark

Ένα από τα καλύτερα χαρακτηριστικά γνωρίσματα του Wireshark είναι η δυνατότητά του να ξανασυγκεντρώνει όλα τα πακέτα από μία TCP συνομιλία και να παρουσιάζει τον κώδικα ASCII σε μία πιο εύκολα αναγνώσιμη μορφή. Αυτό το στοιχείο μπορεί έπειτα να σωθεί ή να τυπωθεί, και να χρησιμοποιηθεί παραδείγματος χάριν για να αναδημιουργήσει μία ιστοσελίδα, Simple Mail Transfer Protocol (SMTP) ή Telnet συνομιλία. Για να αναδημιουργήσουμε μία ιστοσελίδα, ακολουθούμε το ρεύμα (stream) Hypertext Transfer Protocol (HTTP) session και σώζουμε την παραγωγή σε ένα αρχείο. Πρέπει έπειτα να είμαστε σε θέση να τη δούμε αναδημιουργημένη στη γλώσσα HTML (Hypertext Markup Language) δουλεύοντας εκτός σύνδεσης σε έναν φυλλομετρητή Ιστού (Web Browser).



Εικόνα 3.20: Παραγωγή ενός TCP σε FTP.

3.6.6 Φίλτρα

Φιλτράροντας πακέτα μας βοηθά να βρούμε ένα επιθυμητό πακέτο χωρίς να χρειάζεται να ψάξουμε όλα τα υπόλοιπα. Το Wireshark έχει τη δυνατότητα να χρησιμοποιήσει και τα φίλτρα σύλληψης και εμφάνισης (capture and display filters). Η σύνταξη των φίλτρων σύλληψης ακολουθεί την ίδια σύνταξη την οποία το tcpdump χρησιμοποιεί από τη βιβλιοθήκη libpcap. Χρησιμοποιείται στη γραμμή εντολής ή στο πλαίσιο διαλόγου "φίλτρων σύλληψης" για να συλλάβουμε συγκεκριμένους τύπους «κυκλοφορίας».

Ο παρακάτω Πίνακας 5 παρουσιάζει ένα παράδειγμα υποστηριζόμενων πρωτοκόλλων και των φίλτρων επίδειξής τους:

Internet Protocol (IP) Field	Name	Type
ip.addr	Source or Destination Address	IPv4 address
ip.checksum	Header checksum	Unsigned 16-bit integer
ip.checksum_bad	Bad Header checksum	Boolean
ip.dsfield	Differentiated Services field	Unsigned 8-bit integer
ip.dsfield.ce	ECN-CE, Explicit Congestion Notification: Congestion Experienced	Unsigned 8-bit integer
ip.dsfield.dscp	Differentiated 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.overlap.conflict	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_in	Reassembled IP in frame	Frame number
ip.src	Source	IPv4 address
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

Πίνακας 5: Υποστηριζόμενα πρωτόκολλα και τα φίλτρα επίδειξής τους

3.6.7 Ενισχυτικά προγράμματα

Οι περισσότεροι άνθρωποι που είναι εξοικειωμένοι με το Wireshark χρησιμοποιούν τον «Οδηγό» του Wireshark. Εντούτοις, όταν εγκαθίσταται το Wireshark, έρχεται επίσης με διάφορα άλλα προγράμματα υποστήριξης. Η «έκδοση γραμμών - εντολών» του Wireshark (το tshark) περιέχει τα ακόλουθα τρία προγράμματα για να βοηθήσει στη σωστότερη διαδικασία σύλληψης των αρχείων.

Tshark

Το Tshark είναι η έκδοση «γραμμών- εντολών» του Wireshark, το οποίο μπορεί να χρησιμοποιηθεί για να συλλάβει ζωντανά πακέτα από τη σύνδεση ή να διαβάσει αποθηκευμένα αρχεία. Από προεπιλογή, το tshark εμφανίζει τις συνοπτικές πληροφορίες στην οθόνη. Αυτές είναι οι ίδιες πληροφορίες που περιλαμβάνονται στο επάνω παράθυρο του Wireshark. [35]

1.199008 192.168.100.132 -> 192.168.100.122 TCP 1320 > telnet [SYN]
Seq=1102938967 Ack=0 Win=16384 Len=0
1.199246 192.168.100.132 -> 192.168.100.122 TCP 1320 > telnet [SYN]
Seq=1102938967 Ack=0 Win=16384 Len=0
1.202244 192.168.100.122 -> 192.168.100.132 TCP telnet > 1320 [SYN
ACK] Seq=3275138168 Ack=1102938968 Win=49640 Len=0
1.202268 192.168.100.132 -> 192.168.100.122 TCP 1320 > telnet [ACK]
Seq=1102938968 Ack=3275138169 Win=17520 Len=0
1.202349 192.168.100.132 -> 192.168.100.122 TCP 1320 > telnet [ACK]
Seq=1102938968 Ack=3275138169 Win=17520 Len=0

Κατά τη χρησιμοποίηση tshark για να σώσουμε τα στοιχεία πακέτων σε ένα αρχείο, αυτό από προεπιλογή παρουσιάζει τα αποτελέσματα σε libpcap μορφή. Το Tshark μπορεί να διαβάσει με τον ίδιο τρόπο που συλλαμβάνει τα αρχεία και χρησιμοποιεί τα ίδια φίλτρα επίδειξης (also known as *read* filters) και τα φίλτρα σύλληψης το

[35] Online Wireshark User's Manual, www.syngress.com (σελ. 66)

Wireshark. Το Tshark μπορεί επίσης να αποκωδικοποιήσει τα ίδια πρωτόκολλα με το Wireshark. Βασικά, έχει τις περισσότερες από τις δυνατότητες του Wireshark σε μια πιο εύχρηστη έκδοση.

Editcap

Το Editcap χρησιμοποιείται για να αφαιρέσει πακέτα από ένα αρχείο, και για να μεταφράσει τη μορφή των συλληφθέντων αρχείων. Είναι παρόμοιο με την επιλογή «Save As», αλλά αρκετά καλύτερη. Το Editcap μπορεί να διαβάσει όλους τους ίδιους τύπους αρχείων που το Wireshark μπορεί, και τα καταγράφει σε αρχεία της μορφής του libpcap από προεπιλογή. Το Editcap μπορεί επίσης να καταγράψει τα συλληφθέντα αρχεία στις τυποποιημένες και τροποποιημένες εκδόσεις των παρακάτω:

- libpcap
- Sun snoop
- Novel LANalyzer
- Network Access Identifier (NAI) Sniffer
- Microsoft NetMon
- Visual Network traffic capture
- Accellent 5Views capture
- Network Instruments Observer version 9

Το Editcap έχει τη δυνατότητα να διαχωρίσει με βάση κάποια στοιχεία όλα ή μερικά από τα πακέτα που μεταφράζει.

Το παρακάτω είναι ένα παράδειγμα editcap για να μεταφράσουμε τα πρώτα πέντε πακέτα από ένα αρχείο σύλληψης tshark libpcap (αποκαλούμενο σύλληψη) σε ένα αρχείο snoop (ή snoop capture): [36]

C:\Program Files\Wireshark>editcap -r -v -F snoop capture capture_snoop 1-5
File capture is a libpcap (tcpdump Wireshark etc.) capture file.

[36] Online Wireshark User's Manual, www.syngress.com (σελ. 69)

Add_Selected: 1-5
Inclusive ... 1
5
Record: 1
Record: 2
Record: 3
Record: 4
Record: 5

Mergecap

Το Mergecap χρησιμοποιείται για να συνδυάσει πολλά αποθηκευμένα αρχεία σε ένα ενιαίο αρχείο παραγωγής. Το Mergecap μπορεί να διαβάσει όλους τους ίδιους τύπους αρχείων με το Wireshark και τα καταγράφει σε αρχεία μορφής libpcap από προεπιλογή. Το Mergecap μπορεί επίσης να γράψει ότι η παραγωγή συλλαμβάνει στις τυποποιημένες και τροποποιημένες εκδόσεις των παρακάτω:

- libpcap
- Sun snoop
- Novel LANalyzer
- NAI Sniffer
- Microsoft NetMon
- Visual Network traffic capture
- Accellent 5Views capture
- Network Instruments Observer

Από προεπιλογή, τα πακέτα από τα αρχεία εισαγωγής συγχωνεύονται κατά χρονολογική σειρά, με βάση τη «χρονική ταυτότητα»(timestamp) κάθε πακέτου. Εάν η επιλογή διευκρινίζεται, τα πακέτα αντιγράφονται άμεσα από κάθε αρχείο εισαγωγής στο αρχείο παραγωγής ανεξάρτητα από την «χρονική ταυτότητα».

Το ακόλουθο είναι ένα παράδειγμα mergecap για να συγχωνεύσετε τέσσερα αρχεία (capture1, capture2, capture3, and capture4) σε έναν ενιαίο Sun snoop αρχείο

παραγωγής αποκαλούμενο merge_snoop που θα συνεχίσει να διαβάζει τα πακέτα μέχρι και το τέλος του τελευταίου αρχείου: [37]

C:\Program Files\Wireshark>mergecap -v -F snoop -w merge_snoop capture1 capture2 capture3 capture4

3.6.8 Χρησιμοποιώντας το Wireshark μέσα στην δικτυακή αρχιτεκτονική μας

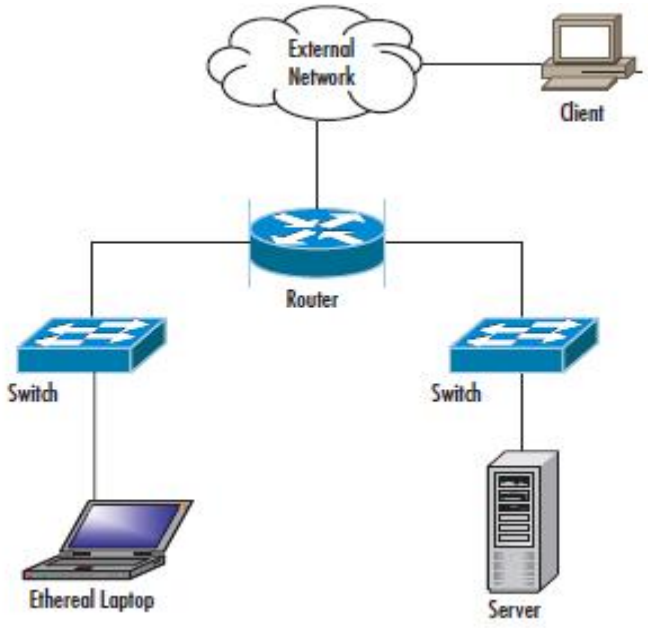
Αυτό το τμήμα εξετάζει μερικά στοιχεία από την αρχιτεκτονική του δικτύου και κάποια κρίσιμα σημεία του Wireshark.

Η τοποθέτηση δικτύων είναι κρίσιμη για κατάλληλη ανάλυση και ανίχνευση λαθών. Επιπλέον, πρέπει να είναι σίγουρο ότι βρισκόμαστε στο κατάλληλο τμήμα δικτύων. Όταν ανιχνεύουμε και επιλύουμε λάθη και προβλήματα των δικτύων, μπορούμε να κινηθούμε μεταξύ των διάφορων θέσεων καλωδίωσης ή ακόμα και ανάμεσα σε διαφορετικά κτήρια!

Για αυτόν τον λόγο, είναι ευεργετικό ή αν προτιμάτε πιο εύκολο να εκτελείται το Wireshark σε ένα lap-top. Είναι επίσης καλή ιδέα να υπάρχει ένα hub και μερικά καλώδια δικτύων (crossover and straight-through) με το φορητό μας Η/Υ για να έχουμε ένα πλήρες πακέτο εργαλείων ανίχνευσης λαθών.

[37] Online Wireshark User's Manual, www.syngress.com (σελ. 70)

Η Εικόνα 3.21 παρουσιάζει τη λανθασμένη τοποθέτηση του Wireshark εάν θελήσουμε να συλλάβουμε την επικοινωνία μεταξύ του εξωτερικού πελάτη και του κεντρικού υπολογιστή (server). Ο φορητός Η/Υ με το Wireshark και ο διακόπτης (switcher) που συνδέεται με αυτό δεν θα δουν την κυκλοφορία που προορίζεται για τον κεντρικό υπολογιστή επειδή καθοδηγείται στο διακόπτης του κεντρικού υπολογιστή.

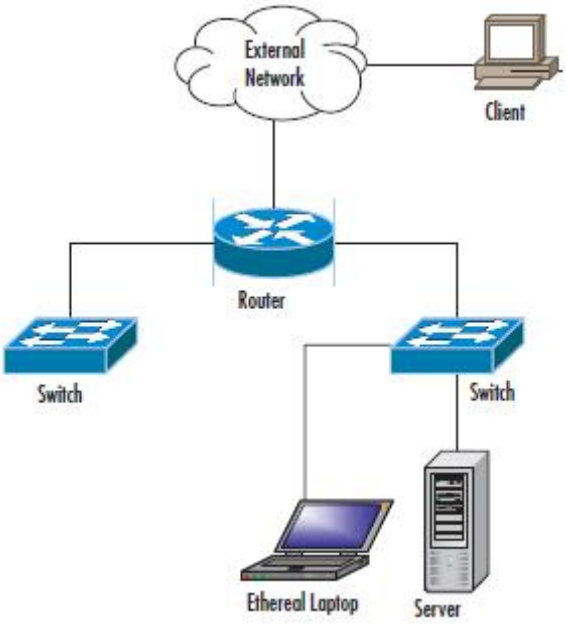


Εικόνα 3.21: Λανθασμένη Τοποθέτηση του Wireshark

Η Εικόνα 3.22 επιδεικνύει πώς να συλλάβουμε την κυκλοφορία από τον εξωτερικό πελάτη στον κεντρικό υπολογιστή με τη χρησιμοποίηση της ανίχνευσης θυρών (port spanning). Ο φορητό Η/Υ πρέπει να συνδεθεί με τον ίδιο μεταγωγέα στον οποίο είναι συνδεδεμένος ο κεντρικός υπολογιστής.

Στη συνέχεια, το port spanning ενεργοποιείται για να αντανακλά όλη την κυκλοφορία από τη θύρα του κεντρικού υπολογιστή στη θύρα που το Wireshark είναι συνδεμένο.

Η χρήση αυτής της μεθόδου δεν θα προκαλέσει οποιαδήποτε διακοπή της κυκλοφορίας προς και από τον κεντρικό υπολογιστή.

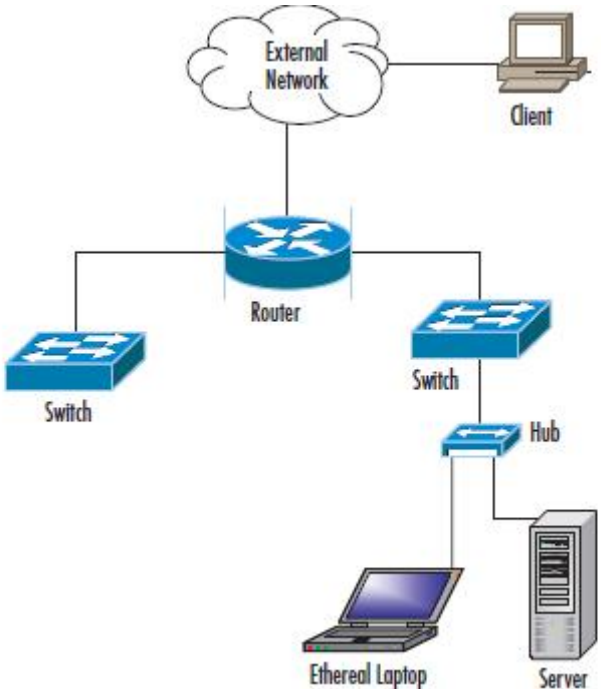


Εικόνα 3.22: Σωστή τοποθέτηση του Wireshark

Η Εικόνα 3.23 επιδεικνύει πώς να συλλάβουμε την κυκλοφορία από τον εξωτερικό πελάτη στον κεντρικό υπολογιστή χρησιμοποιώντας ένα hub. Εάν εγκαταστήσουμε ένα hub μεταξύ του κεντρικού υπολογιστή και του μεταγωγέα και συνδέσουμε το φορητό μας Η/Υ σε αυτήν.

Το Wireshark θα δει έπειτα όλη την κυκλοφορία προς και από τον κεντρικό υπολογιστή.

Αυτή η μέθοδος θα παρεμποδίσει προσωρινά την κυκλοφορία.

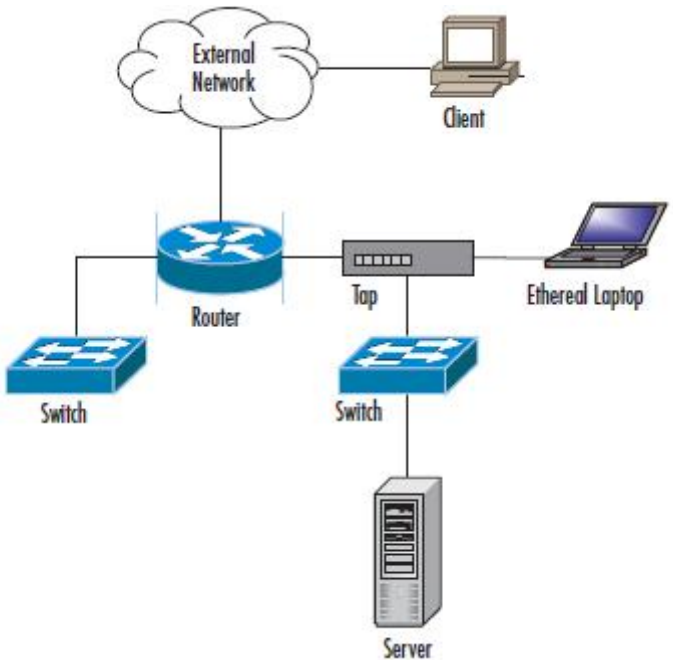


Εικόνα 3.23: Σωστή τοποθέτηση Wireshark χρησιμοποιώντας Hub

Η Εικόνα 3.24 παρουσιάζει τη δικτυακή αρχιτεκτονική που χρησιμοποιεί μια μόνιμη Tap που εγκαθίσταται στον δρομολογητή. Μερικοί διαχειριστές χρησιμοποιούν αυτήν την μέθοδο για ένα μόνιμο σημείο σύνδεσης στις κρίσιμες περιοχές.

Ο φορητός Η/Υ βλέπει έπειτα όλη την κυκλοφορία προς και από τον κεντρικό υπολογιστή συν οποιαδήποτε άλλη κυκλοφορία στο τμήμα. Η χρησιμοποίηση αυτής της μεθόδου δεν παρεμποδίζει την κυκλοφορία προς και από τον κεντρικό υπολογιστή εάν το tap εγκαθίσταται μόνιμα και τα καλώδια είναι ήδη συνδεδεμένα.

Τα taps μπορούν επίσης να είναι φορητά και να χρησιμοποιούνται όπως το hub στην εικόνα 3.24.

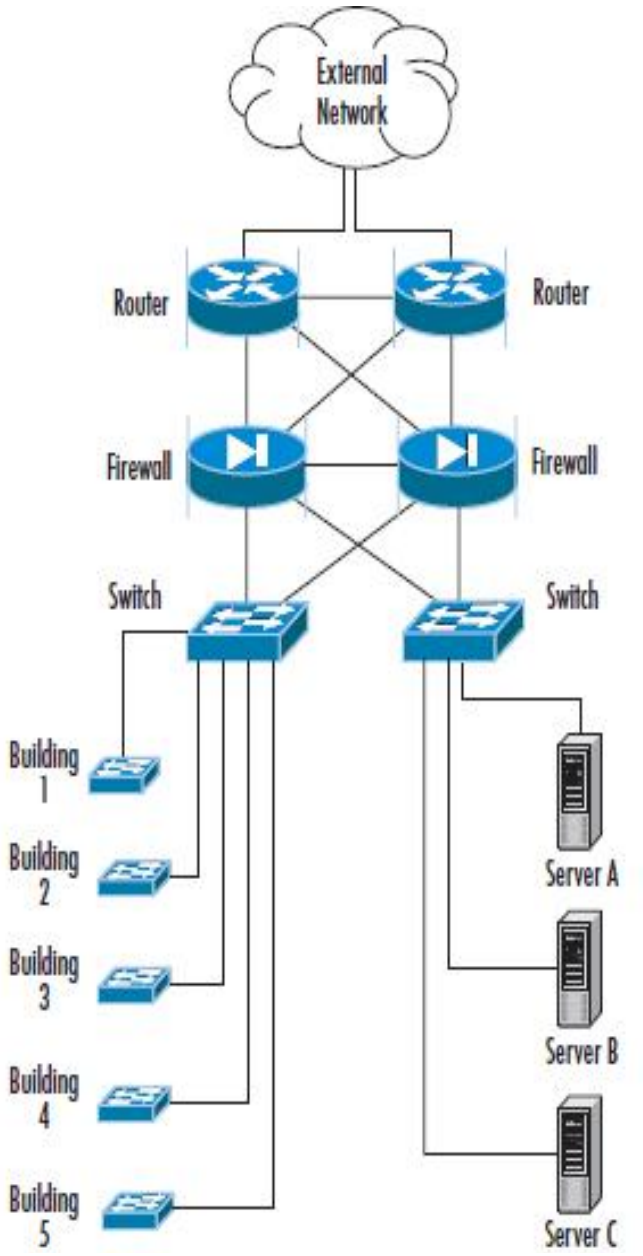


Εικόνα 3.24: Τοποθέτηση Wireshark χρησιμοποιώντας ένα Cable Tap

Οι περισσότερες δικτυακές αρχιτεκτονικές δεν είναι τόσο απλές όσο εκείνες που απεικονίζονται σε αυτές τις εικόνες.

Εντούτοις, αυτά τα παραδείγματα πρέπει να μας δώσουν μια καλή ιδέα για το πώς να χρησιμοποιήσουμε το Wireshark σε διάφορα σημεία στο δίκτυό μας.
Μερικές αρχιτεκτονικές δικτύων είναι αρκετά μπερδεμένες και δύσκολες όσων αφορά τη διασύνδεση μεταξύ των υπολογιστών (Εικόνα 3.25) . Επίσης, τα τμήματα δικτύων μπορούν να διακλαδιστούν έξω για διάφορα επίπεδα όσο το δίκτυό μας επεκτείνεται σε πατώματα μέσα στο κτήριο ή ακόμα και σε άλλα κτήρια.

Πρέπει να έχουμε μια καλή κατανόηση του δικτύου μας προκειμένου να γίνουν οι αποτελεσματικότερες επιλογές για την τοποθέτηση ενός sniffer.



Εικόνα 3.25: Δίκτυο με πολύπλοκη δικτύωση

3.6.9 Χρησιμοποιώντας το Wireshark για αντιμετώπιση προβλημάτων Δικτύου (Network Troubleshooting)

Κάθε διαχειριστής δικτύων είχε τη δυσάρεστη εμπειρία της κλήσης μέσα στη νύχτα για να επιδιορθώσει ένα πρόβλημα δικτύων, το οποίο μπορεί συχνά να οδηγήσει σε ένα κύμα νέων προβλημάτων (πανικός, επείγουσα ανάγκη αποκατάστασης).
Το κλειδί για να γίνει επιτυχώς η ανίχνευση ενός προβλήματος είναι να ξέρουμε πώς το δίκτυο λειτουργεί υπό κανονικές συνθήκες, το οποίο θα μας επιτρέψει να αναγνωρίσουμε γρήγορα τις ασυνήθιστες και αφύσικες διαδικασίες.
Ένας τρόπος για να γίνει γνωστό το πώς είναι οι λειτουργίες του δικτύου μας κανονικά, είναι να χρησιμοποιήσουμε ένα sniffer σε διάφορα σημεία στο δίκτυο.
Αυτό θα επιτρέψει σε εμάς να έχουμε μια αίσθηση των πρωτοκόλλων που τρέχουν στο δίκτυό μας, οι συσκευές σε κάθε τμήμα, και τα top-talkers (υπολογιστές που στέλνουν και λαμβάνουν στοιχεία πολύ συχνά).
Μόλις έχουμε μια ιδέα για το πώς το δίκτυό μας λειτουργεί μπορούμε να αναπτύξουμε μια στρατηγική για την ανίχνευση και αντιμετώπιση λαθών σε αυτό. Με αυτό τον τρόπο μπορούμε να προσεγγίσουμε το πρόβλημα μεθοδικά και να εξυπηρετήσουμε με την ελάχιστη διάσπαση τους πελάτες.
Με την ανίχνευση λαθών (troubleshooting), τα λεπτά που ξοδεύονται για την αξιολόγηση των «συμπτωμάτων» μπορεί να μας σώσουν από ώρες χρόνου που χάνονται για να ανακαλύψουμε το πρόβλημα.

Μια καλή προσέγγιση στην ανίχνευση λαθών δικτύων περιλαμβάνει τα ακόλουθα επτά βήματα:

1. Αναγνώριση συμπτωμάτων (Recognize the symptoms)
2. Καθορισμός προβλήματος (Define the problem)
3. Ανάλυση προβλήματος (Analyze the problem
4. Απομόνωση προβλήματος (Isolate the problem)
5. Προσδιορισμός και δοκιμή της αιτίας (Identify and test the cause of the problem)
6. Επίλυση προβλήματος (Solve the problem)
7. Έλεγχος εάν το πρόβλημα επιλύθηκε (Verify that the problem has been solved)

Το πρώτο βήμα στην ανίχνευση λαθών δικτύων είναι η *αναγνώριση* των συμπτωμάτων. Μπορούμε επίσης να μάθουμε για ένα πρόβλημα δικτύων από ένα άλλο δίκτυο χρηστών, όπου αυτό έχει διαγνωστεί και καταγραφεί (ζητήματα απόδοσης, ζητήματα συνδεσιμότητας, ή άλλες παράξενες συμπεριφορές) στην πρόσβαση του δικτύου.
Συγκρίνουμε αυτήν την συμπεριφορά με την κανονική λειτουργία δικτύων και παρατηρούμε για τυχόν αλλαγές στην όλη λειτουργία:

- Μια αλλαγή που ίσως έγινε στο δίκτυο ή σε ένα server λίγο πριν το πρόβλημα αρχίσει.
- Εάν ξεκίνησε κάποια αυτόματη διαδικασία που είχε οριστεί. Για παράδειγμα ένα backup

Μόλις απαντήσουμε σε αυτές τις ερωτήσεις, το επόμενο βήμα είναι να γραφτεί ένας σαφής καθορισμός του προβλήματος. Μόλις προσδιοριστούν τα συμπτώματα και το πρόβλημα καθοριστεί, το επόμενο βήμα είναι *να* αναλυθεί. Πρέπει να συγκεντρώσουμε τα στοιχεία για την ανάλυση και να γίνει πιο συγκεκριμένο το πρόβλημα.

- Είναι στον πυρήνα του δικτύου, σε ένα μόνο κτήριο, ή σε ένα μακρινό γραφείο?
- Είναι το πρόβλημα σχετικό με ένα ολόκληρο τμήμα δικτύων ή έναν υπολογιστή?
- Μπορεί το πρόβλημα να αναπαραχθεί αλλού στο δίκτυο?

Μπορεί επίσης να χρειαστεί να εξετάσουμε τα διάφορα μέρη του δικτύου μας για να κάνουμε το πρόβλημα περισσότερο σαφές.

Τώρα που έχουμε βρει και αναλύσει το πρόβλημα, μπορούμε να κινηθούμε στο επόμενο βήμα της απομόνωσης του προβλήματος.
Υπάρχουν πολλοί τρόποι να γίνει αυτό, όπως το να αποσυνδέσουμε τον υπολογιστή που προκαλεί τα προβλήματα, να επανεκινήσουμε από την αρχή το server (reboot a

server), να ενεργοποιήσουμε έναν τοίχο προστασίας από υιούς για να σταματήσει όποια ανώμαλη κυκλοφορία, ή να καταφύγουμε σε μια εφεδρική σύνδεση με το Διαδίκτυο.

Το επόμενο βήμα είναι να προσδιοριστεί και να εξεταστεί η αιτία του προβλήματος. Τώρα που έχουμε μια θεωρία για την αιτία του προβλήματος πρέπει να την εξετάσουμε.
Η συσκευή ανάλυσης του δικτύου μας μπορεί να δει τι συμβαίνει πίσω από τις σκηνές.
Σε αυτό το σημείο, μπορούμε να ψάξουμε το πρόβλημα στο διαδίκτυο, ή τους διάφορους προμηθευτές υλικού ή λογισμικού, ή στο φορέα παροχής υπηρεσιών Διαδικτύου μας (Internet Service Provider –ISP-).[38]

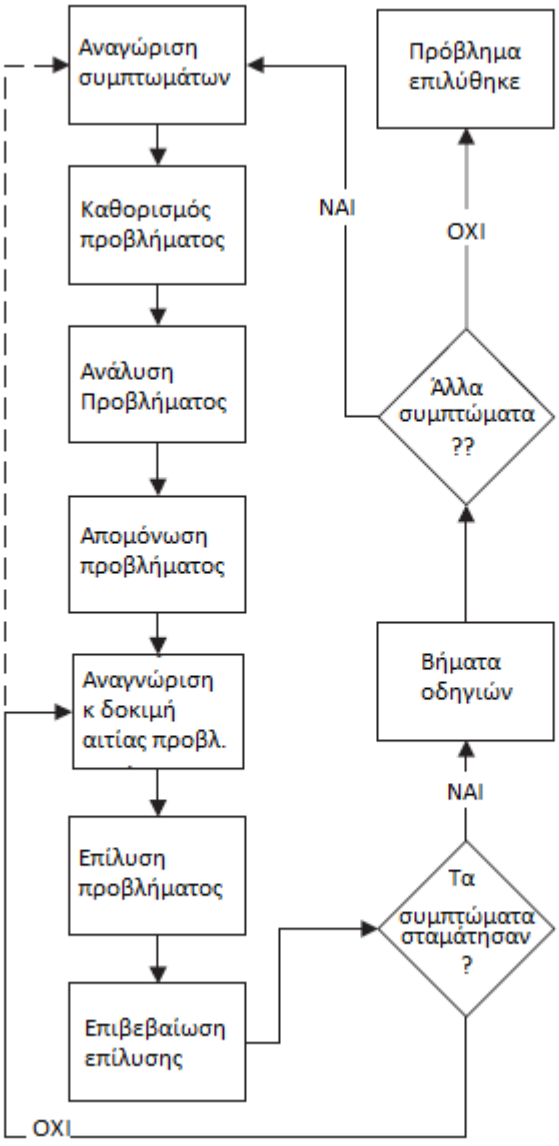
Μόλις έχουμε μία λύση στο πρόβλημα, πρέπει *να την εφαρμόσουμε*. Αυτό θα μπορούσε να περιλαμβάνει εφαρμογή υλικού ή λογισμικού αναβάθμισης, εφαρμογή ενός τοίχους προστασίας, επανατοποθέτηση ενός δοκιμασμένου συστήματος, αντικατάσταση του αποτυχημένου υλικού, ή επανασχεδιασμός των τμημάτων του δικτύου μας.
Το τελευταίο βήμα της ανίχνευσης λαθών δικτύων *ελέγχει* ότι το πρόβλημα έχει επιλυθεί. Πρέπει να σιγουρευτούμε ότι η αποτύπωση για αυτό το πρόβλημα δεν δημιούργησε οποιαδήποτε νέα προβλήματα ή ότι το πρόβλημα που λύσαμε δεν είναι ενδεικτικό ενός βαθύτερου προβλήματος που ελλοχεύει.

Μέρος αυτού του βήματος αποτελεί η τεκμηρίωση των μέτρων που λαμβάνονται για να επιλύσουν το πρόβλημα, η οποία θα βοηθήσει στις μελλοντικές προσπάθειες ανίχνευσης λαθών.
Εάν δεν έχουμε λύσει το πρόβλημα, πρέπει να επαναλάβουμε τη διαδικασία από την αρχή.

---

[38] Μπορούμε να το κάνουμε απευθείας στα εξής sites : www.cert.org ή www.incidents.org

Το διάγραμμα ροής στην εικόνα 3.26 απεικονίζει τη διαδικασία ανίχνευσης σφαλμάτων δικτύων.



Εικόνα 3.26: Διαδικασία Αντιμετώπισης Προβλημάτων

3.6.10 Χρησιμοποιώντας το Wireshark για διοίκηση ασφάλειας

"Είναι αυτό το πρωτόκολλο ασφαλές;"

Ένας από τους πιο κοινούς στόχους που έχουν οι διαχειριστές ασφάλειας δικτύων, είναι να ελέγχουν την ασφάλεια ενός αυθαίρετου πρωτοκόλλου. Το Wireshark είναι το ιδανικό εργαλείο που μπορεί να χρησιμοποιηθεί για αυτό.

Ένα από τα δημοφιλέστερα και χρήσιμα χαρακτηριστικά γνωρίσματα του Wireshark είναι η επανασυναρμολόγηση πακέτων, η οποία μας επιτρέπει να δούμε το περιεχόμενο των στοιχείων που διέρχονται από το δίκτυό μας.
Για τα πρωτόκολλα όπως το Telnet και το FTP, το Wireshark σαφώς επιδεικνύει το όνομα χρήστη και τον κωδικό πρόσβασης για τη σύνδεση, χωρίς οποιαδήποτε επανασυναρμολόγηση.

Για κάποιο άγνωστο, ή ειδάλλως «σκοτεινό» πρωτόκολλο, η επανασυναρμολόγηση πακέτων μπορεί να χρησιμοποιηθεί.

Για να χρησιμοποιήσουμε την επιλογή επανασυναρμολόγησης, πρέπει να συλλάβουμε την κυκλοφορία μέσω Wireshark ή ενός άλλου εργαλείου και να φορτώσουμε έπειτα το αρχείο σύλληψης στο Wireshark.
Επιλέγουμε την επιλογή 'Follow TCP Stream'.

Ένα παράθυρο θα εμφανιστεί επάνω με όλη την επικοινωνία που πραγματοποιήθηκε σε εκείνη την σύνοδο.
Μπορεί να βοηθήσει αν επιλέξουμε την επιλογή ASCII, και εάν το πρωτόκολλο είναι θορυβώδες μπορούμε να επιλέξουμε τον συγκεκριμένο εκείνο αποστολέα, δέκτη, ή ακόμα και Ολόκληρη συνομιλία *να* εμφανίζεται.

3.6.11 Γνωρίζοντας τα κύρια «χαρακτηριστικά» του Wireshark

Το Wireshark παρέχει την οπτική δυνατότητα αυτού που εμφανίζεται σε ένα δίκτυο, η οποία είναι χρήσιμη κατά την εφαρμογή των πρωτοκόλλων, την εφαρμογή διόρθωσης δικτύων, την εξέταση-έλεγχο ενός δικτύου, και την 'ζωντανή διόρθωση' δικτύου.

Στις καταστάσεις που περιλαμβάνουν την αλληλεπίδραση με ένα δίκτυο σε τεχνικό επίπεδο, τα περισσότερα προβλήματα μπορεί να επιλυθούν χρησιμοποιώντας το Wireshark.

Το Wireshark είναι μια άριστη εκπαιδευτική ενίσχυση. Στο να είσαι σε θέση να δεις και να αναλύσεις το δίκτυο και την κυκλοφορία είναι πολύ διδακτικό.

Εάν τρέχουμε μια διανομή Linux είναι πιθανό ότι στη διανομή μας υπάρχει ήδη το ethereal, το οποίο είναι ο προκάτοχος σε Wireshark. Λόγω της πρόσφατης αλλαγής ονόματος για το πρόγραμμα, είναι απίθανο το Wireshark να έχει περιληφθεί και θα πρέπει να το εγκαταστήσουμε.

Εάν τρέχουμε Windows ή κάποια έκδοση UNIX (Solaris, HPUX, AIX, κλπ) θα πρέπει να αποκτήσουμε το Wireshark και να το εγκαταστήσουμε.

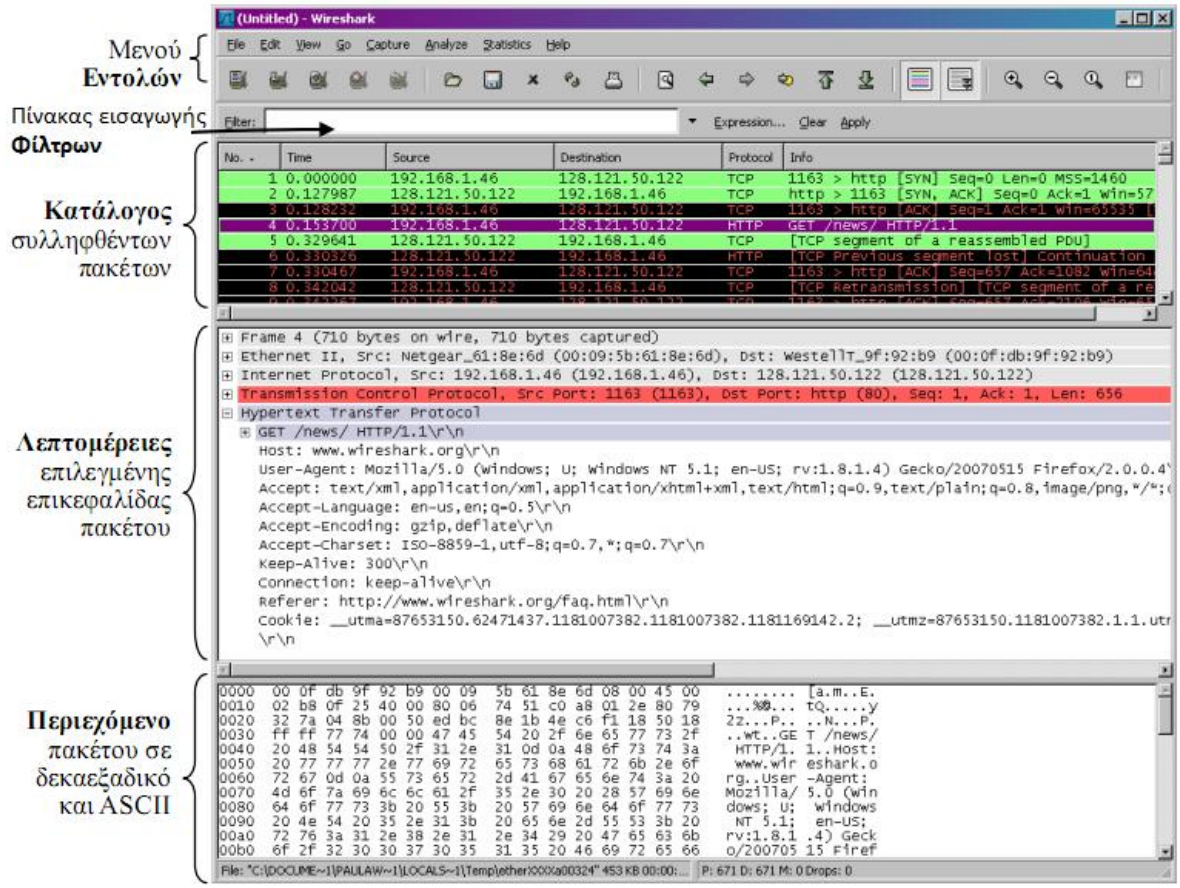
Μπορούμε να «κατεβάσουμε» το Wireshark από τον ιστοχώρο Wireshark http://www.wireshark.com.

Εάν δεν υπάρχει για την πλατφόρμα μας, εάν δεν είναι ενημερωμένοι, συνταγμένοι και με επιλογές που χρειαζόμαστε, μπορούμε να κατεβάσουμε τον κώδικα πηγής από τον ιστοχώρο του Wireshark και να μεταφράσουμε το Wireshark οι ίδιοι κάτι το οποίο βέβαια είναι αρκετά εξειδικευμένο.

3.7 Wireshark Εξερεύνηση του κύριου παραθύρου

Είναι σημαντικό να καθοριστεί ένα κοινό σύνολο ετικετών για τα διαφορετικά συστατικά του κύριου παράθυρου έτσι ώστε να είναι περισσότερο κατανοητό τι φαίνεται σε αυτό.

Η Εικόνα 3.27 παρουσιάζει το κύριο παράθυρο του Wireshark με τα κυριότερα του συστατικά επονομαζόμενα.



Εικόνα 3.27: Κύριο παράθυρο του Wireshark

Περιβάλλον χρήσης του Wireshark

Το περιβάλλον χρήσης του Wireshark περιλαμβάνει πέντε κύρια συστατικά στοιχεία:

3.7.1 Τα μενού των εντολών

Τα μενού των εντολών (command menus) είναι συνηθισμένα μενού που βρίσκονται στο επάνω μέρος του παραθύρου. Προς το παρόν μας ενδιαφέρουν τα μενού File και Capture. Το μενού File επιτρέπει την αποθήκευση δεδομένων για πακέτα που έχουν συλληφθεί ή το άνοιγμα ενός αρχείου που περιέχει δεδομένα πακέτων που είχαν συλληφθεί προηγουμένως και την έξοδο από το Wireshark. Το μενού Capture σας επιτρέπει να ξεκινήσετε τη σύλληψη πακέτων.

3.7.2 Παράθυρο δέντρων/λεπτομερειών πρωτοκόλλου (Protocol tree Window)

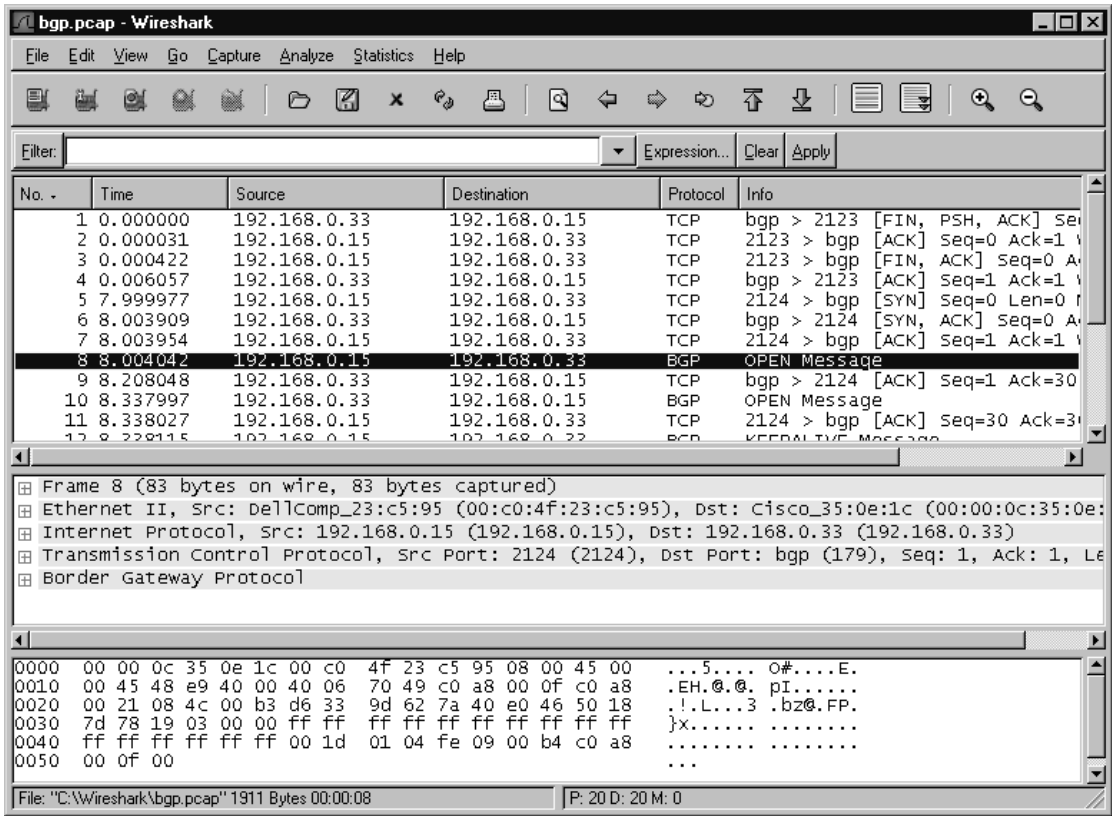
Μπορούμε να αντιληφθούμε ένα πακέτο ως δέντρο τομέων με 'υποδέντρα'. Για κάθε πρωτόκολλο, υπάρχει ένας κόμβος δέντρων που μπορεί να επεκταθεί για να παρέχει τις τιμές στους τομείς εκείνου του πρωτοκόλλου που χρειάζεται.

Μέσα σε μερικά πρωτόκολλα, μπορούν να υπάρξουν κόμβοι δέντρων που συνοψίζουν τις πιο περίπλοκες δομές δεδομένων στο πρωτόκολλο. Αυτοί οι κόμβοι δέντρων μπορούν να απενεργοποιηθούν για να παρουσιάσουν εκείνες τις δομές δεδομένων που θέλουμε.

Για οποιοδήποτε δεδομένο κόμβο που έχει subtree, μπορείτε να επεκτείνετε τα subtree για να αποκαλύψετε περισσότερες πληροφορίες, ή το συντμήσετε για να παρουσιάσετε μόνο την περίληψη.

Το παράθυρο λεπτομερειών πρωτοκόλλου επιτρέπει να εξεταστεί το δέντρο που δημιουργείται από το Wireshark από την αποκωδικοποίηση ενός πακέτου.

Συνεχίζοντας θα παρουσιαστεί το παράθυρο δεδομένων πρωτοκόλλου με το πακέτο που επιλέχτηκε στο προηγούμενο παράδειγμα (Εικόνα 3.28).



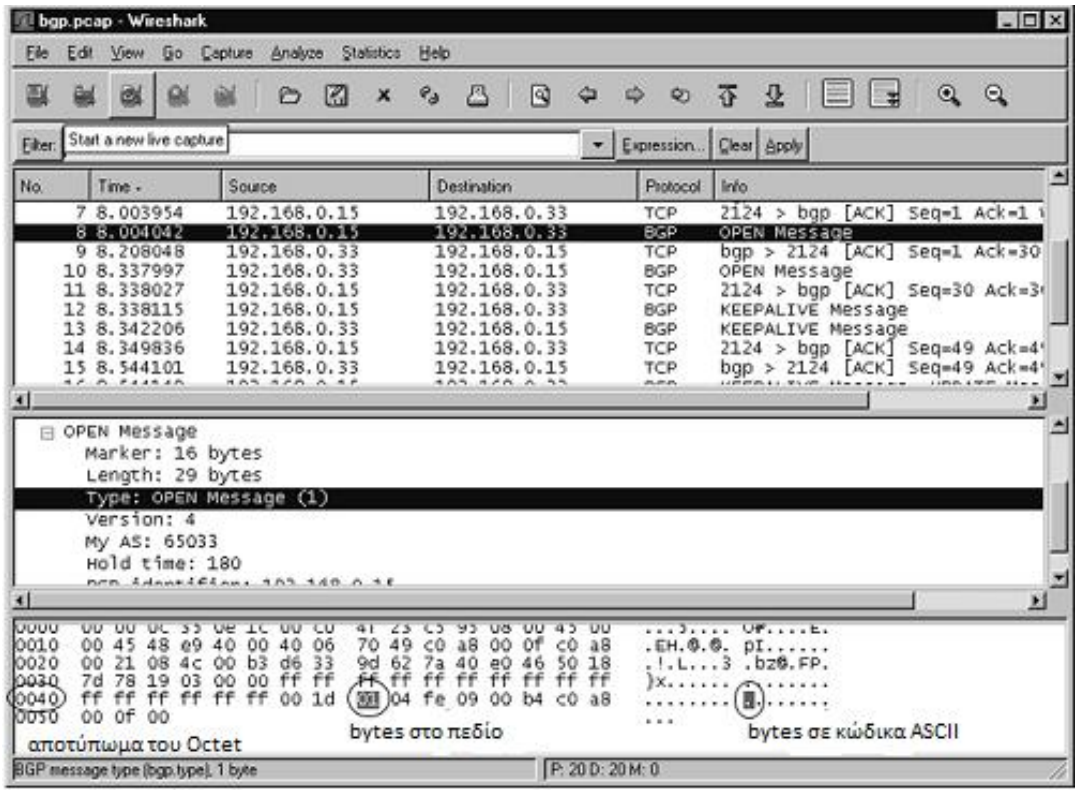
Εικόνα 3.28 Παράθυρο δεδομένων Πρωτοκόλλου

Στο παράθυρο δέντρων/λεπτομερειών πρωτοκόλλου, κάθε στρώμα στη λίστα πρωτοκόλλου για κάθε πακέτο περιέχει μια περίληψη μιας γραμμής.

3.7.3 Παράθυρο εμφάνισης στοιχείων (Data view window)

Το παράθυρο εμφάνισης στοιχείων περιέχει μια ακολουθία σειρών που κάθε μια αρχίζει με έναν τετραψήφιο

αριθμό που αντιπροσωπεύει τον αριθμό ψηφίο-λέξεων σε ένα *octet*. (Ένα octet αποτελείται από είτε 8 μπιτ, 1 ψηφίο-λέξη, είτε 2 δεκαεξαδικά ψηφία). Ο πρώτος octet σε εκείνη την σειρά αποτυπώνεται από την αρχή του πακέτου (Εικόνα 3.29).



Εικόνα 3.29 Παράθυρο εμφάνισης στοιχείων

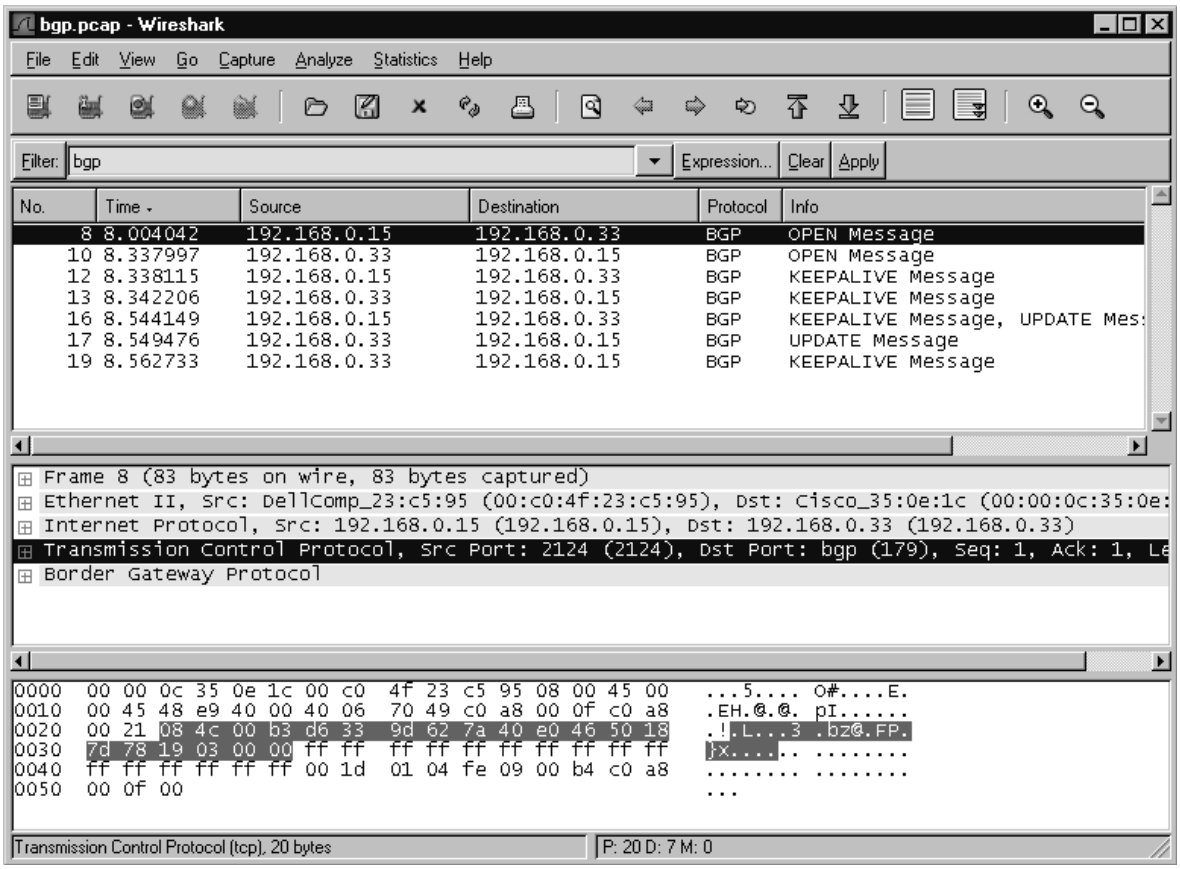
Όταν ένας τομέας στο παράθυρο δέντρων πρωτοκόλλου επιλέγεται, η αντιστοιχία ψηφίων σε εκείνο τον τομέα τονίζεται στο παράθυρο εμφάνισης στοιχείων.
Στην Εικόνα 3.29 επιλέξαμε το μήνυμα BGP στο παράθυρο δέντρων πρωτοκόλλου. Το «BGP» αναφέρεται στο *Border Gateway Protocol* (αποτελεί τον πυρήνα πρωτοκόλλου δρομολόγησης του Διαδικτύου).
Όταν επιλέγουμε σε μια δεκαεξαδική ψηφίο-λέξη ή το χαρακτήρα ASCII κατά την άποψη στοιχείων το παράθυρο**,** το Wireshark δίνει έμφαση στον τομέα στο παράθυρο δέντρων πρωτοκόλλου που αντιστοιχεί στην επιλεγμένη ψηφίο-λέξη και σε όλες τις ψηφίο-λέξεις στο παράθυρο άποψης στοιχείων που συνδέεται με εκείνο τον τομέα πρωτοκόλλου.

3.8 Άλλα τμήματα παραθύρων

Τα ακόλουθα είναι διάφορα πρόσθετα συστατικά του παραθύρου Wireshark που μπορούμε να βρούμε αρκετά χρήσιμα κατά την εξέταση των πακέτων όπως η ,πάρα φίλτρων.

3.8.1 Μπάρα «Φίλτρων» (Filter Bar)

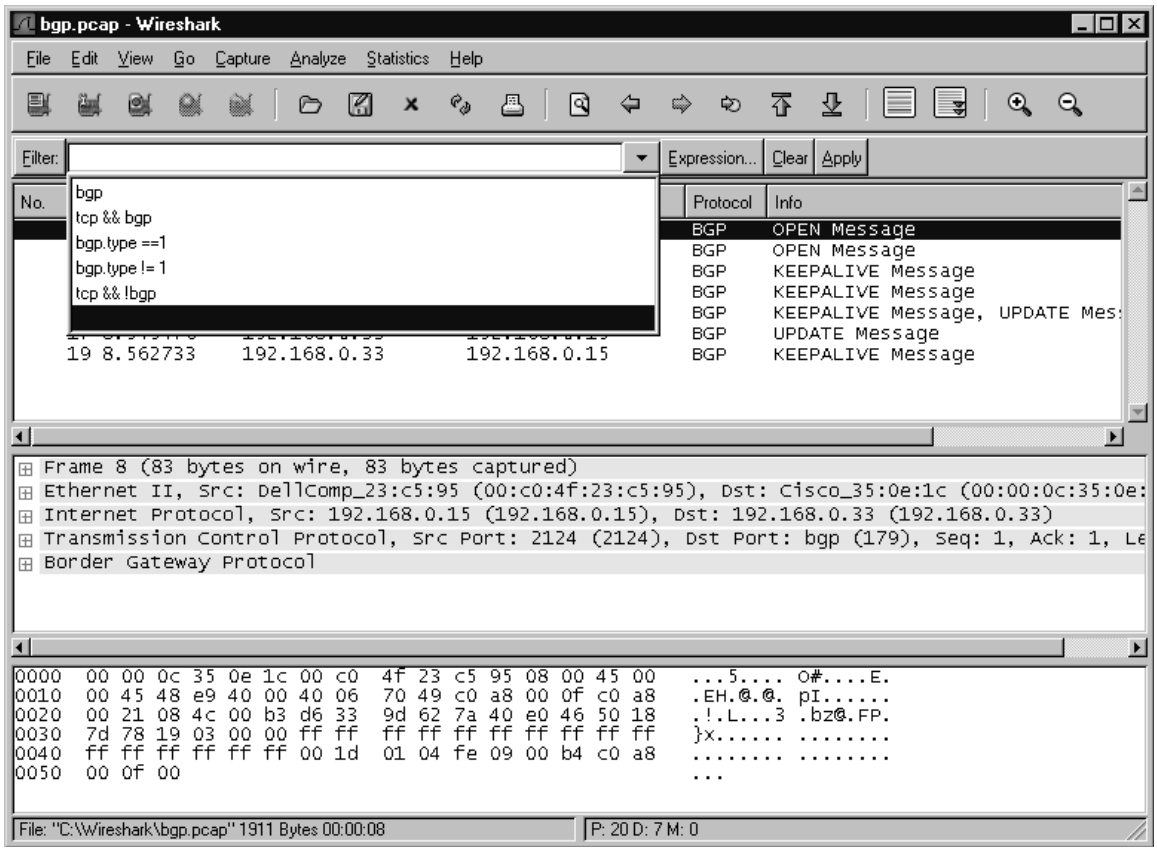
Η μπάρα φίλτρων (Εικόνα 3.30) μας επιτρέπει να εισαγάγουμε μια σειρά φίλτρων που περιορίζει το ποια πακέτα θα εμφανίζονται στο παράθυρο περίληψης. Μόνο πακέτα που ταιριάζουν με την επιλογή στη σειρά φίλτρων εμφανίζεται στο συνοπτικό παράθυρο. Μια σειρά φίλτρων εμφάνισης καθορίζει τους όρους σε ένα πακέτο που μπορεί ή δεν ταιριάζει με το πακέτο (Π.χ., το φίλτρο (ip.addr == 10.15.162.1 & & BGP) θα ταιριάζει με όλα τα πακέτα με διεύθυνση IP [Πηγή ή προορισμό] του 10.15.162.1 που είναι πακέτα πρωτοκόλλων BGP).



Εικόνα 3.30: Μπάρα Φιλτραρίσματος

Στην Εικόνα 3.30 ένα φίλτρο *bgp* έχει εφαρμοστεί. Για να εφαρμοστεί ένα φίλτρο, γίνεται εισαγωγή του επιθυμητού ονόματος στη γραμμή επιλογής φίλτρου (σαν κείμενο) και πατάμε Enter (ή επιλέγουμε την επιλογή Apply).

Μόλις εφαρμοστεί η σειρά φίλτρων επίδειξης bgp, μόνο τα πακέτα BGP επιδεικνύονται μέσα από το παράθυρο περίληψης. Επίσης τα φίλτρα που έχουν χρησιμοποιηθεί προηγουμένως μπορούν να επανέλθουν εύκολα (Εικόνα 3.31).



Εικόνα 3.31: Λίστα επιλογής Χρησιμοποιηθέντων Φίλτρων

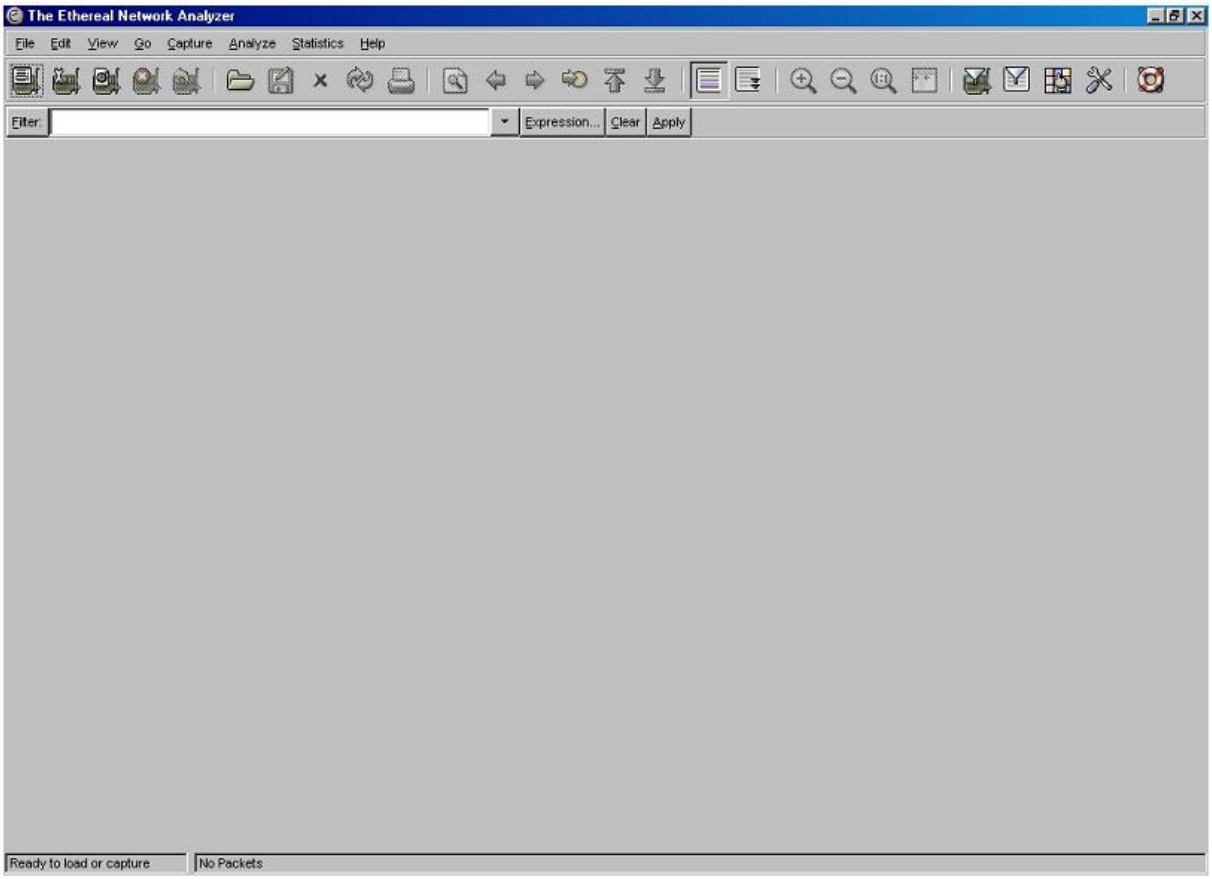
Πατώντας το βελάκι στο τέλος της μπάρας φιλτραρίσματος, μπορείτε να έχετε πρόσβαση στον κατάλογο προηγούμενων εφαρμοσμένων φίλτρων. Για να χρησιμοποιήσουμε ένα από αυτά τα φίλτρα, το επιλέγουμε από τον κατάλογο και πατάμε Enter ή πατάμε το πλήκτρο Apply**.** Για να αφαιρέσουμε όλες τις περιοριστικές επιλογές φίλτρων και να παρουσιάσουμε πάλι όλα τα πακέτα, πατάμε το κουμπί Reset.

3.9 Σύλληψη Πακέτων χρησιμοποιώντας το Wireshark

Ο καλύτερος τρόπος να γνωρίσει κανείς ένα νέο κομμάτι λογισμικού είναι με τη δοκιμή. Ακολουθήστε τα παρακάτω βήματα:

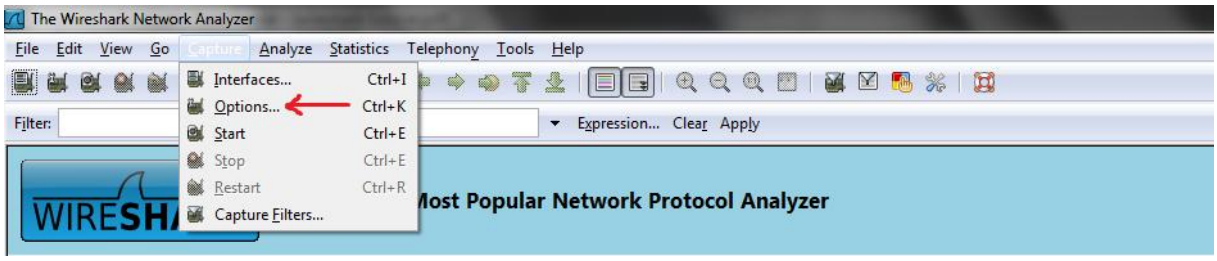
1. Ξεκινήστε τον φυλλομετρητή της αρεσκείας σας, ο οποίος θα εμφανίσει την αρχική σελίδα που έχετε επιλέξει.

2. Ξεκινήστε το λογισμικό Wireshark, θα δείτε αρχικά ένα παράθυρο παρόμοιο με αυτό που φαίνεται στην εικόνα 3.32 με τη διαφορά ότι δε θα εμφανίζονται δεδομένα πακέτων στα παράθυρα packet-listing, packet-header, ή packet-contents, αφού το Wireshark δεν έχει αρχίσει ακόμη να συλλαμβάνει πακέτα.

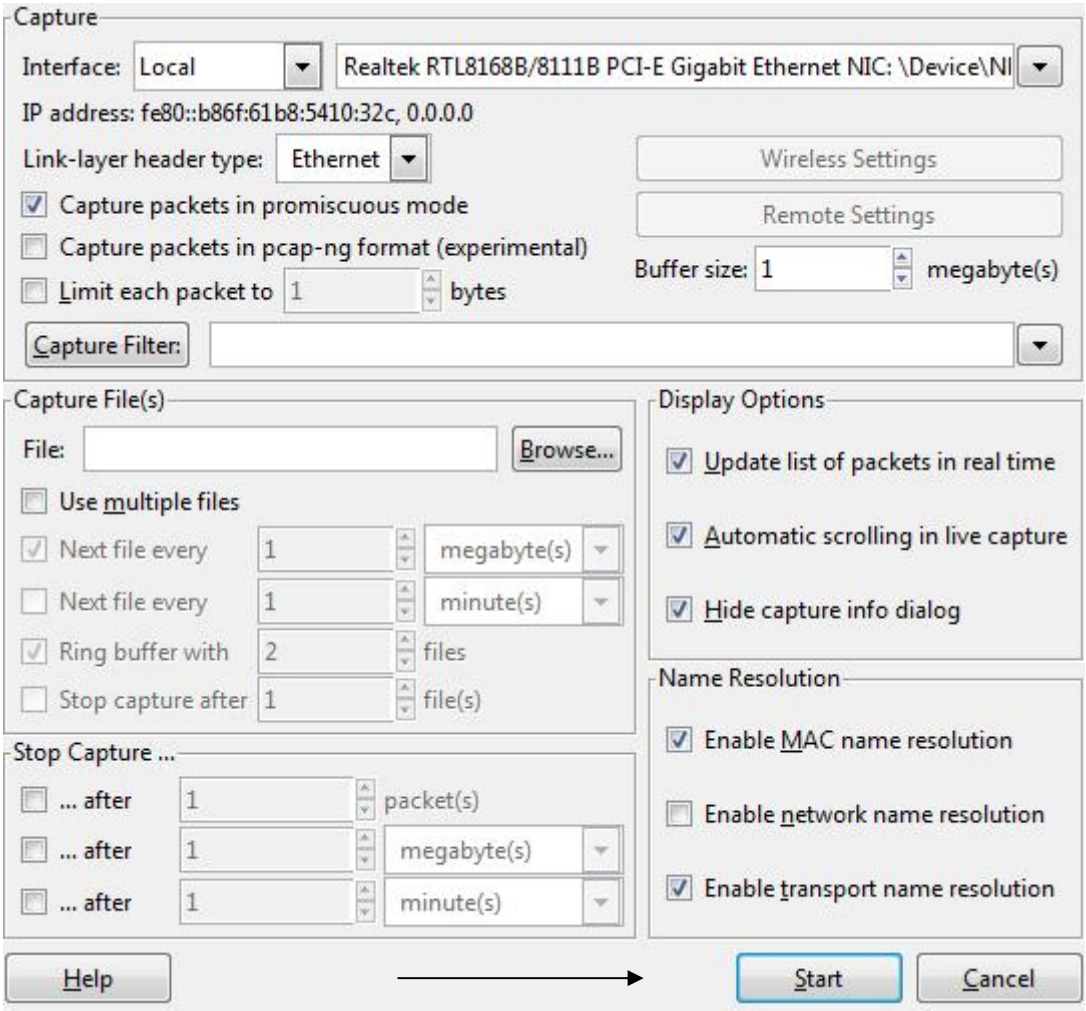


Εικόνα 3.32: Αρχική οθόνη Wireshark

3. Για να αρχίσει η σύλληψη πακέτων, επιλέξτε Start στο μενού Capture. Αυτό θα έχει ως αποτέλεσμα την εμφάνιση του παραθύρου "Wireshark: Capture Options" όπως φαίνεται στην εικόνες 3.33, 3.34.

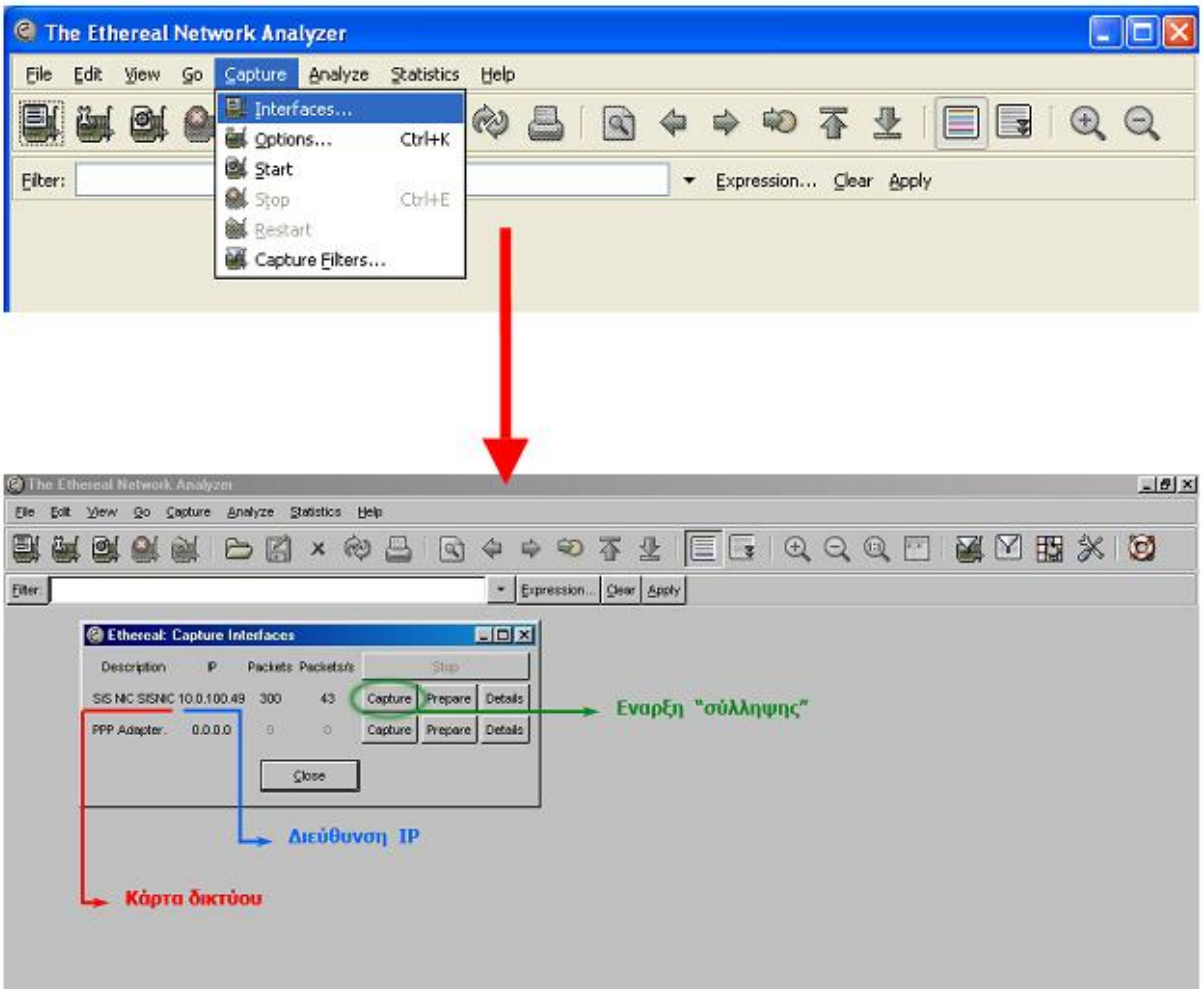


Εικόνα 3.33: Μενού επίλογων σύλληψης



Εικόνα 3.34: Παράθυρο επίλογων

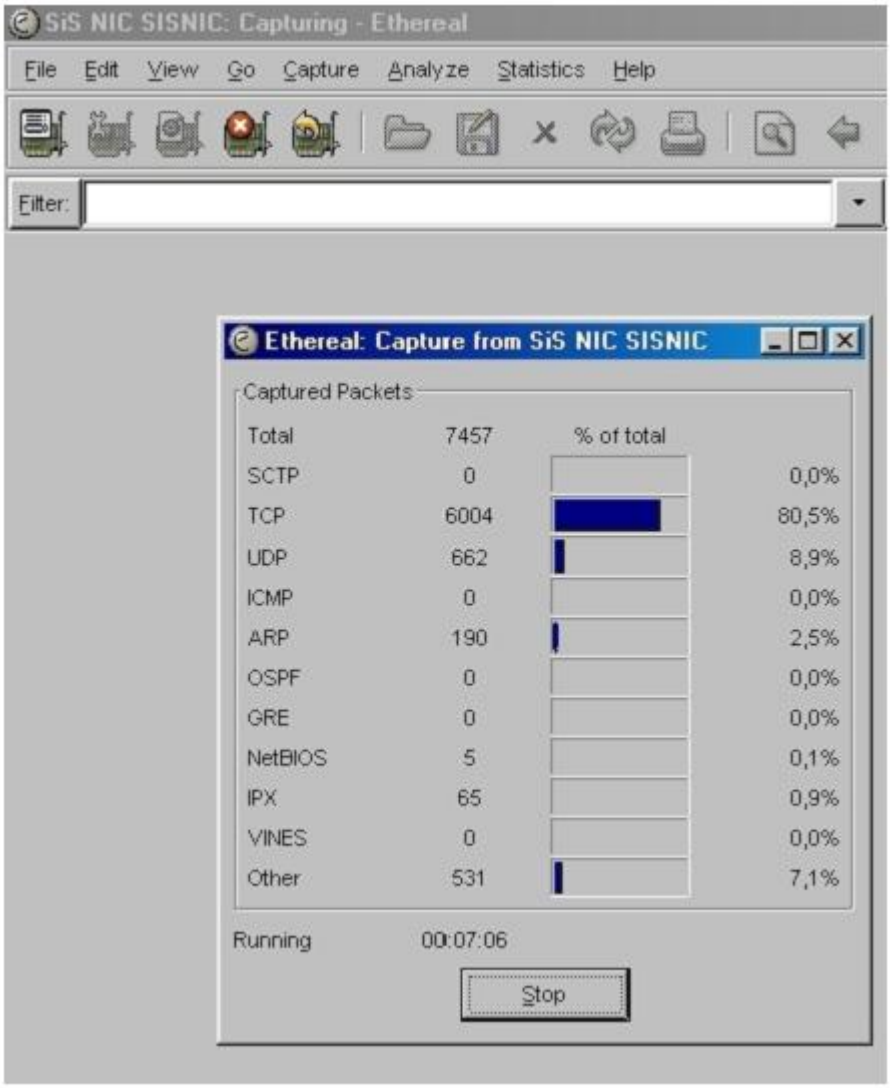
Υπάρχει βέβαια και ένας 2ος τρόπος για να ξεκινήσει η σύλληψη πακέτων: από το menu .. Capture --> Interfaces όπως δείχνει και η παρακάτω εικόνα 3.35



Εικόνα 3.35: Επιλογές 2^{ου} τρόπου σύλληψης

4. Μπορούν να χρησιμοποιηθούν όλες οι προεπιλεγμένες τιμές αυτού του παραθύρου. Οι διεπαφές δικτύου (δηλαδή οι φυσικές συνδέσεις) του υπολογιστή σας με το δίκτυο θα εμφανίζονται στο μενού Interface στο επάνω μέρος του παραθύρου Capture Options. Σε περίπτωση που ο υπολογιστής σας έχει περισσότερες από μία ενεργές διεπαφές δικτύου (π.χ. εάν έχετε αμφότερες μία ασύρματη και μία ενσύρματη σύνδεση Ethernet), θα χρειαστεί να επιλέξετε μία διεπαφή την οποία θα χρησιμοποιήσετε για να στέλνετε και να λαμβάνετε πακέτα (το πιθανότερο την ενσύρματη διεπαφή). Αφού επιλέξετε τη διεπαφή δικτύου (ή χρησιμοποιήσετε την προεπιλεγμένη διεπαφή που επιλέγει το Wireshark), κάντε κλικ στο OK. Στο σημείο αυτό αρχίζει η σύλληψη των πακέτων: όλα τα πακέτα που στέλνονται ή λαμβάνονται από τον υπολογιστή σας συλλαμβάνονται από το Wireshark.

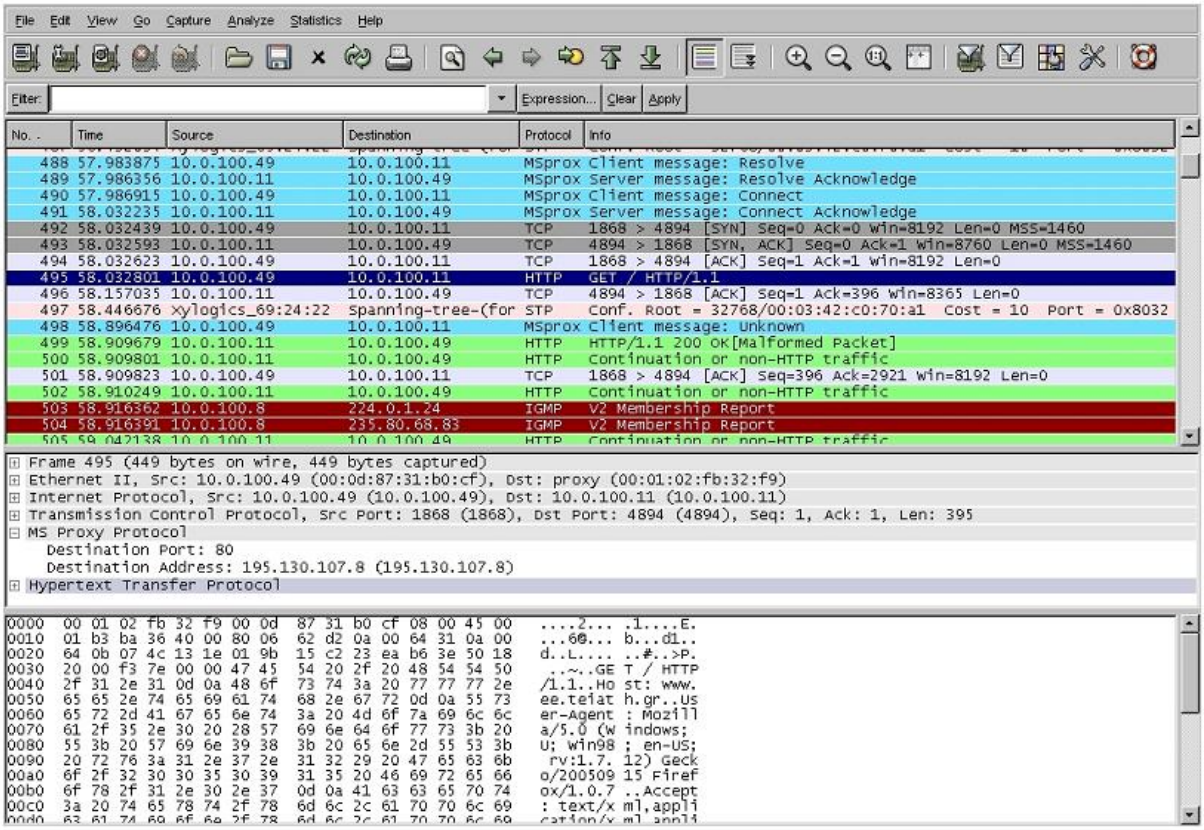
5. Μόλις αρχίσει η σύλληψη πακέτων θα εμφανισθεί ένα παράθυρο περίληψης σύλληψης πακέτων (packet capture summary window) όπως φαίνεται στην παρακάτω εικόνα 3.36. Το παράθυρο αυτό συνοψίζει τον αριθμό των διαφόρων ειδών πακέτων που συλλαμβάνονται και περιέχει το κουμπί *Stop* το οποίο θα σας επιτρέψει να διακόψετε τη σύλληψη πακέτων. Μην σταματήσετε τη σύλληψη πακέτων ακόμη.



Εικόνα 3.36: Παράθυρο περίληψης σύλληψης πακέτων

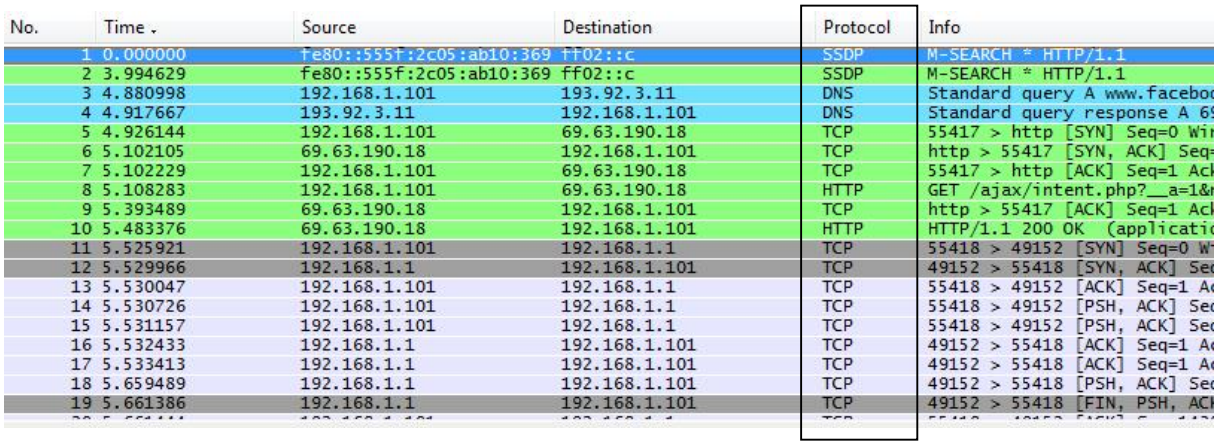
6. Ενώ το Wireshark τρέχει, εισάγετε μια διεύθυνση στο φυλλομετρητή (*browser*): π.χ. http://www.teiath.gr ώστε ο browser να παρουσιάσει αυτήν την ιστοσελίδα. Για να παρουσιάσει αυτή τη σελίδα, ο browser σας θα επικοινωνήσει με τον HTTP server και θα ανταλλάξει μηνύματα HTTP με τον server. Τα πακέτα Ethernet που περιέχουν αυτά τα μηνύματα HTTP θα συλληφθούν από το Wireshark.

7. Αφού ο browser σας παρουσιάσει τη σελίδα www.teiath.gr, σταματήστε τη σύλληψη πακέτων επιλέγοντας stop στο παράθυρο capture του Wireshark. Αυτό θα έχει ως αποτέλεσμα να εξαφανισθεί το παράθυρο capture του Wireshark και το κύριο παράθυρο του Wireshark να εμφανίζει όλα τα πακέτα που συνελήφθησαν από τότε που αρχίσατε τη σύλληψη πακέτων. Το κύριο παράθυρο του Wireshark θα πρέπει τώρα να μοιάζει με αυτό της εικόνας 3.37.



Εικόνα 3.37: Παράθυρο σύλληψης πακέτων

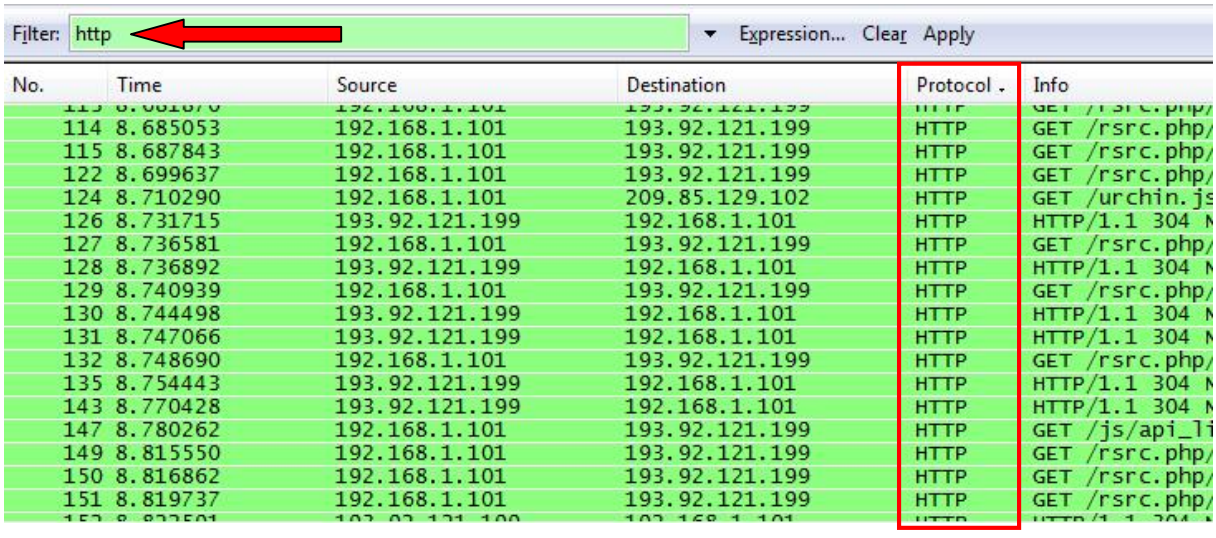
Έχετε τώρα στη διάθεση σας "ζωντανά" δεδομένα πακέτων τα οποία περιέχουν όλα τα μηνύματα πρωτοκόλλων που ανταλλάχθηκαν μεταξύ του υπολογιστή σας και άλλων δικτυακών οντοτήτων. Οι ανταλλαγές μηνυμάτων HTTP με τον web server θα πρέπει να εμφανίζονται κάπου στον κατάλογο πακέτων που συνελήφθησαν. Όμως θα εμφανίζονται επίσης και πολλά άλλα είδη πακέτων (προσέξτε, για παράδειγμα, το μεγάλο αριθμό διαφορετικών ειδών πρωτοκόλλων που φαίνονται στη στήλη Protocol της εικόνα 3.38). Αν και η μόνη δική σας ενέργεια ήταν να φορτώσετε μία ιστοσελίδα, προφανώς στον υπολογιστή σας έτρεχαν πολλά άλλα πρωτόκολλα χωρίς να τα αντιλαμβάνεται ο χρήστης.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::555f:2c05:ab10:369	ff02::c	SSDP	M-SEARCH * HTTP/1.1
2	3.994629	fe80::555f:2c05:ab10:369	ff02::c	SSDP	M-SEARCH * HTTP/1.1
3	4.880998	192.168.1.101	193.92.3.11	DNS	Standard query A www.faceboo
4	4.917667	193.92.3.11	192.168.1.101	DNS	Standard query response A 69
5	4.926144	192.168.1.101	69.63.190.18	TCP	55417 > http [SYN] Seq=0 Win
6	5.102105	69.63.190.18	192.168.1.101	TCP	http > 55417 [SYN, ACK] Seq=
7	5.102229	192.168.1.101	69.63.190.18	TCP	55417 > http [ACK] Seq=1 Ack
8	5.108283	192.168.1.101	69.63.190.18	HTTP	GET /ajax/intent.php?__a=1&r
9	5.393489	69.63.190.18	192.168.1.101	TCP	http > 55417 [ACK] Seq=1 Ack
10	5.483376	69.63.190.18	192.168.1.101	HTTP	HTTP/1.1 200 OK (applicatio
11	5.525921	192.168.1.101	192.168.1.1	TCP	55418 > 49152 [SYN] Seq=0 Wi
12	5.529966	192.168.1.1	192.168.1.101	TCP	49152 > 55418 [SYN, ACK] Seq
13	5.530047	192.168.1.101	192.168.1.1	TCP	55418 > 49152 [ACK] Seq=1 Ac
14	5.530726	192.168.1.101	192.168.1.1	TCP	55418 > 49152 [PSH, ACK] Seq
15	5.531157	192.168.1.101	192.168.1.1	TCP	55418 > 49152 [PSH, ACK] Seq
16	5.532433	192.168.1.1	192.168.1.101	TCP	49152 > 55418 [ACK] Seq=1 Ac
17	5.533413	192.168.1.1	192.168.1.101	TCP	49152 > 55418 [ACK] Seq=1 Ac
18	5.659489	192.168.1.1	192.168.1.101	TCP	49152 > 55418 [PSH, ACK] Seq
19	5.661386	192.168.1.1	192.168.1.101	TCP	49152 > 55418 [FIN, PSH, ACK

Εικόνα 3.38: Δείγμα σύλληψης πακέτων δεδομένων

8. Πληκτρολογήστε "http" (χωρίς τα εισαγωγικά και με μικρά γράμματα - στο Wireshark όλα τα ονόματα πρωτοκόλλων είναι με μικρά γράμματα) στο παράθυρο προδιαγραφών του φίλτρου παρουσίασης, στο επάνω μέρος του κυρίου παραθύρου του Wireshark. Στη συνέχεια επιλέξτε Apply (δεξιά από εκεί όπου εισάγατε "http"). Αυτό θα έχει ως αποτέλεσμα στο παράθυρο packet-listing να εμφανίζονται μόνο τα μηνύματα HTTP.

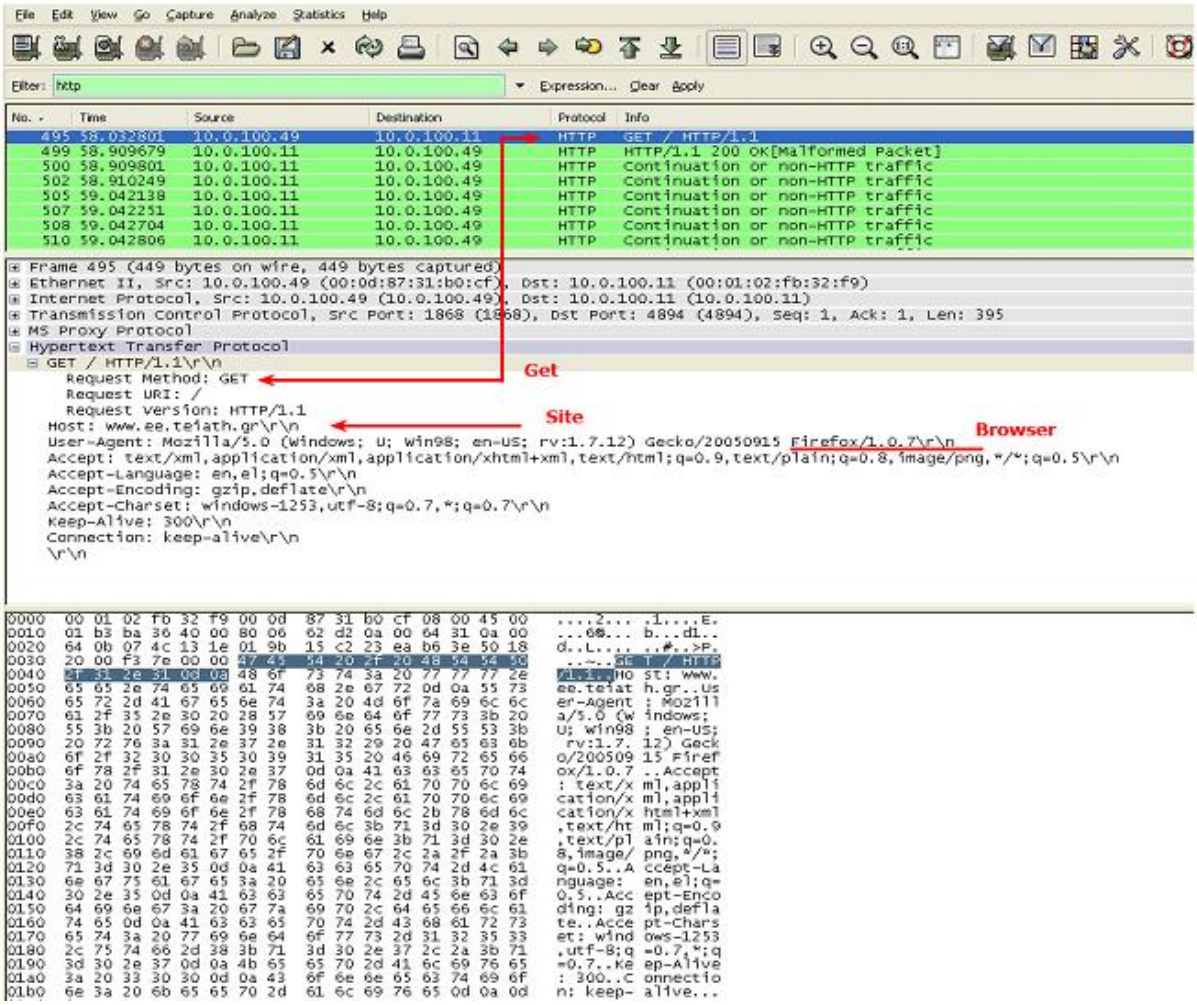


No.	Time	Source	Destination	Protocol	Info
114	8.685053	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
115	8.687843	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
122	8.699637	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
124	8.710290	192.168.1.101	209.85.129.102	HTTP	GET /urchin.js
126	8.731715	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
127	8.736581	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
128	8.736892	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
129	8.740939	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
130	8.744498	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
131	8.747066	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
132	8.748690	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
135	8.754443	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
143	8.770428	193.92.121.199	192.168.1.101	HTTP	HTTP/1.1 304 N
147	8.780262	192.168.1.101	193.92.121.199	HTTP	GET /js/api_li
149	8.815550	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
150	8.816862	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/
151	8.819737	192.168.1.101	193.92.121.199	HTTP	GET /rsrc.php/

Εικόνα 3.39: Δείγμα εφαρμογής φίλτρου

9. Επιλέξτε το μήνυμα HTTP που εμφανίζεται στο τμήμα παραθύρου με την λίστα στων πακέτων. Αυτό θα πρέπει να είναι το μήνυμα HTTP GET το οποίο στάλθηκε από τον υπολογιστή σας στον HTTP server. Όταν επιλέξετε το μήνυμα HTTP GET, οι πληροφορίες για το πλαίσιο Ethernet, το IP πρωτόκολλο, το TCP και την επικεφαλίδα του μηνύματος HTTP θα εμφανισθούν στο παράθυρο επικεφαλίδα πακέτου (packet header). Κάνοντας κλικ στα βέλη που δείχνουν δεξιά και στα βέλη που δείχνουν

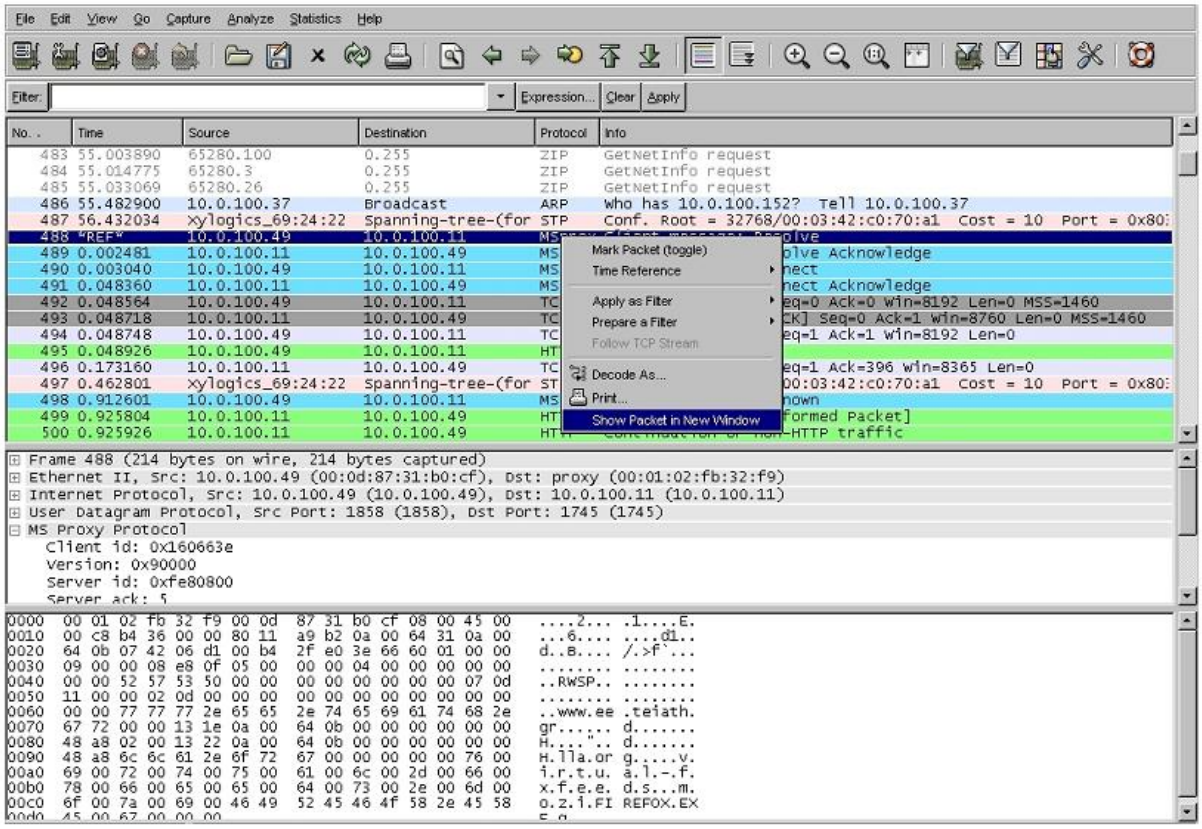
προς τα κάτω στην αριστερή πλευρά του παραθύρου packet-header details, ελαχιστοποιείστε το ποσό πληροφορίας που εμφανίζεται για το πλαίσιο, το πρωτόκολλο Ethernet, το πρωτόκολλο Internet και το TCP.



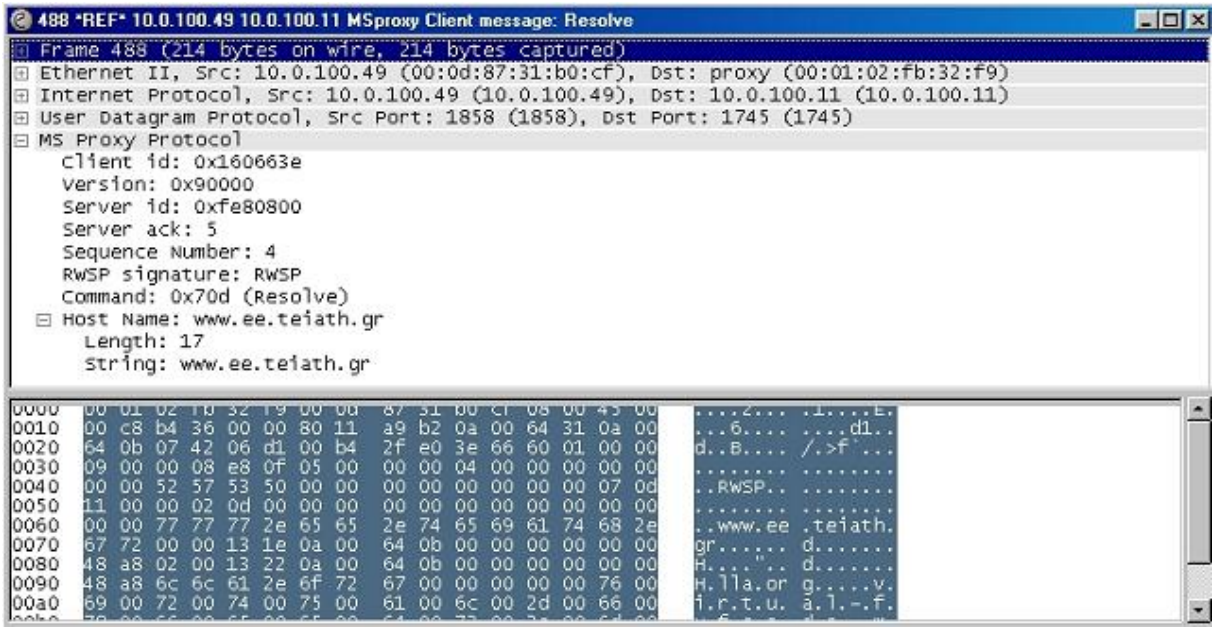
Εικόνα 3.40: Παράθυρο πληροφοριών πακέτου με πρωτόκολλο HTTP

Μεγιστοποιείστε το ποσό πληροφορίας που εμφανίζεται για το πρωτόκολλο HTTP. Το κύριο παράθυρο του Wireshark θα πρέπει τώρα να μοιάζει σε γενικές γραμμές με αυτό που φαίνεται στην εικόνα 3.40. (Δώστε ιδιαίτερη προσοχή στο ελαχιστοποιημένο ποσό πληροφοριών πρωτοκόλλου για όλα τα πρωτόκολλα εκτός από το HTTP και το μεγιστοποιημένο ποσό πληροφοριών πρωτοκόλλου για το HTTP στο παράθυρο packet-header details.)

10. Στις παρακάτω εικόνες φαίνεται η δυνατότητα επιλογής ενός μονό πακέτου και το άνοιγμα αυτού του πακέτου σε νέο παράθυρο

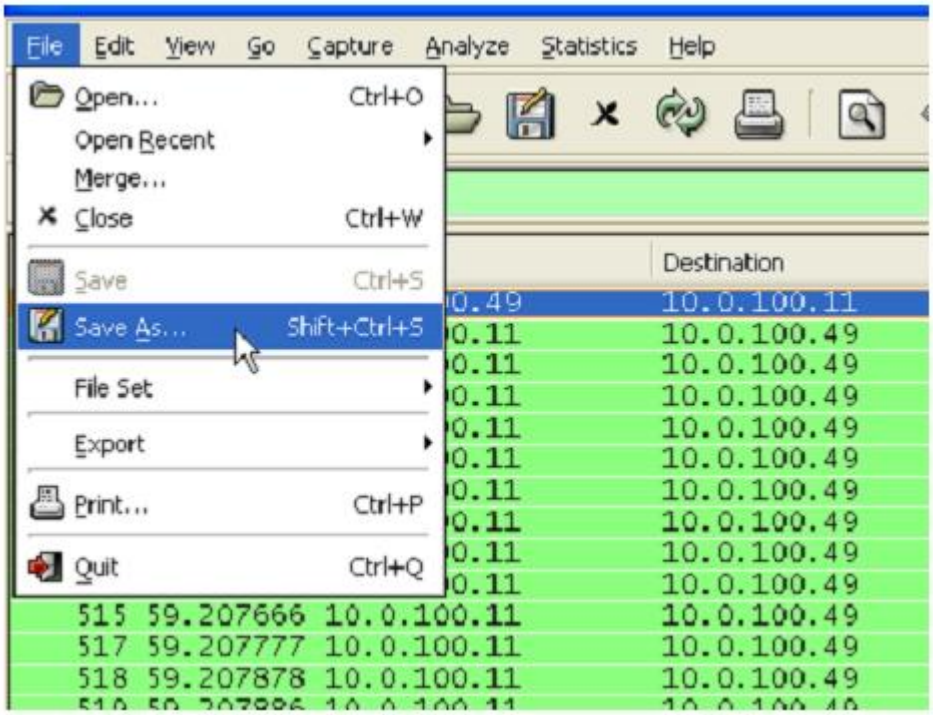


Εικόνα 3.41: Επιλογή μεμονωμένου πακέτου



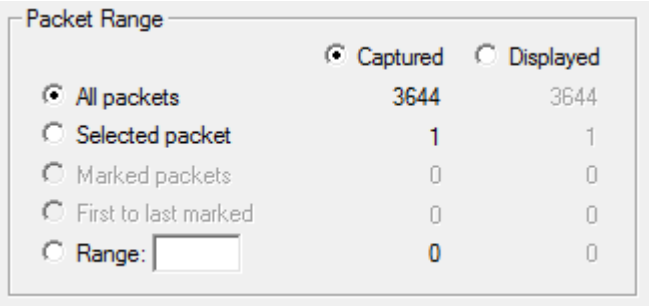
Εικόνα 3.42: Προβολή μεμονωμένου πακέτου

11. Κλείνοντας, μπορούμε να αποθηκεύσουμε την «σύλληψη» μας από το File -> Save As … με μία ονομασία που να μας θυμίζει κάτι χαρακτηριστικό π.χ. 2006-May-25—http κλπ.

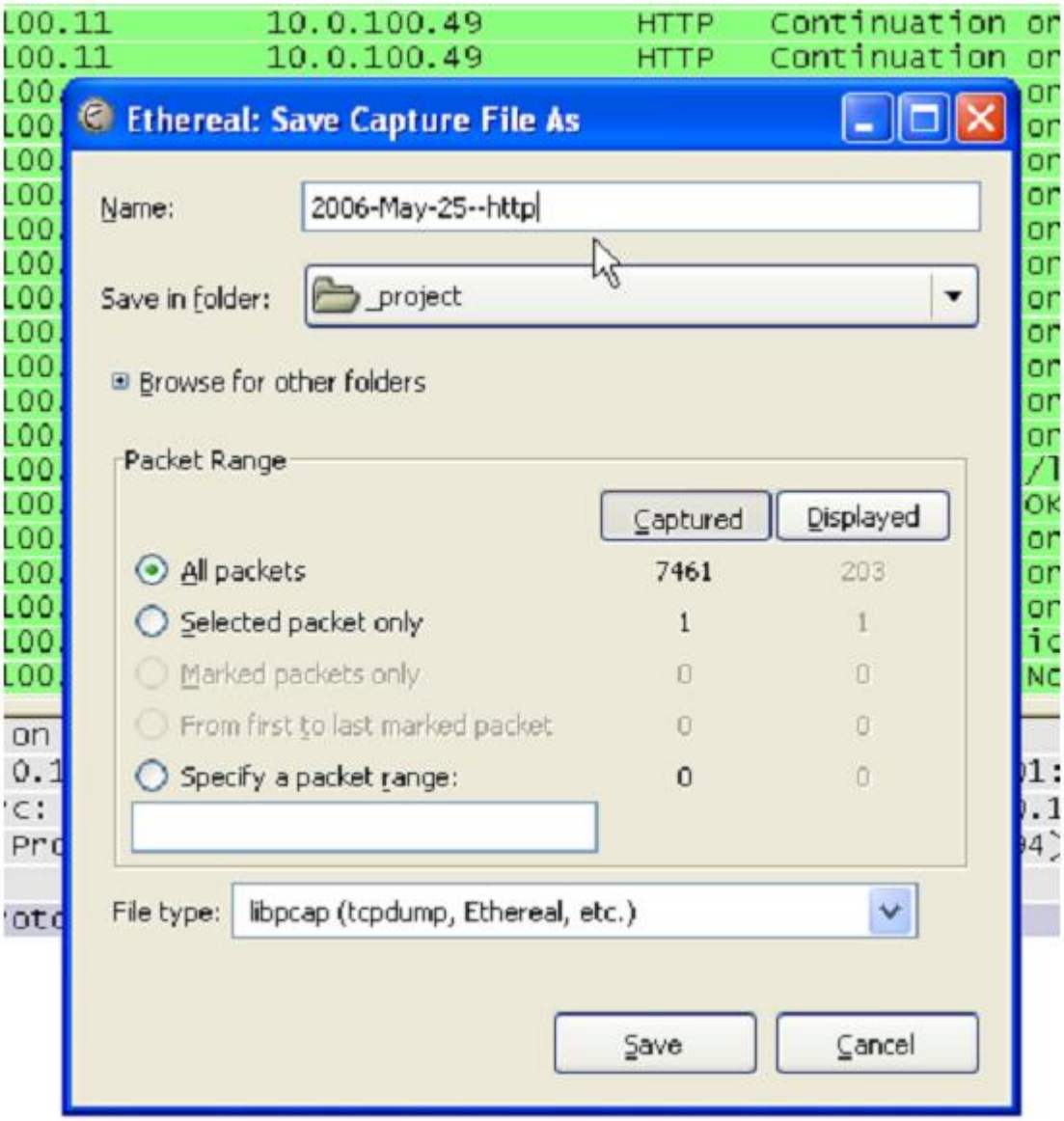


Εικόνα 3.43: Μενού αποθήκευσης αρχείου σύλληψης

Έχουμε επίσης την δυνατότητα να επιλέξουμε αν θέλουμε να αποθηκεύσουμε ένα, όλα, μία περιοχή ή ακόμη μία επιλογή από τα πακέτα που μόλις «συλλάβαμε», όπως φαίνεται στις εικόνες 3.44, 3.45.



Εικόνα 3.44: Επιλογή τρόπου αποθήκευσης



Εικόνα 3.45: Μενού αποθήκευσης επιλεγμένων πακέτων

ΚΕΦΑΛΑΙΟ 4

4. Επίλογος

Με τις υπάρχουσες συνθήκες κάθε διαχειριστής ενός δικτύου αλλά ακόμα και ένας απλός χρήστης αντιμετωπίζει ένα τεράστιο όγκο αρχείων και δεδομένων που κινούνται ασταμάτητα. Πολλά από αυτά είναι αρχεία μέγιστης σημασίας για πολλές επιχειρήσεις και ιδιώτες. Αυτό επιβάλει την προστασία από οποιοδήποτε «παράνομο εισβολέα» στο δίκτυό μας.

Αντιλαμβανόμαστε λοιπόν ότι πολλές φορές ερχόμαστε αντιμέτωποι με καταστάσεις οι οποίες προκαλούνται από τρίτους που μπορεί να έχουν σκοπό απλά να δημιουργήσουν αναστάτωση, ή στη χειρότερη περίπτωση να κλέψουν αρχεία επαγγελματικά ή προσωπικά μέσα από συνεχή παρακολούθηση του δικτύου μας.

Προηγουμένως είδαμε κάποια από τα πιο συνηθισμένα αλλά «ισχυρά» εργαλεία που μας επιτρέπουν να έχουμε τον έλεγχο στο δίκτυό μας. Είναι εργαλεία τα οποία θεωρητικά έχουν σχεδόν την ίδια χρήση αλλά στην ουσία κάποια είναι πολύ διαφορετικά.

Αρχικά όλα τα εργαλεία είναι κατασκευασμένα για τις πλατφόρμες τις Microsoft, τα Windows. Μπορούμε εύκολα να αντιληφθούμε το λόγο, ο οποίος δεν είναι άλλος από τη μαζική παγκόσμια χρήση των Windows. Όλοι οι υπολογιστές παγκοσμίως εκτός ίσως από ελάχιστες εξαιρέσεις χρησιμοποιούν λογισμικό από τη συγκεκριμένη εταιρία. Αυτό έχει ως αποτέλεσμα όλα τα sniffers να έχουν ως βάση χρήσης τα windows και έτσι γίνονται «επιθέσεις» και «παρακολουθήσεις, κυρίως λόγω κάποιων δικλίδων ασφαλείας που παρακάμπτονται πιο εύκολα από έμπειρους hackers και crackers.

Εξετάζοντας τη χρονολογική εξέλιξη των προγραμμάτων βλέπουμε ότι όσα είχαν αναπτυχθεί σε περασμένες δεκαετίες πριν το 2000 έχουν τη δυνατότητα να τρέξουν σε περισσότερες πλατφόρμες οι οποίες χρησιμοποιούνταν περισσότερο. Αυτά είναι το Tcpdump το Wireshark (πρώην Ethereal) και το Kismet. Όσα έχουν αναπτυχθεί αργότερα μέχρι τα τελευταία χρόνια όπως το Cain and Abel και το Carnivore έχουν προσανατολισμό κυρίως για πλατφόρμες της Microsoft όπως και το Microsoft Network Monitor φυσικά.

Ο πίνακας 8 αμέσως μετά δείχνει το διαχωρισμό αυτό:

Πρόγραμμα/Πλατφόρμα	Microsoft Windows	Mac OS	Linux
Cain and Avel	Yes	No	No
Carnivore	Yes	No	No
Kismet	Yes	Yes	Yes
Microsoft network Monitor	Yes	No	No
Tcpdump (windump)	Yes	Yes	Yes
Wireshark (Former Ethereal)	Yes	Yes	Yes

Πίνακας 8: Προγράμματα Σύλληψης και συμβατές πλατφόρμες

Οι σημαντικές διαφορές που μπορούμε να βρούμε ανάμεσα σε αυτά τα προγράμματα είναι κυρίως στον τρόπο χρήσης αλλά και στο λόγο για τον οποίο αρχικά δημιουργήθηκαν.
Κάνοντας αυτό το διαχωρισμό θα κατά λήξουμε στα εξής συμπεράσματα για κάθε ένα από αυτά:

Τα προγράμματα τα οποία αναπτύχθηκαν κυρίως σε πανεπιστήμια και από έμπειρους ακαδημαϊκούς ή προγραμματιστές με σκοπό να διευκολύνουν τους χρήστες είναι κυρίως το Tcpdump και το Wireshark το οποίο αναλύσαμε εκτενέστερα στο προηγούμενο κεφάλαιο. Ο κύριος σκοπός τους είναι να παρέχουν στο διαχειριστή ενός δικτύου τη δυνατότητα να «παρακολουθεί» ο ίδιος την κυκλοφορία στο δίκτυο με πολλές επιλογές πρωτοκόλλων και σύλληψης έτσι ώστε να μπορεί να αποφεύγει προβλήματα στην δικτυακή κυκλοφορία και επίσης ανεπιθύμητες εισβολές. Το Tcpdump είδαμε ότι έχει τη δυνατότητα να διαβάσει αρχεία συλλήψεων

και από άλλα προγράμματα και αυτό το καθιστά ένα από τα σημαντικότερα εργαλεία και βάση για τα υπόλοιπα.

Δύο διαφορετικές περιπτώσεις είναι το Cain and Abel και το Kismet. Το πρώτο είναι ένα εργαλείο κυρίως για αποκατάσταση κωδικών - για Windows- που ίσως έχουμε χάσει ή ξεχάσει. Το Kismet είναι ένα πρόγραμμα με διπλή χρήση. Είναι χρήσιμο αρχικά γιατί μπορεί να εντοπίζει ασύρματα κυρίως δίκτυα (όχι επακριβώς τη θέση τους αλλά την περιοχή) και να λαμβάνει δεδομένα τα οποία αποθηκεύονται για μελλοντική ανάγνωση και από άλλα προγράμματα όπως το Tcpdump για σωστότερη ανάλυση.

Ένα πρόγραμμα με τελείως διαφορετικό προσανατολισμό είναι το Carnivore. Είναι ένα από τα πιο επικίνδυνα προγράμματα αφού είναι σχεδιασμένο κυρίως για να «κλέβει» ,στην ουσία, δεδομένα από υπολογιστές χρησιμοποιώντας κάποια «κλειδιά» που έχουν περαστεί, όπως η παρακολούθηση του Ηλεκτρονικού Ταχυδρομείου για παράδειγμα. Εγκαθίσταται μόνο εντός των Η.Π.Α. αλλά είναι κάτι που ενδιαφέρει όλο τον πλανήτη διότι όλες οι πληροφορίες που λαμβάνουμε ή στέλνουμε στο Διαδίκτυο περνούν κυρίως μέσα από Sites των Η.Π.Α.

Το πιο απλό εργαλείο είναι το εργαλείο της Microsoft το Microsoft Network Monitor το οποίο διευκολύνει πιο άπειρους χρήστες αφού γίνεται online, όταν αναφέρει κάποιος το πρόβλημα που έχει στην ίδια την εταιρία μέσω Internet.

Βλέπουμε λοιπόν ότι με βάση την υπάρχουσα τεχνολογία μας δίνονται πολύ μεγάλες δυνατότητες για παρακολούθηση Δικτύων με διαφορετικούς τρόπους αλλά και διαφορετικούς σκοπούς. Το ίδιο Sniffer λογισμικό στα χέρια δύο διαφορετικών χρηστών μπορεί να χρησιμοποιηθεί είτε απλά για την αποκατάσταση της ομαλής λειτουργίας ενός δικτύου κάτι που είναι εξαιρετικά χρήσιμο κυρίως για επαγγελματίες ή για κάποιο άλλο χειρότερο σκοπό όπως την υποκλοπή δεδομένων.

ΠΗΓΕΣ

1. http://en.wikipedia.org/wiki/History_of_the_Internet
2. http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF
3. http://en.wikipedia.org/wiki/Network_topology#cite_note-FS1037C-1#cite_note-FS1037C-1
4. http://el.wikipedia.org/wiki/OSI
5. http://www.rfc-archive.org/getrfc.php?rfc=871
6. http://el.wikipedia.org/wiki/OSI
7. http://en.wikipedia.org/wiki/Ethernet
8. http://el.wikipedia.org/wiki/Peer-to-peer
9. http://el.wikipedia.org/wiki/Token_ring
10. http://www.ericom.com/serverbased.asp
11. http://el.wikipedia.org/wiki/Packet_sniffer
12. http://en.wikipedia.org/wiki/Ethernet
13. http://cs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm
14. http://www.sc.edu/
15. http://docstore.mik.ua
16. http://mechanicshell.wordpress.com
17. http://www.oxid.it/cain.html
18. http://www.worldlingo.com/ma/enwiki/el/Carnivore_(software)
19. http://athens.indymedia.org
20. http://articles.techrepublic.com
21. http://www.kismetwireless.net/documentation.shtml
22. http://support.microsoft.com/kb/148942/el
23. http://en.wikipedia.org/wiki/Promiscuous_mode
24. http://www.wireshark.org/about.html#authors
25. http://www.syngress.com /online manual/

ΑΝΑΦΟΡΕΣ

1. “Άρθρο από Βικιπαιδεία” (http://en.wikipedia.org/wiki/History_of_the_Internet)
2. “Άρθρο από Βικιπαιδεία” (http://el.wikipedia.org/wiki/BF)
3. “Τοπολογίες Δικτύων από Βικιπαιδεία” (www.wikipedia.org/wiki/Network_topology)
4. “Peer to Peer” (http://el.wikipedia.org/wiki/Peer-to-peer)
5. “Server-Based Computing” (http://www.ericom.com/serverbased.asp)
6. “Ethernet Protocol” Από Βικιπαιδεία, (http://en.wikipedia.org/wiki/Ethernet)
7. “Token ring - Δακτύλιος με κουπόνι” Από Βικιπαιδεία (http://el.wikipedia.org/wiki/Token_ring)
8. “Μοντέλο αναφοράς OSI” από Βικιπαιδεία (http://el.wikipedia.org/wiki/OSI)
9. Άρθρο από τον M. A. Padlipsky (www.rfc-archive.org)
10. “Μοντέλο αναφοράς OSI” από Βικιπαιδεία (http://el.wikipedia.org/wiki/OSI)
11. “Packet sniffer” (http//el.wikipedia.org/wiki/Packet_sniffer)
12. “Packet sniffer”, (http//el.wikipedia.org/wiki/Packet_sniffer)
13. «Ετηερνετ» Από Βικιπαιδεία, (http://en.wikipedia.org/wiki/Ethernet)
14. Βλέπε Λεξικό όρων (Τέλος Εργασίας)
15. Βλέπε Λεξικό όρων (Τέλος Εργασίας)
16. Official site for tcpdump (and libpcap) (http://www.tcpdump.org/)
17. “Tcpdump for Windows” (http://www.winpcap.org/windump/)
18. “Tcpdump for Windows” (http://www.winpcap.org/windump/)
19. “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)
20. “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)
21. “Network troubleshooting tools” Chapter 5.4 (http://docstore.mik.ua)
22. Άρθρο, 5 Ιανουαρίου 2008 “Cain & Abel – το απόλυτο windows hacking tool”http://mechanicshell.wordpress.com)
23. http://www.oxid.it/cain.html
24. “Ηλεκτρονικό Εγχειρίδιο Cain and Abel” http://www.oxid.it/ca_um/
25. http://www.worldlingo.com/ma/enwiki/el/Carnivore_(software)
26. “Άρθρο” Κυριακή 1 Δεκεμβρίου 2002 (http://athens.indymedia.org)

27. Άρθρο από τον James McPherson 09 Ιαν 2001 (http://articles.techrepublic.com)
28. Άρθρο από τον James McPherson 09 Ιαν 2001 (http://articles.techrepublic.com)
29. "Kismet Readme Manual" από τον Mike Kershaw 2010 (http://www.kismetwireless.net/documentation.shtml)
30. "Kismet Readme Manual" από τον Mike Kershaw 2010 (http://www.kismetwireless.net/documentation.shtml)
31. "Κεντρική σελίδα Υποστήριξης Microsoft" (http://support.microsoft.com/kb/148942/el)
32. "Ετερόκλητη Λειτουργία" (http://en.wikipedia.org/wiki/Promiscuous_mode)
33. "Λίστα συγγραφέων Wireshark" (www.wireshark.org/about.html#authors)
34. "Λίστα με τα 752 πρωτόκολλα που υποστηρίζονται" (Online Wireshark User's Manual, www.syngress.com)
35. Online Wireshark User's Manual, www.syngress.com (σελ. 66)
36. Online Wireshark User's Manual, www.syngress.com (σελ. 69)
37. Online Wireshark User's Manual, www.syngress.com (σελ. 70)
38. Μπορούμε να το κάνουμε απευθείας στα εξής sites : www.cert.org ή www.incidents.org

ΕΥΡΕΤΗΡΙΟ - ΛΕΞΙΚΟ ΞΕΝΗΣ ΟΡΟΛΟΓΙΑΣ

ARCnet είναι ένα πρωτόκολλο δικτύων τοπικής περιοχής (τοπικό LAN), παρόμοιο με το Ethernet.

ARP (Address Resolution Protocol) (Ελλ: Πρωτόκολλο Μετατροπής Διεύθυνσης) Το πρωτόκολλο αυτό είναι ένα χαμηλού επιπέδου πρωτόκολλο το οποίο αντιστοιχίζει δυναμικά μια λογική διεύθυνση (για παράδειγμα μία διεύθυνση IP) στη σωστή φυσική διεύθυνση. Χρησιμοποιείται στα δίκτυα που έχουν δυνατότητα εκπομπής όπως για παράδειγμα το Ethernet.

Backbone [ραχοκοκαλιά] αναφέρεται στις κύριες διαδρομές δεδομένων μεταξύ μεγάλων στρατηγικά δικτύων και δρομολογητών στο Διαδίκτυο

Bitnet ήταν το συνεταιριστικό πανεπιστημιακό δίκτυο που ιδρύεται το 1981 στο Πανεπιστήμιο της Νέας Υόρκης (**CUNY**). Η πρώτη σύνδεση δικτύων ήταν μεταξύ **CUNY** και **Yale**.

Browser *φυλλομετρητής* Ιστού π.χ Internet explorer, firefox, opera

Buffer μνήμη που χρησιμοποιείται για την προσωρινή αποθήκευση παραγωγή ή εισαγωγή δεδομένων

Bus Network topology (Linear, Linear Bus) αρτηρίας είναι μια δικτυακή αρχιτεκτονική στην οποία ένα σύνολο π.χ. οι πελάτες συνδέονται μέσω μιας κοινής γραμμής επικοινωνιών, που λέγεται Δίαυλος.

CERN (Conseil **E**uropeenne pour la **R**echerche **N**ucleaire) είναι το μεγαλύτερο σε έκταση (πειραματικό) κέντρο πυρηνικών ερευνών και ειδικότερα επί της σωματιδιακής φυσικής στον κόσμο. Βρίσκεται δυτικά της Γενεύης, στα σύνορα Ελβετίας και Γαλλίας. Ιδρύθηκε το 1954 από δώδεκα ευρωπαϊκές χώρες και σήμερα

αριθμεί 20 κράτη-μέλη, μεταξύ των οποίων και η Ελλάδα, η οποία είναι και ιδρυτικό μέλος

Client-server model [μοντέλο πελάτη- εξυπηρετητή] ο client-πελάτης θέτει μια αίτηση και ο server-εξυπηρετητής επιστρέφει μια ανταπόκριση ή κάνει μια σειρά από ενέργειες

Crackers βλέπε *Hackers- Crackers*

Snoop Capture file Το Snoop αρχείο είναι ένα αρχείο σύλληψης ικανό να διαβάσει και να ερμηνεύσει τα πακέτα (ή περίληψη πακέτων) σχεδόν χωρίς μεγάλη προσπάθεια. Είναι μια δυνατή επιλογή με μεγάλη δύναμη φιλτραρίσματος πακέτων σχεδόν αντίστοιχη με το tcpdump.

DARPA (Defense Advanced Research Projects Agency) είναι υπηρεσία του υπουργείου Άμυνας των Η.Π.Α. αρμόδια για την ανάπτυξη τεχνολογίας για στρατιωτικούς σκοπούς
Dissector είναι κάποιο μέρος ενός στοιχείου πακέτων που πρέπει να καταχωρηθεί ώστε να είναι εύκολα αντιληπτό.

Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών, αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο **802.3** για ενσύρματα τοπικά δίκτυα (LAN).

FDDI (Fiber Distributed Data Interconnect) παρέχει ταχύτητα 100 MBIT/S για μετάδοση στοιχείων σε ένα δίκτυο τοπικής περιοχής που μπορεί να επεκτείνει τη μετάδοση μέχρι 200 χιλιόμετρα
Fidonet είναι ένα παγκόσμιο δίκτυο υπολογιστών που χρησιμοποιείται για την επικοινωνία ανάμεσα σε συστήματα πινάκων δελτίων. Ήταν το δημοφιλέστερο στις

αρχές της δεκαετίας του '90, πριν από την εύκολη και προσιτή πρόσβαση στο Διαδίκτυο

Fully connected mesh τύπος τοπολογίας δικτύων στον οποίο κάθε ένας από τους κόμβους του δικτύου συνδέεται με κάθε έναν από τους άλλους κόμβους στο δίκτυο με ένα από σημείο σε σημείο το οποίο καθιστά πιθανό τα στοιχεία να διαβιβαστούν ταυτόχρονα από οποιοδήποτε ενιαίο κόμβο σε όλους τους άλλους κόμβους. Η φυσική πλήρως συνδεδεμένη τοπολογία πλέγματος είναι γενικά πάρα πολύ δαπανηρή και σύνθετη για τα πρακτικά δίκτυα, αν και η τοπολογία χρησιμοποιείται όταν υπάρχει μόνο ένας μικρός αριθμός κόμβων που διασυνδέονται

Gigabit Ethernet (GbE or 1 GigE) είναι ένας όρος περιγράφοντας τις διάφορες τεχνολογίες για τη διαβίβαση των πλαισίων Ethernet με ρυθμό ενός gigabit ανά δευτερόλεπτο, όπως καθορίζεται από το IEEE 802.3-2008 πρότυπο.

Hackers – Crackers “χάκερς” είναι εκείνοι που ενδιαφέρονται έντονα για τις μυστικές και “κρυφές” λειτουργίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Προσπαθούν να ανακαλύψουν τα “κενά” στα συστήματα υπολογιστών καθώς και τους λόγους ύπαρξης αυτών των “κενών”. Οι “χάκερς” αναζητούν σταθερά πρόσθετη γνώση, μοιράζονται ελεύθερα ότι έχουν ανακαλύψει και ποτέ δεν καταστρέφουν δεδομένα σκοπίμως.
“κράκερς” είναι εκείνοι που διεισδύουν ή διαφορετικά παραβιάζουν την ακεραιότητα ενός συστήματος, με κακή πρόθεση. Έχοντας αποκτήσει παράνομη πρόσβαση, οι “κράκερς” καταστρέφουν σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν σοβαρά προβλήματα στα θύματά τους. Οι “κράκερς” χαρακτηρίζονται γενικά από κακόβουλες πράξεις.

Host υπολογιστής ή λογισμικό που παρέχει υπηρεσίες σε ένα δίκτυο, ή ένας υπολογιστής που παρέχει τις υπηρεσίες στις μικρότερες ή λιγότερο ικανές συσκευές

Hub κόμβος - διανομέας σε ένα δίκτυο υπολογιστών, μια δικτυακή συσκευή που επιτρέπει την διασύνδεση πολλών υπολογιστών σχηματίζοντας ένα δίκτυο αστέρα..

Οι υπολογιστές μπορούν να επικοινωνούν απευθείας ο ένας με τον άλλον μέσω αυτού του δικτύου

Hybrid Είναι υπολογιστές που παρουσιάζουν τα χαρακτηριστικά των αναλογικών ηλεκτρονικών υπολογιστών και των ψηφιακών ηλεκτρονικών υπολογιστών μαζί. Το ψηφιακό μέρος λειτουργεί κανονικά ως ο υπεύθυνος της επεξεργασίας και προβλέπει λογικές πράξεις, ενώ το αναλογικό μέρος λειτουργεί κανονικά ως λύτης των διαφορικών εξισώσεων.

Idle network Δίκτυο αδρανές

ICMP (Internet Control Message Protocol) Είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο..

ISO ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, διακριτική ονομασία: ISO), είναι μια διεθνής οργάνωση δημιουργίας και έκδοσης προτύπων που αποτελείται από αντιπροσώπους των εθνικών οργανισμών τυποποίησης. Ο οργανισμός ιδρύθηκε στις 23 Φεβρουαρίου του 1947 και παράγει τα παγκόσμια βιομηχανικά και εμπορικά πρότυπα, τα επονομαζόμενα πρότυπα ISO

LAN είναι ένα δίκτυο υπολογιστών που καλύπτει μια μικρή φυσική περιοχή, όπως ένα σπίτι, ένα γραφείο, ή μικρές ομάδες κτηρίων, όπως ένα σχολείο

Libpcap [lib+pcap] (**p**acket **cap**ture) το libpcap αναπτύχθηκε αρχικά από τους υπεύθυνους για την ανάπτυξη του tcpdump, είναι μια βιβλιοθήκη όπου καταγράφονται όλα τα πακέτα οποιουδήποτε επιπέδου που συλλαμβάνονται

MAC address (Media Access Control address) είναι ένα μοναδικό προσδιοριστικό που ορίζεται στην κάρτα δικτύου δηλαδή από τον κατασκευαστή της για τον ακριβή προσδιορισμό της θέσης στο δίκτυο.

MAN (metropolitan area network) είναι ένα μεγάλο δίκτυο υπολογιστών που εκτείνεται συνήθως μια πόλη ή μια μεγάλη πανεπιστημιούπολη

Mesh Network topology είναι ένας τύπος δικτύωσης όπου κάθε κόμβος στο δίκτυο μπορεί να ενεργήσει ως ανεξάρτητος δρομολογητής, ανεξάρτητα από εάν συνδέεται με ένα άλλο δίκτυο ή όχι

Monitoring (μετ. παρακολούθηση) ο όρος network monitoring περιγράφει τη χρήση ενός συστήματος που ελέγχει και παρακολουθεί συνεχώς το δίκτυο υπολογιστών για τυχών σφάλματα ή για κάθε περίπτωση διακοπής λειτουργίας , όπως για παράδειγμα του ηλεκτρονικού ταχυδρομείου.

Network layer (στρώμα δικτύων) είναι το στρώμα 3 των επτά-στρωμάτων Προτύπου της OSI για τη δικτύωση υπολογιστών.

NIC card (Network Interface Card) η NIC αποδίδεται ως προσαρμογέας δικτύου που υλοποιει την διεπαφή επικοινωνίας κλπ

OSI Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI (αγγλ. *OSI reference model*) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως *μοντέλο των επτά επιπέδων*.

Packet switching Ο ορός αναφέρεται στην τεχνική προώθησης πληροφορίας με μεταγωγή πακέτων

PAN (**personal area network**) είναι ένα δίκτυο υπολογιστών που χρησιμοποιείται για την επικοινωνία μεταξύ των συσκευών υπολογιστών, συμπεριλαμβανομένων των

τηλεφώνων και των προσωπικών ψηφιακών βοηθών, στην εγγύτητα στο σώμα ενός ατόμου

Partially connected mesh (or simply 'mesh') τοπολογία δικτύων στην οποία μερικά μέρη του δικτύου συνδέονται με περισσότερους από έναν κόμβους στο δίκτυο με μια από σημείο σε σημείο σύνδεση

Peer-to-Peer είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα

Plaintext επικοινωνία Είναι επικοινωνία μεσω μη κρυπτογραφημένου κειμένου, απλης μορφής

Promiscuous μετ. = ανακατωμένος, ετερόκλητος, ανάμικτος, αδιάκριτος, επιπόλαιος, πρόχειρος. Είναι διαμόρφωση μιας κάρτας δικτύου που επιτρέπει να καταγραφεί όλη η κυκλοφορία που θα λαμβάνει. Χαρακτηριστικό δικτύωσης για καταγραφή οπτικού υλικού όπως video ή εικόνας.

RFC Requests for Comments είναι μια σειρά κειμένων (εγγράφων) και σημειώσεων για την τεχνική και την οργάνωση που διέπουν το Internet ξεκινώντας από το 1969.

Ring Network topology δακτύλιος είναι μια τοπολογία δικτύων στην οποία κάθε κόμβος συνδέεται με ακριβώς δύο άλλους κόμβους, διαμορφώνοντας μια ενιαία συνεχή διάβαση για τα σήματα μέσω κάθε κόμβου - ένα δαχτυλίδι

Router (δρομολογητής) θεωρείται ένα ειδικού σκοπού συσκευή ο οποίος κατευθύνει τα πακέτα δεδομένων στο δίκτυο. Είναι συσκευές που μπορούν να ανιχνεύσουν εάν ένα μέρος του δικτύου δεν λειτουργεί ή βρίσκεται σε συμφόρηση και να επανακατευθύνουν την πληροφορία.

Server (εξυπηρετητής) είναι ένας συνδυασμός από hardware ή software σχεδιασμένος για να παρέχει υπηρεσίες σε πελάτες

Server-based μοντέλο *βλέπε client-server model*

Sniffing (παρακολούθηση) χρησιμοποιείται σαν όρος της διαδικασίας σύλληψης πακέτων σε ένα δίκτυο

Spoofing Ο όρος **IP spoofing** στην επιστήμη των υπολογιστών αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.

Star Network topology αστέρας με απλούστερη μορφή του, ένα δίκτυο αστέρα αποτελείται από το ένα κεντρικό μεταγωγέα, hub ή υπολογιστή, ο οποίος ενεργεί ως αγωγός για να διαβιβαστούν τα μηνύματα

Switch (μεταγωγέας) είναι μια μικρή συσκευή που επιτυγχάνει διασύνδεση υπολογιστών σε χαμηλό επίπεδο. Τεχνικά, οι switches λειτουργούν στο επίπεδο 2 (Data Layer) του OSI Model.

TCP/IP *(Transmission Control Program/Internet Protocol=Πρόγραμμα Ελέγχου Μετάδοσης και πρωτόκολλο του Internet)'* είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων.

Token Ring είναι ένας τύπος τοπικού δικτύου υπολογιστών

Tree επίσης γνωστός ως ιεραρχικό δίκτυο, τύπος τοπολογίας δικτύων στον οποίο ένας κεντρικός κόμβος "ρίζα" (το κορυφαίο επίπεδο της ιεραρχίας) συνδέεται με έναν ή περισσότερους άλλους κόμβους που είναι ένα επίπεδο χαμηλότερα στην ιεραρχία

Troubleshooting ανίχνευση λαθών σε ένα δίκτυο με τη βοήθεια εξειδικευμένου λογισμικού

Usenet είναι ένα παγκοσμίως διανεμημένο σύστημα επικοινωνίας και συζήτησης Διαδικτύου

WAN (wide area network) είναι ένα δίκτυο υπολογιστών που καλύπτει μια ευρεία περιοχή, δηλ. οποιοδήποτε δίκτυο του οποίου οι συνδέσεις επικοινωνιών, διασχίζουν τα μητροπολιτικά, περιφερειακά, ή εθνικά όρια

WLAN (Wireless LAN) ασύρματο LAN

WMAN (Wireless MAN) ασύρματο MAN

WPAN (Wireless PAN) ασύρματο PAN

WWAN (Wireless WAN) ασύρματο WAN