



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ
ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ



ΕΣΩΤΕΡΙΚΗ
ΥΠΗΡΕΣΙΑ
ΕΚΠΑΙΔΕΥΣΗΣ
ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ
ΚΕ.Κ. ΠΕ.Σ.Σ.Ε.

ΕΠ ΚτΠ
Χρηματοδότηση:
Ευρωπαϊκό Κοινωνικό Ταμείο: 75%
Εθνικοί Πόροι: 25%

Εκπαιδευτικό Υλικό για την Ενότητα

«Μηχανισμοί και εργαλεία διαχείρισης ΣΕΠΕΗΥ με Windows Server
2003 και Windows XP»

Ανάδοχος: Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών

Ιούνιος 2008

Αναπτύχθηκε στο πλαίσιο υλοποίησης του Υποέργου 2
«Πρακτική Εκπαίδευση Εκπαιδευτικών Πληροφορικής»

της Πράξης «Δράσεις Επιμόρφωσης Εκπαιδευτικών Πληροφορικής»
της Κατηγορίας Πράξεων 1.2.2

«Επιμόρφωση εκπαιδευτικών και Πιστοποίηση»
του Μέτρου 1.2

«Εισαγωγή και Αξιοποίηση των Νέων Τεχνολογιών στην Εκπαίδευση»

Περιεχόμενα

1	Εισαγωγή	4
2	Κονσόλες Διαχείρισης - MMC Consoles (Security Configuration and Analysis)	5
3	Διαχείριση Συμβάντων - Event Viewer.....	19
4	Διαχείριση Συσκευών - Device Manager (Hidden Devices)	23
5	Διαχείριση Υπηρεσιών - Services.....	26
6	Remote Desktop.....	30
7	Scheduled Tasks	33
8	Dependency Walker	40
9	Έλεγχος δίσκων - HD Tune	43
10	Έλεγχος μνήμης - RMMA	46
11	Σημεία εκκίνησης προγραμμάτων - AutoRuns	49
12	Διαχείριση Διεργασιών - Process Explorer.....	52
13	Δομημένη Καλωδίωση	56
13.1	Κατασκευή καλωδίου UTP Category 5 / 5E	56
13.2	Οδηγίες ελέγχου utp καλωδίων	59
14	Ασκήσεις	64

1 Εισαγωγή

Στο παρόν παρουσιάζονται βασικές εργασίες διαχείρισης συστημάτων Windows Σχολικών Εργαστηρίων. Συγκεκριμένα παρουσιάζονται τα ακόλουθα θέματα:

1. Η χρήση κονσολών για τη διευκόλυνση διαφορετικών διαχειριστικών διαδικασιών.
2. Η Διαχείριση Συμβάντων με χρήση του Event Viewer
3. Η Διαχείριση Συσκευών με χρήση του Device Manager
4. Η Διαχείριση Υπηρεσιών μέσα από την κονσόλα Services
5. Η χρήση του Remote Desktop για την απομακρυσμένη πρόσβαση και διαχείριση συστημάτων
6. Ο χρονοπρογραμματισμός περιοδικών διαχειριστικών εργασιών με χρήση των Scheduled Tasks
7. Η εξεύρεση συσχετίσεων μεταξύ προγραμμάτων και βιβλιοθηκών με χρήση του Dependency Walker, με σκοπό την αντιμετώπιση προβλημάτων στην ορθή εκτέλεση εφαρμογών
8. Ο Έλεγχος δίσκων με χρήση του εργαλείου HD Tune
9. Ο Έλεγχος μνήμης με χρήση του εργαλείου RMMA
10. Ο έλεγχος των σημείων εκκίνησης προγραμμάτων με χρήση του εργαλείου AutoRuns
11. Η Διαχείριση Διεργασιών με το εργαλείο Process Explorer, που είναι κατά πολύ ανώτερο του Task Manager
12. Εργασίες Δομημένης Καλωδίωσης με κατασκευή και έλεγχο καλωδίων UTP Cat 5/5e
13. Ασκήσεις στα ανωτέρω αντικείμενα.

Το υλικό συμπληρώνεται από την πρώτη ενότητα των διαφανειών των ημερήσιων σεμιναρίων Υπευθύνων ΣΕΠΕΗΥ (Συστηματικές Εργασίες).

2 Κονσόλες Διαχείρισης - MMC Consoles (Security Configuration and Analysis)

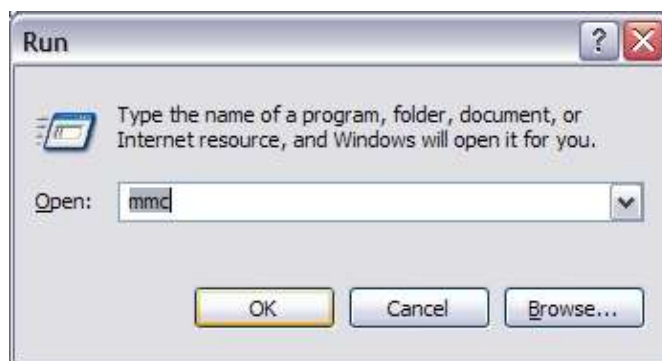
Για την πραγματοποίηση σύνθετων διαχειριστικών εργασιών στα υπολογιστικά συστήματα Windows Server 2003 και Windows XP, αξιοποιείται η Microsoft Management Console (MMC). Στην MMC μπορούν να συνδυαστούν τα απαραίτητα διαχειριστικά εργαλεία, δημιουργώντας ένα ολοκληρωμένο περιβάλλον χρήσης τους.

Το MMC μπορεί να χρησιμοποιηθεί με δύο διαφορετικούς τρόπους:

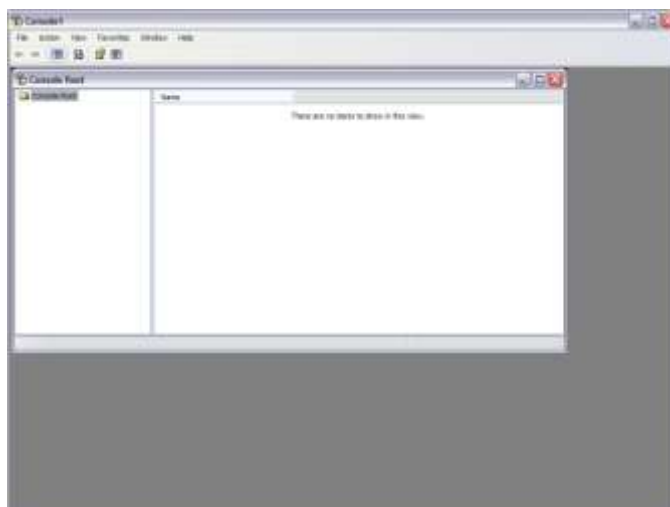
1. σε user mode, όπου ήδη περιλαμβάνει ένα σύνολο βασικών διαχειριστικών εργαλείων, π.χ. επισκόπηση των συμβάντων του ΛΣ (Event Viewer), Διαχείριση Διαμοιραζόμενων φακέλων (Shared Folders), Διαχείριση Συσκευών Συστήματος (Device Manager) κ.α.
2. σε author mode, όπου ο διαχειριστής μπορεί να εντάξει τα απαραίτητα για αυτόν διαχειριστικά εργαλεία.

Στις επόμενες παραγράφους παρουσιάζεται ο τρόπος χρήσης της MMC σε author mode, για την αξιοποίηση του εργαλείου «Security Configuration and Analysis».

Για να φορτώσουμε κάποια MMC Console, τρέχουμε από Start —Run το mmc:

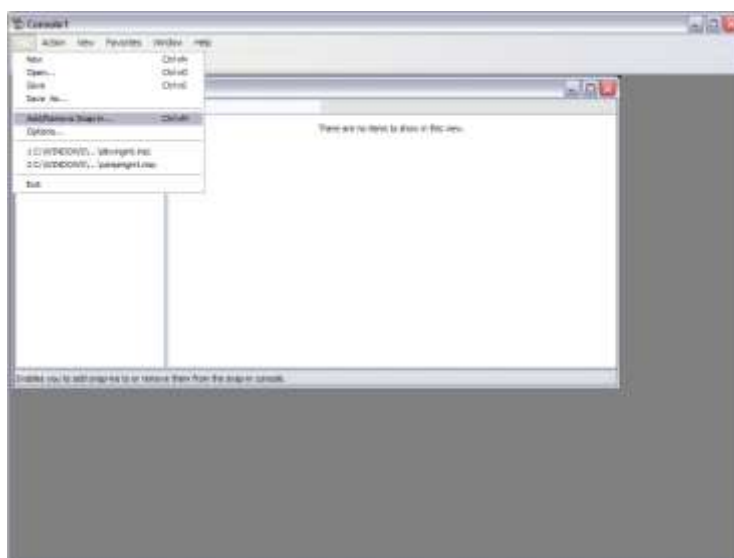


Εικόνα 2-1



Εικόνα 2-2

Για την προσθήκη μιας MMC Console επιλέγουμε File → Add/Remove Snap-In:



Εικόνα 2-3



Εικόνα 2-4

Πατάμε το κουμπί Add για να δούμε τα διαθέσιμα Snap-Ins:



Εικόνα 2-5

Για παράδειγμα επιλέγουμε το Snap-In “Security Configuration and Analysis”:

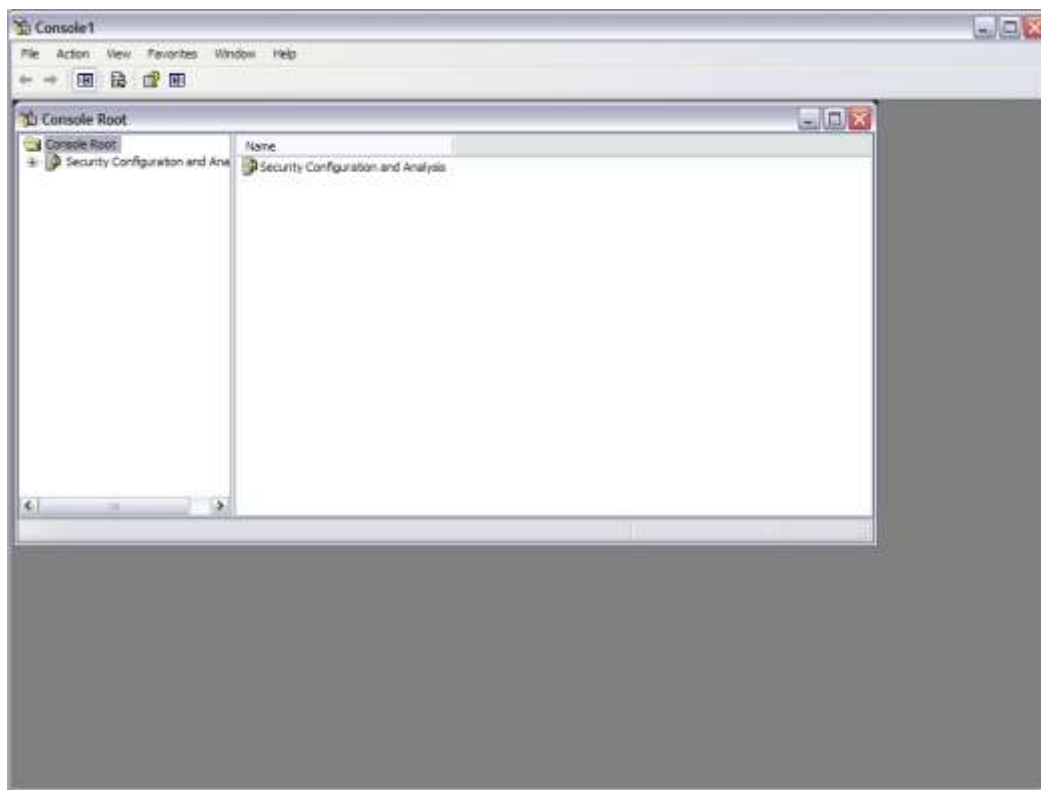


Εικόνα 2-6

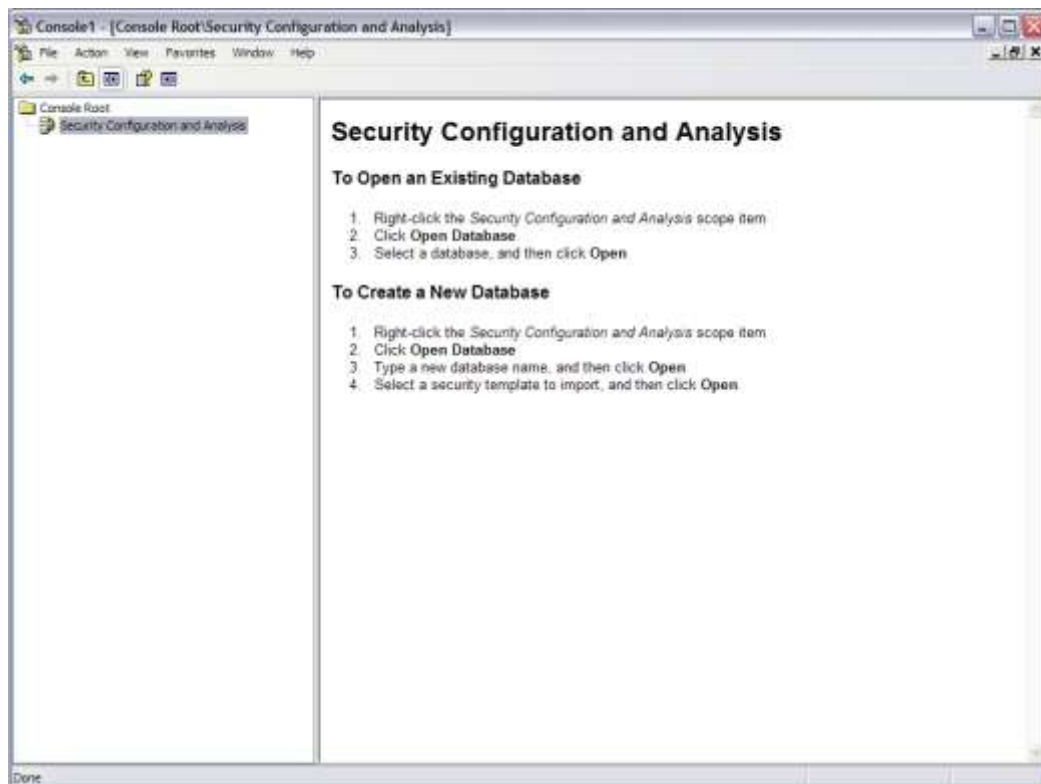
Πατάμε στο κουμπί Add, μετά στο κουμπί Close και κατόπιν στο κουμπί OK:



Εικόνα 2-7

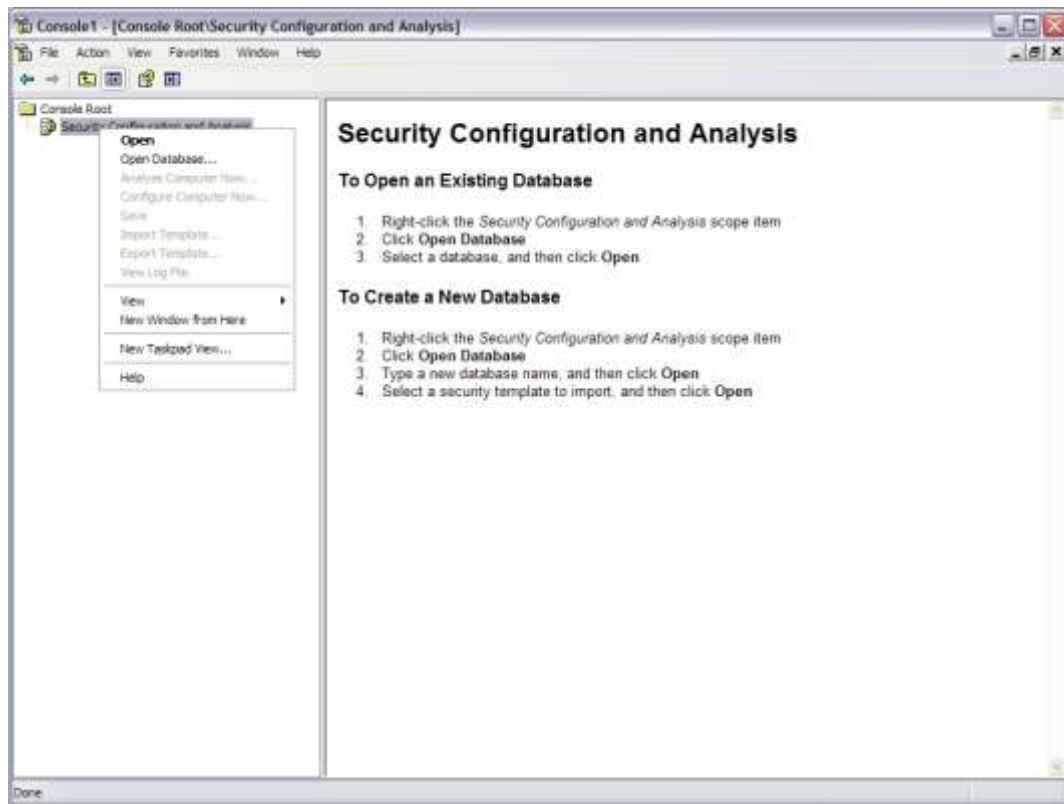


Εικόνα 2-8



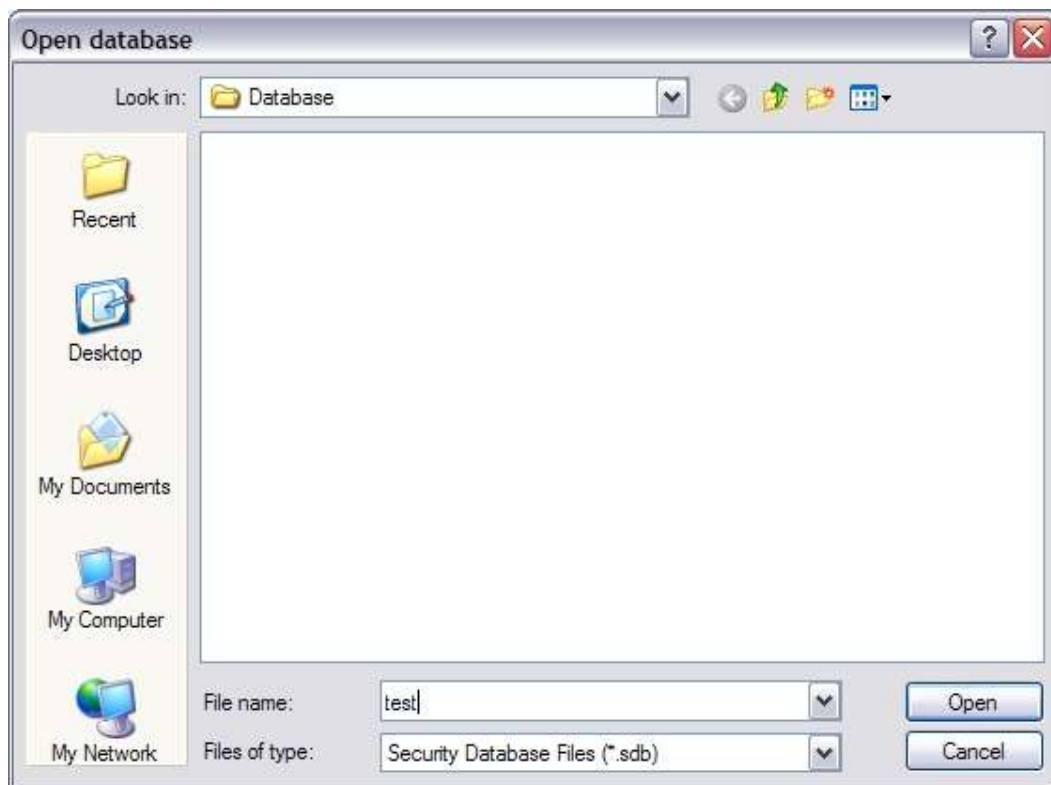
Εικόνα 2-9

Με δεξί κλικ επιλέγουμε το Open Database:



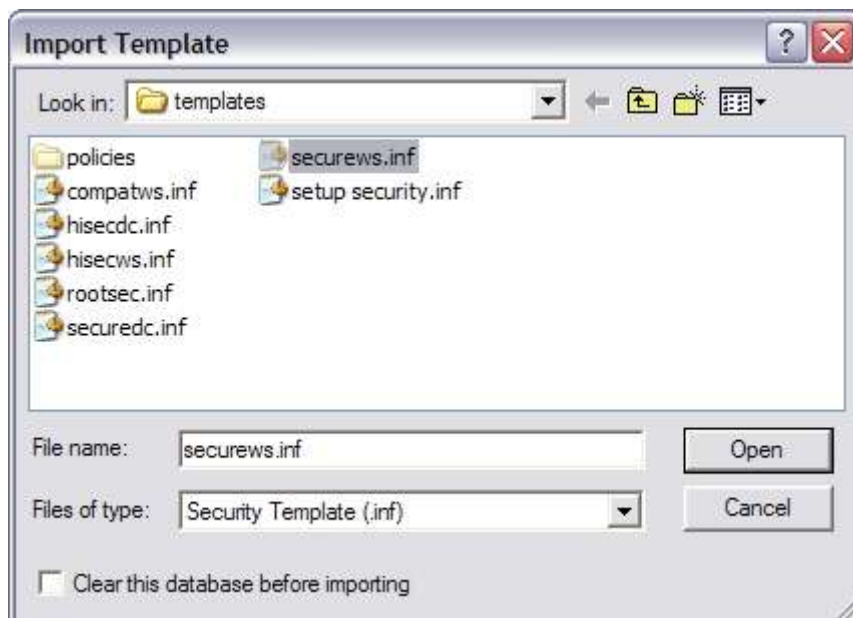
Εικόνα 2-10

Επιλέγουμε όνομα για τη database που θα δημιουργηθεί:



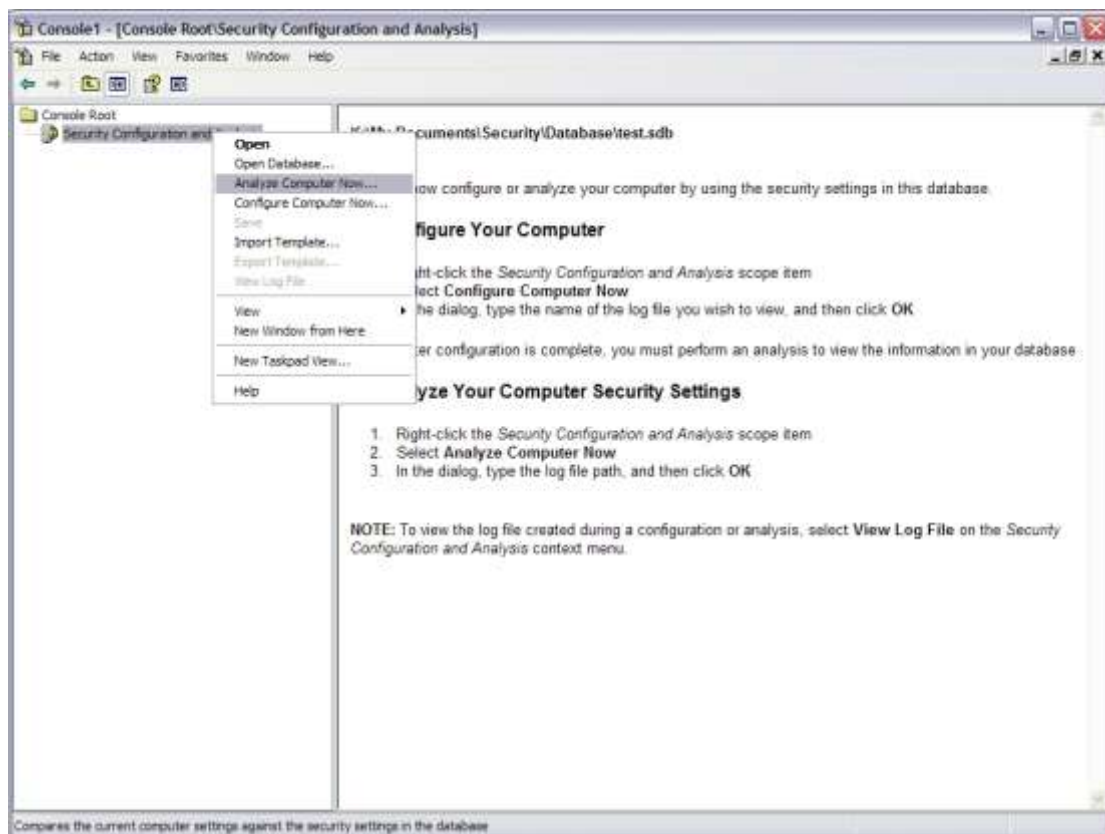
Εικόνα 2-11

Επιλέγουμε template βάσει του οποίου θέλουμε να ρυθμίσουμε το σύστημά μας:



Εικόνα 2-12

Κατόπιν δεξί κλικ και επιλέγουμε “Analyze Computer Now”:



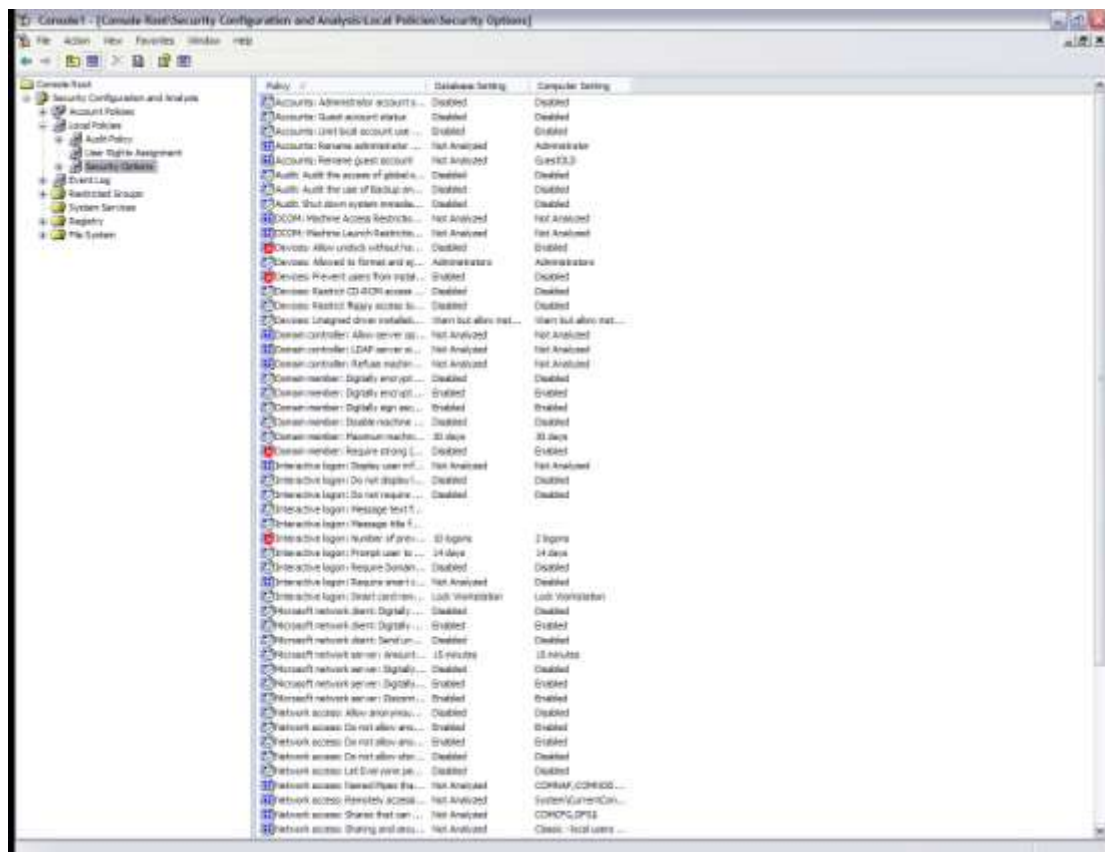
Εικόνα 2-13

Επιλέγουμε κατάλογο για το log file:



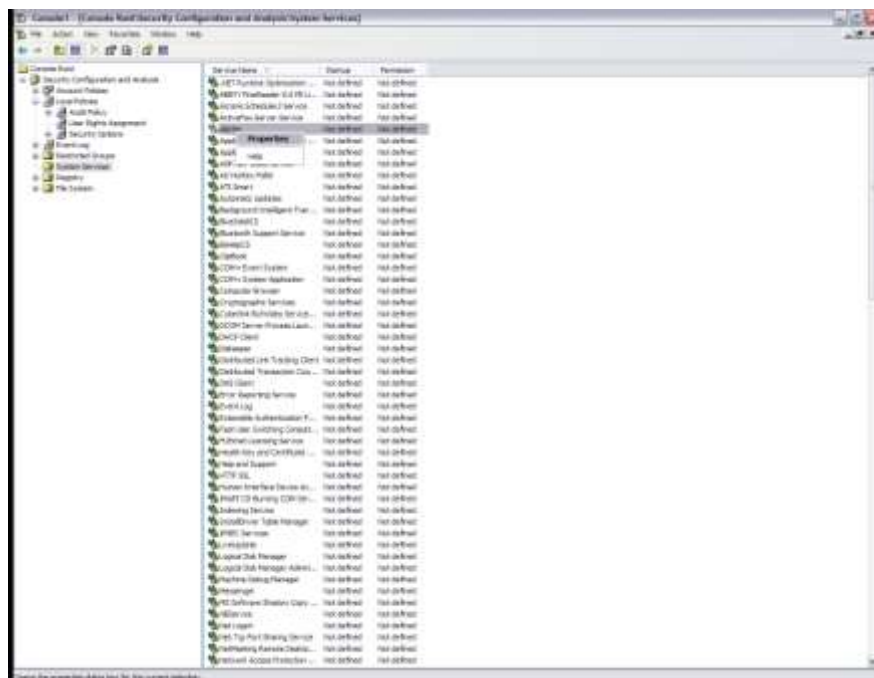
Εικόνα 2-14

Στην επόμενη οθόνη εμφανίζονται τα αποτελέσματα της ανάλυσης. Με πράσινο είναι όσα συμφωνούν με το template, με κόκκινο όσα δε συμφωνούν ενώ ενδέχεται να υπάρχουν και επιλογές που δεν αναλύθηκαν γιατί δεν υπήρχαν στο template:



Εικόνα 2-15

Από την επιλογή System Services, με δεξί κλικ σε κάποια υπηρεσία επιλέγουμε Properties:

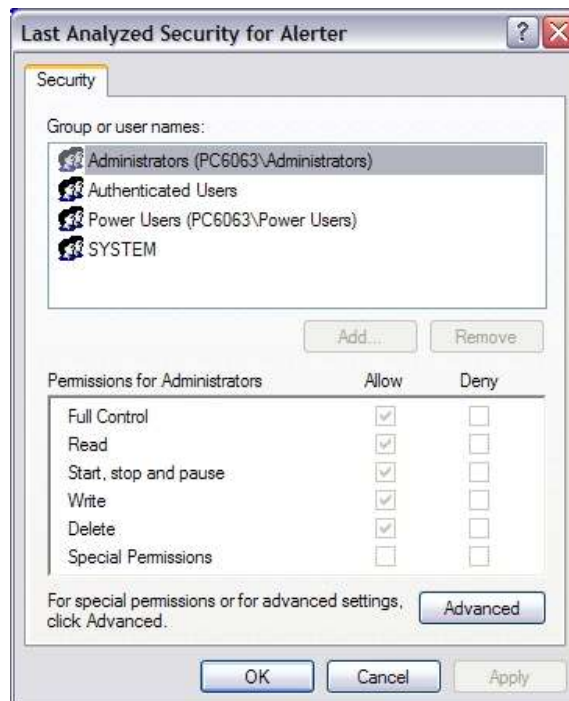


Εικόνα 2-16



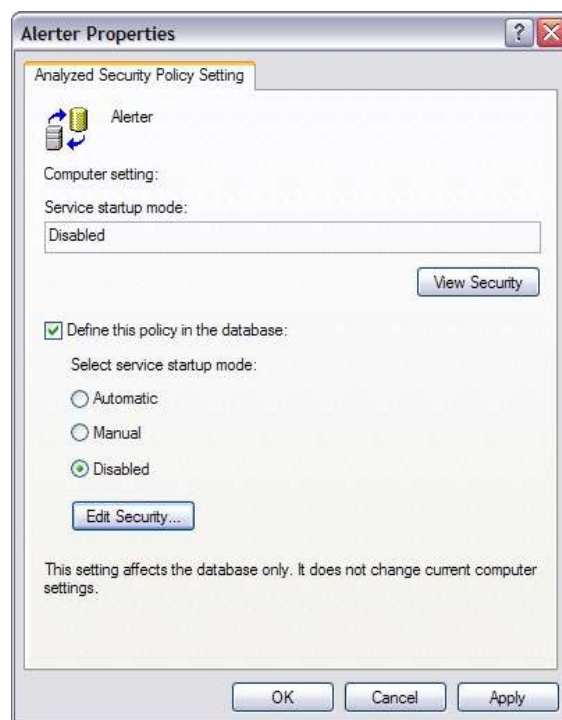
Εικόνα 2-17

Πατώντας στο κουμπί “View Security” βλέπουμε την καρτέλα Security για την υπηρεσία:



Εικόνα 2-18

Επιλέγοντας “Define this policy in the database” και κατόπιν πατώντας στο κουμπί “Edit Security”:



Εικόνα 2-19

Μπορούμε να αλλάξουμε την καρτέλα Security για την υπηρεσία:



Εικόνα 2-20

3 Διαχείριση Συμβάντων - Event Viewer

Για τη γρήγορη επισκόπηση του αρχείου καταγραφής συμβάντων χρησιμοποιείται το εργαλείο Event Viewer, μέσα από την MMC σε user mode. Σε κάθε σύστημα Windows πραγματοποιούνται καταγραφές για τις ακόλουθες κατηγορίες συμβάντων:

1. Application
2. Security
3. System

Ανάλογα με τις επιπλέον λειτουργίες ή υπηρεσίες που είναι εγκατεστημένες στο σύστημα είναι δυνατόν να πραγματοποιούνται καταγραφές συμβάντων για περισσότερες κατηγορίες, όπως για παράδειγμα:

1. DNS Server, για τη λειτουργία της υπηρεσίας DNS,
2. Directory Service και File Replication Service για τη λειτουργία του Server ως Domain Controller.

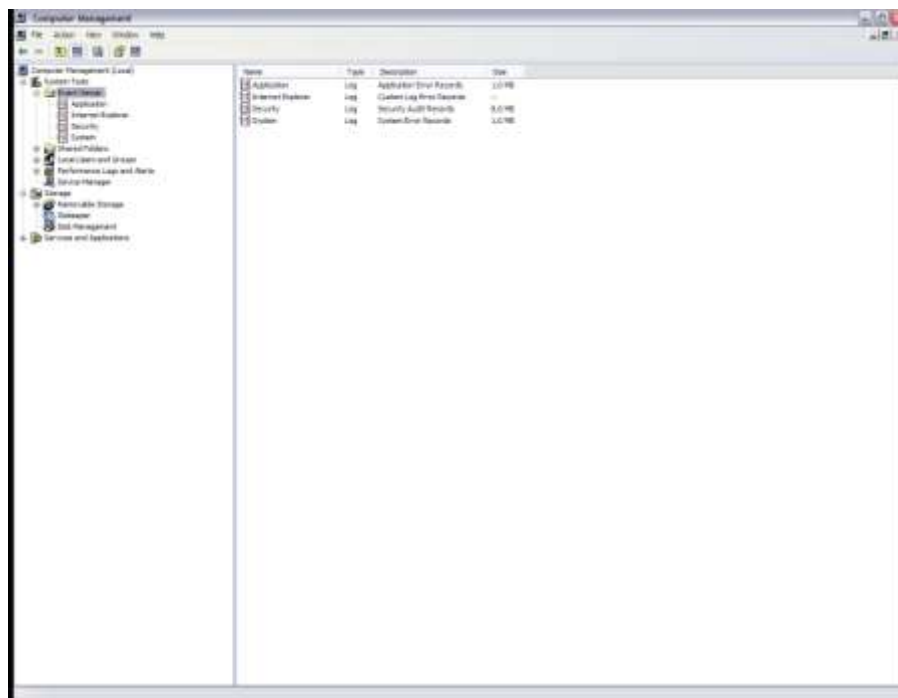
Κάθε καταγραφή συμβάντος κατηγοριοποιείται ως προς την κρισιμότητά της σε:

1. Λάθος (Error)
2. Προειδοποιητικό μήνυμα (Warning)
3. Πληροφοριακό μήνυμα (Information)

Για κάθε συμβάν καταγράφονται τα ακόλουθα στοιχεία:

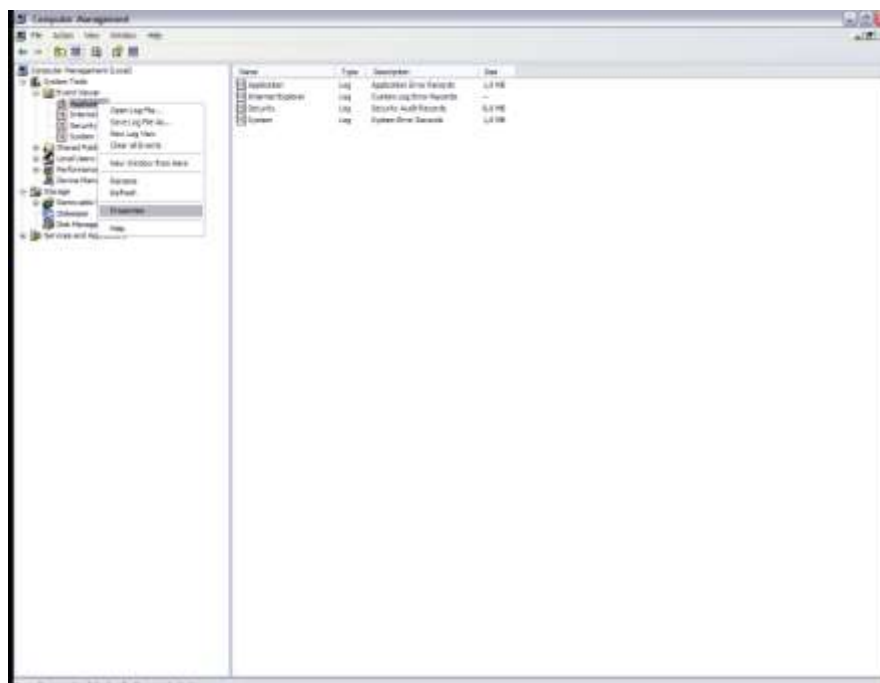
1. Η κατηγοριοποίηση της κρισιμότητάς του
2. Στοιχεία χρόνου
3. Η πηγή από την προήλθε το συμβάν (υπηρεσία ή εφαρμογή)
4. Επιμέρους κατηγοριοποίηση του συμβάντος ως προς την πηγή
5. Αριθμητικός Κωδικός
6. Ο χρήστης για τον οποίο έτρεχε η εφαρμογή ή η υπηρεσία (SYSTEM)
7. Ο υπολογιστής στον οποίο καταγράφηκε το συμβάν

Με δεξί κλικ στο My Computer και επιλέγοντας Manage, μπορούμε να έχουμε πρόσβαση στο Computer Management MMC και από εκεί στον Event Viewer:



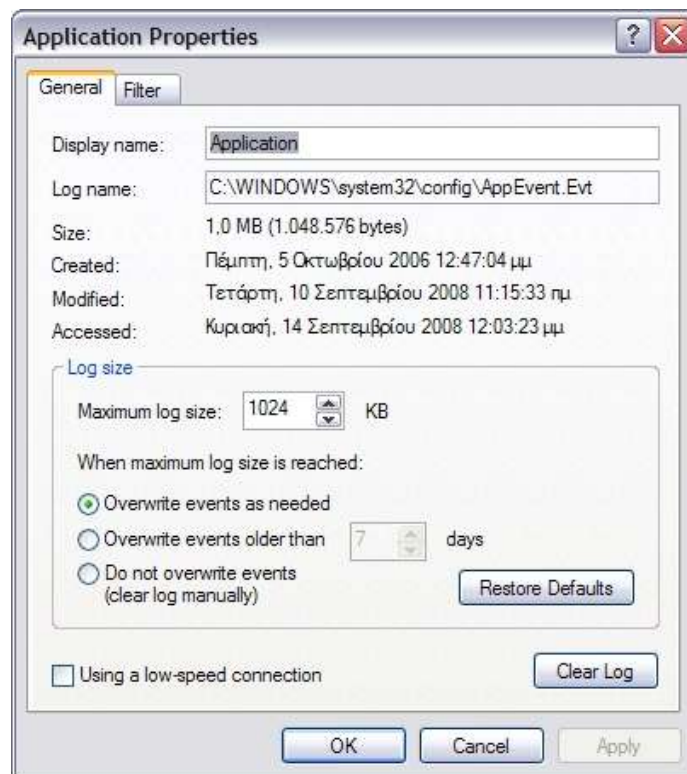
Εικόνα 3-1

Με δεξί κλικ σε κάποια κατηγορία Events και επιλέγοντας Properties:



Εικόνα 3-2

έχουμε πρόσβαση στις ιδιότητες αυτής της ενότητας των Events:



Εικόνα 3-3

Στην καρτέλα Filter μπορούμε να εισάγουμε κριτήρια ώστε να περιορίσουμε τον αριθμό των εμφανιζόμενων events και να επεξεργαστούμε ευκολότερα πληροφορίες για συγκεκριμένη υπηρεσία ή χρονικό διάστημα:

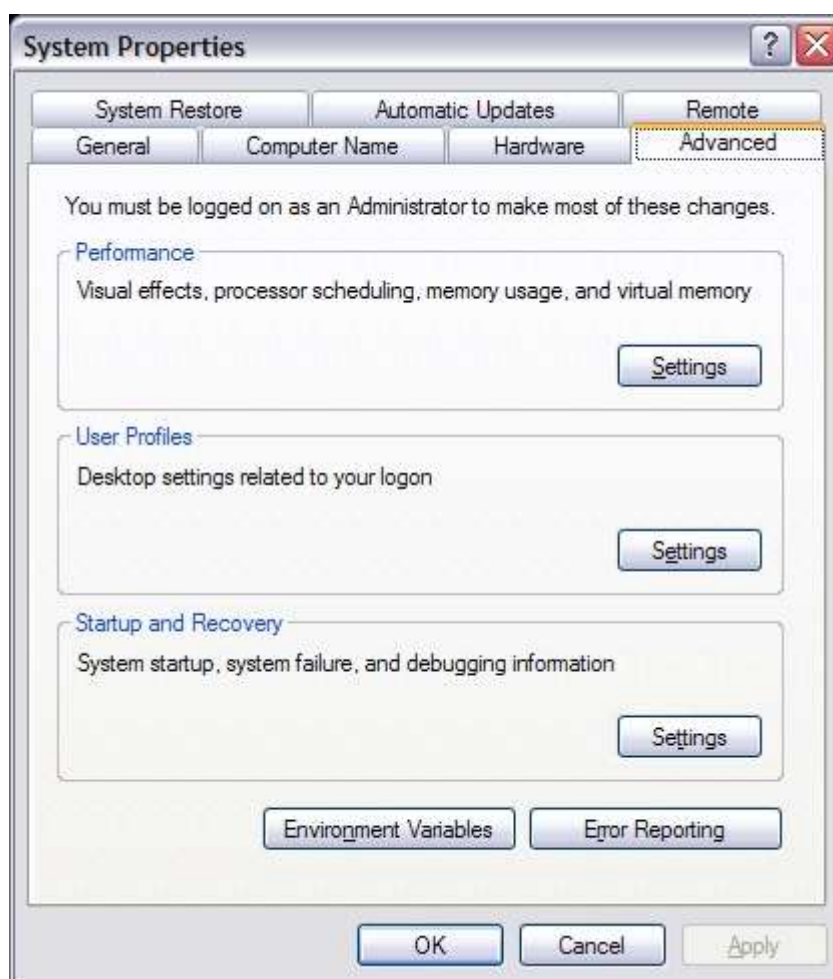


Εικόνα 3-4Επιλογή events βάσει των ιδιοτήτων τους

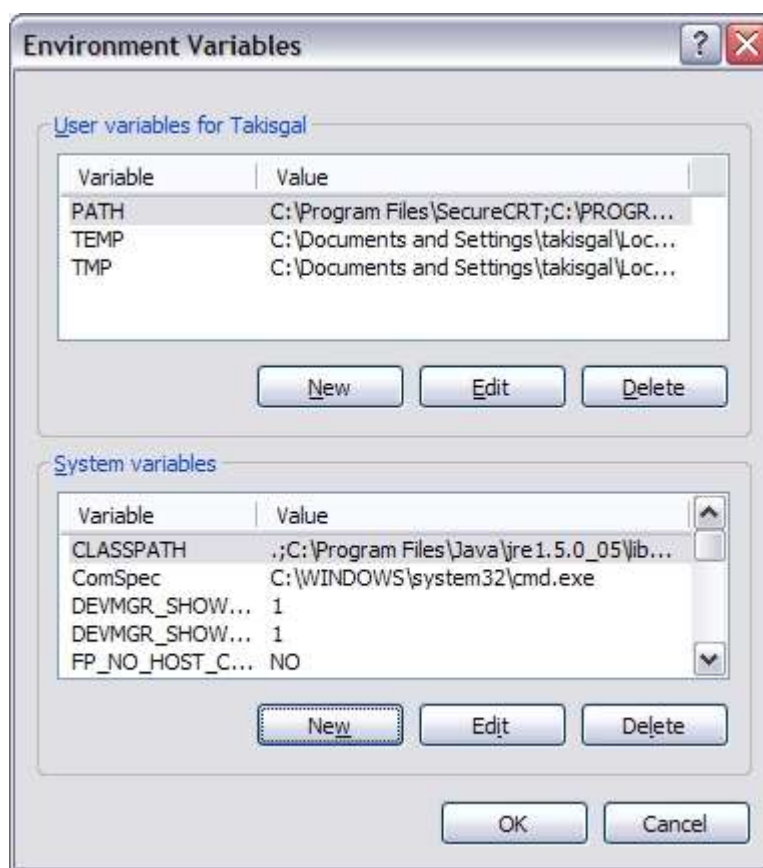
4 Διαχείριση Συσκευών - Device Manager (Hidden Devices)

Από το Computer Management μπορούμε να έχουμε πρόσβαση και στο Device Manager (devmgmt.msc), ώστε να δούμε τις εγκατεστημένες συσκευές. Μία χρήσιμη δυνατότητα είναι η αφαίρεση από αυτή τη λίστα (άρα και από το μητρώο), συσκευών που κάποτε είχαν εγκατασταθεί στο σύστημα, αλλά πλέον έχουν απομακρυνθεί από αυτό. Πραγματοποιείτε τα ακόλουθα βήματα:

1. Κάντε δεξί κλικ στο εικονίδιο **Ο Υπολογιστής μου (My Computer)**.
2. Κάντε κλικ στην εντολή **Ιδιότητες (Properties)**.
3. Κάντε κλικ στην καρτέλα **Για προχωρημένους (Advanced)**.
4. Κάντε κλικ στην καρτέλα **Μεταβλητές περιβάλλοντος (Environment Variables)**.
5. Ορίστε τις μεταβλητές στο πλαίσιο **Μεταβλητές συστήματος (System Variables)**.

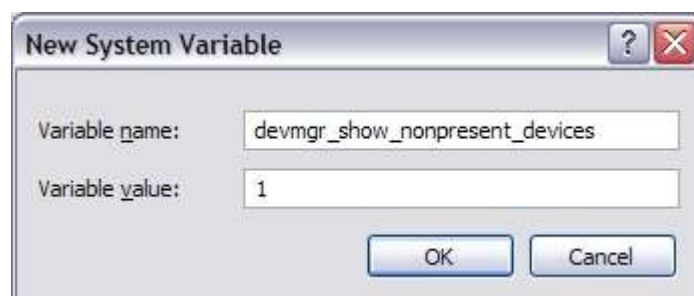


Εικόνα 4-1

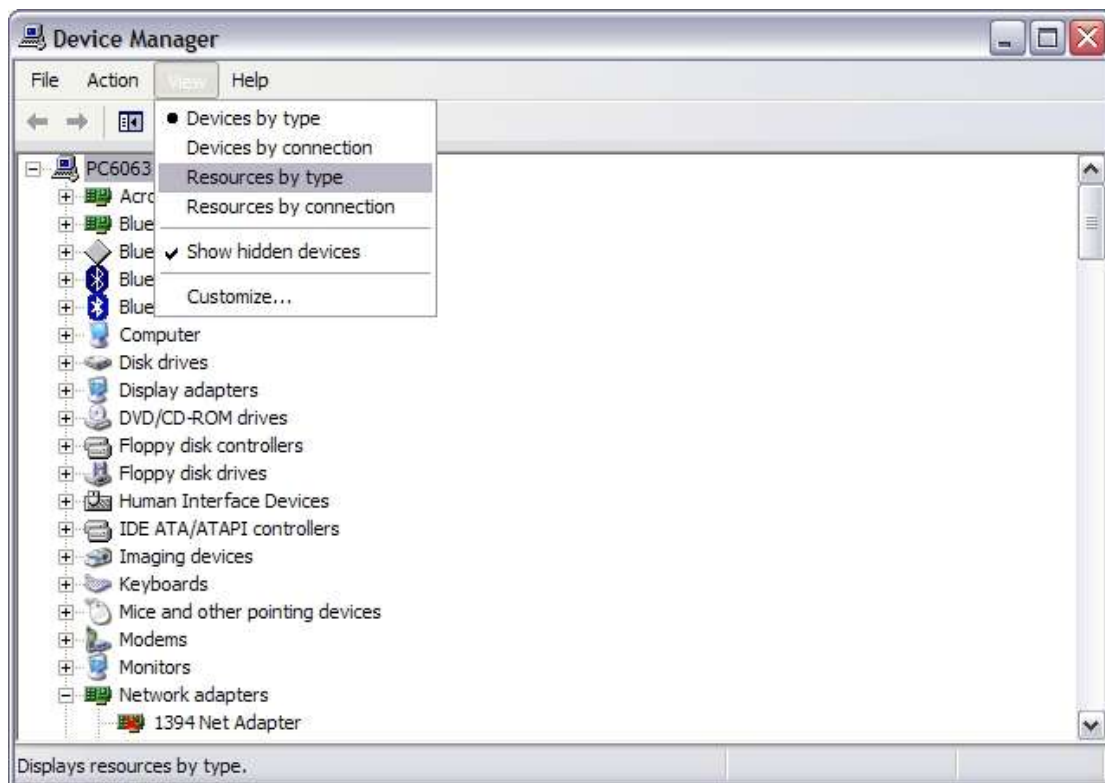


Εικόνα 4-2

Ορίζουμε την ακόλουθη νέα μεταβλητή συστήματος devmgr_show_nonpresent_devices στην τιμή '1':



Εικόνα 4-3



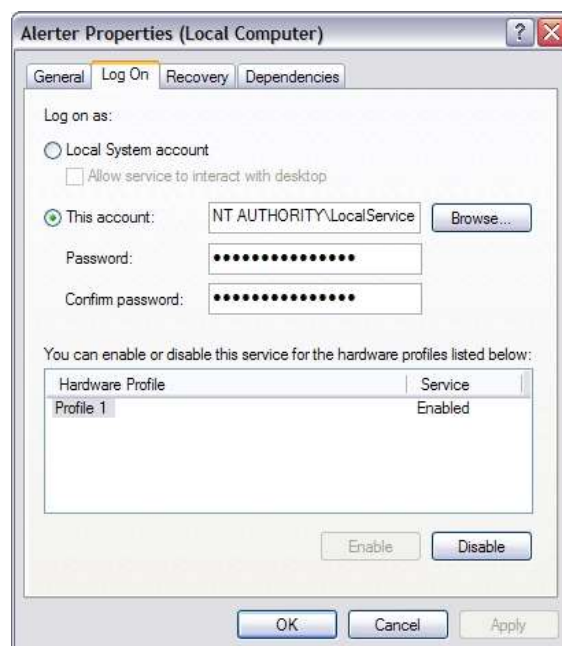
Εικόνα 4-4

Για να μπορέσετε να δείτε τις συσκευές που δεν είναι συνδεδεμένες στον υπολογιστή, κάντε κλικ στην επιλογή **Εμφάνιση των κρυφών συσκευών (Show hidden devices)** στο μενού **Προβολή (View)** της Διαχείρισης Συσκευών (Device Manager).

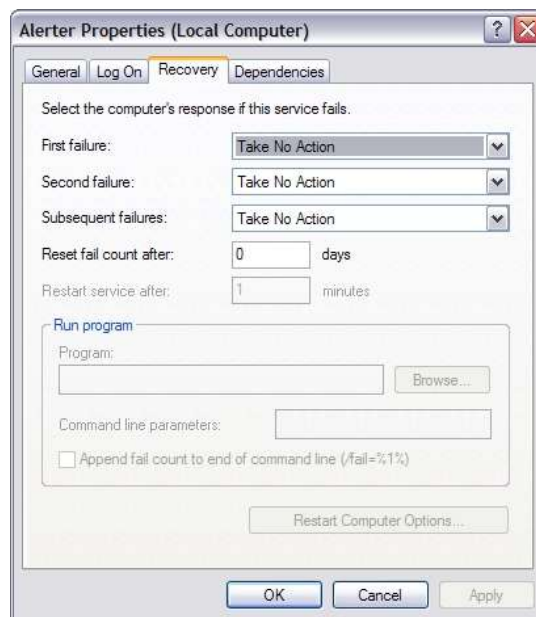


Εικόνα 5-2

Από την καρτέλα “Log On” μπορούμε να αλλάξουμε το λογαριασμό που εκκινεί την υπηρεσία:

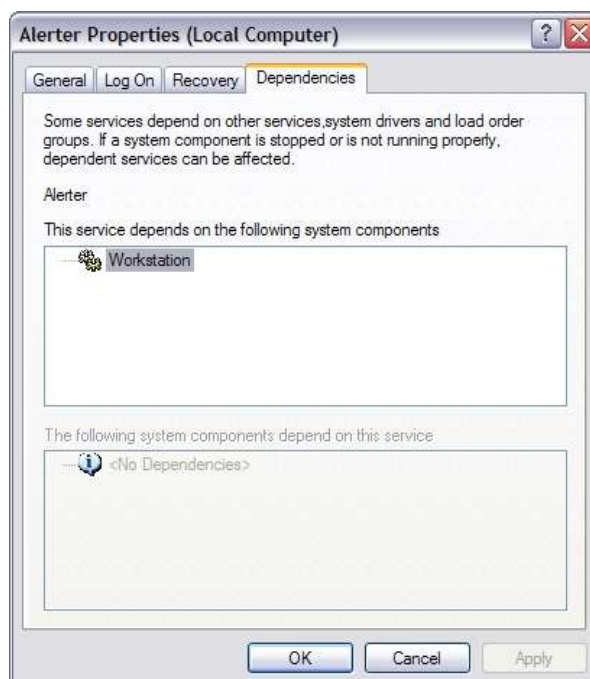


Εικόνα 5-3

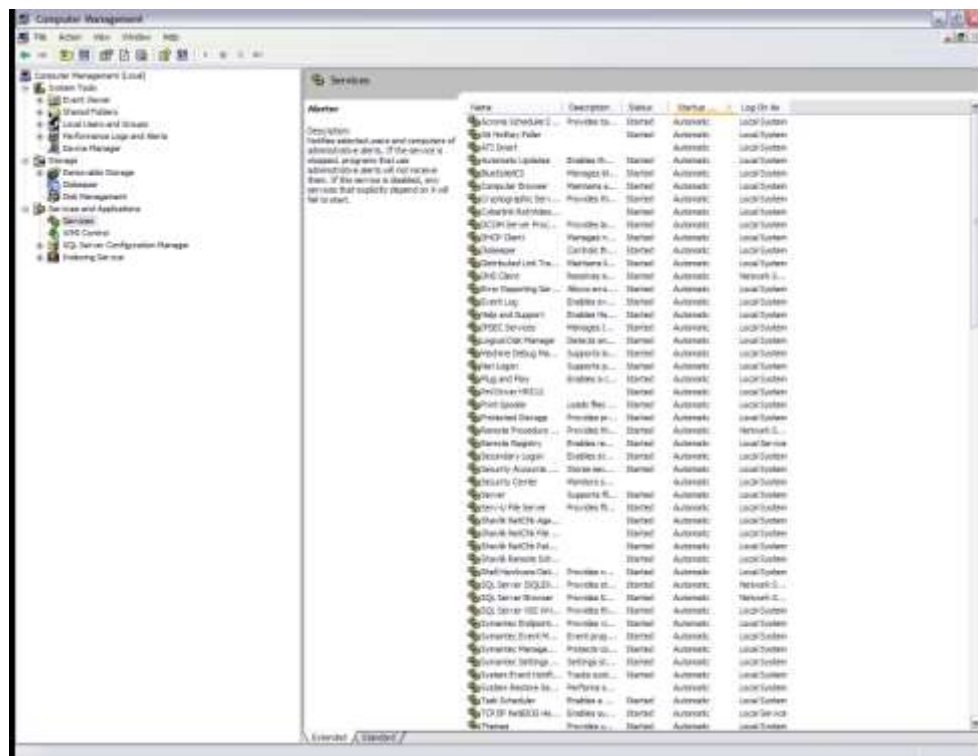


Εικόνα 5-4

Από την καρτέλα “Dependencies” είμαστε σε θέση να δούμε αν αυτή η υπηρεσία εξαρτάται από άλλες για να εκκινηθεί ή χρειάζεται να τρέχει ώστε να εκκινηθούν άλλες υπηρεσίες:



Εικόνα 5-5

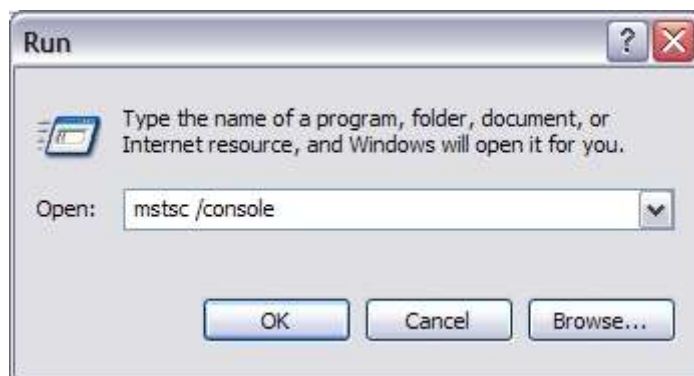


Εικόνα 5-6

Πολλές φορές είναι χρήσιμο να διατάσσουμε τις υπηρεσίες κατά Startup Type ώστε να εντοπίζουμε εκείνες που είναι τύπου Automatic, αλλά δεν έχουν ξεκινήσει (δεν είναι σε κατάσταση Started). Ενδεχομένως να πρόκειται για πρόβλημα αν εντοπίσουμε κάτι τέτοιο, αν και υπάρχουν περιπτώσεις τέτοιων υπηρεσιών (π.χ. Computer Browser, Security Center) που δεν παραπέμπουν σε πρόβλημα.

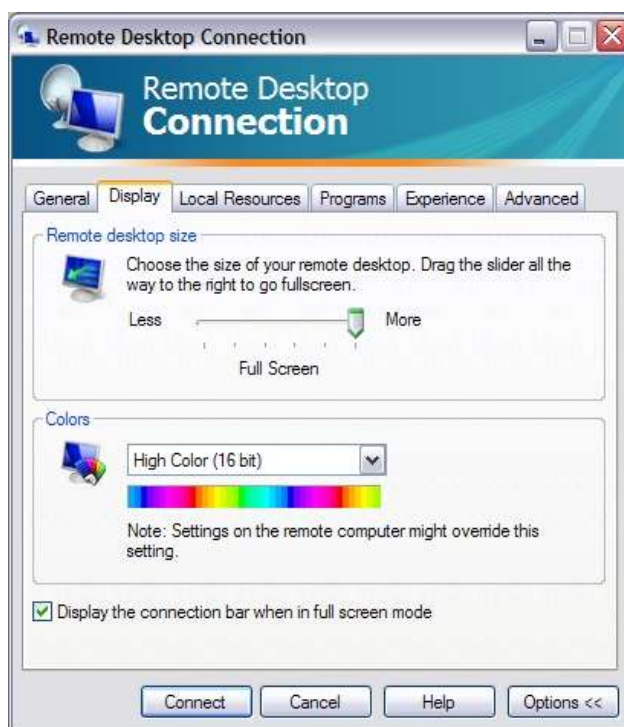
6 Remote Desktop

Η απομακρυσμένη πρόσβαση μπορεί να εκκινηθεί και με την εντολή *mstsc*. Αν η εντολή αυτή συνοδεύεται από το switch */console* (*/admin* για Windows XP SP3, Windows Vista και Windows 2008) τότε η σύνδεση πραγματοποιείται στο λεγόμενο console session του απομακρυσμένου συστήματος.



Εικόνα 6-1 Εκκίνηση απομακρυσμένης πρόσβασης

Στις επιλογές, από την καρτέλα Display μπορούμε να αλλάξουμε τις παραμέτρους σχετικά με τις ρυθμίσεις οθόνης για την απομακρυσμένη πρόσβαση:



Εικόνα 6-2 Ρυθμίσεις λειτουργίας

Από την καρτέλα Local Resources μπορούμε να επιλέξουμε αν θα μεταφέρεται και ο ήχος από το απομακρυσμένο σύστημα καθώς και ποιοι από τους τοπικούς πόρους (π.χ. εκτυπωτές, δίσκοι) θα είναι διαθέσιμοι στο απομακρυσμένο σύστημα:



Εικόνα 6-3 Χρήση τοπικών πόρων στον απομακρυσμένο υπολογιστή

Από την καρτέλα Experience μπορούμε να επιλέξουμε προφίλ ανάλογα με την ταχύτητα της σύνδεσης ή και συγκεκριμένα στοιχεία που θα μεταφέρονται, ώστε να είναι ομαλή και απρόσκοπτη η απομακρυσμένη πρόσβαση:



Εικόνα 6-4 Ρύθμιση λειτουργίας ανάλογα με την ταχύτητα της δικτυακής πρόσβασης

Από την καρτέλα Advanced διαθέτουμε επιλογές τόσο για το Server Authentication από το απομακρυσμένο μηχάνημα καθώς και αν θα χρησιμοποιηθεί κάποιος Terminal Services Gateway για την απομακρυσμένη πρόσβαση:



Εικόνα 6-5 Ρυθμίσεις αυθεντικοποίησης και σύνδεσης μέσω TS Gateway

7 Scheduled Tasks

Με την εφαρμογή Scheduled Tasks μπορούμε να χρονοπρογραμματίζουμε εργασίες σε υπολογιστικά συστήματα MS Windows. Η εφαρμογή ενεργοποιείται από Start > Control Panel.



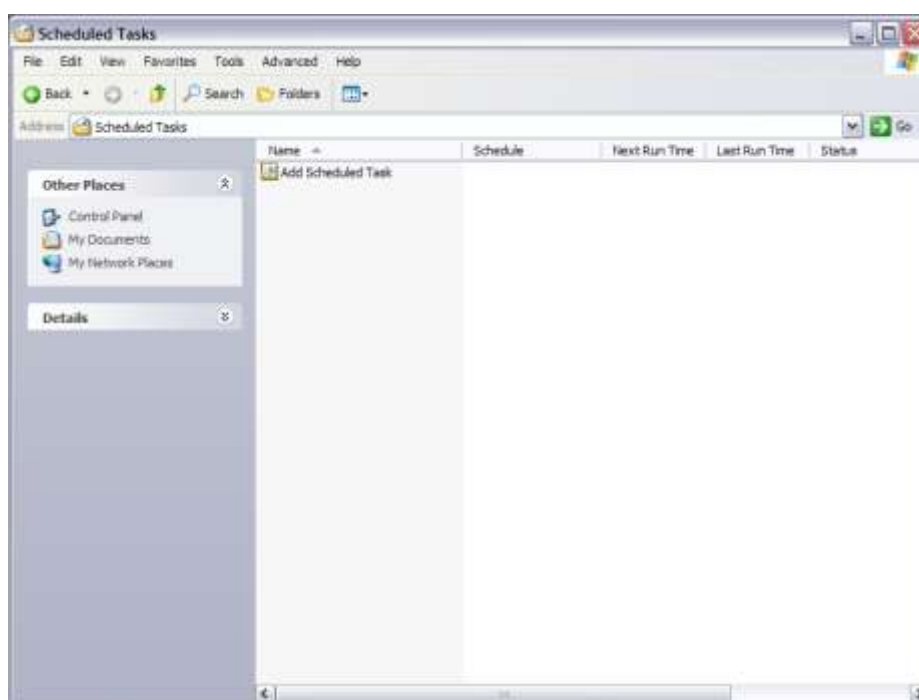
Εικόνα 7-1

Στο Control Panel ανοίγουμε τα Schedules Tasks (ή Task Scheduler σε παλιότερες εκδόσεις).



Εικόνα 7-2

Προσθέτουμε νέα χρονοπρογραμματισμένη εργασία με την επιλογή «Add Scheduled Task». Έστω πως θέλουμε να κάνουμε ανασυγκρότηση του δίσκου/κατάτμησης C: στον υπολογιστή μας κάθε μήνα.



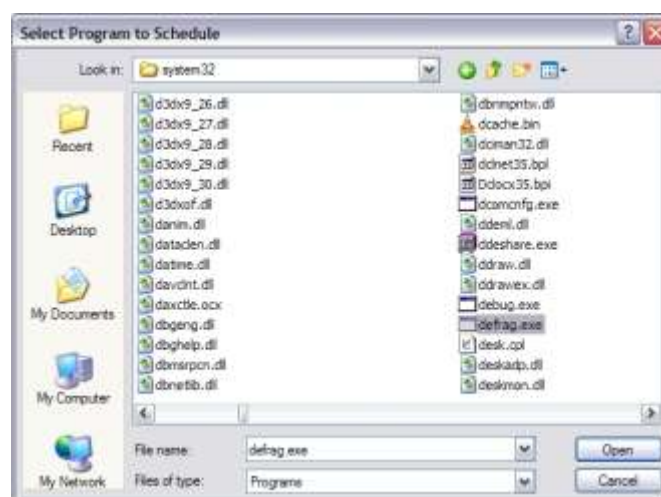
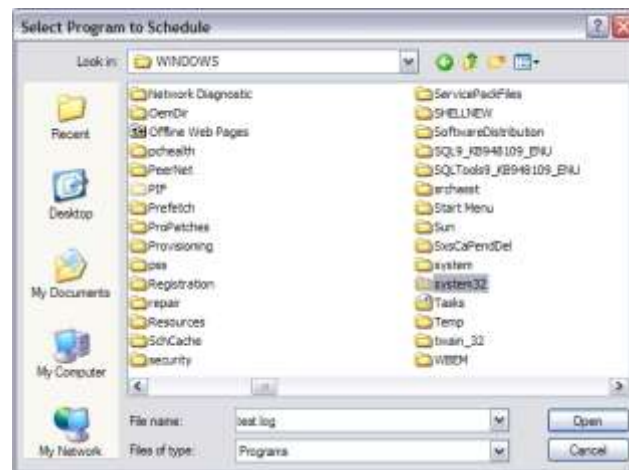
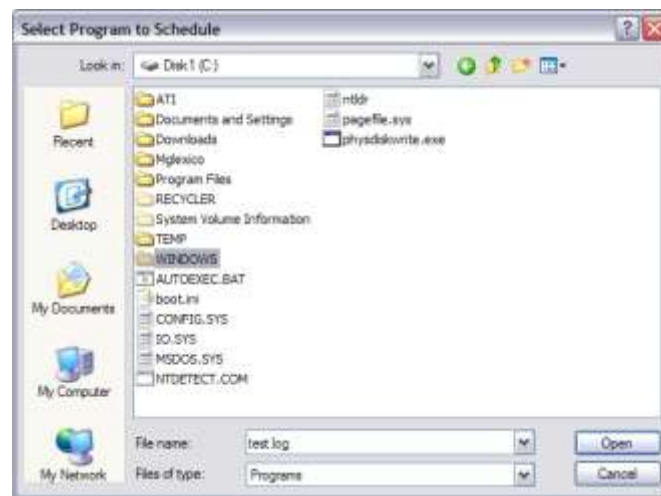
Εικόνα 7-3

Επιλέγουμε next στην επόμενη οθόνη.



Εικόνα 7-4

Με browse εντοπίζουμε και επιλέγουμε το πρόγραμμα defrag.exe.



Εικόνα 7-5

Επιλέγουμε τη συχνότητα με την οποία θα πραγματοποιείται η εργασία.



Δίνουμε τα στοιχεία του χρήστη με τα οποία θα πραγματοποιείται η χρονοπρογραμματισμένη εργασία.

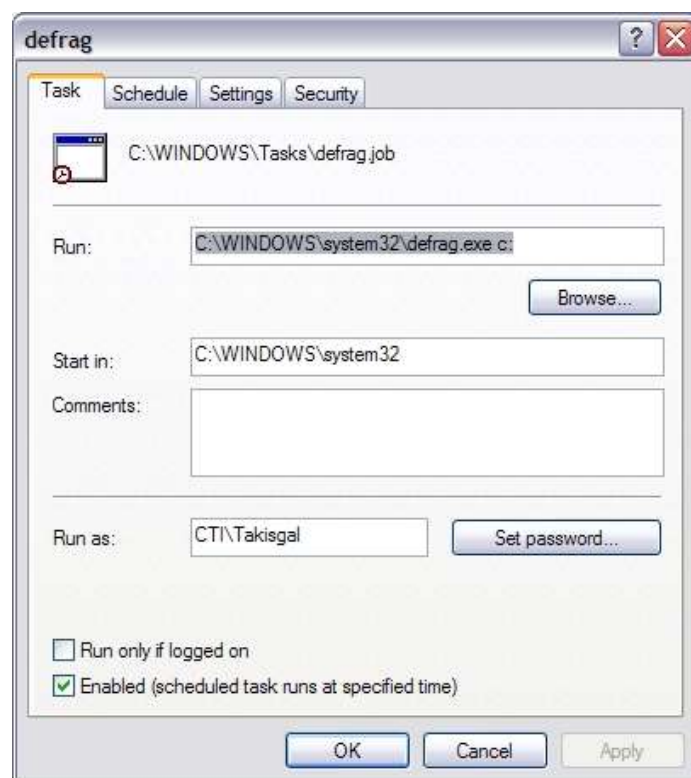


Αφήνουμε να ανοίξουν οι προχωρημένες ρυθμίσεις.



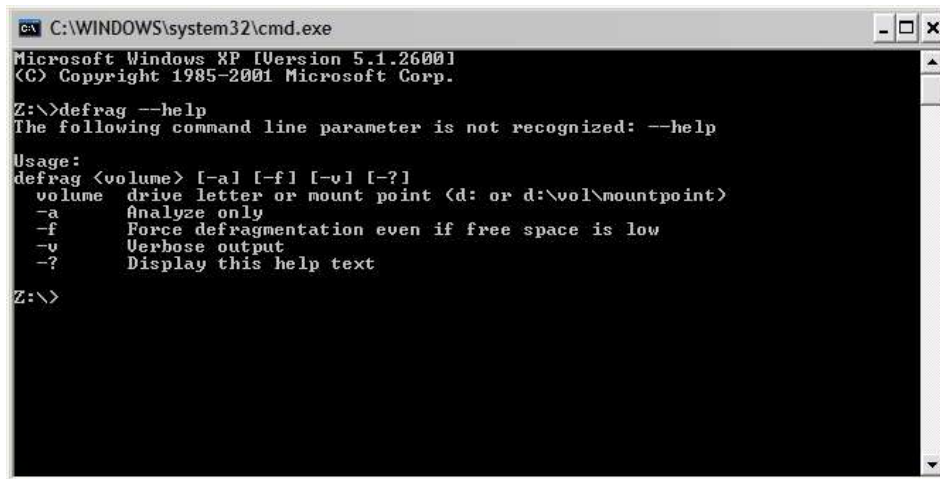
Εικόνα 7-6

Στις προχωρημένες ρυθμίσεις προσθέτουμε την κατάτμηση στην οποία θέλουμε να κάνουμε ανασυγκρότηση.



Εικόνα 7-7

Μπορούμε επίσης να προσθέσουμε και άλλες ρυθμίσεις από τις διαθέσιμες της εφαρμογής.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

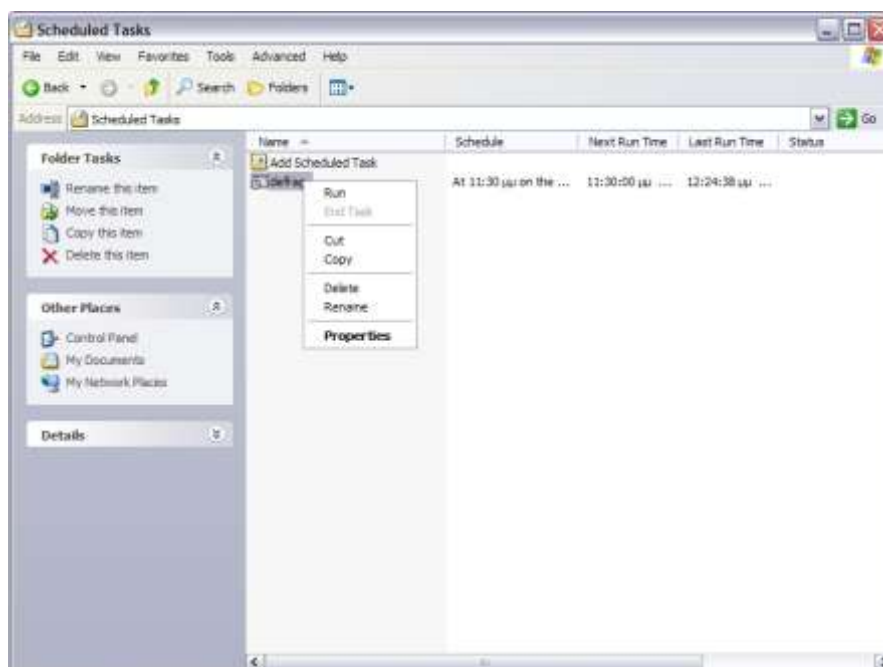
Z:\>defrag --help
The following command line parameter is not recognized: --help

Usage:
defrag <volume> [-a] [-f] [-v] [-?]
    volume    drive letter or mount point <d: or d:\vol\mountpoint>
    -a        Analyze only
    -f        Force defragmentation even if free space is low
    -v        Verbose output
    -?        Display this help text

Z:\>
```

Εικόνα 7-8

Η χρονοπρογραμματισμένη εργασία εμφανίζεται στη λίστα εργασιών, απ' όπου με ξεζί κουμπί του ποντικιού επιλέγουμε Run, ώστε να δοκιμάσουμε άμεσα πως η εργασία εκτελείται σύμφωνα με τις επιθυμητές ρυθμίσεις.

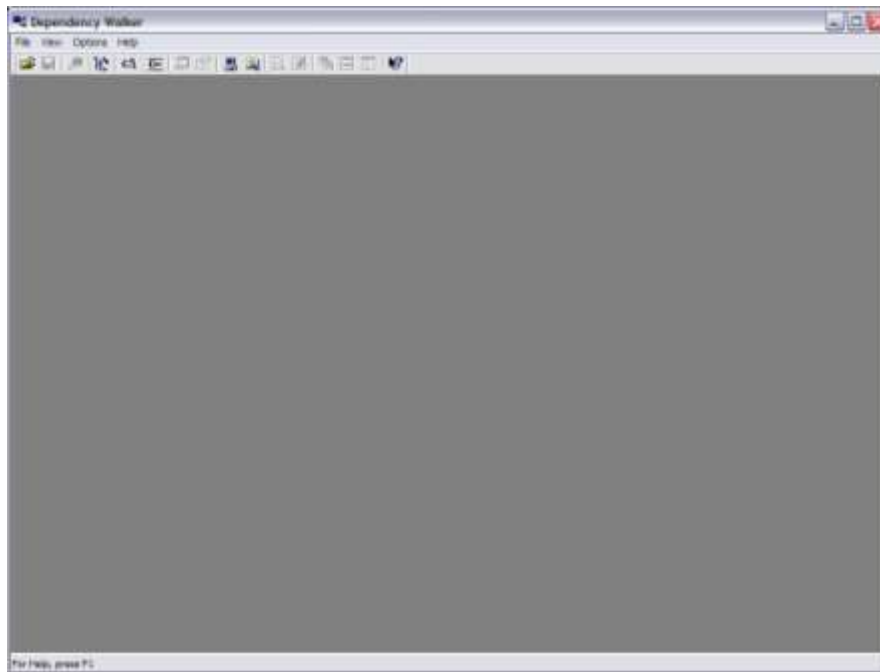


Εικόνα 7-9

8 Dependency Walker

Ένα χρήσιμο εργαλείο των Support Tools των Windows είναι ο Dependency Walker, με το οποίο εντοπίζονται βιβλιοθήκες συναρτήσεων που πρέπει να φορτωθούν κατά τη λειτουργία μιας εφαρμογής και αναλύονται τα πιθανά προβλήματα που προκύπτουν στις ανωτέρω διαδικασίες.

Το εργαλείο ξεκινά από Start/Run: “depends.exe”.

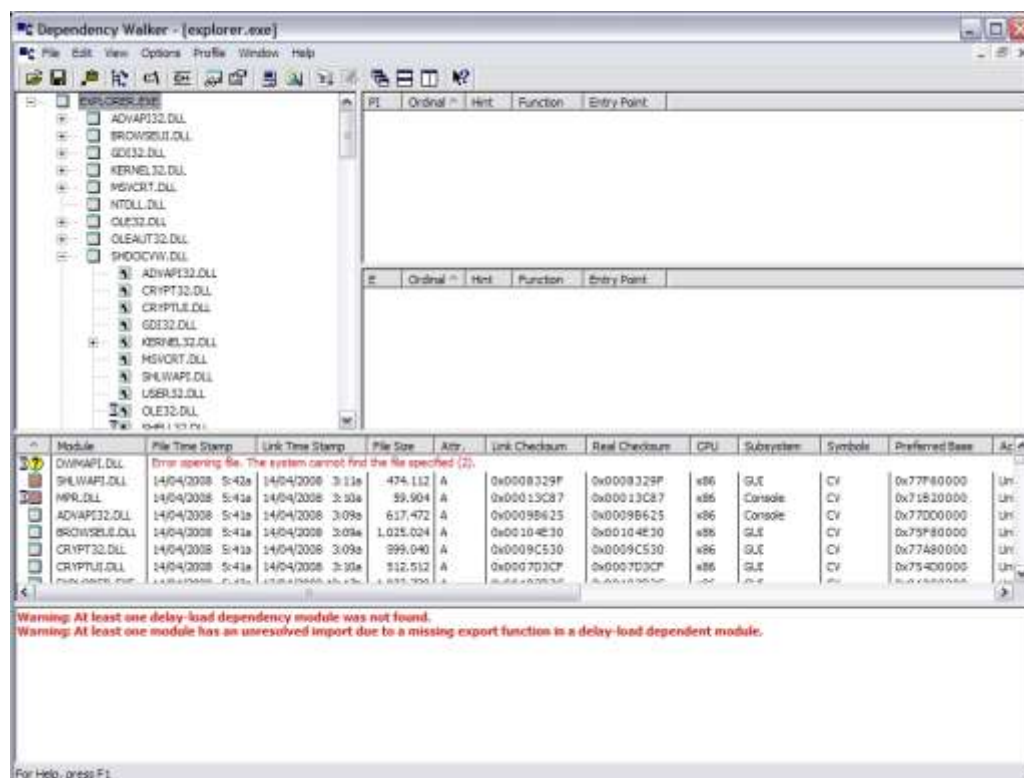


Εικόνα 8-1

Από File →Open επιλέγουμε το αρχείο του οποίου θέλουμε να βρούμε τις εξαρτήσεις από άλλα αρχεία (π.χ. βιβλιοθήκες dll):



Εικόνα 8-2



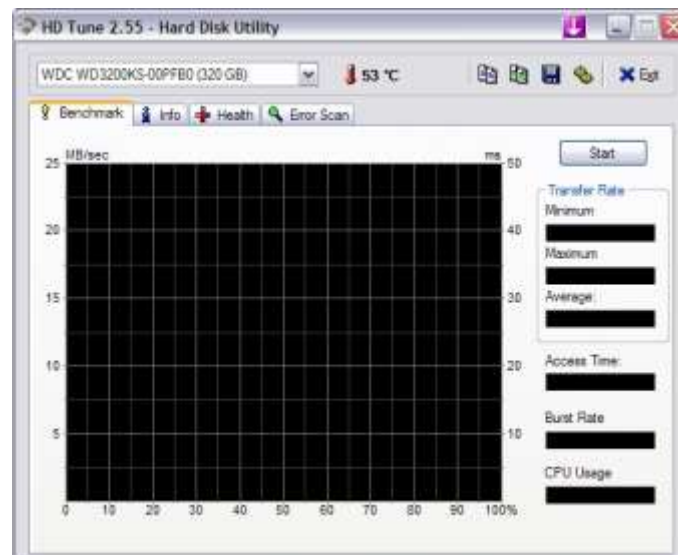
Εικόνα 8-3

Για παράδειγμα, διαπιστώνουμε ότι ο explorer.exe εξαρτάται από πολλά dll αρχεία και μπορούμε να δούμε πληροφορίες για καθένα από αυτά:

Εικόνα 8-4

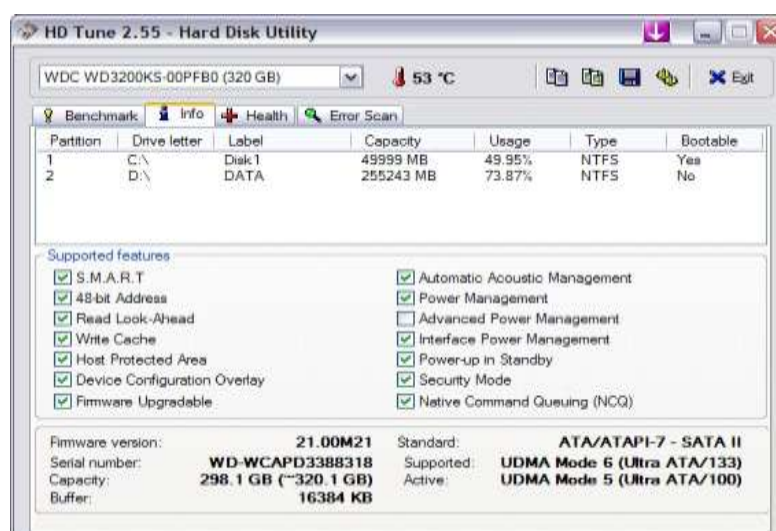
9 Έλεγχος δίσκων - HD Tune

Ένα χρήσιμο εργαλείο για τη μέτρηση απόδοσης, την επισκόπηση πληροφοριών και τον έλεγχο της κατάστασης των σκληρών δίσκων για λάθη είναι το HD Tune (<http://www.hdtune.com> , freeware v2.55).



Εικόνα 9-1

Από την καρτέλα Info μπορούμε να δούμε πληροφορίες για τους σκληρούς δίσκους:



Εικόνα 9-2

Από την καρτέλα Health μπορούμε να δούμε πληροφορίες για τα SMART attributes των σκληρών μας δίσκων. Μία ορθή ανάγνωση αυτών μας επιτρέπει

να αξιολογήσουμε την υγεία των σκληρών δίσκων (Status: Ok). Εν ολίγοις, ιδιότητες που έχουν μη μηδενικό κατώφλι (Threshold) θα πρέπει να έχουν μηδενικές τιμές στα δεδομένα (Data).

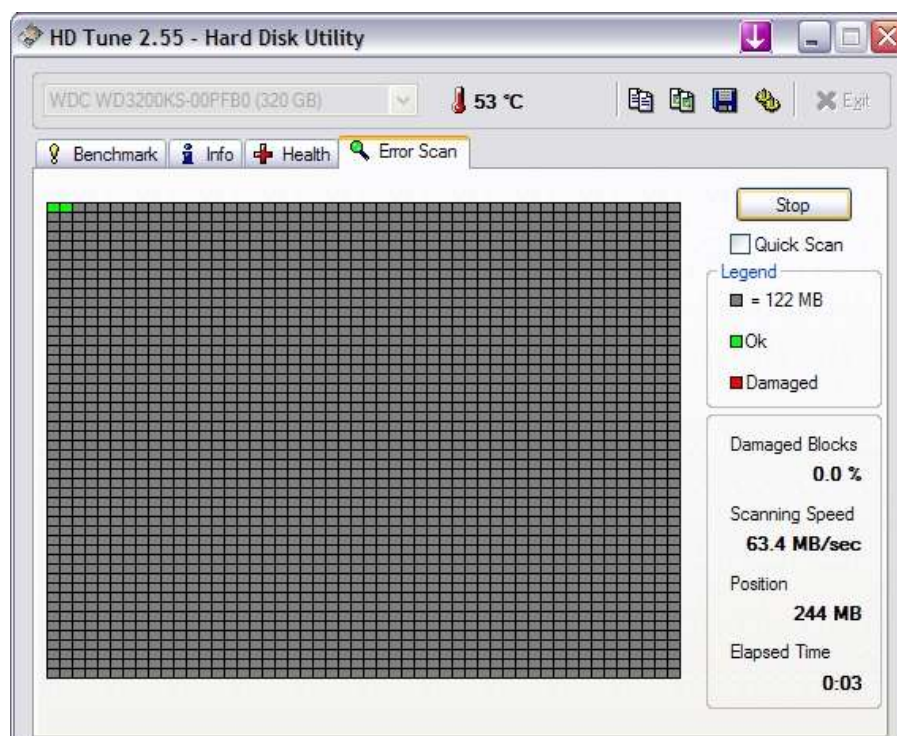


ID	Current	Worst	Threshold	Data	Status
(01) Raw Read Error Rate	200	200	51	0	Ok
(03) Spin Up Time	189	188	21	5533	Ok
(04) Start/Stop Count	99	99	0	1171	Ok
(05) Reallocated Sector Count	200	200	140	0	Ok
(07) Seek Error Rate	200	200	51	0	Ok
(09) Power On Hours Count	81	81	0	14185	Ok
(0A) Spin Retry Count	100	100	51	0	Ok
(0B) Calibration Retry Count	100	253	51	0	Ok
(0C) Power Cycle Count	100	100	0	30	Ok
(0E) Airflow Temperature	47	38	0	53	Ok
(12) Temperature	97	88	0	53	Ok
(C4) Reallocated Event Count	200	200	0	0	Ok
(C5) Current Pending Sector	200	200	0	0	Ok
(C6) Offline Uncorrectable	200	200	0	0	Ok
(C7) Ultra DMA CRC Error Count	200	200	0	310	Ok
(C8) Write Error Rate	200	200	51	0	Ok

Power On Time: 14185 Health Status: **Ok**

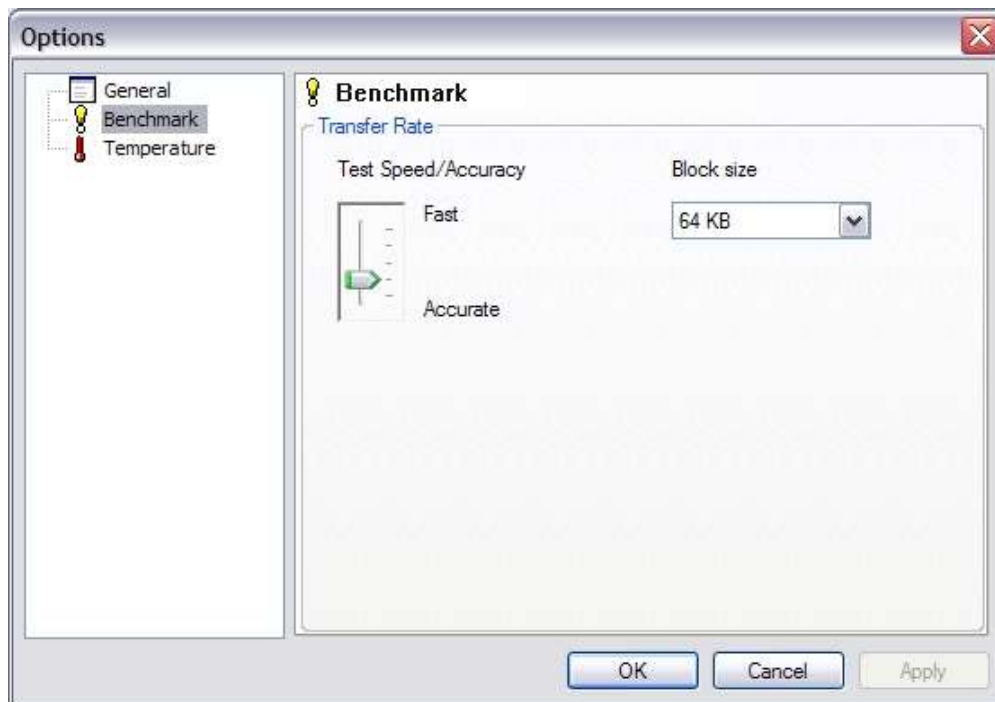
Εικόνα 9-3

Από την καρτέλα Error Scan μπορούμε να εξετάσουμε το δίσκο για bad sectors:



Εικόνα 9-4

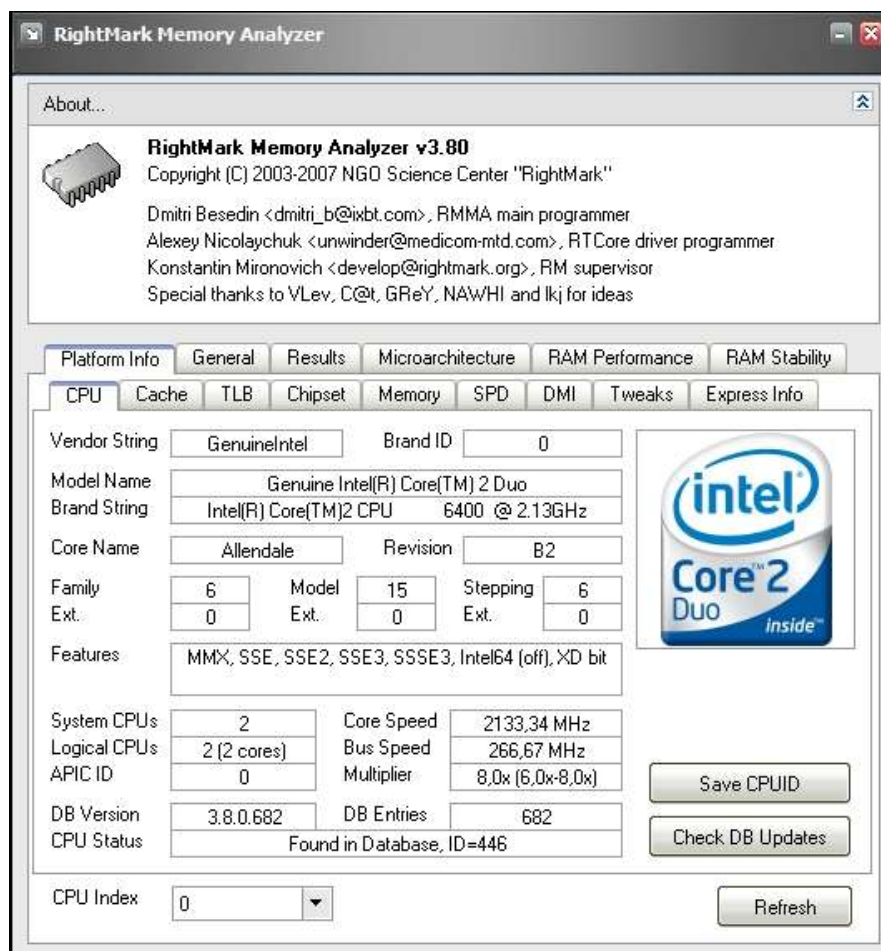
Αξίζει να σημειώσουμε ότι στις Επιλογές (Options), μπορούμε να αλλάξουμε τις παραμέτρους του Benchmark του σκληρού δίσκου, ώστε να είναι πιο ακριβές ή να ολοκληρώνεται γρηγορότερα:



Εικόνα 9-5

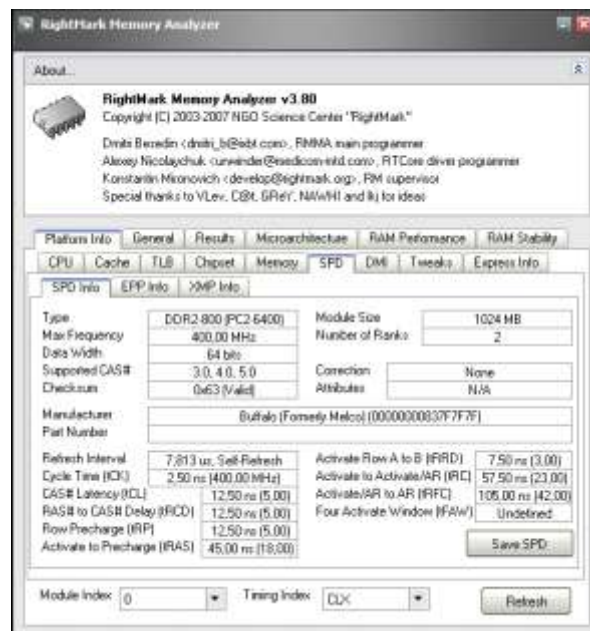
10 Έλεγχος μνήμης - RMMA

Το RightMark Memory Analyzer (<http://cpu.rightmark.org/products/rmma.shtml>) παρέχει πληροφορίες για διάρθρωση της μνήμης του συστήματος, ενώ παρέχει και εργαλεία ελέγχου της μνήμης για λάθη.



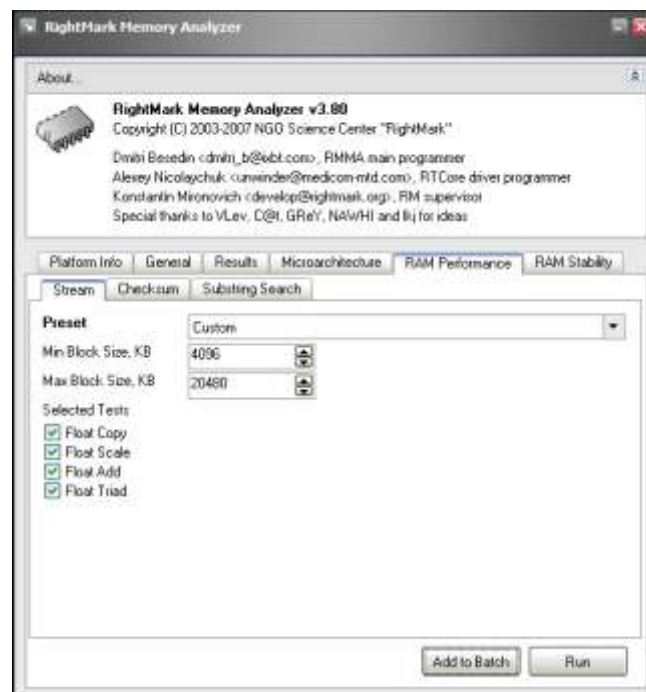
Εικόνα 10-1

Για παράδειγμα, στην καρτέλα SPD βλέπουμε αναλυτικότερες πληροφορίες για τον κατασκευαστή της μνήμης και τα τεχνικά χαρακτηριστικά της:



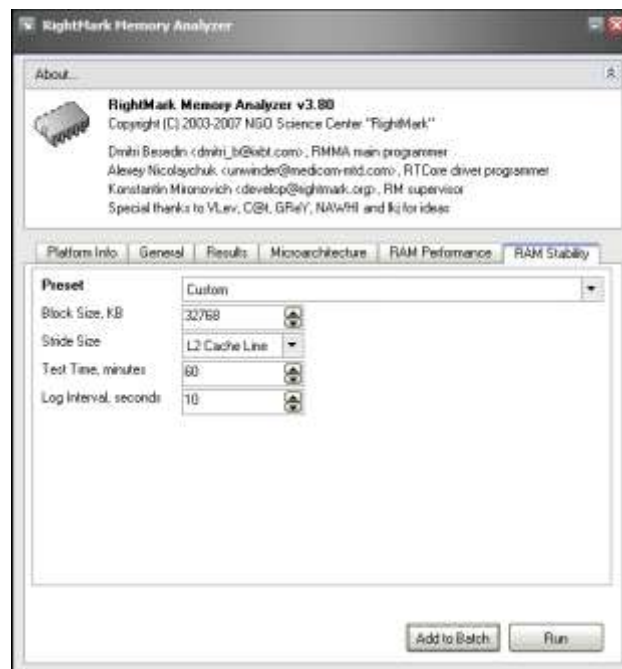
Εικόνα 10-2

Στην καρτέλα RAM Performance μπορούμε να πραγματοποιήσουμε μέτρηση της απόδοσης της μνήμης του συστήματός μας:



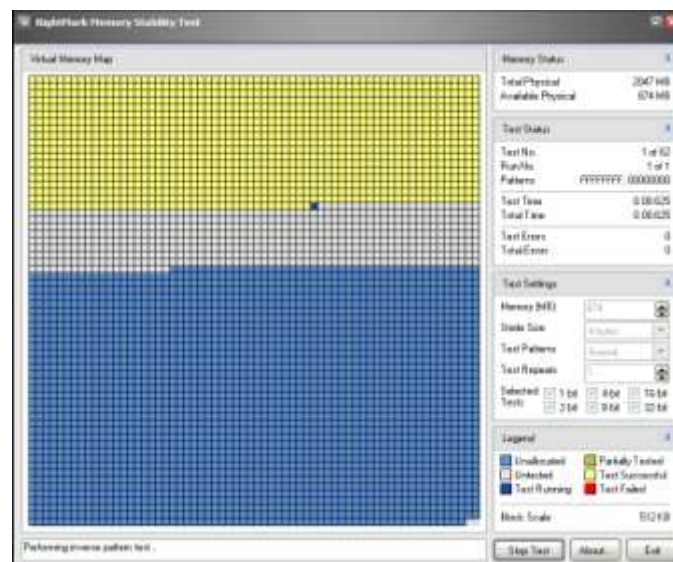
Εικόνα 10-3

Στην καρτέλα RAM Stability μπορούμε να πραγματοποιήσουμε έλεγχο της σταθερότητας της μνήμης του συστήματός μας:



Εικόνα 10-4

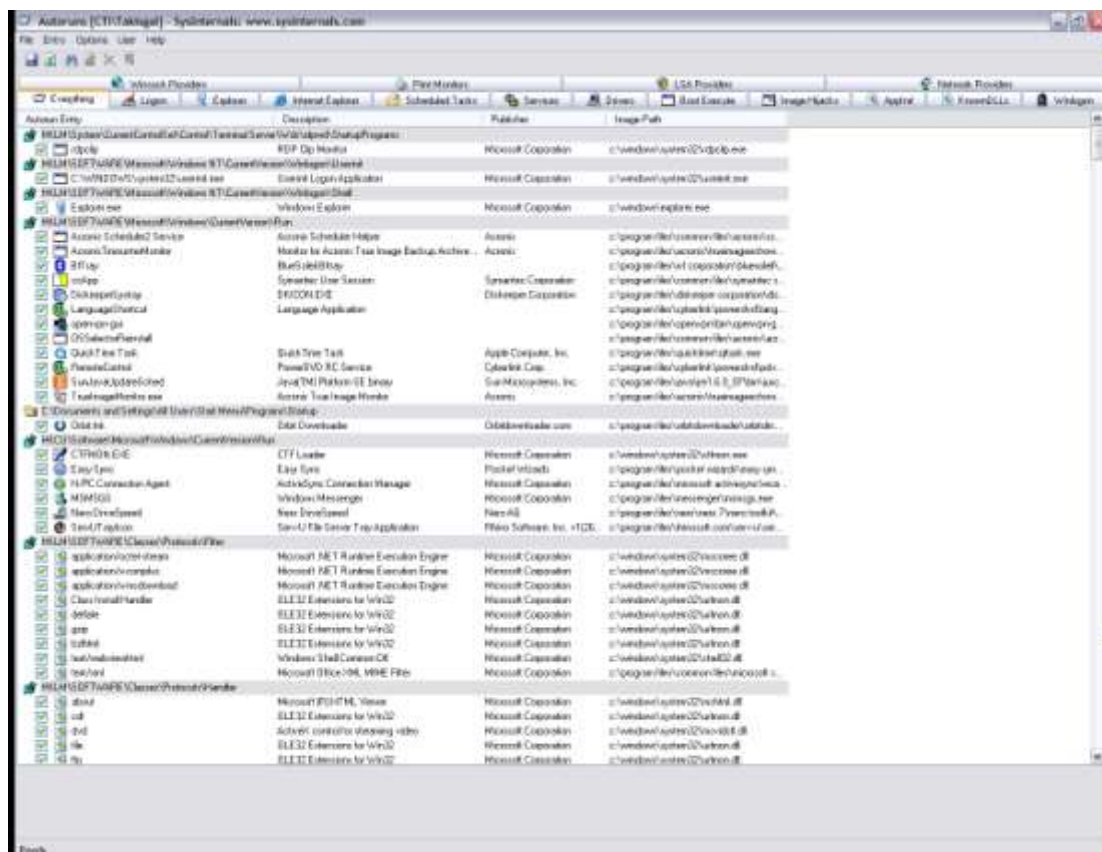
Ένα ακόμα εκτελέσιμο αρχείο του προγράμματος είναι το `rmms.exe`, το οποίο μας παρέχει έναν όμορφο γραφικό τρόπο για τον έλεγχο της σταθερότητας της μνήμης του συστήματός μας:



Εικόνα 10-5

11 Σημεία εκκίνησης προγραμμάτων - AutoRuns

Το AutoRuns της SysInternals (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>) είναι εφαρμογή για την εύρεση όλων των σημείων που είναι δυνατό να φορτώνεται ένα πρόγραμμα κατά την εκκίνηση των Windows. Το AutoRuns είναι πολύ χρήσιμο όταν προσπαθούμε να καθαρίσουμε ένα σύστημα μολυσμένο από κακόβουλο λογισμικό.



Εικόνα 11-1

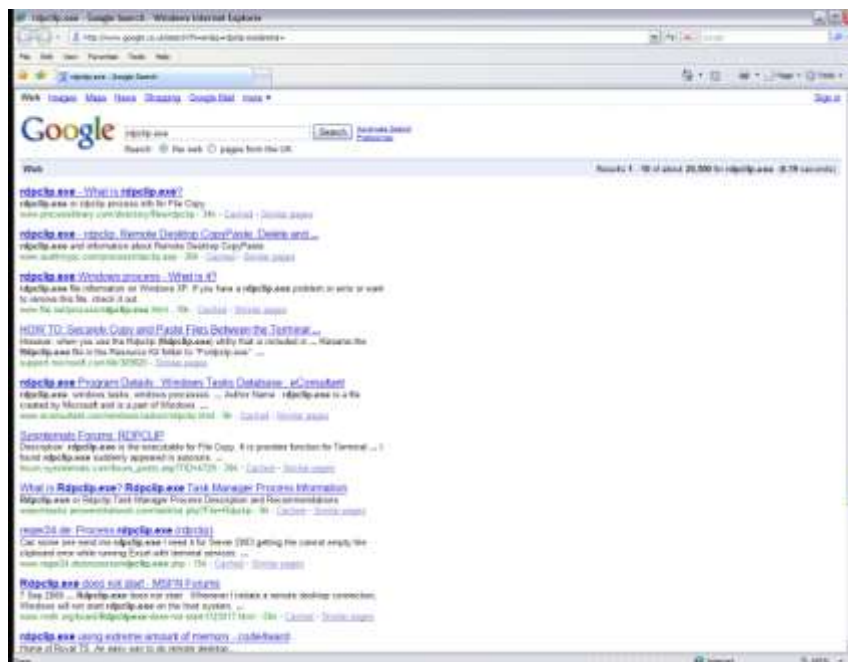
Μπορούμε να έχουμε τόσο μια εποπτική εικόνα για ό,τι εκκινείται κατά την έναρξη των Windows, όσο και ομαδοποιημένα ανά κατηγορίες.

Για παράδειγμα, μία ενδιαφέρουσα καρτέλα είναι η Winlogon, μιας και πολλά κακόβουλα λογισμικά επιλέγουν να φορτωθούν μαζί με το winlogon process:

[illegible]

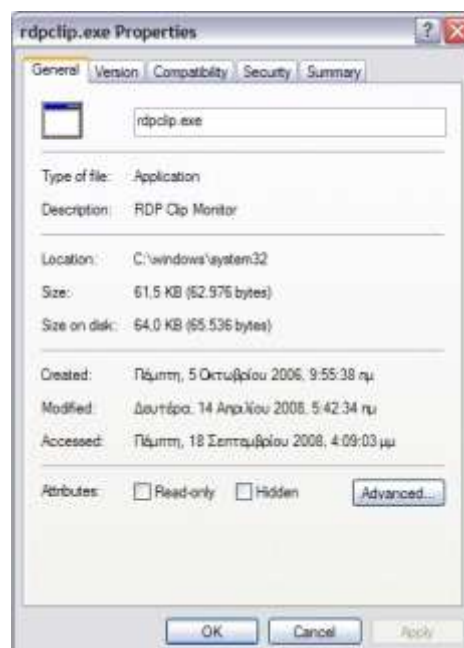
Εικόνα 11-3

50



Εικόνα 11-4

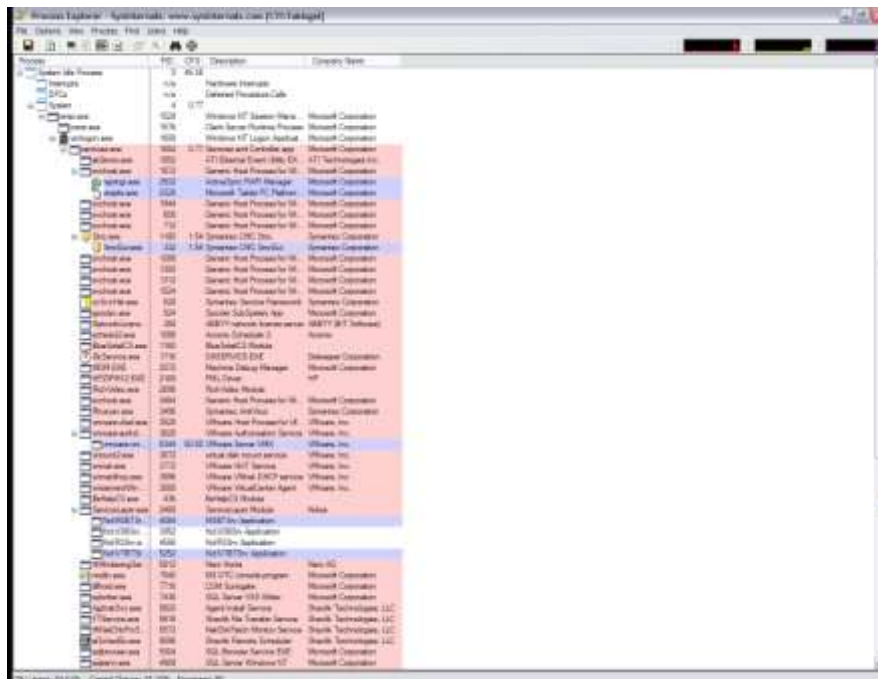
είτε Properties και να δούμε πληροφορίες από explorer για αυτό το αρχείο.



Εικόνα 11-5

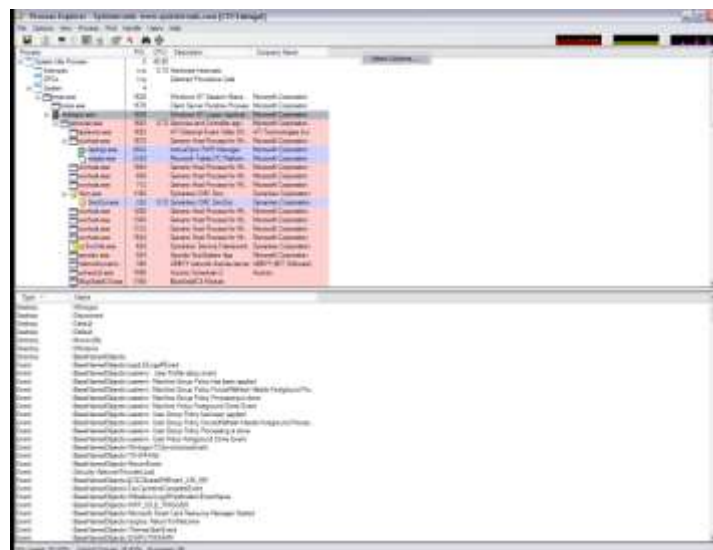
12 Διαχείριση Διεργασιών - Process Explorer

Ένα εξαιρετικό εργαλείο που μοιάζει με Task Manager αλλά διαθέτει πολύ περισσότερες δυνατότητες ο Process Explorer της SysInternals (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>). Το εργαλείο αυτό είναι πολύ χρήσιμο όταν προσπαθούμε να καθαρίσουμε ένα σύστημα μολυσμένο από κακόβουλο λογισμικό.



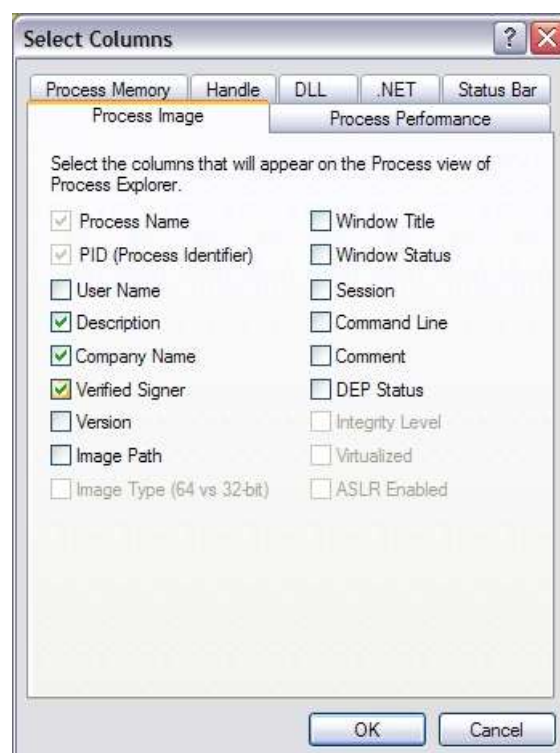
Εικόνα 12-1

Στο κάτω μέρος του παραθύρου μπορούμε να δούμε πληροφορίες για τη διεργασία που έχουμε επιλέξει στο πάνω μέρος:



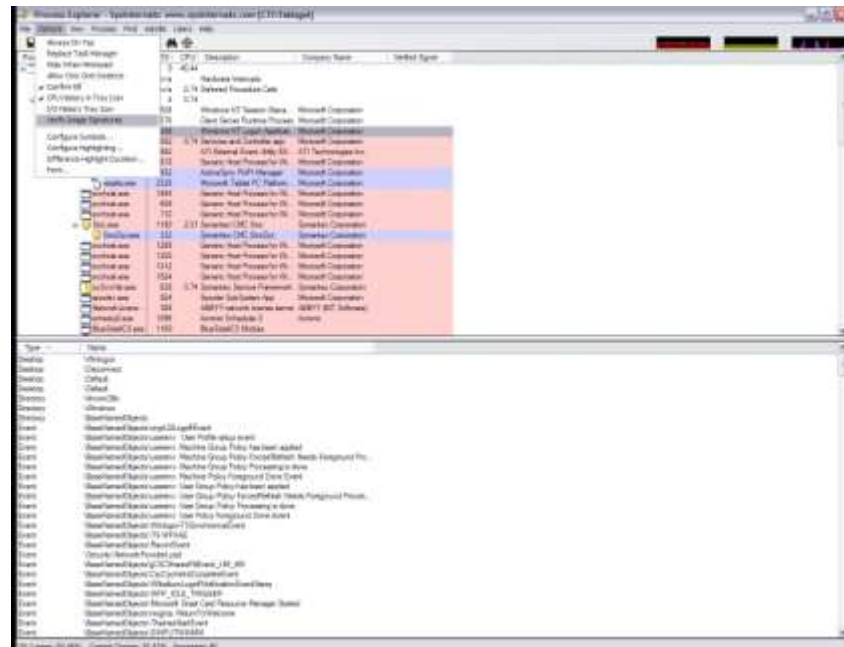
Εικόνα 12-2

Με δεξί κλικ στις στήλες και επιλέγοντας “Select Columns” έχουμε τη δυνατότητα να εμπλουτίσουμε τις εμφανιζόμενες πληροφορίες. Για παράδειγμα, μπορούμε να επιλέξουμε τη στήλη “Verified Signer”:



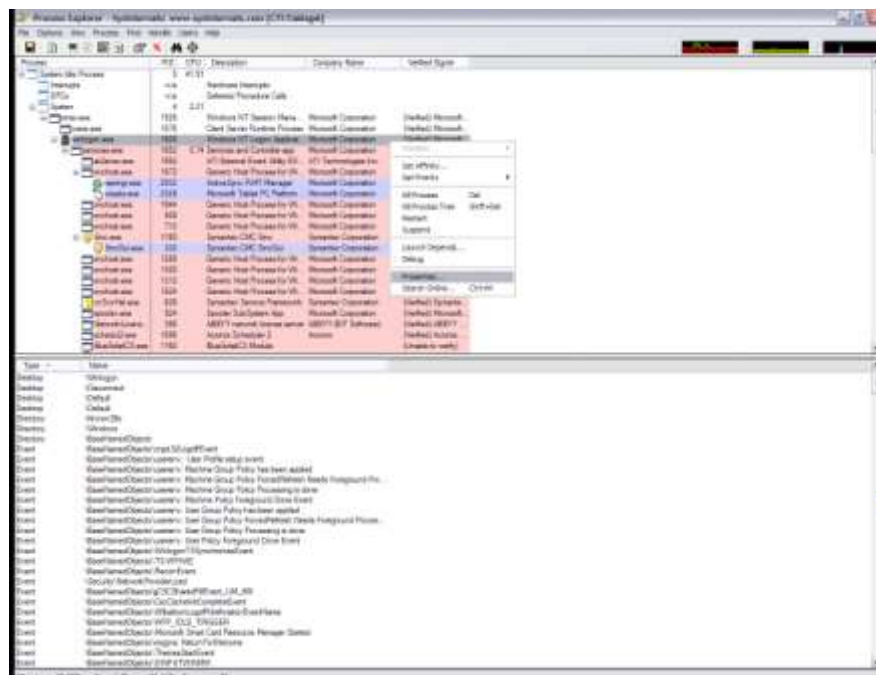
Εικόνα 12-3

Επιλέγοντας τώρα Options → Verify Image Signatures γίνεται ένας δικτυακός έλεγχος για τις διεργασίες του συστήματος, ώστε να προσδιοριστεί αν τα αρχεία που τρέχουν είναι αυθεντικά ή όχι:



Εικόνα 12-4

Με δεξί κλικ και επιλέγοντας Properties:



Εικόνα 12-5

μπορούμε να δούμε τις ιδιότητες του αρχείου, οργανωμένες σε πολύ χρήσιμες καρτέλες:



Εικόνα 12-6

Ο χρωματικός κώδικας των εμφανιζόμενων διεργασιών μπορεί να τροποποιηθεί. Οι εξ ορισμού επιλογές φαίνονται στην ακόλουθη εικόνα. Ιδιαίτερη προσοχή πρέπει να δοθεί στα “Packed Images”, διότι στην πλειοψηφία των περιπτώσεων υποκρύπτουν την ύπαρξη κάποιου κακόβουλου λογισμικού:



Εικόνα 12-7

13 Δομημένη Καλωδίωση

13.1 Κατασκευή καλωδίου UTP Category 5 / 5E

Υπάρχουν δύο ειδών patch cords τα straight (ευθύ) και τα crossover (ανεστραμμένα). Τα πρώτα χρησιμοποιούνται για την σύνδεση υπολογιστών σε switches και τα δεύτερα χρησιμοποιούνται για την σύνδεση switches μεταξύ τους. Ορισμένα switches υποστηρίζουν την διασύνδεση με άλλα switch και με straight patch cords χρησιμοποιώντας την λειτουργία MDI/MDX.

Τα απαραίτητα εργαλεία και υλικά που χρειάζεται να διαθέτουμε για να φτιάξουμε ένα patch cord είναι τα εξής (Εικόνα 8):

- Μία πρέσα για RJ-45 διεπαφές
- 2 connectors RJ-45
- 1 utp καλώδιο
- Ένα απογυμνωτή καλωδίων ή λεπίδι (προαιρετικά) αν δεν έχει την δυνατότητα η πρέσα για την απογύμνωση του καλωδίου.



Εικόνα 8: Υλικά για την κατασκευή ενός utp patch cord.

Υπάρχουν δύο πρότυπα για την δημιουργία ενός utp καλωδίου το 568-A και 568-B. Αυτά τα πρότυπα έχουν να κάνουν με τον τρόπο που τοποθετούνται τα καλώδια στο RJ-45 connector και είναι ισοδύναμα. Πιο κοινό στην χρήση είναι το πρότυπο 568-B. Η παρακάτω εικόνα δείχνει την διαφορά στην τοποθέτηση των καλωδίων ανάμεσα στα δύο πρότυπα.



Εικόνα 9: Διαφορές μεταξύ 568-A και 568-B

Για την δημιουργία ενός straight καλωδίου θα πρέπει οι δύο άκρες να ακολουθούν το ίδιο πρότυπο, ενώ για το crossover θα πρέπει να καλωδιωθούν η μία με το 568-A και η άλλη με το 568-B.

Οδηγίες Κατασκευής Καλωδίου Patch Cable

1. Απογυμνώνουμε με την βοήθεια του απογυμνωτή ή της λεπίδας το εξωτερικό περίβλημα του καλωδίου κατά περίπου 4 εκατοστά.



2. κάθε ζεύγος καλωδίου και ισιώστε τα καλώδια.
3. Διατάξτε τα καλώδια με τη σωστή σειρά σύμφωνα με τα δύο διαγράμματα (568B ή 568A). Φέρτε τα καλώδια παράλληλα κοντά το ένα

στο άλλο, μέχρι να εφάπτονται. Σε αυτό το σημείο ελέγξτε ότι η σειρά των καλωδίων είναι σύμφωνη με το διάγραμμα.

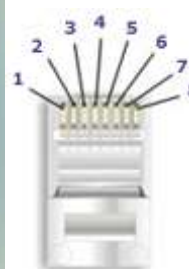
4. Κρατήστε σταθερά τα ομαδοποιημένα και διατεταγμένα καλώδια μαζί ανάμεσα στον αντίχειρα και στον δείκτη.



5. Κόψτε όλα τα καλώδια, με τη βοήθεια ενός ψαλιδιού ή του κόφτη που έχει η πρέσα, έτσι ώστε το μέτωπό τους να είναι επίπεδο και κάθετο ως προς το καλώδιο. Το μήκος των καλωδίων θα πρέπει να είναι περίπου 1,3 εκατοστά από την άκρη του απογυμνωμένου περιβλήματος.



6. Εισάγετε τα καλώδια μέσα στο βύσμα (με την μεριά των pins να κοιτάει προς τα πάνω).



7. Πιέστε σχετικά δυνατά τα καλώδια μέσα ώστε να εξασφαλίσετε ότι όλα τα καλώδια έχουν φτάσει μέχρι το τέρμα του βύσματος. Φροντίστε ώστε το προστατευμένο μέρος του καλωδίου να εισέλθει μέσα στο πίσω μέρος του βύσματος κατά περίπου 0,5 εκατοστό.
8. Τοποθετήστε την άκρη του καλωδίου με το βύσμα μέσα στο ειδικό εργαλείο-πένσα και σφίξτε δυνατά μέχρι η λαβή να φτάσει στο τέλος της διαδρομής της.



9. Επαναλάβετε την ίδια διαδικασία και για το άλλο άκρο. Για ένα κανονικό straight καλώδιο, χρησιμοποιήστε την ίδια καλωδίωση. Για ένα ανεστραμμένο "crossover" καλώδιο, καλωδιώστε το ένα άκρο ως 568A, και το άλλο ως 568B.
10. Ένας γρήγορος έλεγχος για την ορθή λειτουργία του καλωδίου είναι να το χρησιμοποιήσετε σε μια υπάρχουσα σύνδεση και να ελέγξετε αν ο σταθμός εργασίας συνδέεται στο δίκτυο με το καλώδιο αυτό χρησιμοποιώντας την εντολή ping.
11. Για να βεβαιωθούμε ότι το καλώδιο που φτιάξαμε πληροί τις προδιαγραφές του cat5/cat5e προτύπου θα πρέπει να χρησιμοποιήσουμε ένα cable tester που παρέχει αυτού του είδους τον έλεγχο.

13.2 Οδηγίες ελέγχου utp καλωδίων

Στο παρακάτω κείμενο παρουσιάζονται οδηγίες για τον έλεγχο της ορθής λειτουργίας των patch cords που έχουμε δημιουργήσει.

Για τον έλεγχο των καλωδίων θα χρησιμοποιηθούν οι δύο συσκευές της Agilent το WireScope 350 και το DualRemote 350 (βλ. Εικόνες 1 και 2)



Εικόνα 10: WireScope 350



Εικόνα 11: DualRemote 350

Οι συσκευές αυτές μπορούν να πραγματοποιήσουν ένα μεγάλο αριθμό από ελέγχους καλωδίων όπως χαλκού και οπτικά. Στο συγκεκριμένο κείμενο θα δείξουμε πως μπορούμε να ελέγξουμε αν το καλώδιο που κατασκευάσαμε λειτουργεί ομαλά και πληροί τις προδιαγραφές της κατηγορίας 5e και 6.

Για την πραγματοποίηση και των δύο ελέγχων για τα καλώδια UTP θα πρέπει να χρησιμοποιηθούν οι κατάλληλοι προσαρμογείς για τις διεπαφές RJ45 (βλ. Εικόνα 12)

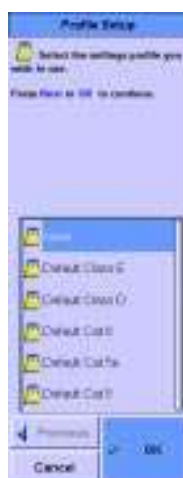


Εικόνα 12: Προσαρμογείς για RJ45

1. Κατ' αρχήν συνδέουμε τους προσαρμογείς στις συσκευές και έπειτα συνδέουμε το καλώδιο που θέλουμε να ελέγξουμε στις υποδοχές των προσαρμογέων.
2. Στο κεντρικό μενού επιλέγουμε το κουμπί Autotest



3. Στη συνέχεια πατάμε το κουμπί Select Settings Profile για να επιλέξουμε την κατηγορία προδιαγραφών που θα συγκριθούν τα αποτελέσματα των μετρήσεων του καλωδίου. Στην συγκεκριμένη περίπτωση επιλέγουμε την κατηγορία Default Cat5e. Μόλις επιλεγεί η κατηγορία πατάμε το πλήκτρο OK



4. Στη συνέχεια στην οθόνη που εμφανίζεται επιλέγουμε το Start Test για να ξεκινήσει ο έλεγχος του καλωδίου για την κατηγορία 5e.



5. Με την ολοκλήρωση του ελέγχου βγαίνουν τα αποτελέσματα αν το καλώδιο πληροί τις προδιαγραφές της κατηγορίας που επιλέχθηκε και εμφανίζεται η αντίστοιχη οθόνη. Οι έλεγχοι που γίνονται είναι οι εξής:
- Wire-map
 - Distance
 - NEXT
 - Attenuation
 - Return Loss
 - ELFEXT



6. Με το πέρας του ελέγχου δίνεται η δυνατότητα να αποθηκεύσουμε τα αποτελέσματα στην μνήμη της συσκευής και να τα αντιγράψουμε στον υπολογιστή μας με την μορφή pdf αρχείου.

Οι συγκεκριμένοι έλεγχοι που γίνονται με την διαδικασία του Autotest μπορούν να γίνουν και μεμονωμένα από το μενού Tools της συσκευής WireScope. Επίσης μπορεί να ελεγχθεί σε ποια δίκτυα μπορεί να λειτουργήσει το καλώδιο που κατασκευάσαμε (π.χ. 10Base-T, 100Base-T, 1000Base-T, 155 Mbps ATM κ.α.)

14 Ασκήσεις

1. Διαμορφώστε μία Κονσόλα Διαχείρισης, ώστε εκτός των εργαλείων διαχείρισης που περιλαμβάνονται στο Computer Management, να περιλαμβάνει και το εργαλείο της ρύθμισης πολιτικών του σταθμού εργασίας.
2. Εντοπίστε τα events που σχετίζονται με τη διαδικασία εγκατάστασης/απεγκατάστασης/διαμόρφωσης εφαρμογών. Διαφοροποιούνται ανάλογα με την επιτυχή ή μη έκβαση των ανωτέρω διαδικασιών;
3. Εντοπίστε ένα Error στην καταγραφή συμβάντων και αναλύστε την αιτία που το προκάλεσε. Προχωρήστε σε διορθωτικές ενέργειες.
4. Εντοπίστε την υπηρεσία με την οποία λειτουργούν τα Event Logs και επιβεβαιώστε πως έχει ξεκινήσει.
5. Δημιουργήστε ένα χρονοπρογραμματισμένο task, με το οποίο σε μηνιαία βάση καθαρίζει ο υπολογιστής από άχρηστα αρχεία.
6. Είστε στην επιτροπή οριστικής παραλαβής νέου ΣΕΠΕΗΥ μετά από δοκιμαστική λειτουργία 30 ημερών. Πώς θα ελέγξετε πως ο εξοπλισμός δεν αντιμετωπίζει προβλήματα λειτουργίας.
7. Κατασκευάστε ένα patch cord UTP Cat 5E και ελέγξτε την ορθή κατασκευή και λειτουργία του.