ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Νομικά και Πληροφορική: Μηχανισμοί συνδρομής δικονομικής διαδικασίας

Σπουδαστής: ΚΑΤΣΙΑΔΡΑΜΗΣ ΔΗΜΗΤΡΙΟΣ
ΑΜ: 1415

Επιβλέπων καθηγητής: ΑΣΗΜΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ

ΑΝΤΙΡΡΙΟ – ΟΚΤΩΒΡΙΟΣ 2015

Περίληψη

Όταν διαπράττεται ή καταγγέλλεται ένα έγκλημα, ανεξαρτήτως του είδους του εγκλήματος, καλείται η εγκληματολογική υπηρεσία της αστυνομίας στο σημείο, ώστε να περισυλλέξει τυχόν αποδεικτικά στοιχεία για να τα εξετάσει μετέπειτα και να βγάλει ένα πόρισμα για το πως και γιατί διαπράχθηκε το έγκλημα.

Μέσα σ 'αυτά τα αποδεικτικά στοιχεία, μπορεί να υπάρχουν και στοιχεία που βρίσκονται σε ηλεκτρονικό υπολογιστή ή σε κάποια συσκευή με δυνατότητα σύνδεσης στο Διαδίκτυο.

Τότε μιλάμε για **ψηφιακά αποδεικτικά στοιχεία**, των οποίων η επεξεργασία από την εγκληματολογική υπηρεσία γίνεται με χρήση διαφόρων εργαλείων, είτε *hardware* είτε *software*, ώστε να παραμείνει η ακεραιότητα τους για να μπορούν να χρησιμοποιηθούν νόμιμα στο δικαστήριο, όταν θα δικάζεται ο κατηγορούμενος, σε περίπτωση που τον εμπλέκουν στο έγκλημα τα ψηφιακά στοιχεία.

Summary

When a crime is committed or reported, regardless of the type, the forensics service of the police is summoned at the crime scene, so to collect any evidence to examine later and make a conclusion regarding how and why the crime was committed.

Within these evidence, there may be clues found in a computer or a device with internet connection.

Then we talk about **digital evidence**, the processing of which is performed by the forensics service using various tools, either hardware or software, so to maintain their integrity in order to be used legally in court, when the accused will be tried, in case the digital evidence involve him in the crime.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην ολοκλήρωση αυτής της πτυχιακής εργασίας.

Τον καθηγητή κ. Γεώργιο Ασημακόπουλο που ανέλαβε την επίβλεψη του θέματος της εργασίας μου και για την βάση που μου έδωσε ώστε να μελετήσω και να φτιάξω την πτυχιακή.

Την οικογένεια μου και τους φίλους μου που οποιεσδήποτε υποδείξεις και αναφορές βοήθησαν στην σύνταξη και ολοκλήρωση της εργασίας.

Και τέλος, να ευχαριστήσω το τμήμα Τηλεπικοινωνιακών Συστημάτων & Δικτύων (τέως Μηχανικών Πληροφορικής Τ.Ε.) και τους καθηγητές του για τις βάσεις που προσέφερε και τις γενικές γνώσεις πάνω στο αντικείμενο της πληροφορικής.

Περιεχόμενα

Εικόνες

1. Εισαγωγή

Στην συγκεκριμένη πτυχιακή εργασία, θα γνωρίσουμε τις μεθόδους που ακολουθούνται για την αναζήτηση των αποδεικτικών στοιχείων σε έναν υπολογιστή ή σε μια δικτυακή συσκευή, καθώς επίσης και τα εργαλεία που χρησιμοποιούνται για την αναζήτηση επίσης, αλλά κυρίως για την επεξεργασία των αποδεικτικών στοιχείων.

Τα εργαλεία αυτά μπορεί να είναι μια απλή εφαρμογή ή ένα σύνολο εφαρμογών, η λεγόμενη σουίτα, οι οποίες εφαρμογές μπορεί να είναι ειδικά σχεδιασμένες για χρήση σε εγκληματολογική έρευνα ή να είναι κοινά εργαλεία που χρησιμοποιούνται από απλούς χρήστες για διάφορους σκοπούς, αλλά εξυπηρετούν και τις ανάγκες της εγκληματολογικής έρευνας.

Τα λειτουργικά συστήματα με τα οποία θα ασχοληθούμε είναι κυρίως τα Windows και τα Linux. Σε κάποιες περιπτώσεις θα αναφερθούμε και σε άλλα λειτουργικά όπως τα OS X, Solaris, FreeBSD και τα υπόλοιπα της οικογένειας των Unix συστημάτων. Κάποια εργαλεία και λογισμικά που θα δούμε παρακάτω, υποστηρίζονται από πολλά OS, οπότε έτσι διευκολύνεται σχετικά η δουλειά που έχει να κάνει ένας ερευνητής σε μια συσκευή.

Επίσης θα περιγράψουμε το νομικό πλαίσιο που ισχύει στην Ελλάδα και διέπει την εγκληματολογική επιστήμη ως προς την εφαρμογή της και την χρήση των πειστηρίων, ακόμη και για τα προσωπικά δεδομένα.

2. Επιστήμη της Εγκληματολογίας

Η Εγκληματολογία, είναι η επιστήμη που ασχολείται με την μελέτη του εγκλήματος, από πλευράς κοινωνικού φαινομένου και προϊόν της δραστηριότητας, καθώς επίσης και με τις μεθόδους πρόληψης και καταστολής του. Συγκεκριμένα, πρόκειται για ένα σύνολο διαφόρων κλάδων της επιστήμης, αφού επιστήμες όπως αυτή της Κοινωνιολογίας, Ψυχιατρικής, Στατιστικής, Βιολογίας, Πληροφορικής κ.ά., συνεισφέρουν με πορίσματα και μεθόδους στην λύση της υπόθεσης.

Κατά την διάρκεια της εγκληματολογικής έρευνας, ακολουθούνται τρία βήματα:

- ✓ Συλλογή αποδεικτικών στοιχείων από τον χώρο του εγκλήματος
- ✓ Ανάλυση και επεξεργασία των αποδεικτικών στοιχειών

- ✓ Παρουσίαση αποτελεσμάτων στο δικαστήριο

Ανάλογα με την υπόθεση, τα αποδεικτικά στοιχεία μπορεί να διαφέρουν σε όγκο και πλήθος και έτσι να διαφέρει και ο χρόνος που χρειάζεται για την επεξεργασία τους. Επίσης, ανάλογα με την δυσκολία της φύσης των αποδεικτικών στοιχείων, καλούνται να συμμετάσχουν στην έρευνα ειδικοί σε διάφορους κλάδους, όπως της πληροφορικής, της ιατρικής, της χημείας και άλλων επιστημών. Αυτοί οι ερευνητές εργάζονται ξεχωριστά για την επεξεργασία των αποδεικτικών στοιχείων και στο τέλος συνδυάζουν τα αποτελέσματα τους για να συγκροτηθεί το προφίλ της υπόθεσης.

Όταν γίνεται η παρουσίαση των αποτελεσμάτων της εγκληματολογικής εξέτασης των πειστηρίων στο δικαστήριο, πρέπει επίσης να αποδειχθεί ότι κατά την διάρκεια της συλλογής και επεξεργασίας τους, δεν αλλοιώθηκαν τα αποδεικτικά στοιχεία.

2.1 Επιστήμη της Ψηφιακής Εγκληματολογίας

Η Ψηφιακή Εγκληματολογία είναι κλάδος της ευρύτερης επιστήμης της Εγκληματολογίας και περιλαμβάνει την συνεργασία των κλάδων της Πληροφορικής. Είναι ένας κλάδος ο οποίος χρόνια με τα χρόνια εξελίσσεται συνεχώς, ώστε να καλύπτει όσο το δυνατόν περισσότερες ανάγκες της εγκληματολογίας και για την εξεύρεση περισσότερων πληροφοριών από τα αποδεικτικά στοιχεία.

Στην Ψηφιακή Εγκληματολογία, υπάγονται 3 κλάδοι:

- Εγκληματολογία Υπολογιστών
- Εγκληματολογία Δικτύων
- Εγκληματολογία Κινητών Συσκευών

Η Ψηφιακή Εγκληματολογία δεν αφορά μόνο σε επίπεδο λογισμικού, δηλαδή λειτουργικό σύστημα, αλλά και σε επίπεδο υλικού, όπως για παράδειγμα ένας πομπός GPS ο οποίος βρίσκεται εντός μιας κινητής συσκευής, λειτουργεί ανεξάρτητα από το κινητό και εκπέμπει σήμα συνεχώς.

Εφαρμογές του κλάδου αυτού υπάρχουν παντού, εκτός από συμμετοχή σε υποθέσεις ενώπιον δικαστηρίου, επίσης και σε θέματα δικτυακής ασφάλειας για εταιρίες ή υπηρεσίες

του δημοσίου, συνήθως για δικτυακές εισβολές.

2.1.1 Εγκληματολογία Υπολογιστών

Η Εγκληματολογία Υπολογιστών, αφορά με την εφαρμογή ειδικών τεχνικών σε επίπεδο εφαρμογών, λειτουργικού συστήματος και δομών αρχείων, με σκοπό την εξαγωγή πληροφοριών, όπως το πότε προσπελάστηκε τελευταία φορά ένα αρχείο, τις αναζητήσεις έκανε στο Διαδίκτυο, τι email έλαβε, ώστε να αποφασιστεί για παράδειγμα κατά πόσο είχε γνώση ο κατηγορούμενος για το περιεχόμενο ενός αρχείου ή για πληροφορίες για ένα θέμα. Είναι η κύρια κατηγορία που εμπίπτει στην εγκληματολογική έρευνα, καθώς σχεδόν πάντα σε υποθέσεις τέτοιου είδους βρίσκουμε σημαντικές πληροφορίες σε έναν υπολογιστή.

2.1.2 Εγκληματολογία Δικτύων

Η Εγκληματολογία Δικτύων, αφορά την απόκτηση πληροφοριών σχετικά με την κίνηση σε ένα δίκτυο, οι οποίες μπορεί να φανούν σημαντικές στην εξέλιξη της υπόθεσης. Τις περισσότερες φορές, αυτού του είδους η εγκληματολογία χρησιμοποιείται για αναζήτηση στοιχείων σχετικά με απομακρυσμένες δικτυακές επιθέσεις και αφορά δηλαδή κυρίως την δικτυακή ασφάλεια των υπολογιστικών συστημάτων, κάτι που δεν έχει σχέση πολλές φορές με συνηθισμένες υποθέσεις της αστυνομίας.

2.1.3 Εγκληματολογία Κινητών Συσκευών

Η Εγκληματολογία Κινητών Συσκευών, αφορά την ανάκτηση ψηφιακών αποδεικτικών στοιχείων από κινητές συσκευές, όπως κινητό τηλέφωνο, GPS, φωτογραφική μηχανή, smartphone, tablet και άλλα. Τα αποδεικτικά στοιχεία μπορεί να βρίσκονται είτε στην εσωτερική μνήμη της συσκευής είτε σε εξωτερική μνήμη, όπως MicroSD κάρτες, είτε επίσης σε κάρτα SIM. Τα στοιχεία που συνήθως έχουν σημασία είναι οι κλήσεις, τα μηνύματα, οι φωτογραφίες και τα βίντεο.

2.2 Νομικό Πλαίσιο Εγκληματολογίας

Το νομικό πλαίσιο που διέπει την εφαρμογή της Εγκληματολογίας στην Ελλάδα, αποτελείται από μια σειρά νόμων, αποφάσεων, Προεδρικών Διαταγμάτων και άρθρων του Ποινικού Κώδικα σχετιζόμενα κυρίως με τα προσωπικά δεδομένα και το απόρρητο των επικοινωνιών.

Θα δούμε μερικά παραδείγματα νόμων και Προεδρικών Διαταγμάτων, όπως ισχύουν μέχρι σήμερα.

Νόμος 2472/1997

Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (με ενσωματωμένες τις τροποποιήσεις)

Άρθρο 2
α) "Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. β) "Ευαίσθητα δεδομένα", τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
Άρθρο 4
1. Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει : α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών. β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας. γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
Άρθρο 10
1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του.

2. Για τη διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Άρθρο 14

1. Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή, νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.

2. Το δικαίωμα του παρόντος άρθρου μπορεί να ικανοποιηθεί και όταν δεν συντρέχουν οι λοιπές ουσιαστικές προϋποθέσεις της προσωρινής δικαστικής προστασίας, όπως προβλέπονται κάθε φορά.

Νόμος 2867/2000

Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις

Άρθρο 9

5. Υπό την επιφύλαξη των διατάξεων της κείμενης νομοθεσίας για την προστασία των προσωπικών δεδομένων, οι τηλεπικοινωνιακές επιχειρήσεις που παρέχουν υπηρεσίες Φωνητικής Τηλεφωνίας ή Κινητής και Προσωπικής Επικοινωνίας οφείλουν να εκδίδουν σε έντυπη ή/και ηλεκτρονική μορφή ονομαστικούς τηλεφωνικούς καταλόγους των συνδρομητών που δεν έχουν δηλώσει ρητά αντίρρηση στην καταχώρηση τους στους ως άνω τηλεφωνικούς καταλόγους. Σε όλους τους Χρήστες, συμπεριλαμβανομένων των Χρηστών κοινοχρήστων τηλεφώνων, διατίθεται μία τουλάχιστον υπηρεσία πληροφοριών τηλεφωνικού καταλόγου, η οποία καλύπτει όλους τους καταχωρημένους συνδρομητικούς αριθμούς Φωνητικής Τηλεφωνίας ή Κινητής και Προσωπικής Επικοινωνίας.

Νόμος 3115/2003

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Άρθρο 6 (Παράγραφος 1)

δ) Προβαίνει στην κατάσχεση μέσων παραβίασης του απορρήτου, που υποπίπτουν στην

αντίληψη της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

ε) Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

Προεδρικό Διάταγμα 47

Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του.

Άρθρο 3

1. Η άρση του απορρήτου δεν αφορά την δια ζώσης επικοινωνία, αλλά κάθε είδους επικοινωνία, η οποία διεξάγεται μέσω δικτύου επικοινωνίας ή παρόχου υπηρεσιών επικοινωνιών και την οποία χρησιμοποιεί ο συνδρομητής ή χρήστης κατά του οποίου λαμβάνεται το μέτρο της άρσης.

Άρθρο 8

7. Σε περίπτωση που ένας πάροχος υπηρεσίας χρησιμοποιεί μεθόδους κωδικοποίησης, συμπίεσης ή κρυπτογράφησης, υποχρεούται κατά την εκτέλεση μιας διάταξης να παραδίδει ή διαβιβάζει τα ζητούμενα στοιχεία σε αποκωδικοποιημένη μορφή.

Νόμος 3471/2006

Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Άρθρο 6

1. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον φορέα παροχής δημοσίου δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών υπηρεσιών, με τη λήξη της επικοινωνίας καταστρέφονται ή καθίστανται ανώνυμα με κατάλληλη κωδικοποίηση, με την επιφύλαξη της παραγράφου 2 του παρόντος άρθρου και της παραγράφου 5 του άρθρου 5.

Ποινικός Κώδικας

Άρθρο 370Α

3. Με φυλάκιση τουλάχιστον ενός έτους τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

4. Η πράξη της παραγράφου 3 δεν είναι άδικη, αν η χρήση έγινε ενώπιον οποιασδήποτε δικαστικής ή άλλης ανακριτικής αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος, που δεν μπορούσε να διαφυλαχθεί διαφορετικά.

3. Εγκληματολογική εξέταση μαγνητικών μέσων αποθήκευσης

Όταν αναφερόμαστε στα μαγνητικά μέσα αποθήκευσης δεδομένων, μιλάμε για οτιδήποτε περιέχετε μέσα σ ’αυτά, δηλαδή file system και λειτουργικό σύστημα, όπου είναι οι πληροφορίες για τα αρχεία και το περιεχόμενο τους. Η ανάκτηση αυτών των πληροφοριών μπορεί να γίνει και σε επίπεδο software, δηλαδή μέσα από command line ή μέσα από ειδικά προγράμματα, και σε επίπεδο hardware, για παράδειγμα ειδική ανάλυση των δίσκων ως φυσικό μέσο.

Κάθε λειτουργικό σύστημα έχει διαφορετικούς τρόπους όπου αποθηκεύει πληροφορίες για τις εφαρμογές. Κάτι παρόμοιο ισχύει και για τα file systems, όπου το κάθε ένα αποθηκεύει διαφορετικές πληροφορίες για τα αρχεία και διαφορετικό τρόπο όπου αποθηκεύει τις πληροφορίες αυτές.

Operating Systems

Όπως είπαμε και πιο πάνω, υπάρχουν διάφορα λειτουργικά συστήματα είτε για υπολογιστές είτε για κινητές συσκευές, όμως εμείς θα ασχοληθούμε κυρίως με **Windows** & **Linux** για υπολογιστές και **Android** & **iOS** για κινητές συσκευές, μιας και είναι τα πιο διαδεδομένα και πιο εμπορικά OS που υπάρχουν μέχρι ώρας.

Για τα **Windows**, οι πιο χρησιμοποιημένες κατηγορίες είναι τα Windows 9x και Windows NT. Τα Windows 9x περιλαμβάνουν τα 95, 98 και ΜΕ. Τα Windows NT χρησιμοποιούνται από το 2000 και ύστερα περισσότερο όπου ιδιαίτερη φήμη και χρησιμότητα έχουν τα XP, 7 και 8.

Παρά την λήξη της υποστήριξης των XP από τον Απρίλιο του 2014, υπάρχουν αρκετοί υπολογιστές που έχουν XP πάνω τους κι αυτό κυρίως γιατί κάποια υπηρεσίες και προγράμματα που τρέχουν, δεν υποστηρίζονται από πιο καινούργια λειτουργικά.

Για τα **Linux**, οι πιο γνωστές διανομές είναι τα Debian, Fedora, Gentoo και Ubuntu. Πιο χρησιμοποιημένα για απλή χρήση είναι τα Ubuntu, ενώ για πιο εξειδικευμένες χρήσεις, όπως για στήσιμο server, είναι τα Debian.

File Systems

Όπως για τα λειτουργικά, έτσι και τα file systems είναι πολλά και κάποια μοιάζουν μεταξύ τους. Κάποια file systems είναι σχεδιασμένα για συγκεκριμένα λειτουργικά συστήματα, τα οποία θα δούμε παρακάτω.

Στα **Windows** χρησιμοποιούνται κατά κόρον δύο file systems, το **NTFS** ή το **FAT**, το οποίο περιλαμβάνει τις εκδόσεις **FAT12**, **FAT16** και **FAT32**. Ένα χαρακτηριστικό αυτών των file systems είναι ότι για συντομεύσεις αρχείων, δημιουργούν αρχεία link με κατάληξη **.lnk**. Οι συντομεύσεις αυτές δημιουργούνται όταν εκτελείται ένα αρχείο και βρίσκονται σε προκαθορισμένες διαδρομές.

Για παράδειγμα, στα *Windows 7* τα **.lnk** αρχεία μπορεί να τα βρει κανείς σε θέσεις, όπως:

- **C:\Users\user\Recent**, η οποία δεν φαίνεται στον explorer
- **C:\Users\user\AppData\Roaming\Microsoft\Office\Recent**
- **C:\Users\user\AppData\Roaming\Microsoft\Office\Πρόσφατο**
- **C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent**

Στα **Linux**, λόγω του ότι είναι open source, έχουν δημιουργηθεί διάφορα file systems, με το πιο καινούργιο να έχει δημοσιευθεί το 2012. Από προεπιλογή όμως τα Linux χρησιμοποιούν το **ext**, το οποίο περιλαμβάνει τις εκδόσεις **ext2**, **ext3** και **ext4**. Ένα χαρακτηριστικό των file systems των Linux, είναι ότι για συντομεύσεις αρχείων, δημιουργούν **inodes**.

8.3 ονόματα αρχείων

Είναι συντομευμένα ονόματα αρχείων, ξεκίνησαν από τα **DOS** και χρησιμοποιούνται κυρίως για ευκολία χρήσης των φακέλων και αρχείων στο command prompt, όταν οι διαδρομές αρχείων και καταλόγων είναι μεγάλες είτε έχουν κενούς χαρακτήρες. Αξίζει να σημειωθεί ότι τα ονόματα αυτά είναι πάντα με κεφαλαία.

Ο τρόπος που μετατρέπεται ένα όνομα από συμβατό σε 8.3 μορφή, είναι 8 χαρακτήρες για το βασικό όνομα του αρχείου, και 3 χαρακτήρες για την επέκταση του αρχείου. Στους 8

χαρακτήρες, όταν οι πρώτοι 6 είναι ίδιοι, τότε ο 7ος χαρακτήρας είναι το σύμβολο ~ και ο 8ος χαρακτήρας είναι ένας αύξων αριθμός, που ξεκινά από το 1.

Διεγραμμένα αρχεία

Όταν διαγράφεται ένα αρχείο, δεν διαγράφεται πραγματικά. Τα δεδομένα του παραμένουν στα clusters του δίσκου όπου ήτανε, απλώς τώρα θα επισημανθούν ότι είναι για διαγραφή κι έτσι θα μπορεί ο δίσκος να πηγαίνει να γράψει άλλα δεδομένα από πάνω.

Γι' αυτό όταν διαγράφεται ένα αρχείο κατά λάθος, πρέπει να σταματήσουν άμεσα οποιεσδήποτε εργασίες στον υπολογιστή, ώστε να μην μειωθούν οι πιθανότητες να ανακτηθεί το αρχείο ή μέρος αυτού. Αν τύχει και ο δίσκος γράψει νέα δεδομένα στο cluster που υπάρχουν τα παλιά, αυτά μπορεί να γραφτούν σε μικρότερο μήκος από τα παλιά κι έτσι να σωθούν έστω και λίγα δεδομένα, αλλιώς αν γράψει σε ίσο ή μεγαλύτερο μήκος, τότε είναι αδύνατο να ανακτηθούν τα δεδομένα.

3.1 Μέθοδοι

Ως μέθοδοι, αναφερόμαστε όχι μόνο στο που μπορεί κάποιος να βρει κάποια συγκεκριμένα αρχεία με σημαντικές πληροφορίες, αλλά και στα εργαλεία που εμπεριέχονται στα ίδια τα OS και μπορούν να χρησιμοποιηθούν από οποιονδήποτε, χωρίς να κατεβάσει κάποιο τρίτο πρόγραμμα για να κάνει την δουλειά του.

Εδώ, θα δούμε για κάθε λειτουργικό σύστημα και για κάθε file system πως και ποιές πληροφορίες των αρχείων αποθηκεύονται.

3.1.1 attrib

Η **attrib** είναι εντολή που υπάρχει στα DOS, OS/2 και Windows και μπορεί να τροποποιήσει τα χαρακτηριστικά ενός αρχείου ή καταλόγου.

Η σύνταξη της εντολής είναι:

attrib [options] <*file* | *directory*>

+	Ορισμός ενός χαρακτηριστικού.
–	Απαλοιφή ενός χαρακτηριστικού.
A	Χαρακτηριστικό φύλαξης αρχείου.
H	Χαρακτηριστικό κρυφού αρχείου.

I	Χαρακτηριστικό αρχείου χωρίς ευρετήριο περιεχομένων.
R	Χαρακτηριστικό αρχείου μόνο για ανάγνωση.
S	Χαρακτηριστικό αρχείου συστήματος.
/D	Επεξεργάζεται επίσης καταλόγους.
/L	Εργασία στα χαρακτηριστικά της συμβολικής σύνδεσης ως προς τον προορισμό της συμβολικής σύνδεσης.
/S	Επεξεργάζεται τα αρχεία που βρίσκονται και σε υποκαταλόγους.

Αν η εντολή γραφτεί σκέτη, τότε θα εμφανίσει όλα τα αρχεία του τρέχοντος καταλόγου και τι ιδιότητες έχουν.

Τα αρχεία τα όποια έχουν τα χαρακτηριστικά **S** και **H**, δηλαδή αρχείο συστήματος και κρυφό αρχείο, τότε αυτά τα αρχεία δεν θα φαίνονται στον Explorer των Windows, αλλά ούτε και στην εντολή **dir**.

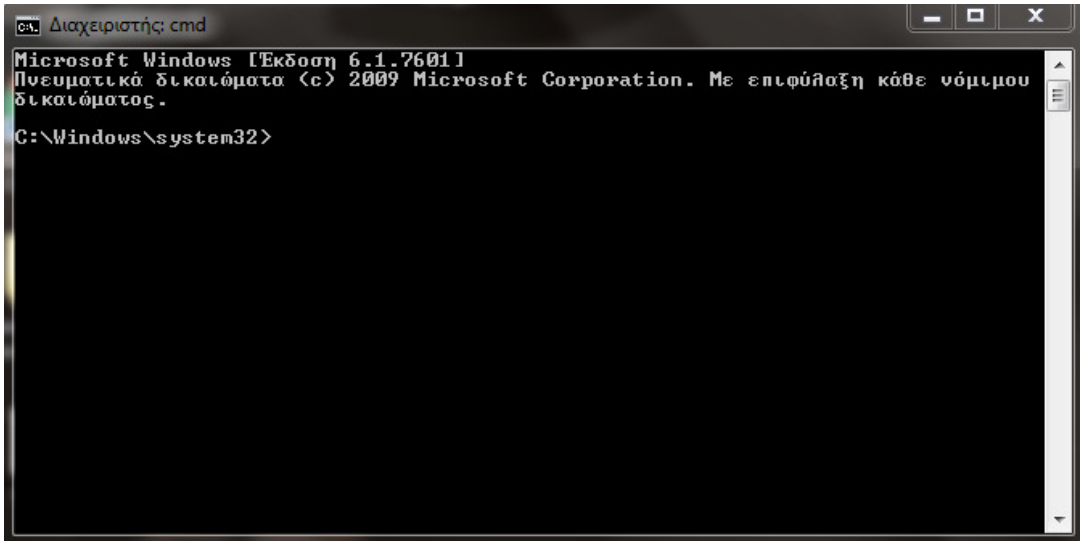
3.1.2 Command prompt

Το **command prompt** είναι εργαλείο γραμμής εντολών, το οποίο είναι προ-εγκατεστημένο σε οποιοδήποτε OS. Η λειτουργία του είναι η επικοινωνία χρήστη-μηχανής μέσω εντολών, οι οποίες μπορεί να είναι είτε ενεργές, δηλαδή να αλλάζουν ρυθμίσεις ή να κάνουν κάποια άλλη πράξη, είτε παθητικές, δηλαδή να εμφανίζουν το αποτέλεσμα μιας αναζήτησης ή τις πληροφορίες του συστήματος.

Για κάθε OS, το εργαλείο αυτό ονοματίζεται διαφορετικά, για παράδειγμα στα **Windows** ονομάζεται **cmd.exe**, στα **Unix** ονομάζεται **Bash** και στα **Mac** συστήματα ονομάζεται **Terminal**. Επίσης, ανά οικογένεια OS, διαφοροποιείται και το σύνολο των εντολών που εμπεριέχονται μέσα σε αυτό. Αυτά τα τρία εργαλεία είναι τα προεπιλεγμένα των λειτουργικών αυτών συστημάτων, καθώς υπάρχουν ένα σωρό άλλα παρόμοια εργαλεία.

Επειδή υπάρχουν προγράμματα που υποστηρίζουν εντολές τύπου γραμμής εντολών, χρησιμοποιείται ένα command line interface, δηλαδή μια διεπαφή για επικοινωνία χρήστη-προγράμματος.

Όσο θα προχωράμε παρακάτω, θα βρίσκουμε εργαλεία τα οποία χρησιμοποιούν CLI και εντολές χρήσιμες για την εγκληματολογική έρευνα, οπότε θα είναι υποχρεωτική η χρήση ενός command prompt.

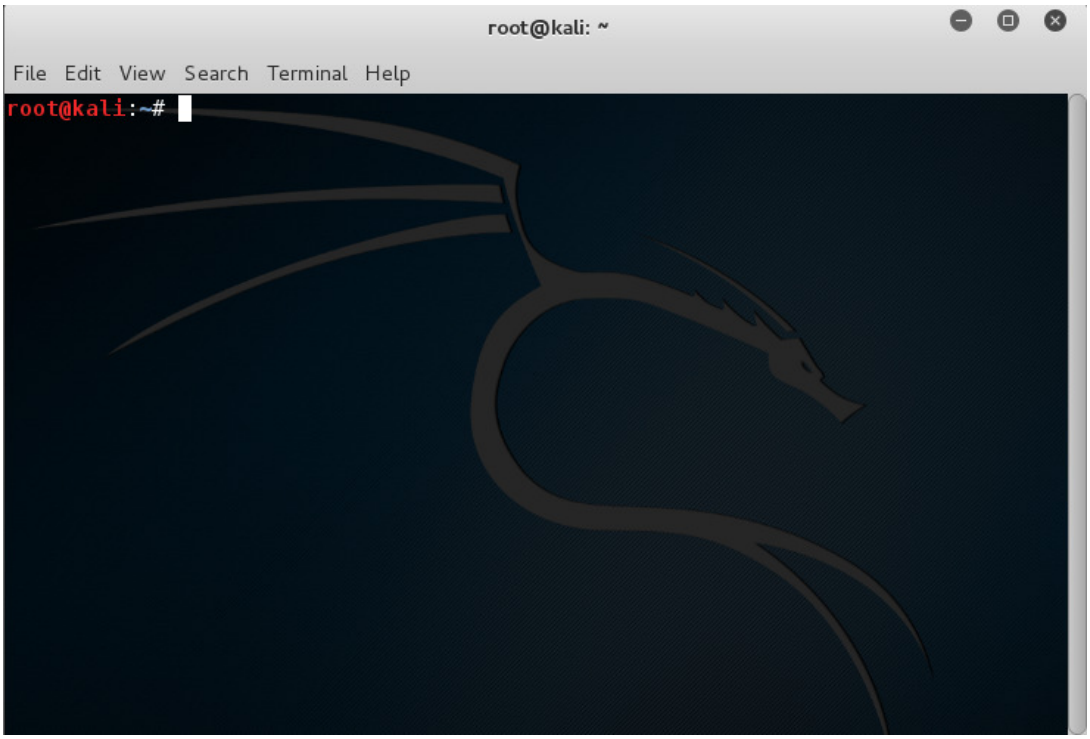


Εικόνα 3.1: Το cmd των Windows

Το **cmd.exe** υπάρχει στα eComStation, OS/2, Windows CE και Windows NT.

Για να το ανοίξετε στα Windows XP και πριν, πηγαίνετε στο μενού Έναρξη, μετά στην Εκτέλεση, γράψτε cmd και πατήστε **Enter**. Ή αλλιώς, πηγαίνετε **Όλα τα προγράμματα > Βοηθήματα > Γραμμή εντολών**.

Για να το ανοίξετε στα Windows Vista και μετά, πηγαίνετε στο μενού Έναρξη και γράψτε πλαίσιο κάτω αριστερά cmd και πατήστε **Enter**, για απλή εκτέλεση ή **Ctrl+Shift+Enter** για να το τρέξετε ως διαχειριστής, καθώς κάποιες εντολές χρειάζονται άδεια διαχειριστή για να εκτελεστούν.



Εικόνα 3.2: Το terminal των Kali Linux

Στα Linux συστήματα, το προεπιλεγμένο command prompt που χρησιμοποιείται, είναι το

Bash, το οποίο είναι διερμηνέας γραμμής εντολών όπως το cmd.exe των Windows, φτιαγμένο για το GNU Project και από το 1989 που δημοσιεύτηκε, χρησιμοποιείται ευρέως και εκτός των Unix, σε συστήματα που βασίζονται στον Linux Kernel, όπως στα Windows μέσω Cygwin και στα Android.

Το **Terminal.app** είναι του OS X και είναι εξομοιωτής τερματικού. Η διαφορά με τα δύο προηγούμενα, είναι ότι το **Terminal.app** είναι ένα γραφικό περιβάλλον στο οποίο ο χρήστης έχει μεγαλύτερη αλληλεπίδραση σε σύγκριση με τον διερμηνέα γραμμής εντολών.

3.1.3 df

Το **df** είναι εργαλείο των Unix συστημάτων και δείχνει πόσο ελεύθερο χώρο έχουν τα file systems για τα οποία έχει δικαιώματα ανάγνωσης ο χρήστης.

Η σύνταξη της εντολής είναι:

df [options]

–a	Συμπεριλαμβάνει ψεύτικα file systems.
–B	Εμφανίζει τα μεγέθη ανάλογα με το δοθέν μέγεθος.
--total	Παράγει ένα σύνολο.
–h	Τυπώνει τα μεγέθη σε ευανάγνωστη για τον άνθρωπο μορφή.
–H	Αντίστοιχα με την **–h**, αλλά χρησιμοποιεί δυνάμεις του 1000 αντί του 1024.
–i	Τυπώνει πληροφορίες για το inode αντί για την χρήση του μπλοκ.
–k	Η επιλογή **–B** για μέγεθος K.
–l	Περιορίζει την λίστα σε τοπικά file system.
--no-sync	Δεν επιδιώκει συγχρονισμό πριν πάρει τις πληροφορίες χρήσης.
–P	Χρησιμοποιεί την μορφή εξόδου POSIX.
--sync	Επιδιώκει συγχρονισμό πριν πάρει τις πληροφορίες χρήσης.
–t	Τυπώνει τα file systems ανάλογα με τον δοθέν *τύπο*.
–T	Τυπώνει τον τύπο του file system.
–x	Δεν τυπώνει τα file systems που είναι του δοθέντος *τύπου*.

Για την επιλογή **–B**, το δοθέν μέγεθος μπορεί να είναι από τα εξής:

- **K** ή **KB**
- **M** ή **MB**
- **G** ή **GB**
- **T** ή **TB**
- **P** ή **PB**
- **E** ή **EB**
- **Z** ή **ZB**
- **Y** ή **YB**

Μπορεί να περιέχεται και αριθμός μπροστά, για παράδειγμα 1000 ή 1000*1000 ή 1024 ή 1024*1024.

3.1.4 dir / ls

Η **dir** είναι εντολή των DOS και Windows και εμφανίζει λίστα με τα αρχεία και τους φακέλους ενός καταλόγου. Το ίδιο ακριβώς ισχύει και για την **ls**, η οποία υπάγεται στα Unix συστήματα. Και οι δύο είναι σημαντικές εντολές και απαιτούνται τόσο στην εγκληματολογική ανάλυση, όσο και στην καθημερινή χρήση των συστημάτων.

Η σύνταξη της **dir** είναι απλή, έχει όμως και διάφορες χρήσιμες επιλογές:

dir <*file* | *directory*> [flags]

/A:*attribute*	Εμφανίζει αρχεία με καθορισμένα χαρακτηριστικά.
/B	Εμφανίζει μόνο τους τίτλους των αρχείων.
/C	Δεν τοποθετούνται τα διαχωριστικά στα μεγέθη, δηλαδή οι τελείες ή τα κόμματα.
/D	Τα αρχεία εμφανίζονται σε στήλες, ώστε να μην απαιτείται σκρολλάρισμα.
/L	Εμφανίζει τα αρχεία με πεζά γράμματα.
/N	Εμφανίζει την λίστα με τα ονόματα των αρχείων στα δεξιά.
/O:*sort_order*	Εμφανίζει τα αρχεία ταξινομημένα.
/P	Σταματά κάθε φορά που η οθόνη γεμίζει. Χρήσιμο όταν είναι πολλά αρχεία.
/Q	Εμφανίζει το όνομα του κατόχου του αρχείου.
/R	Εμφανίζει εναλλακτικές ροές δεδομένων του αρχείου.
/S	Εμφανίζει και τα αρχεία που βρίσκονται στους υποκαταλόγους.
/T:*time_field*	Εμφανίζει τον χρόνο της δοσμένης δράσης.
/W	Όπως η επιλογή **/D**, αλλά η ταξινόμηση γίνεται οριζόντια.
/X	Εμφανίζει και τα σύντομα ονόματα των αρχείων, της μορφής 8.3.
/4	Εμφανίζει τετραψήφια έτη.

Για την επιλογή **/A**, τα attributes είναι:

1. **A**, αρχεία έτοιμα προς αρχειοθέτηση.
2. **D**, κατάλογοι.
3. **H**, κρυφά αρχεία.
4. **I**, αρχεία χωρίς ευρετήριο περιεχομένων.
5. **L**, σημεία νέας ανάλυσης.
6. **R**, αρχεία μόνο για ανάγνωση.
7. **S**, αρχεία συστήματος.
8. **–**, αρνητικό πρόθεμα, δηλαδή «όχι».

Η επιλογή **/C** χρησιμοποιείται από προεπιλογή. Για να μην χρησιμοποιηθεί, γράψτε **/-C**.

Η επιλογή **/N** χρησιμοποιείται από προεπιλογή. Για να εμφανίζονται τα ονόματα των αρχείων στα αριστερά, γράψτε **/-N**.

Για την επιλογή **/O**, τα χαρακτηριστική ταξινόμησης που δέχεται είναι:

- **D**, κατά αύξων ημερομηνία/ώρα.
- **E**, κατά αλφαβητική επέκταση αρχείου.
- **G**, πρώτα οι κατάλογοι ομάδων.
- **N**, κατά αλφαβητική σειρά.
- **S**, κατά αύξων μέγεθος αρχείου.
- –, αντιστρέφει την σειρά των από πάνω.

Για την επιλογή **/T**, αναφερόμαστε στα τρία ευρέως γνωστά timestamps:

1. **A**, για την τελευταία πρόσβαση.
2. **C**, για την δημιουργία.
3. **W**, για την τελευταία τροποποίηση.

Η σύνταξη της **ls** είναι ίδια, αλλά οι επιλογές της είναι περισσότερες και πιο ποικίλες:

ls [options] <*file* | *directory*>

-a	Να μην αγνοήσει εγγραφές που αρχίζουν με '**.**'.
-A	Να μην εμφανίσει τις εγγραφές '**.**' και '**..**'.
--author	Εκτυπώνει τον συντάκτη κάθε αρχείου.
-b	Εκτυπώνει οκταδικές ακολουθίες για μη-γραφικούς χαρακτήρες.
--block-size=*SIZE*	Χρησιμοποιεί block μεγέθους *SIZE*.
-B	Να μην εμφανίσει τις εγγραφές που τελειώνουν σε '**~**'.
-c	Ταξινομεί με βάση τον χρόνο τελευταίας τροποποίησης. Μαζί με την **–lt**, ταξινομεί και δείχνει τον χρόνο. Μαζί με την **–l**, δείχνει τον χρόνο και ταξινομεί με βάση το όνομα.
-C	Εμφανίζει τις εγγραφές ανά στήλη.
-d	Εμφανίζει τις εγγραφές του καταλόγου αντί των περιεχομένων και δεν διαφοροποιεί τα symlinks.
-D	Δημιουργεί έξοδο σχεδιασμένη για την λειτουργία καταλόγου του Emacs.
-f	Δεν ταξινομεί. Ενεργοποιεί την **–aU** και απενεργοποιεί την **–lst**.
-F	Προσθέτει ένδειξη στις εγγραφές, π.χ. το '**/**' για τους καταλόγους.
-g	Σαν την **–l**, αλλά δεν εμφανίζει τον κάτοχο.
-G	Εμποδίζει την εμφάνιση πληροφοριών για την ομάδα.
-h	Εμφανίζει τα μεγέθη αναγνώσιμες για τον άνθρωπο μορφές, όπως KB.
--si	Το ίδιο, αλλά χρησιμοποιείται η δύναμη του 1000, αντί του 1024.
-H *symlink*	Ακολουθεί τα symbolic links που αναφέρονται στην εντολή.
-i	Τυπώνει τον αριθμό καταλόγου του κάθε αρχείο, το λεγόμενο inode.
-l	Εμφανίζει τις εγγραφές σε μορφή μακριάς λίστας.
-L	Δείχνει πληροφορίες για το αρχείο στο οποίο παραπέμπει το symlink.
-m	Προσθέτει κόμματα ανάμεσα στις εγγραφές.
-n	Σαν την **–l**, αλλά εμφανίζει τα ID χρήστη και ομάδας, αντί του ονόματος.
-o	Σαν την **–l**, αλλά δεν εμφανίζει την ομάδα.
-p	Το ίδιο με την **–F**.
-q	Τυπώνει '**?**' αντί για μη-γραφικούς χαρακτήρες.
-Q	Τοποθετεί τα ονόματα των εγγραφών ανάμεσα σε εισαγωγικά.
-r	Αντίστροφη σειρά όταν ταξινομεί.
-R	Εμφανίζει τα περιεχόμενα όλων των υποκαταλόγων.
-s	Εμφανίζει το μέγεθος κάθε αρχείου, σε μπλοκ.
-S	Ταξινομεί με βάση το φθίνων μέγεθος αρχείου.
--show-control-chars	Εμφανίζει τους μη-γραφικούς χαρακτήρες όπως είναι.
--time=*WORD*	Μαζί με την **–l** αναγράφονται τα διάφορα timestamps των αρχείων.
--time-style=*STYLE*	Εμφανίζει το αναγραφόμενο timestamp σε συγκεκριμένη *μορφή*.
-t	Ταξινομεί με βάση τον χρόνο τροποποίησης.
-u	Ταξινομεί με βάση τον χρόνο προσπέλασης. Μαζί με την **–lt**, ταξινομεί και δείχνει τον χρόνο. Μαζί με την **–l**, δείχνει τον χρόνο και ταξινομεί με

	βάση το όνομα.
-U	Δεν ταξινομεί. Εμφανίζει τις εγγραφές όπως είναι στον κατάλογο.
-v	Ταξινομεί με βάση την έκδοση.
-x	Εμφανίζει τις εγγραφές σε σειρές αντί σε στήλες.
-X	Ταξινομεί αλφαβητικά με βάση την επέκταση του αρχείου.
-Z	Εμφανίζει το περιβάλλον ασφαλείας. Για τα **SELinux** κυρίως.
-1	Εμφανίζει μια εγγραφή ανά γραμμή.

Για τις επιλογές **–F** και **–p**, οι ενδείξεις που μπαίνουν μπροστά απ' τα αρχεία είναι:

- ***** για **εκτελέσιμο**
- **/** για **κατάλογο**
- @ για **symlink**
- **|** για **επώνυμο δίαυλο** ή αλλιώς **FIFO**
- **=** για **υποδοχή**
- **>** για **πόρτα**

Για την επιλογή **--time=***WORD*, το WORD δέχεται τις εξής τιμές:

1. Για το timestamp προσπέλασης: 'atime' ή 'access' ή 'use'.
2. Για το timestamp δημιουργίας: 'ctime' ή 'status'.

Για την επιλογή **--time-style=***STYLE*, το STYLE δέχεται τις εξής τιμές:

1. **full-iso**
2. **long-iso**
3. **iso**
4. **locale**
5. **+FORMAT**, στο οποίο μπορούν να αναφερθούν ένα ή πολλά εκ των:
    - **%Y**, για χρονολογία
    - **%m**, για μήνα
    - **%d**, για ημέρα
    - **%H**, για ώρα
    - **%M**, για λεπτά
    - **%S**, για δευτερόλεπτα

3.1.5 file

Το **file** είναι εργαλείο των Unix συστημάτων, το οποίο περιγράφει διάφορες ιδιότητες και πληροφορίες για ένα αρχείο. Μπορεί να χρησιμοποιηθεί επίσης και στην διαδικασία του debugging.

Η σύνταξη της εντολής είναι:

file [options] *file*

-b	Δεν αναγράφονται τα ονόματα των αρχείων στην έξοδο.
-c	Στην έξοδο ελέγχει την αναλυμένη μορφή του αρχείου.
-C	Δημιουργεί το αρχείο magic.mgc το οποίο περιέχει μια προ-αναλυμένη έκδοση του αρχείου.

-d	Τυπώνει μηνύματα debugging.
-e *test*	Εξαιρεί την *δοκιμή* από την λίστα δοκιμών που θα διεξαχθούν στο αρχείο.
-f *file*	Διαβάζει το *αρχείο* που θα εξεταστεί.
-F	Χρησιμοποιεί string ως διαχωριστή, αντί του '**:**'.
-h	Δεν ακολουθεί τα symlinks.
-k	Δεν σταματάει στην πρώτη αντιστοιχία.
-L	Ακολουθεί τα symlinks. Προεπιλογή.
-n	Δεν περιορίζει την έξοδο μετά τον έλεγχο κάθε αρχείου.
-N	Δεν διαφοροποιεί την μορφή της εξόδου.
-p	Διατηρεί το timestamp πρόσβασης, ώστε να μην αλλοιωθεί με την ανάγνωση του αρχείου από την file.
-r	Δεν μεταφράζει τους μη εκτυπώσιμους χαρακτήρες σε \ooo.
-s	Αντιμετωπίζει τα ειδικά αρχεία (συσκευές) ως συνηθισμένα αρχεία.
-v	Εμφανίζει πληροφορίες για την έκδοση της file.
-z	Προσπαθεί να κοιτάξει μέσα στα συμπιεσμένα αρχεία.

Για την επιλογή **–e**, οι αποδεκτές τιμές δοκιμών είναι:

- **ascii**
- **apptype**
- **compress**
- **elf**
- **soft**
- **tar**
- **tokens**
- **troff**

3.1.6 find

Το **find** είναι εργαλείο των Unix συστημάτων, το οποίο αναζητά αρχεία στο file system.

Μπορεί να κάνει αναζήτηση με βάση το όνομα του αρχείου, την επέκταση του και τα timestamps. Ιδιαίτερα χρήσιμο εργαλείο όταν θέλουμε να αναζητήσουμε ένα αρχείο ή ένα φάκελο και δεν θυμόμαστε σε ποιόν κατάλογο του root βρίσκεται.

Η σύνταξη της εντολής εμπλέκει ξεχωριστά τις λειτουργίες και τις εκφράσεις, οι οποίες μπορούν να συνδυαστούν αν χρειαστεί:

find [options] [expressions]

Τα options είναι τα εξής:

-H	Δεν ακολουθεί τα symlinks, εκτός αν τεθεί από τις παραμέτρους της εντολής.
-L	Ακολουθεί τα symlinks.
-P	Ποτέ δεν ακολουθεί τα symlinks.

Τα expressions που αποτελούνται από τελεστές, δοκιμές και επιλογές είναι:

-amin *n*	Το αρχείο προσπελάστηκε τα τελευταία *n* λεπτά.
-anewer *file*	Το *αρχείο* προσπελάστηκε πιο πρόσφατα από ότι έχει επεξεργαστεί.
-atime *n*	Το αρχείο προσπελάστηκε πριν από *n* μέρες.
-cmin *n*	Η κατάσταση του αρχείου άλλαξε τελευταία φορά πριν από *n* λεπτά.
-cnewer *file*	Η κατάσταση του *αρχείου* άλλαξε πιο πρόσφατα από ότι έχει επεξεργαστεί.
-ctime *n*	Η κατάσταση του αρχείου άλλαξε πριν από *n* μέρες.
-daystart	Μετρά τους χρόνους για τα timestamps από την αρχή της μέρες και όχι από 24 ώρες πριν.
-depth	Επεξεργάζεται τα περιεχόμενα κάθε καταλόγου πριν τον ίδιο τον κατάλογο.
-d	Συνώνυμο της επιλογής **–depth** για συμβατότητα με FreeBSD, NetBSD, OS X και OpenBSD.
-empty	Το αρχείο ή ο κατάλογος είναι άδειος.
-fstype *type*	Το αρχείο υπάγεται σε filesystem συγκεκριμένου *τύπου*.
-gid *n*	Το αριθμητικό ID της ομάδας του αρχείου είναι *n*.
-group *name*	Το αρχείο ανήκει στην *ομάδα*.
-ilname *pattern*	Όπως η επιλογή **–lname**, αλλά case insensitive.
-iname *pattern*	Όπως η επιλογή **–name**, αλλά case insensitive.
-inum *n*	Το αρχείο έχει αριθμό inode *n*.
-iregex *pattern*	Όπως η επιλογή **–regex**, αλλά case insensitive.
-iwholename *pattern*	Όπως η επιλογή **–wholename**, αλλά case insensitive.
-links *n*	Το αρχείο έχει *n* συνδέσεις.
-lname *pattern*	Το αρχείο είναι symlink του οποίου το περιεχόμενο αντιστοιχεί στο *μοτίβο*.
-maxdepth *n*	Κατεβαίνει μέχρι *n* επίπεδα καταλόγων.
-mindepth *n*	Δεν εφαρμόζει καμία ενέργεια σε λιγότερο από *n* επίπεδα καταλόγων.
-mmin *n*	Τα δεδομένα του αρχείου έχουν υποστεί επεξεργασία *n* λεπτά πριν.
-mount	Δεν κατεβαίνει επίπεδα καταλόγων σε άλλα filesystems.
-mtime *n*	Τα δεδομένα του αρχείου έχουν υποστεί επεξεργασία *n* μέρες πριν.
-name *pattern*	Αντιστοιχεί το όνομα του αρχείου με το *μοτίβο*.
-newer *file*	Το αρχείο έχει επεξεργαστεί πιο πρόσφατα από το *αρχείο*.
-nogroup	Εμφανίζει το αριθμητικό ID της ομάδας.
-noleaf	Λαμβάνει υπόψη και τους υποκαταλόγους '**.**' και '**..**'.
-nouser	Εμφανίζει το αριθμητικό ID του χρήστη.
-perm *mode*	Αρχεία που έχουν συγκεκριμένα δικαιώματα.
-regex *pattern*	Αρχεία που αντιστοιχούν με το regular expression.
-regextype *type*	Αλλάζει ο τύπος του regular expression που καταλαβαίνει η εντολή.
-samefile *inode*	Το αρχείο παραπέμπει στο ίδιο inode με αυτό που έχει δοθεί.
-size *n*	Το αρχείο χρησιμοποιεί *n* μονάδες χώρου.
-type *x*	Το αρχείο είναι τύπου *x*.
-uid *n*	Το αριθμητικό ID του χρήστη του αρχείου είναι *n*.
-used *n*	Το αρχείο έχει προσπελαστεί *n* μέρες μετά την τελευταία αλλαγή κατάστασης του.
-user *name*	Το αρχείο ανήκει στον *χρήστη*.
-wholename *pattern*	Το όνομα του αρχείου αντιστοιχεί με το *μοτίβο*.
-xdev	Δεν κατεβαίνει επίπεδα καταλόγων σε άλλα filesystems.
-xtype *x*	Το ίδιο με την επιλογή –type, εκτός αν είναι symlink.

Από προεπιλογή, η εντολή εμφανίζει όλα τα αρχεία στον τρέχοντα κατάλογο και στους υποκαταλόγους.

Για καλύτερη σαφήνεια της εκτέλεσης της εντολής, προτείνεται να μπαίνουν οι επιλογές των expressions στην αρχή, ειδάλλως προειδοποίηση θα εμφανιστεί.

Τα expressions αποτελούνται και από ενέργειες οι οποίες στην ουσία είναι άλλες εντολές των Unix και χρησιμοποιούνται με το πρόθεμα '**–** '.

Για όσες επιλογές χρησιμοποιείται και κάποιος αριθμός *n*, μπορεί να γραφτεί με 3 περιπτώσεις:

1. **+n**, για μεγαλύτερο του *n*.
2. **n**, για ακριβώς *n*.
3. **–n**, για μικρότερο του *n*.

Για την επιλογή **–anewer**, ο συνδυασμός με την επιλογή **–H** ή **–L**, εμφανίζει συνέχεια τον χρόνο προσπέλασης.

Για την επιλογή **–fstype**, μερικοί τύποι filesystems που είναι αποδεκτοί από κάποιες εκδόσεις των Unix, είναι:

- **rootfs**
- **ramfs**
- **devtmpfs**
- **sysfs**
- **nfs**
- **ufs**
- **tmp**
- **4.2**
- **4.3**
- **S51K**
- **S52K**
- **mfs**

Για την επιλογή **–perm** *mode*, το *mode* μπορεί να είναι είτε οκταδικό είτε συμβολικό.

Για την επιλογή **–regextype** *type*, το *type* έχει τις μορφές:

- **emacs**, από προεπιλογή
- **posix-awk**
- **posix-basic**
- **posix-egrep**
- **posix-extended**

Για την επιλογή **–size** *n*, μαζί με το νούμερο χρησιμοποιείται μια εκ των εξής μονάδων:

- ✓ **b** – μπλοκ των 512 byte. Προεπιλογή.
- ✓ **c** – bytes.
- ✓ **w** – λέξεις – δύο byte.
- ✓ **k** – Kilobytes – μονάδες των 1024 bytes.
- ✓ **M** – Megabytes – μονάδες των 1048576 bytes.
- ✓ **G** – Gigabytes – μονάδες των 1073741824 bytes.

Για την επιλογή **–type** *x*, οι *τύποι* αρχείου είναι:

- ➢ **b** – μπλοκ
- ➢ **c** – χαρακτήρας
- ➢ **d** – κατάλογος

- **p** – επώνυμος δίαυλος ή FIFO
- **f** – τυπικό αρχείο
- **l** – symlink
- **s** – υποδοχή
- **D** – πόρτα στο Solaris

3.1.7 grep / egrep / fgrep

Το **grep** είναι εργαλείο αναζήτησης κειμένου σε αρχεία και καταλόγους για τα Unix.

Χρήσιμο εργαλείο για σχετικά γρήγορη αναζήτηση κειμένου ακόμα και σε δυαδικά αρχεία, χωρίς να χρειαστεί να ανοιχτούν κι έτσι να εκτελεστεί για παράδειγμα κάποιος αυθαίρετος κώδικας.

Τα εργαλεία **egrep** και **fgrep** δημιουργήθηκαν με σκοπό να υλοποιήσουν ένα παραπάνω χαρακτηριστικό το οποίο προστέθηκε αργότερα και στο αρχικό grep.

Συγκεκριμένα, το **egrep** έχει την δυνατότητα να διαβάζει το μοτίβο ως εκτεταμένη έκφραση, ενώ το **fgrep** έχει την δυνατότητα να διαβάζει το μοτίβο ως σταθερά strings.

Η σύνταξη της εντολής και για τα τρία εργαλεία είναι ακριβώς η ίδια:

grep [options] <*text*> <*file*>
egrep [options] <*text*> <*file*>
fgrep [options] <*text*> <*file*>

-*n*	Ισοδύναμο με την επιλογή **–C**.
-a	Ίδια με την επιλογή **--binary-files=***text*.
-A *n*	Τυπώνει τις *n γραμμές* του τέλους του περιβάλλοντος.
-b	Τυπώνει το όφσετ με τις γραμμές εξόδου.
--binary-files=*type*	Θεωρεί ότι τα δυαδικά αρχεία είναι του δοσμένου *τύπου*.
-B *n*	Τυπώνει τις *n γραμμές* της αρχής του περιβάλλοντος.
-c	Τυπώνει τον αριθμό των αντιστοιχισμένων γραμμών
-C *n*	Τυπώνει τις *n γραμμές* του συνόλου του περιβάλλοντος.
-d *action*	Ορίζει τον τρόπο *διαχείρισης* των καταλόγων.
-D	Ορίζει τον τρόπο *διαχείρισης* των συσκευών, FIFOs και υποδοχών.
-e	Χρησιμοποιεί το *κείμενο* για αντιστοίχιση.
--exclude=*files*	Δεν ψάχνει σε αντιστοιχισμένα *αρχεία* και *καταλόγους*.
--exclude-from=*file*	Δεν ψάχνει σε αρχεία που αντιστοιχούν στα μοτίβα από το δοσμένο *αρχείο*.
--exclude-dir=*text*	Δεν ψάχνει στους καταλόγους με το συγκεκριμένο *μοτίβο*.
-E	Διαβάζει το *κείμενο* ως εκτεταμένη έκφραση.
-f *file*	Λαμβάνει το *κείμενο* από το δοσμένο *αρχείο*.
-F	Διαβάζει το *κείμενο* ως σταθερό string.
-G	Διαβάζει το *κείμενο* ως βασική έκφραση.
-h	Δεν τυπώνει το όνομα του αρχείου στην έξοδο.
-H	Τυπώνει το όνομα αρχείου για κάθε αντιστοίχιση.
-i	Αγνοεί την διάκριση των κεφαλαίων.
--include=*files*	Ψάχνει μόνο στα αντιστοιχισμένα *αρχεία*.

-I	Ίδια με την επιλογή **--binary-files=***without-match*.
-l	Τυπώνει μόνο τα ονόματα των αρχείων που περιέχουν αντιστοιχίσεις.
-L	Τυπώνει μόνο τα ονόματα των αρχείων που δεν περιέχουν αντιστοιχίσεις.
-m *n*	Σταματάει μετά τις *n αντιστοιχίσεις*.
-n	Τυπώνει τον αριθμό της γραμμής στην έξοδο.
-o	Δείχνει μόνο ένα μέρος της αντιστοιχισμένης γραμμής.
-P	Διαβάζει το *κείμενο* ως έκφραση τύπου Perl.
-q	Τυπώνει λίγα πράγματα.
-r / -R	Διαβάζει τους καταλόγους αναδρομικά. Ίδια με την επιλογή **–d** *recurse*.
-s	Δεν τυπώνει τα μηνύματα λάθους.
-T	Ευθυγραμμίζει τις καρτέλες στην έξοδο.
-v	Επιλέγει μη αντιστοιχισμένες γραμμές.
-w	Αντιστοιχίζει το *κείμενο* μόνο με ολόκληρες λέξεις.
-x	Αντιστοιχίζει το *κείμενο* μόνο με ολόκληρες γραμμές.
-z	Μια γραμμή δεδομένων τελειώσει με κενό και όχι με νέα γραμμή.
-Z	Τυπώνει κενό μετά το όνομα του αρχείου.

Δέχεται ως είσοδο το *κείμενο* που θα αναζητήσει και το *αρχείο* ή τα *αρχεία* στα οποία θα αναζητήσει.

Για την επιλογή **--binary-files=***type*, οι τύπου είναι:

- **binary**
- **text**
- **without-match**

Η επιλογή **–c** σε συνδυασμό με την επιλογή **–v**, τυπώνει τον αριθμό των μη αντιστοιχισμένων γραμμών.

Για την επιλογή **–d**, οι τρόποι διαχείρισης των καταλόγων είναι:

- **read** → Απλή ανάγνωση.
- **recurse** → Αναδρομική ανάγνωση.
- **skip** → Παράλειψη

Για την επιλογή **–D**, οι τρόποι διαχείρισης των καταλόγων είναι:

- **read**
- **skip**

3.1.8 md5sum

Το **md5sum** είναι εργαλείο για Linux, το οποίο υπολογίζει και επαληθεύει την τιμή hash ενός αρχείου.

Η σύνταξη της εντολής είναι:

md5sum [options] *file*

-b	Διαβάζει σε λειτουργία δυαδικού.
-c	Διαβάζει τα MD5 sums των αρχείων και τα ελέγχει.
--quiet	Δεν τυπώνει OK για κάθε επιτυχημένη επιβεβαίωση αρχείου.
-t	Διαβάζει σε λειτουργία κειμένου. Προεπιλογή.

-w	Προειδοποιεί για ακατάλληλα σχεδιασμένες γραμμές του checksum.

Η προεπιλεγμένη λειτουργία είναι να τυπώνει μια γραμμή με το checksum, έναν χαρακτήρα υπόδειξης τύπου (‘*’ για δυαδικό, ‘ ‘ για κείμενο) και όνομα για κάθε αρχείο.

Μια κατάσταση εξόδου με τιμή 0 δηλώνει επιτυχία, ενώ μια μη-μηδενική τιμή δηλώνει αποτυχία.

3.1.9 more

Το **more** είναι εργαλείο που συναντάει και σε Windows και σε Unix συστήματα και χρησιμοποιείται κατά κόρον για προβολή του περιεχομένου ενός αρχείου χωρίς να χρησιμοποιηθεί κάποιο άλλο πρόγραμμα.

Αυτό γίνεται συνήθως για έλεγχο αν υπάρχει επιβλαβής κώδικας, χωρίς να εκτελεστεί κατά λάθος το αρχείο.

Η σύνταξη της εντολής στα Windows είναι:

more [commands] *files*

/c	Καθαρισμός οθόνης πριν την εμφάνιση της σελίδας.
/e	Ενεργοποίηση εκτεταμένων δυνατοτήτων.
/p	Ανάπτυξη χαρακτήρων αλλαγής σελίδας.
/s	Συμπίεση πολλών κενών γραμμών σε μία.
/t *n*	Ανάπτυξη χαρακτήρων tab σε *n* διαστήματα. Προεπιλογή 8.
+*n*	Έναρξη εμφάνισης πρώτου αρχείου από την γραμμή *n*.

Τα αρχεία που δέχεται η εντολή, διαχωρίζονται με κενά.

Εάν είναι ενεργοποιημένες οι εκτεταμένες δυνατότητες της εντολής, οι επιπρόσθετες εντολές λειτουργούν:

f	Εμφάνιση επόμενου αρχείου.
p *n*	Εμφάνιση των επόμενων *n* γραμμών.
q	Έξοδος.
s *n*	Παράλειψη των επόμενων *n* γραμμών.
=	Εμφάνιση αριθμού γραμμής.
?	Εμφάνιση γραμμής βοήθειας.
<διάστημα>	Εμφάνισης επόμενης σελίδας.
<Enter>	Εμφάνιση επόμενης γραμμής.

Η σύνταξη της εντολής στα Unix είναι:

more [options]

-c	Δεν σκρολλάρει και εμφανίζει το κείμενο από την κορυφή, καθαρίζοντας τις υπόλοιπες γραμμές καθώς εμφανίζεται.
-d	Εμφανίζει βοήθεια και δεν κουδουνίζει όταν πατιούνται λάθος κουμπιά.
-f	Μετράει λογικά αντί για γραμμές οθόνης.
-l	Δεν σταματά μετά από κάθε γραμμή που περιέχει χαρακτήρα αλλαγής σελίδας.
-*n*	Ορίζει τον *αριθμό των γραμμών* ανά οθόνη.

+*n*	Εμφανίζει την αρχή του αρχείου από την γραμμή *n*.
-p	Δεν σκρολλάρει, καθαρίζει την οθόνη και έπειτα εμφανίζει το κείμενο.
-s	Ενώνει πολλαπλές κενές γραμμές σε μία.
+/*string*	Εμφανίζει την αρχή του αρχείου από την αντιστοίχιση της αναζήτησης του *string*.
-u	Καταστέλλει τις υπογραμμίσεις.
-V	Εμφανίζει πληροφορίες έκδοσης.

3.1.10 nm

Η **nm** είναι εντολή των Unix και δίνει την δυνατότητα εξέτασης δυαδικών αρχείων, συμπεριλαμβανομένου βιβλιοθήκες, μεταγλωττισμένα object modules, shared-object αρχεία και standalone εκτελέσιμα. Μπορεί να εμφανίσει τα περιεχόμενα των αρχείων και τις meta πληροφορίες τους, όπως τον πίνακα συμβόλων.

Η σύνταξη της εντολής είναι:

nm [options] *file*

–a	Εμφανίζει μόνο σύμβολα του debugger.
–A	Εμφανίζει το όνομα του αρχείου πριν από κάθε σύμβολο.
–B	Ίδια με την επιλογή **–f**, έχοντας ως έξοδο την μορφή BSD.
–C	Αποκωδικοποιεί ονόματα συμβόλων χαμηλού επιπέδου σε ονόματα επιπέδου χρήστη. Προαιρετικά δίνεται συγκεκριμένη *μορφή* αποκωδικοποίησης.
–D	Εμφανίζει δυναμικά σύμβολα αντί για κανονικά σύμβολα.
--defined-only	Εμφανίζει μόνο καθορισμένα σύμβολα.
–f	Χρησιμοποιεί έξοδος της δοσμένης *μορφής*.
–g	Εμφανίζει μόνο εξωτερικά σύμβολα.
–l	Χρησιμοποιεί τις πληροφορίες του debug για να βρει το όνομα αρχείου και τον αριθμό γραμμής για κάθε σύμβολο.
–n	Ταξινομεί τα σύμβολα αριθμητικά ανά διεύθυνση.
–p	Δεν ταξινομεί τα σύμβολα.
–P	Ίδια με την επιλογή **–f**, έχοντας ως έξοδο την μορφή POSIX.
–r	Αντιστρέφει την ταξινόμηση.
--plugin	Φορτώνει το δοθέν *plugin*.
–s	Συμπεριλαμβάνει ευρετήριο για σύμβολα από μέλη του αρχείου.
–S	Τυπώνει το μέγεθος των καθορισμένων συμβόλων.
--size-sort	Ταξινομεί τα σύμβολα ανά μέγεθος.
--special-syms	Συμπεριλαμβάνει ειδικά σύμβολα στην έξοδο.
--synthetic	Εμφανίζει συνθετικά σύμβολα.
–t	Χρησιμοποιεί το σύστημα RADIX για την αναπαράσταση των τιμών των συμβόλων.
–u	Εμφανίζει μόνο μη καθορισμένα σύμβολα.

Για την επιλογή **–C**, η δοσμένη μορφή αποκωδικοποίησης μπορεί να είναι:

- **‘arm’**
- **‘auto’**, προεπιλογή
- **‘edg’**
- **‘gnat’**

- **'gnu'**
- **'gnu-v3'**
- **'hp'**
- **'java'**
- **'lucid'**

Για την επιλογή **–f**, η δοσμένη μορφή εξόδου μπορεί να είναι:

- **'bsd'**, προεπιλογή
- **'sysv'**
- **'posix'**

3.2 Εργαλεία

Εδώ, θα αναφέρουμε τα εργαλεία που χρησιμοποιούνται για την ανάκτηση και/ή επεξεργασία των πληροφοριών που χρειαζόμαστε για την εγκληματολογική εξέταση. Υπάρχει πληθώρα τέτοιων εργαλείων που κυκλοφορούν στο Διαδίκτυο, οπότε σίγουρα θα βρίσκεται το εργαλείο για την οποιαδήποτε ανάγκη.

3.2.1 debugfs

Το **debugfs** είναι file system ειδικά φτιαγμένο για debug mode στα Linux. Μέσω αυτού του file system, μπορεί κανείς να επανασυνδέσει διαγραμμένα αρχεία με τα inodes τους.

Συγκεκριμένα, η εντολή λειτουργεί ως debugger των **ext2**, **ext3** και **ext4**.

Η σύνταξη της εντολής ορίζεται ως εξής:

debugfs [options] <*device*>

–b *n*	Χρησιμοποιεί το δοσμένο *μέγεθος μπλοκ* αντί του συνηθισμένου.
–c	Ορίζει το file system να ανοιχτεί σε καταστροφική λειτουργία.
–d *device*	Ορίζει την *συσκευή* που θα χρησιμοποιεί όταν δεν υπάρχουν μπλοκ ανάγνωσης στο εικονικό αρχείο του ext2.
–f *file*	Διαβάζει και εκτελεί τις εντολές που είναι ορισμένες στο *αρχείο*.
–i	Ορίζει ότι η *συσκευή* είναι εικονικό αρχείο του ext2, το οποίο δημιουργήθηκε με το πρόγραμμα **e2image**.
–R *cmd*	Εκτελεί συγκεκριμένη εντολή.
–s *n*	Ορίζει το υπερμπλόκ του file system να διαβάσει από τον δοσμένο αριθμό μπλοκ, αντί να χρησιμοποιεί το πρωτογενές υπερμπλόκ.
–W	Προσδιορίζει το file system να ανοιχτεί με λειτουργία ανάγνωσης–εγγραφής.

Για την επιλογή **–c**, η καταστροφική λειτουργία σημαίνει ότι τα bitmaps των inodes και των μπλοκ, δεν διαβάζονται αρχικά. Αυτό είναι χρήσιμο για όταν το file system έχει υποστεί σημαντική ζημιά, αλλά ταυτόχρονα θα είναι μόνο για ανάγνωση.

Η επιλογή **–d**, χρησιμοποιείται με την επιλογή **–i** και τα μπλοκ ανάγνωσης που δεν υπάρχουν, μπορεί να είναι δεδομένα, κατάλογος και έμμεσα μπλοκ.

Η επιλογή **–s**, χρησιμοποιείται με την επιλογή **–b** για να προσδιοριστεί και το μέγεθος του μπλοκ του file system.

Χωρίς την επιλογή **–W**, το file system θα ανοιχθεί σε λειτουργίας ανάγνωσης μόνο.

Όταν εκτελεστεί η **debugfs**, θα ανοίξει ένα ξεχωριστό session της γραμμής εντολών στο ίδιο παράθυρο, όπου ισχύουν οι παρακάτω εντολές:

bmap *inode log_block*	Τυπώνει τον αριθμό του φυσικού μπλοκ που αντιστοιχεί στον *αριθμό* του λογικού μπλοκ στο *inode*.
cat *inode*	Εμφανίζει το περιεχόμενο του *inode* αρχείου.
cd *dir*	Αλλάζει τον τρέχοντα κατάλογο στον δοσμένο.
chroot *dir*	Αλλάζει τον ριζικό κατάλογο στον δοσμένο.
close [**-a**]	Κλείνει το τρέχων file system.
clri *inode*	Καθαρίζει τα περιεχόμενα του *inode* αρχείου.
dump [**-p**] *inode file*	Πετάει τα περιεχόμενα του *inode* στο *αρχείο* εξόδου.
dump_extents [**-nl** *inode*	Εμφανίζει το εκτεταμένο δέντρο του inode.
expand_dir *dir*	Επεκτείνει τον δοσμένο *κατάλογο*.
feature (**fs_feature**) (**-fs_feature**)	Θέτει ή καθαρίζει τα χαρακτηριστικά του file system στο υπερμπλόκ. Αφού γίνει αυτό, τότε τυπώνετε η τρέχουσα κατάσταση του σετ των χαρακτηριστικών του file system.
find_free_block *c n*	Αναζητά την $1^{η}$ *μέτρηση* του ελεύθερου μπλοκ, ξεκινώντας από το *n* και το κατανέμει.
find_free_inode *dir mode*	Αναζητά ένα ελεύθερο inode και το κατανέμει.
freeb *block [cnt]*	Ορίζει το συγκεκριμένο μπλοκ ως μη κατανεμημένο.
freei *inode*	Ελευθερώνει το δοσμένο *inode*.
help	Τυπώνει αυτή την λίστα εντολών.
icheck *block(s)*	Τυπώνει λίστα των inodes που χρησιμοποιούν τα δοσμένα *μπλοκς*.
imap *inode*	Τυπώνει την τοποθεσία του δοσμένου *inode* στον πίνακα inode.
init_filesys *dev n*	Δημιουργεί ένα ext2 file system στην *συσκευή* μεγέθους *block*.
kill_file *inode*	Αφαιρεί από την μνήμη το δοσμένο inode και τα μπλοκς του.
lcd *dir*	Αλλάζει τον τρέχοντα κατάλογο του debugfs στον *κατάλογο* του file system.
ln *inode file*	Δημιουργεί έναν σύνδεσμο ονόματι *file* για το αρχείο *inode*.
logdump [**-acs**] [**-b** *block*] [**-i** *inode*] [**-f** *file*] [*output_file*]	Εμφανίζει τα περιεχόμενα της καταγραφής του ext3.
ls [**-ldp**] *dir*	Τυπώνει μια λίστα των αρχείων του δοσμένου καταλόγου.
modify_inode *inode*	Τροποποιεί τα περιεχόμενα του *inode*.
mkdir *dir*	Δημιουργεί κατάλογο.
mknod *name* [**p**|**c**|**b**] [*x y*]	Δημιουργεί αρχείο συσκευής.
ncheck *inode*	Τυπώνει λίστα με διαδρομές προς τους δοσμένους αριθμούς inodes.
open [**-cefiw**] [**-b** *n*] [**-s** *n*]	Ανοίγει ένα file system για επεξεργασία.

pwd	Τυπώνει τον τρέχοντα κατάλογο.
quit	Βγαίνει από το **debugfs**.
rdump *dir dest*	Αναδρομικά αποθηκεύει τον **κατάλογο** και τα περιεχόμενα του (αρχεία, symlinks και άλλοι κατάλογοι) σε υπάρχων δοσμένο *φάκελο*.
rm *path*	Αποσυνδέει το *αρχείο / κατάλογο*.
rmdir *dir*	Διαγράφει τον δοσμένο *κατάλογο*.
setb *block* [*count*]	Μαρκάρει το δοσμένο *μπλοκ* ως κατανεμημένο.
set_block_group *bgnum field value*	Τροποποιεί τον περιγραφέα της ομάδας μπλοκ όπως ορίζεται από το bgnum, ώστε το *πεδίο* του περιγραφέα να έχει την δοσμένη *τιμή*.
seti *inode*	Μαρκάρει το *inode* όπως χρησιμοποιείται στο inode bitmap.
set_inode_field [**-l**] *inode field value*	Τροποποιεί το *inode*, ώστε το *πεδίο* του inode να έχει την δοσμένη *τιμή*.
set_super_value [**-l**] *field value*	Ορίζει την δοσμένη *τιμή* στο *πεδίο*.
show_super_stats [**-h**]	Εμφανίζει τα περιεχόμενα των περιγραφέων των υπερμπλόκ και των ομάδες μπλοκ. Η επιλογή **–h** θα εμφανίζει μόνο τα περιεχόμενα των υπερμπλόκ.
stat *inode*	Εμφανίζει τα περιεχόμενα της δομής του *inode*.
testb *block* [*count*]	Δοκιμάζει αν το *μπλοκ* είναι μαρκαρισμένο ως κατανεμημένο στο block bitmap.
testi *inode*	Δοκιμάζει αν το *inode* είναι μαρκαρισμένο ως κατανεμημένο στο inode bitmap.
undel <*inode***>** *path*	Επαναφέρει το δοσμένο *inode* – μαζί με τις αγκύλες – ώστε αυτό και τα μπλοκ του να μαρκαριστούν για χρήση και προαιρετικά θα επανασυνδεθεί με το *path*.
unlink *path*	Αφαιρεί τον σύνδεσμο από το *αρχείο / κατάλογο* σ' ένα inode.
write *src out*	Αντιγράφει τα περιεχόμενα της πηγής στο αρχείο εξόδου στο file system.

Στην εντολή **close**, η επιλογή **–a** αποθηκεύει τις οποιεσδήποτε αλλαγές των υπερμπλόκ και των περιγραφέων ομάδων μπλοκ σε backup υπερμπλόκ, όχι μόνο στο κεντρικό υπερμπλόκ.

Στην εντολή **dump**, η επιλογή **–p** ορίζει ιδιοκτήτη, ομάδα και δικαιώματα για το *αρχείο εξόδου*.

Στην εντολή **dump_extents**, η επιλογή **–n** θα εμφανίσει μόνο τα εσωτερικά *inodes*, ενώ η επιλογή **–l** θα εμφανίσει μόνο τα άκρα – φύλλα *inodes* του δέντρου.

Για την εντολή **find_free_inode**, το *dir* προσδιορίζει τον inode αριθμό του καταλόγου όπου βρίσκεται το inode. Το *mode* προσδιορίζει τα δικαιώματα του νέου inode.

Για την εντολή **freeb**, το *count* ορίζει το πόσα μπλοκς να οριστούν ως μην κατανεμημένα από το δοσμένο *μπλοκ* και μετά.

Η εντολή **init_filesys**, δεν αρχικοποιεί πλήρως όλες τις δομές δεδομένων. Για να γίνει αυτό, χρησιμοποιείται το πρόγραμμα **mke2fs**, το οποίο ορίζει τους περιγραφείς των υπερμπλόκ και των μπλοκ.

Η εντολή **kill_file**, δεν αφαιρεί εντελώς τις εγγραφές καταλόγου. Για να γίνει αποσύνδεση του *αρχείου*, γίνεται χρήση της εντολής **rm**.

Για την εντολή **ln**, δεν επηρεάζεται ο αριθμός αναφοράς των συνδέσμων του *inode*.

Για την εντολή **logdump**, ισχύουν οι εξής επιλογές:

- Η επιλογή **–a**, τυπώνει τα δεδομένα από όλα τα μπλοκ περιγραφέων.
- Η επιλογή **–b**, τυπώνει όλες τις εγγραφές της καταγραφής που αφορούν το δοσμένο *μπλοκ*.
- Η επιλογή **–c**, τυπώνει τα περιεχόμενα από όλα τα μπλοκ δεδομένων που επιλέχτηκαν από τις επιλογές **–a** και **–b**.

- Για λοιπά *αρχεία* που περιέχουν δεδομένα της καταγραφής, γίνεται χρήση της επιλογής **–f**.
- Η επιλογή **–i** το παρακάμπτει το προεπιλεγμένο αρχείο καταγραφής από το υπερμπλόκ, καθώς ορίζει εκ νέου το *inode* της καταγραφής.
- Η επιλογή **–s** αξιοποιεί τις πληροφορίες από το backup στο υπερμπλόκ για να εντοπίσει την καταγραφή.

Για την εντολή **ls**, ισχύουν οι εξής επιλογές:

- Η επιλογή **–d**, εμφανίζει τις διεγραμμένες εγγραφές του καταλόγου.
- Η επιλογή **–l**, εμφανίζει τα αρχεία σε verbose μορφή.
- Η επιλογή **–p**, εμφανίζει τα αρχεία σε τέτοια μορφή για ευκολότερη ανάλυση από scripts και για πιο ξεκάθαρο αν υπάρχουν κενά και μη εκτυπώσιμοι χαρακτήρες στο τέλος του αρχείου.

Για την εντολή **mknod**, η συσκευή μπορεί να είναι:

- **b** → block device
- **c** → character
- **p** → named pipe

Αν οριστεί το **b** ή το **c**, πρέπει να οριστούν και οι *αριθμοί* της συσκευής.

Για την εντολή **open**, ισχύουν οι εξής επιλογές:

- Οι επιλογές **–b**, **-c**, **–i**, **–s** και **–w**, συμπεριφέρονται το ίδιο ακριβώς όπως αυτές της **debugfs**.
- Η επιλογή **–e**, ορίζει να ανοιχτεί το file system σε αποκλειστική λειτουργία.
- Η επιλογή **–f**, αναγκάζει το file system να ανοιχτεί παρά τις οποιεσδήποτε ασυμβατότητες ή άγνωστα χαρακτηριστικά του, τα οποία θα το απέτρεπαν από το να ανοιχτεί.

Στην εντολή **setb**, το *count* ορίζει ότι το μαρκάρισμα θα γίνεται για τόσα μπλοκ από το *block*.

Για τις εντολές **set_inode_field** και **set_super_value**, η επιλογή **–l** θα εμφανίσει τα έγκυρα *πεδία* που μπορούν να τεθούν αντίστοιχα.

Στην εντολή **testb**, το *count* ορίζει ότι θα δοκιμαστούν τόσα μπλοκς από το *block* και ύστερα.

Για την εντολή **undel**, πρέπει πάντα να εκτελείται μετά και η εντολή **e2fsck**, ώστε να ανακτηθούν τα διεγραμμένα αρχεία.

3.2.2 File Checksum Integrity Identifier (FCIV)

Το **FCIV** είναι εργαλείο γραμμής εντολών της Microsoft, το οποίο έχει την δυνατότητα υπολογισμού και επαλήθευσης της τιμής hash ενός αρχείου. Υποστηρίζεται από τα Windows 2000 και ύστερα.

Έχει την δυνατότητα χρήσης ενός εκ των 2 πιο γνωστών συναρτήσεων κατακερματισμού, τον **MD5** και τον **SHA-1**. Από προεπιλογή, χρησιμοποιείται ο **MD5**.

Ο **MD5** χρησιμοποιεί 128 bit ως μέγεθος σύνοψης μηνύματος και χρειάζονται 4 γύροι για να βγει αυτή η σύνοψη μηνύματος. Η συνάρτηση αυτή με τα χρόνια αποδεικνύεται αναξιόπιστη για χρήση, ώστε να καταλήξει το 2008 να χαρακτηριστεί κρυπτογραφικά σπασμένος και ακατάλληλος για περαιτέρω χρήση.

Ο **SHA-1** χρησιμοποιεί 160 bit για μέγεθος σύνοψης μηνύματος και χρειάζονται 80 γύροι για να βγει αυτή η σύνοψη μηνύματος. Κι αυτή η συνάρτηση με τα χρόνια αποδεικνύεται

αναξιόπιστη κι έτσι αναμένεται η παύση χρήσης της τα επόμενα χρόνια από Google Chrome και Mozilla Firefox.

Η χρήση του εργαλείου γίνεται με την εξής σύνταξη:

fciv.exe [commands] [options]

-add *file* | *dir*	Υπολογίζει και εμφανίζει την τιμή hash για συγκεκριμένο αρχείο ή για ολόκληρο κατάλογο.
-add *dir* **-r**	Αναδρομικά.
-add *dir* **-type**	Συγκεκριμένος τύπος αρχείων.
-add *dir* **-exc** *file*	Λίστα καταλόγων που δεν θα υπολογιστούν.
-add *dir* -**wp**	Χωρίς να εμφανίζει ολόκληρη την διαδρομή.
-add *dir* -**bp**	Αφαιρεί την διαδρομή βάσης από κάθε εγγραφή.
-list	Εμφανίζει λίστα εγγραφών που είναι αποθηκευμένα σε βάση δεδομένων.
-v	Επιβεβαιώνει τιμές hash. Μπορεί να χρησιμοποιηθεί μαζί την επιλογή –bp.
-εντολή **-md5** | **-sha1** | **-both**	Επιλογή που προσδιορίζει συνάρτηση κατακερματισμού.
-εντολή **-xml** *db*	Επιλογή που προσδιορίζει τύπο και όνομα βάσης δεδομένων.

Το xml αρχείο, αποθηκεύει τις διάφορες εγγραφές με την εξής μορφή:

```
<?xml version="1.0" encoding="utf-8"?>
<FCIV>
        <FILE_ENTRY>
                <name> </name>
                <MD5> </MD5>
                <SHA1> </SHA1>
        </FILE_ENTRY>
</FCIV>
```

Μια καλή χρήση αυτού του εργαλείου είναι η δημιουργία μιας βάσης δεδομένων με τιμές hash για γνωστά αρχεία, όπως το *cmd.exe*, ώστε για παράδειγμα όταν γίνεται εγκληματολογική εξέταση ενός υπολογιστή και ελέγχουμε τις τιμές hash, να έχουμε αυτή την βάση δεδομένων για να συγκρίνουμε τις τιμές για τα γνωστά αρχεία κι έτσι να γλυτώνουμε σχετικά χρόνο για τον ειδικό έλεγχο κάθε αρχείου.

3.2.3 FileList

Το **FileList** είναι εργαλείο γραμμής εντολών της JAM Software και έχει αποτέλεσμα ανάλογο της dir με την διαφορά ότι μπορεί να εξάγει το αποτέλεσμα σε αρχείο με μορφή CSV, ιδανικό για εισαγωγή σε βάση δεδομένων και φύλλο εργασίας του Excel. Υποστηρίζεται μόνο από τα Windows XP και ύστερα.

Η λίστα των αρχείων που εμφανίζει, περιέχει τις εξής πληροφορίες:

- όνομα αρχείου

- μέγεθος αρχείου
- διαδρομή αρχείου
- επέκταση αρχείου
- ιδιοκτήτης αρχείου
- τελευταία ημερομηνία τροποποίησης
- τελευταία ημερομηνία προσπέλασης
- ημερομηνία δημιουργίας

Επίσης, μέσω των επιλογών του εργαλείου μπορούν να ζητηθούν επιπλέον πληροφορίες:

- συντάκτης εγγράφων του Office
- MD5 checksum
- SHA256 checksum
- πληροφορίες έκδοσης για αρχεία προγραμμάτων
- επίπεδο βάθους καταλόγου
- αριθμός αναφοράς του NTFS
- ημερομηνίες αρχείου σε μορφή ISO

Η χρήση του εργαλείου γίνεται με την εξής σύνταξη:

FileList.exe [options]

/ATTRIBUTEFILTER	Φιλτράρει τα αρχεία με βάση τα χαρακτηριστικά τους.
/COLUMNS	Συμπεριλαμβάνει ένα σετ από στήλες, διαχωρισμένες με κόμμα.
/FILTER	Επιτρέπει την χρήση φίλτρων, χωρισμένων με ερωτηματικό.
/FULLPATH	Εμφανίζει ολόκληρη την διαδρομή του κάθε αρχείου, αντί να χρησιμοποιεί ξεχωριστές στήλες για όνομα και διαδρομή.
/ISO	Εμφανίζει τις ημερομηνίες σε μορφή ISO.
/LISTSEPARATOR	Επιτρέπει να τεθεί διαφορετικός χαρακτήρας διαχωρισμού των στηλών.
/MINDATE	Εμφανίζει τα αρχεία που τροποποιήθηκαν νωρίτερα από την ημερομηνία που τέθηκε, η οποία έχει την μορφή *yyyy-mm-dd*.
/MINSIZE	Εμφανίζει τα αρχεία που έχουν μεγαλύτερο μέγεθος από αυτό που τέθηκε, το οποίο δίδεται σε bytes.
/NOHEADER	Δεν εμφανίζει τους τίτλους των στηλών.
/NOTITLE	Παραλείπει τις 2 πρώτες σειρές που προσδιορίζουν την τοποθεσία, αλλά εμφανίζει του τίτλους των στηλών.

Στο **/COLUMNS**, οι στήλες που μπορεί να συμπεριληφθούν είναι:

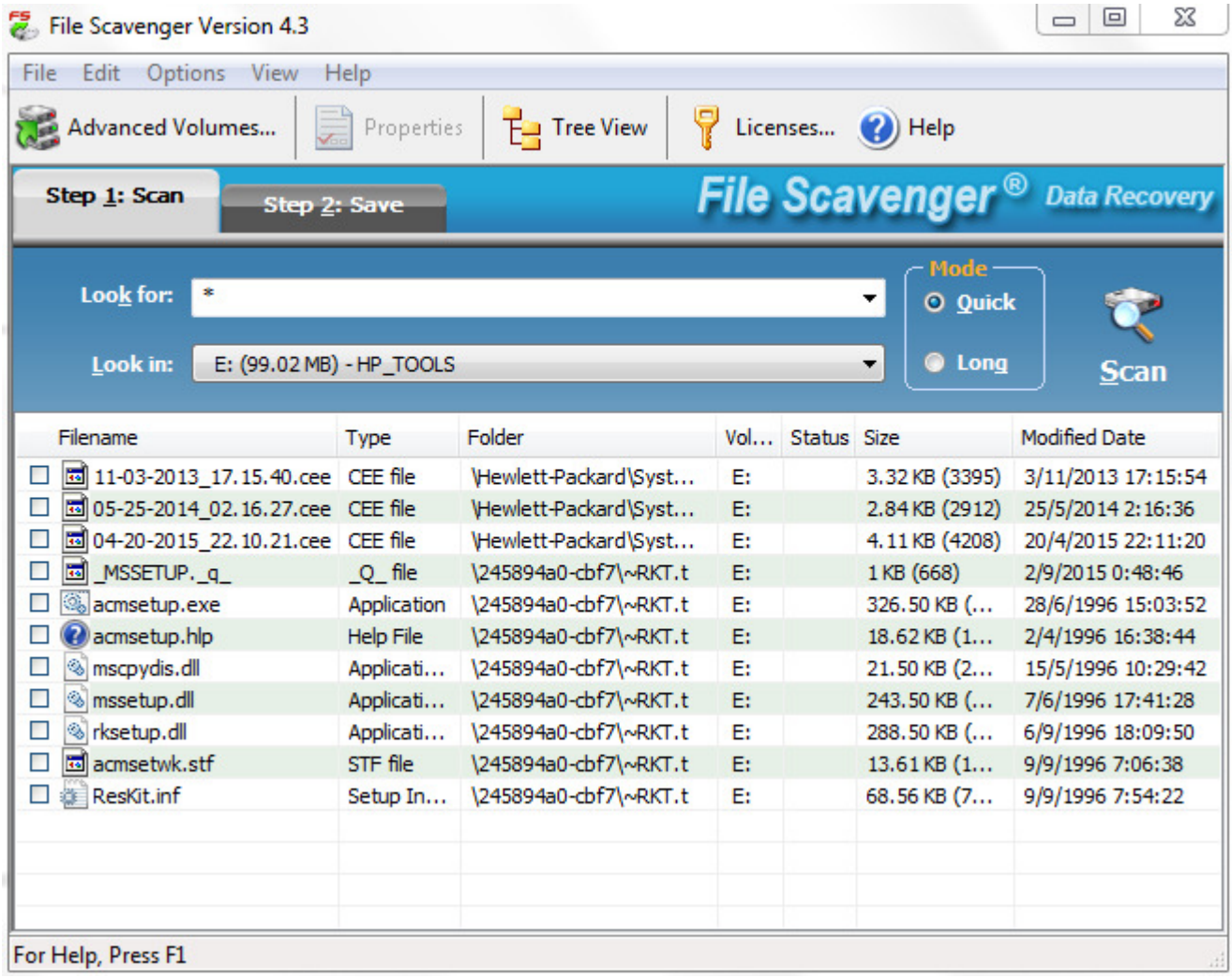
1. **Authors**, ο συντάκτης του εγγράφου του Office.
2. **LastSaveDate**, η ημερομηνία τελευταίας αποθήκευσης του εγγράφου του Office.
3. **Owners**, ο ιδιοκτήτης του κάθε αρχείου.
4. **DirLevel**, το βάθος καταλόγου του κάθε αρχείου.
5. **Versions**, ο αριθμός έκδοσης του αρχείου.
6. **Attributes**, τα χαρακτηριστικά του αρχείου.
7. **MD5**, το ανάλογο checksum.
8. **SHA256**, το ανάλογο checksum.
9. **FRN**, ο αριθμός αναφοράς στο NTFS.

Στο **/FILTER**, μπορούν να χρησιμοποιηθούν οι μπαλαντέρ * και ?. Επίσης, οι διαδρομές μπορούν να έχουν το μοτίβο "*\System32*.DLL".

3.2.4 File Scavenger

Το **File Scavenger** είναι λογισμικό ανάκτησης δεδομένων της QueTek και υποστηρίζεται από Windows 2000 και ύστερα. Εκτός από την δυνατότητα να ανακτά διεγραμμένα αρχεία από τον δίσκο και από εξωτερικές μονάδες μνήμης, μπορεί να εμφανίσει και τον κατάλογο όλων των αρχείων που υπάρχουν στους δίσκους που είναι συνδεδεμένοι πάνω στο σύστημα.

Το File Scavenger υποστηρίζει διάφορα file systems, όπως NTFS, FAT 32/16/12, Ext3, Ext4, USF1, USF2, VMDK, VHD και άλλα. Δεν περιορίζεται στις επεκτάσεις των αρχείων και ανακτά όλες τις πληροφορίες του αρχείου, δηλαδή το όνομα του, το περιεχόμενο του, την διαδρομή του και τις ημερομηνίες.



Εικόνα 3.3: File Scavenger

Πιο συγκεκριμένα, όταν εκτελέσει κανείς το αρχείο εγκατάστασης, έχει την δυνατότητα να εγκαταστήσει ή να τρέξει την εφαρμογή χωρίς να χρειαστεί εγκατάσταση. Έπειτα από την ανάλογη επιλογή, βλέπει δύο καρτέλες, "**Step 1: Scan**" και "**Step 2: Save**".

Στην *1η καρτέλα*, για να δει τα διεγραμμένα αρχεία, επιλέγει για τι είδους αρχεία θέλει να αναζητήσει, ανάλογα με την επέκταση ή και για όλα τα αρχεία, και επιλέγει σε ποιον τόμο ή και συνδεδεμένο δίσκο θέλει να ψάξει η εφαρμογή. Μετά επιλέγει αν θέλει γρήγορη ή αργή αναζήτηση και τέλος πατάει **Scan**. Η λίστα με τα αρχεία εμφανίζονται μετά από λίγη ώρα και εμφανίζονται πληροφορίες σε καρτέλες:

- **Filename**, το όνομα του αρχείου.
- **Type**, το είδος του αρχείου.
- **Folder**, η διαδρομή του αρχείου.
- **Volume**, ο τόμος.
- **Status**, η κατάσταση του αρχείου, δηλαδή κατά πόσο η ποιότητα του περιεχομένου παραμένει ίδια.
- **Size**, το μέγεθος του αρχείου σε bytes, περιεκτικά και πλήρη.
- **Modified Date**, η ημερομηνία τροποποίησης.

Στις ιδιότητες κάθε αρχείου, δείχνει επίσης αριθμό εγγραφής, δηλαδή ποια εγγραφή είναι στο σύνολο αυτών που βρέθηκαν και τον αριθμό του MFT τομέα όπου βρίσκεται η εγγραφή. Υπάρχει η δυνατότητα προβολής των αρχείων και μορφή δέντρου από την μπάρα στο πάνω μέρος.

Στην *2η καρτέλα*, υπάρχει η δυνατότητα αποθήκευσης των επιλεγμένων αρχείων. Αν η αποθήκευση γίνει στον ίδιο δίσκο από όπου γίνεται η ανάκτηση, τότε θα εμφανίσει προειδοποίηση απώλειας δεδομένων από επανεγγραφή του δίσκου. Για να συνεχίσετε με την αποθήκευση σ' σαυτό το σημείο, επιλέξτε "**I have pressed F1 and read the warning.**" και γράψτε ως κωδικό παράκαμψης **Yes**.

3.2.5 Foremost

Το **Foremost** είναι εργαλείο ανάκτησης διαγραμμένων αρχείων για Linux. Δημιουργία ειδικών πρακτόρων του γραφείου Ειδικών Ερευνών της Αμερικάνικης Αεροπορίας, χρησιμοποιεί images των σκληρών δίσκων ως είσοδο. Αυτό επιτρέπει δηλαδή και την ανάκτηση αρχείων από virtual machines.

Η σύνταξη της εντολής είναι:

foremost [options] –i *file*

–a	Ενεργοποιεί την εγγραφή των επικεφαλίδων και δεν κάνει ανίχνευση λάθους σε κατεστραμμένα αρχεία.
–b *n*	Προσδιορίζει το μέγεθος του μπλοκ που χρησιμοποιεί το foremost. Από προεπιλογή είναι 512 bytes.
–c *file*	Ορίζει το *αρχείο* παραμετροποίησης προς χρήση.
–d	Ενεργοποιεί την ανίχνευση έμμεσου μπλοκ. Κατάλληλη για file systems των Unix.
–i *file*	Το *αρχείο* που χρησιμοποιείται ως είσοδος.
–k *n*	Ορίζει πόσα *MB* της μνήμης RAM μπορεί να χρησιμοποιήσει για την εκτέλεση.

–o *dir*	Φάκελος προορισμού για τα ανακτημένα αρχεία.
–q	Ενεργοποιεί την γρήγορη λειτουργία.
–Q	Ενεργοποιεί την ήσυχη λειτουργία. Τα περισσότερα μηνύματα λάθους παραλείπονται.
–s *n*	Παραλείπει *n* μπλοκ πριν αρχίσει να αναζητά για headers.
–t *type*	Ορίζεται ο τύπος του αρχείου που θα ανακτηθεί.
–T	Ονομάζει τον φάκελο εξόδου ως το timestamp της εκτέλεσης της εντολής.
–v	Λειτουργία verbose.

Η εντολή αν εκτελεστεί σκέτη ή το αρχείο δεν μπορεί να διαβαστεί, θα δεχθεί ως είσοδο το **stdin**.

Για την επιλογή **–c**, αν δεν οριστεί κανένα, χρησιμοποιείται το "**foremost.conf**" που βρίσκεται είτε στο τρέχων κατάλογο είτε στο "**/etc**".

Για την επιλογή **–t**, οι συγκεκριμένοι τύποι των αρχείων που υποστηρίζονται, είναι:

1. **avi**
2. **bmp**
3. **cpp**
4. **doc**
5. **exe**
6. **gif**
7. **htm**
8. **jpg**
9. **mov**
10. **mpg**
11. **ole**
12. **png**
13. **pdf**
14. **rar**
15. **riff**
16. **wav**
17. **wmv**
18. **zip**

Μπορούν να δηλωθούν και όλοι οι τύποι με το **all** ή και χωρίς την επιλογή **–t**. Επιπρόσθετοι τύποι που υποστηρίζει η εντολή, μπορούν να τεθούν στο αρχείο παραμετροποίησης.

3.2.6 lsof

Το **lsof** είναι εργαλείο για Unix συστήματα και εμφανίζει λίστα με τα ανοιχτά αρχεία και τις διεργασίες που τις άνοιξαν. Αναπτύχθηκε από τον Victor A. Abell.

Λειτουργεί σε διάφορα λειτουργικά συστήματα των Unix, αλλά δεν ισχύουν απαραίτητα οι ίδιες επιλογές παντού.

Η σύνταξη της εντολής είναι:

lsof [options] <*directory*>

–a	Συνδυάζει οποιεσδήποτε από τις επόμενες επιλογές, με την λογική **AND**.
–A *file*	Τίθεται *αρχείο* με λίστα διευθύνσεων όπου βρίσκονται τα δυναμικά μοντέλα.
–b	Η lsof αποφεύγει λειτουργίες του kernel που μπορεί να την μπλοκάρουν.
–c *x*	Η εντολή που εκτελείται ξεκινάει με τον χαρακτήρα *x*.
+c *n*	Ορίζει τον *μέγιστο αριθμό χαρακτήρων* που θα εμφανιστεί για το όνομα της εντολής στην στήλη '**COMMAND**'.
+d *dir*	Αναζητά για όλα τα ανοιχτά νήματα του καταλόγου *dir*, των αρχείων και των καταλόγων του πάνω μέρους του πεδίου.
+D *dir*	Το ίδιο με την επιλογή **+D**, αλλά και για τους υποκαταλόγους εις βάθος.
–g *id*	Εμφανίζει τις εγγραφές με συγκεκριμένο *ID ομάδας διεργασίας*.
–i	Εμφανίζει τις εγγραφές με διαδικτυακές συνδέσεις.
–l	Δεν μετατρέπει τα IDs των χρηστών σε ονόματα.
+L [*n*]	Επιτρέπει την εμφάνιση των πληθών των συνδέσμων. Προαιρετικά, δηλώνουμε να εμφανίσει εγγραφές που έχουν λιγότερο από *n* συνδέσμους.
–L	Δεν επιτρέπει την εμφάνιση των πληθών των συνδέσμων. Προεπιλογή.
–n	Δεν μετατρέπει τις δικτυακές διευθύνσεις σε ονόματα για τα δικτυακά αρχεία.
–N	Επιλέγει την λίστα των αρχείων του NFS file system.
–o	Εμφανίζει πάντοτε το όφσετ των αρχείων.
–o *n*	Ορίζει πόσα *ψηφία* θα εμφανιστούν για το όφσετ μετά το '0t' και πριν γίνει '0x…'.
–O	Οδηγεί την lsof σε παράκαμψη της στρατηγικής που χρησιμοποιείται για την αποφυγή εμποδισμού από μερικές λειτουργίες του kernel.
–p	Δεν μετατρέπει τους αριθμούς των θυρών σε ονόματα για τα δικτυακά αρχεία.
–p *id*	Εμφανίζει τις εγγραφές με συγκεκριμένο *ID διεργασίας*.
+r *t*	Επανάληψη ανά χρόνο *t*, εκτός αν δεν υπάρχουν ανοιχτά αρχεία.
–r *t*	Επανάληψη ανά χρόνο *t*, συνεχόμενα μέχρις ότου δοθεί σήμα τερματισμού.
–R	Εμφανίζει το ID της γονικής διεργασίας στην στήλη '**PPID**'.
–s [*p:s*]	Εμφανίζει πάντοτε το μέγεθος των αρχείων.
–S *t*	Ορίζει χρόνο παύσης για τις λειτουργείες του kernel που μπλοκάρουν την lsof.
–t	Εμφανίζει μόνο τα IDs των διεργασιών και καθόλου κεφαλίδες.
–u *user*	Εμφανίζει ή όχι, με το σύμβολο '^', τις εγγραφές με *όνομα χρήστη ή ID user*.
–U	Εμφανίζει τα αρχεία τύπου υποδοχή του UNIX χώρου.
–v	Εμφανίζει πλήρης πληροφορίες έκδοσης του εργαλείου.
–V	Αναφέρει οτιδήποτε δεν μπόρεσε να βρει από ότι του ζητήθηκε.
+w | –w	Ενεργοποιεί και απενεργοποιεί αντίστοιχα την εμφάνιση των προειδοποιήσεων.

Κάθε εκτέλεση της εντολής με οποιεσδήποτε επιλογές, εμφανίζει το αποτέλεσμα σε μια λίστα με 9 στήλες:

- **COMMAND** → όνομα της εντολής
- **PID** → ID της διεργασίας
- **USER** → όνομα του χρήστη
- **FD** → συντομευμένη περιγραφή του αρχείου
- **TYPE** → τύπος του αρχείου
- **DEVICE** → νούμερα της συσκευής, χωρισμένα με κόμμα
- **SIZE/OFF** → μέγεθος του αρχείου είτε το όφσετ του σε bytes
- **NODE** → inode
- **NAME** → όνομα του αρχείου ή του καταλόγου

Η επιλογή **–A**, αφορά συστήματα που είναι ρυθμισμένα για το AFS file system, του οποίου ο κώδικας του kernel υλοποιείται μέσω των δυναμικών μοντέλων.

Για την επιλογή **–c**, αν το *x* ξεκινάει με το σύμβολο '**^**', τότε δεν εμφανίζεται το αποτέλεσμα για τις εντολές που ξεκινάνε με τους επακόλουθους χαρακτήρες. Αν το *x* ξεκινάει και τελειώνει με το σύμβολο '**/**', το ενδιάμεσο μεταφράζεται ως expression. Η κάθετος που κλείνει, μπορεί να ακολουθηθεί από τα εξής:

1. **b**: το regular expression είναι βασικό.
2. **i**: αγνόησε την περίπτωση των γραμμάτων.
3. **x**: το regular expression είναι εκτεταμένο. Προεπιλογή.

Για την επιλογή **+c**, αν το *n* είναι 0, τότε θα εμφανιστούν όλοι οι χαρακτήρες. Αν είναι μικρότερο από το μήκος του τίτλου της στήλης '**COMMAND**', τότε θα αυξηθεί σ' αυτό, δηλαδή 7.

Η διαφορά μεταξύ των επιλογών **+d** και **+D**, είναι η **+d** ψάχνει μόνο στο πάνω μέρος του καταλόγου, ενώ η **+D** ψάχνει και στους υποκαταλόγους.

Για τις επιλογές **–g** και **–p** *id*, πολλαπλά IDs μπορούν να τεθούν μαζί, χωρισμένα με κόμμα. Τα IDs με το σύμβολο '**^**' μπροστά, σημαίνει να μην συμπεριληφθούν στην έξοδο.

Για την επιλογή **–i**, η διεύθυνση μπορεί να έχει ένα ή περισσότερα εκ των παρακάτω με την εξής σειρά:

- **46** → Για IPv4 ή IPv6. Αν δεν αναφέρεται κανένα, τότε θεωρούνται και τα δύο.
- **protocol** → Για TCP ή UDP.
- **@hostname | hostaddr** → Για όνομα ή διεύθυνση IP.
- **:service | port** → Για όνομα υπηρεσίας ή αριθμό θύρας.

Η σκέτη επιλογή **–o**, μετατρέπει την στήλη '**SIZE/OFF**' σε '**OFFSET**'.

Η επιλογή **–o** *n*, δεν εμφανίζει πάντοτε το όφσετ, γι' αυτό αν χρειαστεί, πρέπει να γραφτεί και η σκέτη επιλογή **–o** .

Συγκεκριμένα για τις επιλογές **+r | –r**, ο χρόνος είναι σε δευτερόλεπτα και από προεπιλογή είναι 15. Η επιλογή +r σταματάει στον $1^{ο}$ κύκλο επίσης άμα δοθεί σήμα εξόδου.

Για την επιλογή **–s**, η στήλη '**SIZE/OFF**' μετατρέπεται σε '**SIZE**'. Αν συνδυαστεί με αναφορά πρωτοκόλλου *p* και κατάστασης *s*, αν θα συμπεριλαμβάνεται η κατάσταση ή όχι, δηλαδή με '**^**', τότε αντιστοίχως εμφανίζει ή όχι τα δικτυακά αρχεία.

Για την επιλογή **–S**, ο ελάχιστος χρόνος είναι 2 δευτερόλεπτα και ο προεπιλεγμένος 15.

Η επιλογή **–t** είναι χρήσιμη για όταν συνδυάζεται με την εντολή **kill**. Επιλέγεται αυτόματα και η επιλογή **–w**.

3.2.7 rifiuti2 / Rifiuti

Το **rifiuti2** είναι εργαλείο γραμμής εντολών, το οποίο αναλύει τα INFO2 αρχεία του Κάδου Ανακύκλωσης των Windows. Αποτελεί συνέχεια του **Rifiuti** της Foundstone και εκτός από τα Windows, τρέχει σε Linux, OS X και BSD.

Μπορεί να εξάγει τον χρόνο διαγραφής, την πραγματική διαδρομή και το μέγεθος των διεγραμμένων αρχείων και αν μετακινήθηκαν τα αρχεία από την στιγμή που στάλθηκαν στον Κάδο.

Το **rifiuti2** δημιουργήθηκε ως συνέχεια του Rifiuti, γιατί είναι περιορισμένο στην αγγλική έκδοση των Windows, δηλαδή δεν μπορεί να αναλύσει μη-λατινικούς χαρακτήρες. Έτσι, τα χαρακτηριστικά του rifiuti2 είναι:

- Υποστήριξη αρχείων των Windows σε πολλές γλώσσες.
- Υποστήριξη Vista και Server 2008, όπου σταματά η χρήση των INFO2 αρχείων.
- Δυνατότητα μεταφράσεων με την χρήση του πακέτου βιβλιοθηκών glib.
- Πιο αυστηροί έλεγχοι λαθών.
- Δυνατότητα εξαγωγής δεδομένων σε μορφή XML.

Λόγω του ότι από τα Vista και μετά δεν χρησιμοποιούνται πια τα αρχεία INFO2, υπάρχουν 2 εκδοχές του **rifiuti2**, το **rifuiti** και το **rifiuti-vista**.

Η σύνταξη της εντολής **rifiuti** που υποστηρίζεται μέχρι και τα XP, είναι:

rifiuti [Options] *filename*

Αντίστοιχα και για την εντολή **rifiuti-vista** που υποστηρίζεται από τα Vista και μετά, είναι:

rifiuti-vista [Options] <*file / directory*>

-8	Εμφανίζει τα ονόματα των αρχείων με κωδικοποίηση UTF-8.
-l	Εμφανίζει το νόμιμο όνομα αρχείου αντί αυτό του Unicode. Η επιλογή δεν υπάρχει στο **rifiuti-vista**.
-n	Δεν εμφανίζει τις κεφαλίδες των στηλών.
-o *file*	Γράφει την έξοδο στο ορισμένο αρχείο.
-t	Χρησιμοποιεί ένα string σαν διαχωριστικό. Από προεπιλογή είναι το TAB. Η επιλογή δεν υπάρχει στο **rifiuti-vista**.
-x	Εξάγει το αποτέλεσμα σε μορφή XML. Οι επιλογές **–t**, **–n**, **–l** και **–8** δεν έχουν επίδραση.

Η διαφορά στο αποτέλεσμα του **rifiuti** και του **rifiuti-vista** είναι στις στήλες. Το 1^{ο} εμφανίζει 5 στήλες, τις **Index**, **Deleted Time**, **Gone?**, **Size** και **Path**, ενώ το 2^{ο} εμφανίζει 4 στήλες, τις **INDEX_FILE**, **DELETION_TIME**, **SIZE** και **FILE_PATH**. Η στήλη Gone? δηλώνει αν έχει εξαφανιστεί από τον Κάδο Ανακύκλωσης το αρχείο, ασχέτως αν διαγράφτηκε ή έγινε επαναφορά του.

Το **Rifiuti** της Foundstone είναι πιο απλό στην χρήση, καθώς η μόνη επιλογή που παίρνει είναι η **–t**, με την οποία ορίζεται το διαχωριστικό και έτσι η σύνταξη της εντολής είναι:

rifiuti –t *filename*

4. Εγκληματολογική εξέταση δικτυακών δεδομένων

Αυτός ο τομέας, δεν αφορά μόνο για παράδειγμα τις πληροφορίες που αφήνει πίσω του ένας δράστης, αλλά επίσης και κατά κύριο λόγο την ασφάλεια των δικτύων και των συστημάτων τους.

Τα δικτυακά δεδομένα αφορούν την κίνηση των πακέτων σε ένα δίκτυο, από έναν υπολογιστή σε έναν άλλον ή μεταξύ διαφορετικών δικτύων, καθώς επίσης και δικτυακές πληροφορίες για τους υπολογιστές και τις συνδέσεις που βρίσκονται στους ίδιους και σε άλλες δικτυακές συσκευές, όπως ένα *router* και ένα *firewall*.

4.1 Μέθοδοι

Λίγα αλλά αρκετά χρήσιμα είναι τα εργαλεία που έχουν τα ίδια τα λειτουργικά όσον αφορά τις δικτυακές πληροφορίες και την διαχείριση των interfaces. Πιο πολύ στα Linux, λόγω του open-source, το οποίο σημαίνει εις βάθος παραμετροποίηση των δικτυακών ρυθμίσεων.

4.1.1 arp

Το **arp** είναι εργαλείο γραμμής εντολών και εμφανίζει τις MAC διευθύνσεις των συστημάτων με τα οποία επικοινώνησε το σύστημα το τελευταίο λεπτό.
Αυτή η εντολή υπάρχει στα BSD, OS X, Linux και Windows NT.

Βασίζεται στο πρωτόκολλο **Address Resolution Protocol**, το οποίο μετατρέπει μια διεύθυνση IP σε μια φυσική διεύθυνση (**Mac address / Ethernet address**).

Η σύνταξη της εντολής ακολουθεί το εξής πρότυπο:

arp [options]

Στον παρακάτω πίνακα βλέπουμε τις παραμέτρους που δέχεται η εντολή, είτε για όλα τα OS είτε για μερικά.

-a *IP (-N IfAddr)*	Παρουσιάζει τους τωρινούς πίνακες μνήμης του ARP για όλα τα interfaces. Όπου *IP* η διεύθυνση IP για να εμφανιστεί η συγκεκριμένη καταχώρηση. Η **-N** *IfAddr* παράμετρος συνδυάζεται με την **-a**, όπου *IfAddr* η διεύθυνση που δίδεται στο interface, για να εμφανιστεί ο πίνακας για το συγκεκριμένο interface.
-A (Linux)	Προσδιορίζει οικογένεια πρωτοκόλλων.
-d (Linux)	Διαγράφει μια συγκεκριμένη καταχώρηση.
-d *IP (IfAddr)*	Διαγράφει καταχώρηση με συγκεκριμένη διεύθυνση IP. Όπου *IfAddr* η διεύθυνση που δίδεται στο interface, για να διαγραφεί η καταχώρηση συγκεκριμένου interface. Για να διαγραφούν όλες οι καταχωρήσεις ενός interface, στην IP βάλτε τον χαρακτήρα μπαλαντέρ αστερίσκο (*).
-D (Linux)	Διαβάζει την MAC address της δοθέντος συσκευής.
-f (εκτός	Διαβάζει νέες καταχωρήσεις από συγκεκριμένο αρχείο.

Windows)	
-g *IP (-N IfAddr)*	Παρόμοιο με την **-a**.
-i (εκτός Windows)	Προσδιορίζει δικτυακό interface (π.χ. eth0).
-l (OS X)	Δείχνει πληροφορίες προσβασιμότητας του επιπέδου σύνδεσης.
-n (εκτός Windows)	Δεν λαμβάνει υπόψιν τα ονόματα.
-p (Linux)	Το ίδιο με το **–A**.
-s *IP EthdAd (IfAddr)*	Προσθέτει μια στατική καταχώρηση στην μνήμη του ARP, η οποία αντιστοιχεί την διεύθυνση IP στην φυσική διεύθυνση. Για προσθήκη καταχώρησης συγκεκριμένου interface, το ίδιο όπως και στις άλλες παραμέτρους.
-S *IP EthdAd (IfAddr) (OS X)*	Ακριβώς το ίδιο με το **–s**, με την διαφορά ότι οποιαδήποτε ήδη υπάρχουσα πληροφορία για την συγκεκριμένη διεύθυνση, θα διαγραφεί πρώτα.
-v (εκτός OS X)	Εμφανίζει τις τρέχουσες καταχωρήσεις σε κατάσταση λειτουργίας εμφάνισης λεπτομερειών, καθώς επίσης μη έγκυρες καταχωρήσεις και καταχωρήσεις στη διασύνδεση βρόχου επιστροφής.
-x (OS X)	Δείχνει εκτεταμένες πληροφορίες για την προσβασιμότητα του επιπέδου σύνδεσης, όπως αυτές εμφανίζονται από το **–l**.

4.1.2 HyperTerminal

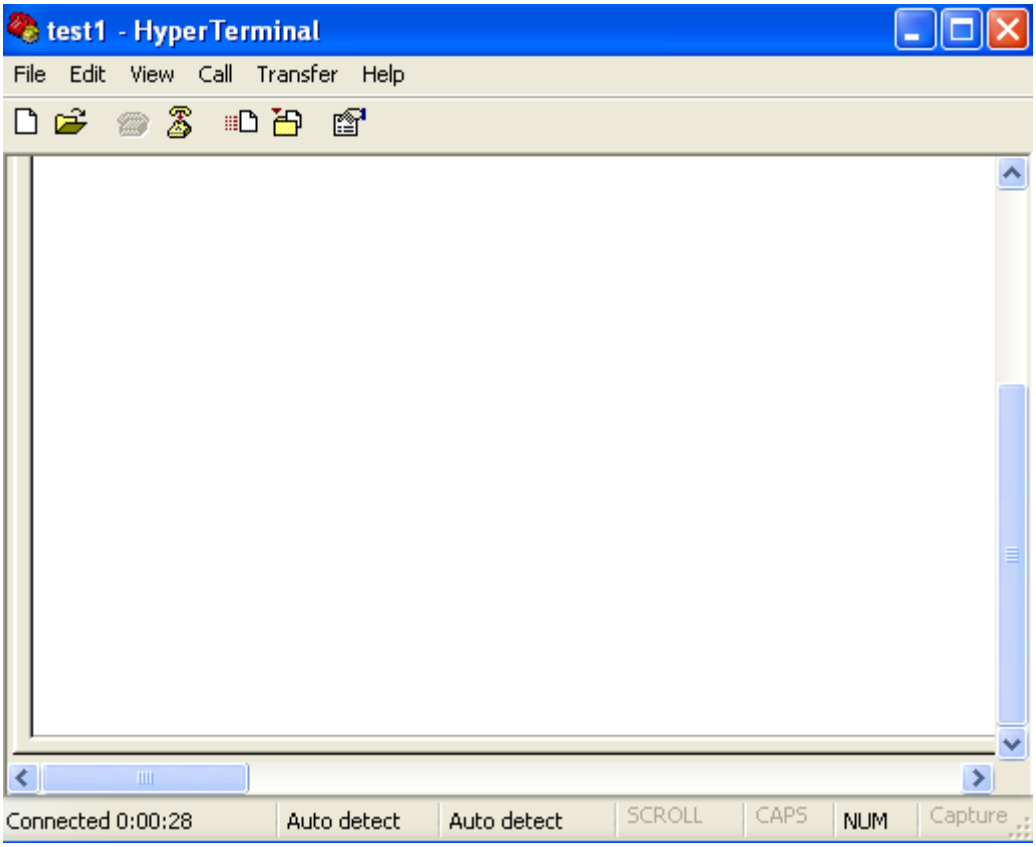
Το **HyperTerminal**, λογισμικό της Hilgraeve, είναι προσομοιωτής τερματικού το οποίο δίνει την δυνατότητα απομακρυσμένης σύνδεσης με έναν δρομολογητή. Βρίσκεται ενσωματωμένο από τα Windows 95 μέχρι και τα XP, καθώς επίσης και στο OS/2. Αντίστοιχο γνωστό λογισμικό είναι το **PuTTY**.

Όταν κάποιος τρέξει το πρόγραμμα, θα του εμφανίσει το παραθυράκι **Connection Description**, όπου βάζεις όνομα και επιλέγεις εικόνα για την σύνδεση, ώστε να μπορεί να αποθηκευτεί μετά.

Μετά, εμφανίζεται το παραθυράκι **Connect To**, στο οποίο ανάλογα με την επιλογή στο Connect using, εμφανίζονται αντίστοιχα τα πεδία που πρέπει να συμπληρωθούν.

1. Στις επιλογές **COM1** και **COM2**, εμφανίζονται τα **Country/region**, **Area code** και **Phone number**. Τα συγκεκριμένα πεδία όμως δεν μπορούν να τροποποιηθούν, καθώς υποτίθεται έχουν οριστεί από όταν έτρεξε για πρώτη φορά το πρόγραμμα.
2. Στην επιλογή **TCP/IP (Winsock)**, εμφανίζονται τα **Host address** και **Port number**.

Όπως φαίνεται κι από πάνω, για μηχανήματα που είναι συνδεδεμένα απευθείας πάνω στον υπολογιστή μέσω της θύρας COM, προτιμάται μια εκ των επιλογών COM. Για απομακρυσμένη σύνδεση, τύπου **telnet** και **ssh**, η επιλογή **TCP/IP (Winsock)** προτιμάται.



Εικόνα 4.1: HyperTerminal

Το κύριο παράθυρο, έχει μια μπάρα με εργαλεία για δημιουργία σύνδεσης, σύνδεση, καθώς επίσης και για αποστολή και λήψη αρχείων, ένα την φορά, χρησιμοποιώντας πρωτόκολλα όπως Zmodem, Xmodem, Kermit κ.α..

Στο κάτω μέρος είναι η μπάρα κατάστασης όπου δείχνει την κατάσταση της σύνδεσης και το είδος της σύνδεσης **– COM** ή **TCP/IP**.

Στο κέντρο, ένα λευκό πλαίσιο όπου εμφανίζονται τα μηνύματα της σύνδεσης και γίνεται η εκτέλεση των εντολών που υποστηρίζονται από τον αντίστοιχο δρομολογητή, οι οποίες εμφανίζονται με την πληκτρολόγηση του χαρακτήρα '**?**', για καθ' ένα από τα τρία επίπεδα λειτουργίας.

4.1.3 ipconfig / ifconfig

Η **ipconfig** είναι εντολή μέσω της οποίας μπορούμε να δούμε τις πληροφορίες για τα interfaces και να αλλάξουμε τις ρυθμίσεις για το DHCP πρωτόκολλο και το σύστημα DNS.

Αυτή η εντολή υπάρχει σε Unix, OS X και Windows (95 και μετά).

Η σύνταξη της εντολής ακολουθεί το εξής πρότυπο:

ipconfig [/allcompartments] [flags]

Στον παρακάτω πίνακα βλέπουμε τις παραμέτρους που δέχεται η εντολή στα **Windows**.

/all	Εμφανίζει πληροφορίες για όλα τα δικτυακά interfaces.
/displaydns	Εμφανίζει το περιεχόμενο της μνήμης cache του DNS.
/flushdns	Καθαρίζει την μνήμη cache του DNS.
/registerdns	Ανανεώνει τις μισθώσεις του DHCP και καταχωρεί πάλι τα ονόματα DNS.
/release	Αποδεσμεύει την IPv4 διεύθυνση για όλα τα interfaces, αν δεν οριστεί συγκεκριμένος.
/release6	Αποδεσμεύει την IPv6 διεύθυνση για όλα τα interfaces, αν δεν οριστεί συγκεκριμένος. Ισχύει από *Windows Vista* και μετά.
/renew	Ανανεώνει την IPv4 διεύθυνση για όλα τα interfaces, αν δεν οριστεί συγκεκριμένος.
/renew6	Ανανεώνει την IPv6 διεύθυνση για όλα τα interfaces, αν δεν οριστεί συγκεκριμένος. Ισχύει από *Windows Vista* και μετά.
/setclassid *Adapter*	Τροποποιεί το αναγνωριστικό κλάσης DHCP. Με * για όλα τα interfaces.
/setclassid6 *Adapter*	Τροποποιεί το αναγνωριστικό κλάσης IPv6 DHCP. Με * για όλα τα interfaces. Ισχύει από *Windows Vista* και μετά.
/showclassid *Adapter*	Εμφανίζει το αναγνωριστικό κλάσης DHCP. Με * για όλα τα interfaces.
/showclassid6 *Adapter*	Εμφανίζει το αναγνωριστικό κλάσης IPv6 DHCP. Με * για όλα τα interfaces. Ισχύει από *Windows Vista* και μετά.

Για το **OS X**, υπάρχουν προσθετικές εντολές, των οποίων η λειτουργία τους είναι παρόμοια με αυτή των Windows.

getifaddr *interface*	Τυπώνει την IP για την πρώτη δικτυακή υπηρεσία που σχετίζεται με το δοσμένο interface. Η έξοδος θα είναι άδεια αν καμία υπηρεσία δεν είναι ενεργοποιημένη στο interface.
getoption *interface (option-name | option-code)*	Τυπώνει την επιλογή DHCP/BOOTP με το δοσμένο όνομα ή την ακέραια τιμή του κωδικού επιλογής. Αν μια επιλογή έχει πολλαπλές τιμές, όπως domain_name_server, θα εμφανιστεί μόνο η πρώτη.
getpacket *interface*	Τυπώνει το πακέτο DHCP/BOOTP όπου ο client αποδέχτηκε από τον αντίστοιχο server. Αυτή η εντολή είναι χρήσιμη στον έλεγχο του τι προμηθεύει ο server και αν οι τιμές είναι λογικές. Δεν τυπώνεται τίποτα αν ο DHCP/BOOTP δεν είναι ενεργός στο interface ή αν η προσπάθεια ανάκτησης διεύθυνσης IP ήταν ανεπιτυχής.

getv6packet *interface*	Τυπώνει το πιο πρόσφατο πακέτο DHCPv6 που δέχτηκε ο client από τον αντίστοιχο server. Στην περίπτωση ενός stateful DHCPv6, ανταποκρίνεται στο τελευταίο πακέτο που περιλαμβάνει πληροφορίες διευθυνσιοδότησης. Αυτή η εντολή είναι χρήσιμη στον έλεγχο του τι παρέχει ο server και αν οι τιμές είναι λογικές. Η έξοδος θα είναι άδεια αν ο DHCPv6 δεν είναι ενεργός σ' αυτό το interface.
getverbose *level*	Ενεργοποιεί ή απενεργοποιεί το verbose mode της καταγραφής. Η τιμή 0 είναι η προεπιλεγμένη και απενεργοποιεί την λειτουργία. Η τιμή 1 την ενεργοποιεί. Όταν ενεργοποιείται, τα αρχεία καταγραφής δημιουργούνται στην τοποθεσία /Library/Logs/CrashReporter .Για την χρήση της εντολής, απαιτούνται δικαιώματα διαχειριστή.
ifcount	Τυπώνει τον αριθμό των interfaces, τα οποία μπορούν να ρυθμιστούν. Η τιμή που τυπώνεται δεν θα αλλάξει, εκτός αν προστεθούν ή αφαιρεθούν από το σύστημα σχετιζόμενα δικτυακά interfaces.
set *interface*	Θέτει στο δοσμένο interface μια νέα προσωρινή δικτυακή υπηρεσία του δοσμένου τύπου. Οποιαδήποτε υπηρεσία του συγκεκριμένου πρωτοκόλλου (IPv4 ή IPv6) απορυθμίζεται πριν τεθεί η νέα υπηρεσία.
set *interface* **6TO4**	Λειτουργεί μόνο σε 6 προς 4 interfaces (IFT_STF), όπως stf0. Αν οριστεί σε μη IFT_STF interface, έχει το ίδιο αποτέλεσμα με το NONE-V6.
set *interface* **AUTOMATIC-V6**	Η διεύθυνση IPv6, το μήκος του προθέματος και η gateway ανακτώνται αυτόματα.
set *interface* (**DHCP** | **BOOTP**)	Η διεύθυνση IP, η μάσκα του υποδικτύου, η gateway και οι πληροφορίες του DNS ανακτώνται αυτόματα.
set *interface* (**MANUAL** | **INFORM**) *ip netmask*	Απαιτεί τον ορισμό μιας διεύθυνσης IP και μιας μάσκας υποδικτύου. Η υπηρεσία INFORM ρυθμίζει την διεύθυνση IP στατικά όπως η MANUAL, αλλά τότε μεταδίδει πακέτα DHCP INFORM για να ανακτήσει τις πληροφορίες της επιλογής DHCP. Αν ο DHCP server ανταποκριθεί και προμηθεύσει μια μάσκα υποδικτύου, τότε αυτή η μάσκα χρησιμοποιείται αντί αυτής που ορίσαμε.
set *interface* **MANUAL-V6** *ipv6 prefix-length*	Απαιτεί τον ορισμό διεύθυνσης IPv6 και ενός μήκους προθέματος.
set *interface* **NONE**	Όλες οι IPv4 υπηρεσίες απορυθμίζονται.
set *interface* **NONE-V6**	Όλες οι IPv6 υπηρεσίες απορυθμίζονται.
waitall	Μπλοκάρει μέχρι όλες οι δικτυακές υπηρεσίες έχουν ολοκληρώσει την ρύθμιση τους ή έχουν λήξει στην διαδικασία της ρύθμισης. Η εντολή είναι χρήσιμη μόνο για αρχικοποίηση συστήματος με δυναμικές δικτυακές αλλαγές ρυθμίσεων.

Αντίστοιχη εντολή στα λοιπά Unix συστήματα, είναι η **ifconfig**. Ενώ οι ενέργειες της είναι ίδιες με της **ipconfig**, η σύνταξη αλλάζει ως εξής:

ifconfig <*interface*> [options] <*IP_addr*>

add *addr*	Προσθέτει μια IPv6 διεύθυνση.
[-]allmulti	Επιτρέπει ή όχι αντίστοιχα την λειτουργία all-multicast. Εάν ενεργοποιηθεί, το interface θα παραλάβει όλα τα multicast πακέτα του δικτύου.
[-]arp	Επιτρέπει ή όχι αντίστοιχα την χρήση του πρωτοκόλλου ARP.
[-]broadcast *[addr]*	Αν δοθεί διεύθυνση, ορίζει το πρωτόκολλο διεύθυνση εκπομπής. Διαφορετικά, ορίζει ή βγάζει την σημαία **IFF_BROADCAST**.

del *addr*	Διαγράφει μια IPv6 διεύθυνση.
down	Ορίζει τον οδηγό του interface να κλείσει.
hw *class addr*	Θέτει την φυσική διεύθυνση, αν υποστηρίζεται η τροποποίηση της από τον οδηγό.
io_addr *addr*	Ορίζει την διεύθυνση εκκίνησης στον χώρο I/O της συσκευής.
irq *addr*	Ορίζει την γραμμή παρεμβολής προς χρήση για την συσκευή.
media *type*	Ορίζει το είδος του μέσου που θα χρησιμοποιηθεί.
mem_start *addr*	Ορίζει την αρχική διεύθυνση για την διαμοιρασμένη μνήμη της συσκευής.
metric *n*	Ορίζει το *μετρικό*. Δεν ισχύει στα Linux.
mtu *n*	Ορίζει το *MTU* (**Maximum Transfer Unit**).
multicast	Ορίζει την σημαία multicast.
[-] pointopoint *[addr]*	Ενεργοποιεί την λειτουργία point-to-point, δηλαδή υπάρχει απευθείας σύνδεση μεταξύ δύο μηχανών, όπου δεν κρυφακούει κανείς. Αν δοθεί διεύθυνση, ορίζει το πρωτόκολλο διεύθυνσης στην άλλη μεριά του συνδέσμου. Διαφορετικά, ορίζει ή βγάζει την σημαία **IFF_POINTOPOINT**.
[-]promisc	Επιτρέπει ή όχι την λειτουργία αδιακρισίας. Εάν ενεργοποιηθεί, το interface θα παραλάβει όλα τα πακέτα του δικτύου ανεξαιρέτως.
tunnel ::*IP*	Δημιουργεί συσκευή **SIT (IPv6 over IPv4)**, για υπόγεια σύνδεση στην δοσμένη *διεύθυνση*.
txqueuelen *n*	Ορίζει το μήκος της ουράς εκπομπής.

Η εντολή συνήθως συνοδεύεται από το δικτυακό interface, καθώς γι' αυτό γίνονται οι περισσότερες ρυθμίσεις και πληροφορίες. Αλλά και σκέτη κάνει την δουλειά της.

Οι επιλογές που τίθενται μετά, αφορούν μόνο το δοσμένο interface.

Για την επιλογή **hw**, οι κλάσεις υλικού που υποστηρίζονται για την ώρα, είναι:

- **ether** (Ethernet)
- **ax25** (AMPR AX.25)
- **ARCnet**
- **netrom** (AMPR NET/ROM)

Για την επιλογή **irq**, δεν μπορούν όλες οι συσκευές να αλλάξουν δυναμικά την ρύθμιση IRQ.

Για την επιλογή **media**, μερικοί τύποι μέσων είναι:

- **10base2** (λεπτό Ethernet)
- **10baseT** (συνεστραμμένο ζεύγος των 10Mbps Ethernet)
- **AUI** (εξωτερικός πομποδέκτης)
- **auto**

Οι επιλογές **media** και **mem_start**, δεν υποστηρίζονται από όλες τις συσκευές και τους οδηγούς.

Η επιλογή **multicast** δεν απαιτείται πολλές φορές, επειδή οι οδηγοί το κάνουν από μόνοι τους.

Αντί για επιλογές, η εντολή μπορεί να δεχθεί την διεύθυνση IP που θα οριστεί για το δοσμένο interface.

4.1.4 nbtstat

Η **nbtstat** είναι εντολή γραμμής εντολών, η οποία εμφανίζει μια λίστα με συνδέσεις του NetBIOS για τα τελευταία 10 λεπτά περίπου. Υπάρχει σε αρκετές εκδόσεις των Windows.

Η εντολή αυτή αναφέρεται ως διαγνωστικό εργαλείο, γιατί σχεδιάστηκε για να βοηθήσει στην αντιμετώπιση προβλημάτων με τα ονόματα NetBIOS.

Επίσης, χρησιμοποιείται και σε συνδυασμό με άλλες εντολές, προσφέροντας έτσι διάφορες επιλογές, όπως τοπική αναζήτηση μνήμης cache, ερώτημα για WINS server και broadcast.

Η σύνταξη της εντολής ακολουθεί το εξής πρότυπο:

nbtstat [options] [interval]

-a *name*	Εμφανίζει τον πίνακα ονομάτων NetBIOS του απομακρυσμένου, ο οποίος δηλώθηκε με το όνομα του, όπως επίσης και την διεύθυνση MAC της κάρτας προσαρμογέα.
-A *IP*	Το ίδιο με την **-a**, αλλά αντί για όνομα, διεύθυνση IP.
-c	Παρουσιάζει τα περιεχόμενα της μνήμης cache των ονομάτων NetBIOS, τον πίνακα των ονομάτων του NetBIOS και τις διευθύνσεις που πήραν.
-n	Παρουσιάζει τα ονόματα τα οποία γράφτηκαν τοπικά στο σύστημα.
-r	Παρουσιάζει το πλήθος όλων των ονομάτων NetBIOS που λήφθηκαν από αναμετάδοση και ερωτώντας έναν WINS server.
-R	Καθαρίζει και ανανεώνει τον απομακρυσμένο cache πίνακα ονόματος.
-RR	Στέλνει πακέτα αποδέσμευσης ονόματος στον WINS και μετά ξεκινά ανανέωση.
-s	Καταγράφει τις τρέχουσες συνεδρίες NetBIOS και την κατάσταση τους, συμπεριλαμβάνοντας στατιστικά.
-S	Καταγράφει πίνακα συνεδριών μαζί με την IP διεύθυνση προορισμού.
Interval	Επανεμφανίζει τις επιλεγμένες πληροφορίες κάθε χρονικό διάστημα (προσδιορισμένο σε δευτερόλεπτα). Πατήστε CTRL+C για να σταματήσετε την επανεμφάνιση. Αν η παράμετρος παραληφθεί, η nbtstat θα τυπώσει τις επιλεγμένες πληροφορίες μόνο μια φορά.

4.1.5 netstat

Η **netstat** είναι εντολή γραμμής εντολών, η οποία εμφανίζει τις δικτυακές θύρες που ακούν εκείνη την στιγμή, καθώς και τις ενεργές συνδέσεις πάνω τους.

Αυτή η εντολή υπάρχει στα BSD, Linux, OS X, Solaris και Windows NT.

Η σύνταξη της εντολής ακολουθεί το εξής πρότυπο:

netstat [options] [interval]

-a	Παρουσιάζει όλες τις ενεργές συνδέσεις και τις TCP & UDP θύρες στις οποίες ακούει ο υπολογιστής.
-b (Windows)	Παρουσιάζει το όνομα του δυαδικού (εκτελέσιμου) προγράμματος που εμπλέκεται στην δημιουργία κάθε σύνδεσης ή θύρας ακρόασης. (από Windows XP και 2003 Server και μετά).
-b (OS X, NetBSD)	Προκαλεί την **-i** να αναφέρει τον συνολικό αριθμό των bytes της κίνησης.
-c (Linux)	Θα εμφανίζει τις επιλεγμένες πληροφορίες κάθε δευτερόλεπτο συνεχόμενα.
-C (Linux)	Εμφανίζει τις δρομολογήσεις από την μνήμη cache.
-e	Παρουσιάζει στατιστικά στοιχεία του Ethernet, όπως το νούμερο των bytes και των πακέτων που λαμβάνονται και αποστέλλονται. Αυτή η παράμετρος μπορεί να συνδυαστεί με την **-s**.
-f (Windows)	Παρουσιάζει πλήρως αναγνωρισμένα domain names για ξένες διευθύνσεις (από Windows Vista και μετά).
-f *Address Family* (FreeBSD)	Περιορίζει την παρουσίαση σε συγκεκριμένη οικογένεια διεύθυνσης socket, **unix**, **inet**, **inet6**.
-F (Linux)	Εμφανίζει τις δρομολογήσεις από τον πίνακα FIB.
-g	Παρουσιάζει πληροφορίες των μελών της ομάδας multicast για IPv4 & IPv6 (μόνο σε καινούργια OS).
-i	Παρουσιάζει δικτυακά interfaces και τα στατιστικά τους (μη διαθέσιμο στα Windows).
-m	Παρουσιάζει τα στατιστικά της μνήμης για τον δικτυακό κώδικα (STREAMS statistics στα Solaris).
-M (Linux)	Εμφανίζει μια λίστα με τις μασκαρεμένες συνδέσεις.
-n	Εμφανίζει διευθύνσεις και αριθμούς θυρών σε αριθμητική μορφή, μόνο για ενεργές TCP συνδέσεις.
-o (Linux)	Εμφανίζει πληροφορίες για τους χρονομετρητές δικτύωσης.
-o (Windows)	Παρουσιάζει ενεργές TCP συνδέσεις και περιλαμβάνει το ID της διεργασίας (PID) για κάθε σύνδεση. Μπορεί να γίνει αντιστοίχιση εφαρμογής και PID στην καρτέλα **Διεργασίες** του **Task Manager**. Η παράμετρος μπορεί να συνδυαστεί με τις **-a, -n,** και **-p** (από Microsoft Windows XP και 2003 Server και μετά).
-p *protocol* (BSD, Windows)	Δείχνει συνδέσεις για το πρωτόκολλο που προσδιορίζεται από το *protocol*, το οποίο μπορεί να είναι **tcp, udp, tcpv6,** ή **udpv6**. Αν χρησιμοποιηθεί η παράμετρος με την **-s** για να δείξει και στατιστικά ανά πρωτόκολλο, τότε αυτά θα είναι **tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6,** ή **ipv6**.

-p (Linux)	Δείχνει ποιές διεργασίες χρησιμοποιούν ποιά sockets (παρόμοιο με την -b για τα Windows) (πρέπει να είστε **root** για να το κάνετε).
-P *protocol* (Solaris)	Δείχνει συνδέσεις για το πρωτόκολλο που προσδιορίζεται από το *protocol*, το οποίο μπορεί να είναι **ip, ipv6, icmp, icmpv6, igmp, udp, tcp,** ή **rawip**.
-r	Παρουσιάζει τα περιεχόμενα του πίνακα δρομολόγησης (είναι ισοδύναμο με την εντολή **route print** για τα Windows).
-s	Παρουσιάζει στατιστικά ανά πρωτόκολλο. Από προεπιλογή, στατιστικά εμφανίζονται για TCP, UDP, ICMP και IP. Αν το IPv6 πρωτόκολλο για Windows XP είναι εγκατεστημένο, στατιστικά θα εμφανιστούν για το TCP πάνω από IPv6, UDP πάνω από IPv6, ICMPv6, και IPv6. Η παράμετρος **-p** μπορεί να χρησιμοποιηθεί για να προσδιοριστεί ένα σύνολο πρωτοκόλλων.
-t (Windows)	Εμφανίζει την τρέχουσα σύνδεση σε κατάσταση μείωσης φόρτου.
-t (Linux)	Εμφανίζει μόνο τις συνδέσεις TCP.
-u (Linux)	Εμφανίζει μόνο τις συνδέσεις UDP.
-v (Linux)	Τυπώνει μερικές χρήσιμες πληροφορίες για τις μη ρυθμισμένες οικογένειες διευθύνσεων.
-v (Windows)	Όταν χρησιμοποιηθεί σε συνδυασμό με την **-b** θα εμφανίσει την ακολουθία των στοιχείων που εμπλέκονται στην δημιουργία σύνδεσης ή θύρας ακρόασης για όλα τα εκτελέσιμα.
-w (Linux)	Εμφανίζει μόνο τις συνδέσεις RAW.
-W (FreeBSD)	Παρουσιάζει ευρεία έξοδο - δεν περικόπτει hostnames ή IPv6 διευθύνσεις.
-x (Linux)	Εμφανίζει όλους τους NetworkDirect listeners, τις συνδέσεις και τα κοινόχρηστα endpoints.
Interval	Επανεμφανίζει τις επιλεγμένες πληροφορίες κάθε χρονικό διάστημα (προσδιορισμένο σε δευτερόλεπτα). Πατήστε CTRL+C για να σταματήσετε την επανεμφάνιση. Αν η παράμετρος παραληφθεί, η netstat θα τυπώσει τις επιλεγμένες πληροφορίες μόνο μια φορά.

4.2 Εργαλεία

Τα εργαλεία και λογισμικά που μπορεί να βρει κανείς στο Διαδίκτυο όσον αφορά τον έλεγχο της δικτυακής κίνησης και την καταγραφή των πακέτων, είναι πολλά. Μερικά χρησιμοποιούνται σε μεγάλο βαθμό ως υποβοήθηση των συστημάτων ανίχνευσης εισβολών.

4.2.1 arpspoof

Το **arpspoof** είναι εργαλείο σύλληψης πακέτων και δρομολόγησης τους μέσω του τρέχοντος υπολογιστή. Είναι δημιουργία του Dun Song και τρέχει σε Linux, OpenBSD και Solaris. Παλαιότερα ήταν γνωστό και ως **arpredirect**.

Η ιδιαιτερότητα του εργαλείου αυτού είναι η δρομολόγηση των πακέτων μέσω του υπολογιστή αντί για απευθείας μέσω του δρομολογητή. Αυτό επιτυγχάνεται με την τεχνική ARP spoofing, όπου με συνεχόμενα «μηνύματα» πείθει τον στόχο ότι αυτός είναι η gateway πια κι έτσι να στέλνει εκεί τα πακέτα για να δρομολογηθούν. Έτσι τα πακέτα περνάνε μέσα από τον υπολογιστή όπου βρίσκεται το arpspoof, όμως δεν τα προωθεί αυτόματα στον δρομολογητή, οπότε πρέπει να το κάνουμε εμείς αλλιώς ο στόχος δεν θα μπορεί να έχει σύνδεση στο υπόλοιπο δίκτυο. Η προώθηση να γίνεται αφού πρώτα έχουμε «ενημερώσει» με τον ίδιο τρόπο τον δρομολογητή ότι εμείς είμαστε ο στόχος.

Η εντολή γράφεται ως εξής:

arpspoof [options] <*host*>

–i *interface*	Προσδιορίζει το *interface* που θα χρησιμοποιηθεί.
–t *target*	Προσδιορίζει τον *στόχο*. Αν δεν αναφερθεί, τότε όλοι οι hosts του δικτύου.

Στον host προσδιορίζεται για ποιόν να διακοπεί η μετάδοση των πακέτων. Μπορεί είναι ακόμη και η τοπική gateway.

4.2.2 Fport

Το **Fport** είναι εργαλείο γραμμής εντολών της Foundstone για Windows NT4, 2000 & XP. Δείχνει ποιες διεργασίες ακούνε σε ποιες θύρες.

Εμφανίζει τις ίδιες πληροφορίες με την **netstat –an**, αλλά επίσης αντιστοιχεί τις θύρες στις τρέχουσες διεργασίες με το ID διεργασίας, το όνομα της διεργασίας και την διαδρομή.

Η σύνταξη της εντολής είναι πολύ απλή:

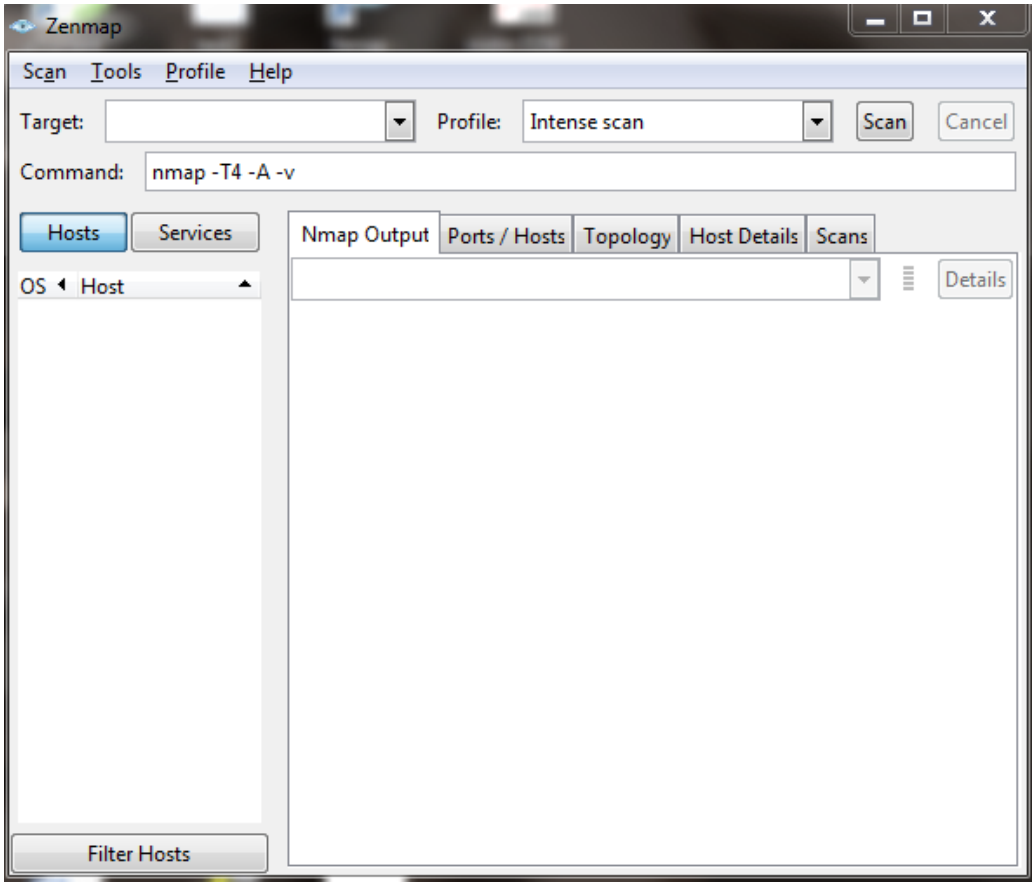
fport [commands]

/a	Ταξινόμηση κατά εφαρμογή.
/ap	Ταξινόμηση κατά διαδρομή εφαρμογής.
/i	Ταξινόμηση κατά ID διεργασίας.
/p	Ταξινόμηση κατά θύρα.

4.2.3 Nmap

Το **Nmap** είναι δικτυακός σαρωτής, υποστηρίζεται από διάφορα λειτουργικά συστήματα και μπορεί να τρέξει είτε μέσω γραμμής εντολών είτε μέσω γραφικού περιβάλλοντος. Δημιουργία του Gordon Lyon, γνωστού και ως Fyodor Vaskovich και συνοδεύεται πολλές φορές από την εφαρμογή **Zenmap**.

Δίνει την δυνατότητα έμμεσα να φτιάχνει τον «χάρτη» ενός δικτύου, καθώς σαρώνει όλες τις δικτυακές συσκευές του δικτύου εμφανίζοντας πληροφορίες για το λειτουργικό σύστημα που υποστηρίζουν, τις δικτυακές υπηρεσίες που τρέχουν και τις ανοιχτές θύρες που έχουν. Ανάλογα όμως με την ασφάλεια των υπολογιστών, εμφανίζεται και η αντίστοιχη ποσότητα πληροφοριών.



Εικόνα 4.2: Zenmap - GUI του Nmap

Το **Zenmap** κάνει την χρήση του nmap πολύ εύκολη, λόγω του ότι υπάρχουν πάρα πολλές επιλογές που μπορούν να χρησιμοποιηθούν στην γραμμή εντολών.

Πιο συγκεκριμένα, όταν εκτελείται η εφαρμογή, στο πάνω μέρος του παραθύρου εμφανίζονται τα εξής πεδία:

- ✓ **Target** – Διεύθυνση IP ή domain name του στόχου.
- ✓ **Profile** – Προφίλ σάρωσης. Μπορεί να δημιουργηθεί νέο από το μενού.
- ✓ **Command** – Σύνταξη της εντολής με βάση τα προηγούμενα πεδία. Μπορεί να τροποποιηθεί και να χρησιμοποιηθεί κανονικά σε γραμμή εντολών.

Στο κεντρικό παράθυρο υπάρχουν πέντε καρτέλες: **Nmap Output**, **Ports/Hosts**, **Topology**, **Host Details**, **Scans**. Στην αριστερή στήλη, φαίνονται οι hosts για τους οποίους έγινε σάρωση.

Στο **Nmap Output**, είναι το αποτέλεσμα της εκτέλεσης της εντολής nmap, με την διαφορά ότι αντί για απλό κείμενο, είναι μορφοποιημένο έτσι ώστε να μπορεί να διαβαστεί πιο εύκολα.

Στο **Ports/Hosts**, φαίνονται οι θύρες στις οποίες έχει ανατεθεί κάποια υπηρεσία και η κατάσταση τους.

Στο **Topology**, παρουσιάζεται ένας ακτινωτός χάρτης της διαδρομής από τον δικό μας υπολογιστή στους στόχους. Ο χάρτης δημιουργείται έπειτα από την εκτέλεση του traceroute, το οποίο ανακαλύπτει την δικτυακή διαδρομή μέσω των δρομολογητών. Στο Hosts Viewer βλέπουμε νέο παράθυρο με περισσότερες πληροφορίες.

Στο **Host Details**, βλέπουμε συνοπτικές πληροφορίες για τον host.

Στο **Scans**, μας δείχνει τις σαρώσεις που κάναμε και αν έχουν αποθηκευτεί ή όχι.

4.2.4 ntop

Το **ntop** είναι ανάλογο του top που είναι για τις διεργασίες, αλλά για την κατάσταση του δικτύου. Μπορεί να τρέξει σε Unix και Windows.

Για να το διαχειριστεί κανείς, καθώς και για να δει καλύτερα το αποτέλεσμα της παρακολούθησης, εκτός από την γραμμή εντολών υπάρχει και web interface το οποίο υπάρχει στην διεύθυνση **http://127.0.0.1:3000**. Πρώτα όμως θα πρέπει να έχει γίνει εκκίνηση της υπηρεσίας του ntop και του αντίστοιχου loopback interface ώστε να ανοίξει η σύνδεση στην θύρα 3000.

Η εντολή γράφεται ως εξής:

ntop [options]

–4	Χρησιμοποιεί IPv4 συνδέσεις.
–6	Χρησιμοποιεί IPv6 συνδέσεις.
–a *file*	*Αρχείο* για το log πρόσβασης στον web server.
–A	Ζητά το όνομα και τον κωδικό του διαχειριστή.
–b	Απενεργοποιεί τους αποκωδικοποιητές των πρωτοκόλλων.
–B *filter*	*Φίλτρο* πακέτων, όπως στο **tcpdump**.
–c	Οι αδρανείς hosts δεν βγαίνουν από την μνήμη.
–C *rate*	*Ρυθμός* δειγματοληψίας σύλληψης πακέτων.
–d	Τρέχει το ntop σε λειτουργία διεργασίας daemon.
–D *name*	Όνομα χώρου στο Διαδίκτυο.
–e *n*	Μέγιστες γραμμές πίνακα όπου θα αναφέρει.
–f *file*	Αρχείο κίνησης.
–g	Ανιχνεύει μόνο τους τοπικούς υπολογιστές.
–i *inter*	Ένα ή πολλά interfaces τα οποία θα επιβλέπει.
–j	Δημιουργεί αρχείο **ntop-other-pkts.XXX.pcap** για λοιπά πακέτα.
–K	Ενεργοποιεί την λειτουργία debug.
–l *path*	Πετάει τα πακέτα που έπιασε σε αρχείο στην δοσμένη *διαδρομή*. Για debug μόνο.
–L	Καταγράφει μέσω της καταγραφής του συστήματος.
–m *addr*	Τοπικά *υποδίκτυα*.
–n *mode*	*Λειτουργία* μετατροπής IP διεύθυνσης σε ονόματα.
–o	Το ntop θα εμπιστευτεί μόνο τις IP διευθύνσεις και όχι τις MAC.
–O *path*	*Διαδρομή* για τα log αρχεία σε μορφή pcap.
–p *list*	*Λίστα* των IP πρωτοκόλλων που θα παρακολουθεί.
–P *path*	*Διαδρομή* για τα αρχεία των εσωτερικών βάσεων δεδομένων του ntop.
–q	Δημιουργεί αρχείο **ntop-suspicious-pkts.XXX.pcap** για ύποπτα πακέτα.

–r *n*	Ρυθμός ανανέωσης σε *δευτερόλεπτα*. Προεπιλεγμένα είναι τα 120.
–s	Απενεργοποιεί την αδιάκριτη λειτουργία.
–t *n*	*Επίπεδο* ιχνών. Από 0 έως 6.
–u *user*	Υπό ποιον *χρήστη* θα τρέξει το ntop.
–U *url*	*Link* στο οποίο θα εμφανίζει την τοποθεσία του host, με την χρήση του **mapper.pl**.
–w *port*	*Θύρα* στην οποία θα ακούει για το πρωτόκολλο HTTP.
–W *port*	*Θύρα* στην οποία θα ακούει για το πρωτόκολλο HTTPS.
–x *n*	*Μέγιστες εγγραφές* hash που μπορεί να χειριστεί το ntop.
–X *n*	*Μέγιστες TCP συνεδρίες* που μπορεί να χειριστεί το ntop.
–z	Απενεργοποιεί την ανίχνευση των TCP συνεδριών.

Για την επιλογή **–C**, η προεπιλεγμένη τιμή είναι το 1, για καθόλου δειγματοληψία.
Για την επιλογή **–n**, οι τιμές για τις λειτουργίες μετατροπής είναι:

- **0** → Καμία μετατροπή
- **1** → Μετατροπή μόνο των τοπικών hosts
- **2** → Μετατροπή μόνο των απομακρυσμένων hosts

4.2.5 Snort

Το **Snort** είναι σύστημα ανίχνευσης και αποτροπής δικτυακής διείσδυσης. Τρέχει σε Windows και Unix συστήματα και δημιουργήθηκε από τον Martin Roesch. Άλλα εργαλεία που χρησιμοποιούν το Snort για γενικές λειτουργίες, είναι τα **Aanval**, **BASE**, **Squil** και **Snorby**.

Λειτουργεί σαν το **tcpdump** και μπορούν να χρησιμοποιηθούν τα αποτελέσματα που εξάγονται, από το tcpdump.

Η εντολή γράφεται ως εξής:

snort [options] <*filter*>

–A *mode*	Θέτει επίπεδο ειδοποίησης.
–b	Καταγράφει τα πακέτα σε μορφή **tcpdump**. Πιο γρήγορο.
–c *rules*	Χρησιμοποιεί το δοσμένο *αρχείο* ως αρχείο κανόνων.
–C	Τυπώνει το payload με χαρακτήρες μόνο και όχι δεκαεξαδικό.
–d	Εμφανίζει τα δεδομένα από τις κεφαλίδες του επιπέδου εφαρμογής.
–D	Τρέχει το snort στο παρασκήνιο.
–e	Εμφανίζει τις πληροφορίες των κεφαλίδων του επιπέδου σύνδεσης.
–F *file*	Διαβάζει τα BPF φίλτρα από το δοθέν *αρχείο*.
–g *group*	Τρέχει το snort ως την δοθείσα *ομάδα*.
–h *IP*	Θέτει το *οικιακό δίκτυο*.
–H	Κάνει τους πίνακες των hashes ντετερμινιστικούς.
–i *inter*	Ακούει στο δοσμένο *interface*.
–I	Προσθέτει το όνομα του interface στην έξοδο ειδοποίησης.
–k *mode*	*Λειτουργία* checksum.
–K *mode*	*Λειτουργία* καταγραφής.
–l *dir*	Η καταγραφή αποθηκεύεται στον δοθέν *κατάλογο*.
–L *file*	Η καταγραφή αποθηκεύεται στο δοθέν *αρχείο tcpdump*.
–m *umask*	Ορίζει τα *δικαιώματα* ενός αρχείου.

–M	Η καταγραφή αποθηκεύεται στην καταγραφή του συστήματος χωρίς ειδοποιήσεις.
–n *n*	Σταματάει μετά από λήψη *n* πακέτων.
–N	Απενεργοποιεί την καταγραφή, ενώ οι ειδοποιήσεις λειτουργούν κανονικά.
–O	Θολώνει τις καταγεγραμμένες IP διευθύνσεις.
–p	Απενεργοποιεί την αδιάκριτη λειτουργία.
–q	Δεν εμφανίζει κεφαλίδες και αναφορά κατάστασης.
–r *file*	Διαβάζει και επεξεργάζεται το δοθέν *tcpdump αρχείο*.
–R *id*	Περιλαμβάνει το *id* στο όνομα του αρχείου **snort_intf<*id*>.pid**.
–s	Η καταγραφή αποθηκεύεται στην καταγραφή του συστήματος.
–t *dir*	Θέτει τον δοθέν *κατάλογο* για τις διεργασίες με το εργαλείο **chroot**.
–T	Τεστάρει και αναφέρει στην τρέχουσα ρύθμιση του snort.
–u *user*	Τρέχει το snort ως τον δοθέν *χρήστη*.
–U	Χρησιμοποιεί UTC μορφή στα timestamps.
–v	Verbose
–x	Έξοδος σε περίπτωση προβλήματος του snort.
–X	Κρατάει τα δεδομένα του πακέτου, ξεκινώντας από το επίπεδο σύνδεσης.
–y	Συμπεριλαμβάνει το έτος στα timestamps.

Για την επιλογή **–A**, οι λειτουργίες ειδοποίησης είναι:

- **console** → Στέλνει γρήγορες ειδοποιήσεις στην οθόνη.
- **fast** → Γράφει την ειδοποίηση σε απλή μορφή με timestamp, μήνυμα, διεύθυνση IP και θύρα πηγής και προορισμού.
- **full** → Πλήρεις ειδοποιήσεις. Προεπιλογή.
- **none** → Απενεργοποιεί τις ειδοποιήσεις.
- **unsock** → Στέλνει ειδοποιήσεις σε UNIX socket ότι άλλο πρόγραμμα μπορεί να ακούσει.

Για την επιλογή **–k**, οι λειτουργίες του checksum είναι:

- **all**
- **noicmp**
- **noip**
- **none**
- **notcp**
- **noudp**

Για την επιλογή **–K**, οι λειτουργίες της καταγραφής είναι:

- **asci**
- **none**
- **pcap** → προεπιλογή

4.2.6 tcpdump / WinDump

Το **tcpdump** είναι εργαλείο ελέγχου, καταγραφής και αποθήκευσης της κίνησης ενός δικτύου. Χρησιμοποιεί την βιβλιοθήκη **libpcap** για την καταγραφή των πακέτων. Υποστηρίζεται από τα περισσότερα Unix συστήματα όπως Linux, Solaris, BSD και OS X.

Το **WinDump** είναι η Windows εκδοχή του tcpdump και έχει τις ίδιες ακριβώς λειτουργίες. Κι αυτό αντίστοιχα χρησιμοποιεί την βιβλιοθήκη **WinPcap** για την σύλληψη των πακέτων, την Windows εκδοχή της libpcap.

Σε όλα τα λειτουργικά, χρησιμοποιείται η ίδια σύνταξη και οι ίδιες επιλογές, αφού στην ουσία πρόκειται για porting:

tcpdump [options] *[expression]*
windump [options] *[expression]*

–#	Τυπώνει τον αριθμό του πακέτου στην αρχή της γραμμής.
–A	Τυπώνει την κεφαλίδα του επιπέδου συνδέσμου κάθε πακέτου σε ASCII.
–b	Τυπώνει τον αριθμό AS στα BGP πακέτα σε ASDOT μορφή αντί για ASPLAIN.
–B *n*	Ορίζει το *μέγεθος του buffer* του OS σε μονάδες των KB.
–c *n*	Σταματάει να λαμβάνει μετά από *n πακέτα*.
–C *n*	Αν το αρχείο αποθήκευσης είναι μεγαλύτερο από *n bytes*, τότε γράφει σε καινούργιο αρχείο.
–d	Διαβάζει τον μεταγλωττισμένο κώδικα αντιστοίχισης πακέτου σε ευκατανόητη μορφή για τον άνθρωπο.
–dd	Διαβάζει τον κώδικα αντιστοίχισης πακέτου ως τμήμα προγράμματος C.
–ddd	Διαβάζει τον κώδικα αντιστοίχισης πακέτου ως δεκαδικούς αριθμούς, ακολουθούμενοι από μετρητή.
–D	Εμφανίζει λίστα με τα διαθέσιμα interfaces.
–e	Τυπώνει την κεφαλίδα του επιπέδου συνδέσμου κάθε πακέτου.
–E *x*	Αποκρυπτογραφεί τα **ESP (Encapsulating Security Payload)** πακέτα που προορίζονται στην δοσμένη IP και περιλαμβάνουν τιμή **SPI (Security Parameter Index)**.
–F *file*	Χρησιμοποιείται το *αρχείο* για την εφαρμογή φίλτρων.
–G *n*	Ορίζει κάθε πόσα *δευτερόλεπτα* θα δημιουργείται καινούργιο αρχείο αποθήκευσης.
–H	Απόπειρα εντοπισμού επικεφαλίδων περί του πρωτοκόλλου IEEE 802.11s.
–i *x*	Ακούει στο ορισμένο *interface*.
–I	Θέτει το interface σε λειτουργία παρακολούθησης.
—immediate-mode	Ενεργοποιεί την **"άμεση λειτουργία"**, όπου τα πακέτα δεν αποθηκεύονται σε αρχείο αποθήκευσης και στέλνονται κατευθείαν στην οθόνη.
–j *type*	Ορίζει τον *τύπο του timestamp* για τα πακέτα.
–K	Δεν επαληθεύει τα checksums των IP, TCP και UDP.
–l	Βγάζει την έξοδο σε γραμμές. Χρήσιμο για επίβλεψη των δεδομένων ταυτόχρονα με την σύλληψη των πακέτων.
–L	Εμφανίζει λίστα με τους γνωστούς τύπους ζεύξης δεδομένων του interface.
–M *text*	Χρησιμοποιεί το *text* ως κοινό κλειδί για την επαλήθευση των hashes στα TCP τμήματα με την επιλογή TCP-MD5, εάν υπάρχουν.
–n	Δεν μετατρέπει τις διευθύνσεις σε ονόματα.
–N	Αναφέρει μόνο το host name αντί για ολόκληρο το domain name.
–q	Τυπώνει λιγότερες πληροφορίες για τα πρωτόκολλα, ώστε οι γραμμές να είναι μικρότερες.
–Q *direc*	Η κατεύθυνση των πακέτων για τα οποία να κάνει σύλληψη.
–r *file*	Διαβάζει τα πακέτα από το δοσμένο αρχείο.
–S	Τυπώνει τους αριθμούς ακολουθίας του TCP απόλυτα και όχι σχετικά.

–t	Δεν τυπώνει το timestamp.
–tt	Τυπώνει το timestamp σε δευτερόλεπτα και σε κλάσματα του δευτερολέπτου από την 1η Ιανουαρίου, 1970, 00:00:00, UTC.
–ttt	Τυπώνει την διαφορά σε μικροδευτερόλεπτα ανάμεσα στην τρέχουσα και την προηγούμενη γραμμή.
–tttt	Τυπώνει το timestamp από τα μεσάνυχτα.
–ttttt	Τυπώνει την διαφορά σε μικροδευτερόλεπτα ανάμεσα στην τρέχουσα και την πρώτη γραμμή.
–T *type*	Εξαναγκάζει τα πακέτα να ερμηνευτούν ως ενός συγκεκριμένου τύπου.
–v	Verbose. Για παράδειγμα, TTL, ID, συνολικό μήκος και επιλογές ενός IP πακέτου.
–vv	Verbose. Για παράδειγμα, επιπρόσθετα πεδία από πακέτα απάντησης του NFS.
–vvv	Verbose. Για παράδειγμα, οι telnet επιλογές γράφονται πλήρως.
–V *file*	Διαβάζει μια λίστα file names από το δοσμένο *αρχείο*.
–w *file*	Γράφει τα πακέτα απευθείας σε *αρχείο*, αντί να τα διαβάσει και να τα τυπώσει.
–W	Σε συνδυασμό με την επιλογή **–C**, περιορίζει τα αρχεία που δημιουργήθηκαν στον δοσμένο αριθμό και αντικαθιστά τα αρχεία από την αρχή.
–x	Τυπώνει τα δεδομένα κάθε πακέτου σε δεκαεξαδικό.
–xx	Τυπώνει τα δεδομένα κάθε πακέτου και της κεφαλίδες επιπέδου σύνδεσης σε δεκαεξαδικό.
–X	Τυπώνει τα δεδομένα κάθε πακέτου σε δεκαεξαδικό και ASCII.
–XX	Τυπώνει τα δεδομένα κάθε πακέτου και της κεφαλίδες επιπέδου σύνδεσης σε δεκαεξαδικό και ASCII.
–y *type*	Ορίζει τον *τύπο* της σύνδεσης δεδομένων.
–z *cmnd*	Εκτελεί *εντολή* αφότου κλείσει η εγγραφή στο τρέχων αρχείο.
–Z *user*	Αλλάζει στον δοσμένο χρήστη πριν ανοιχθούν τα αρχεία εγγραφής.

Οι επιλογές **–A** και **–e** κάνουν λίγο πολύ το ίδιο πράγμα, αλλά η **–A** είναι κατάλληλη για σύλληψη ιστοσελίδων, ενώ η **–e** για την ανάγνωση της διεύθυνση του επιπέδου MAC.

Στην επιλογή **–C**, το μέγεθος του αρχείου μετριέται σε εκατομμύρια bytes, συγκεκριμένα 1.000.000 και όχι 1.048.576.

Επίσης, το όνομα των αρχείων αποθήκευσης πέραν του πρώτου, προσδιορίζονται με την επιλογή **–w** και έναν αριθμό μπροστά, ώστε να αυξάνετε κάθε φορά.

Για την επιλογή **–E**, χρησιμοποιείται για την αποκρυπτογράφηση η σύνταξη *spi@ip algo:text* , όπου:

- **spi** → Η τιμή του SPI.
- **ip** → Η διεύθυνση IP στην οποία απευθύνεται το πακέτο.
- **algo** → Το πρωτόκολλο αποκρυπτογράφησης, το οποίο μπορεί να είναι:
  - **3des-cbc**
  - **blowfish-cbc**
  - **cast128-cbc**
  - **des-cbc**, προεπιλογή
  - **rc3-cbc**
  - **none**
- **text** → Το ASCII κείμενο για το κρυφό κλειδί του ESP. Αν προηγείται το 0x, τότε θα διαβαστεί ως δεκαεξαδική τιμή.

Στην σύνταξη της επιλογής, μπορεί να προστεθεί και όνομα αρχείου το οποίο θα διαβαστεί από το tcpdump αφού λάβει το πρώτο ESP πακέτο.

Για την επιλογή **–i**, αν δεν οριστεί interface, τότε το tcpdump ψάχνει στην λίστα για το παραμετροποιημένο interface με την μικρότερη αρίθμηση πέραν του loopback, όπως το eth0.

Για την επιλογή **–I**, η λειτουργία παρακολούθησης υποστηρίζεται μόνο σε IEEE 802.11 Wi-Fi interfaces και δεν υποστηρίζεται από όλα τα OS.

Για την επιλογή **–j**, οι τύποι timestamp υπάρχουν στο pcap-tstamp και δεν είναι απαραίτητο να είναι έγκυροι όλοι για το interface.

- **host** – Απροσδιόριστη ακρίβεια και μπορεί να είναι ή όχι συγχρονισμένο με το ρολόι του OS.
- **host_lowprec** – Χαμηλή ακρίβεια και συγχρονισμένο με το ρολόι του OS.
- **host_hiprec** – Υψηλή ακρίβεια και μπορεί να είναι ή όχι συγχρονισμένο με το ρολόι του OS. Πιο δύσκολο να επιτευχθεί σε σύγκριση με το **host_lowprec**.
- **adapter** – Υψηλή ακρίβεια και συγχρονισμένο με το ρολόι του OS.
- **adapter_unsynced** – Υψηλή ακρίβεια και ασυγχρόνιστο με το ρολόι του OS.

Οι τρεις πρώτοι τύποι αφορούν τον υπολογιστή στον οποίον γίνεται η σύλληψη, ενώ οι δύο τελευταίοι τον προσαρμογέα ο οποίος κάνει την σύλληψη. Η ακρίβεια αφορά *νανοδευτερόλεπτα*.

Για την επιλογή **–Q**, οι αποδεκτές τιμές είναι:

- **in**
- **out**
- **inout**

Για την επιλογή **–T**, οι τύποι που είναι γνωστοί για την ώρα είναι:

1. **aodv** (Ad-hoc On-demand Distance Vector Protocol)
2. **carp** (Common Address Redundancy Protocol)
3. **cnfp** (Cisco NetFlow Protocol)
4. **lmp** (Link Management Protocol)
5. **pgm** (Pragmatic General Multicast)
6. **pgm_zmtp1** (ZMTP/1.0 inside PGM/EPGM)
7. **radius** (RADIUS)
8. **rpc** (Remote Procedure Call)
9. **rtp** (Real-Time Applications Protocol)
10. **rtcp** (Real-Time Applications Control Protocol)
11. **sack** (RFC 2018 TCP Selective Acknowledgements Options)
12. **snmp** (Simple Network Management Protocol)
13. **tcp** (Transmission Control Protocol)
14. **tftp** (Trivial File Transfer Protocol)
15. **vat** (Visual Audio Tool)
16. **vrrp** (Virtual Router Redundancy Protocol)
17. **vxlan** (Virtual eXtensible Local Area Network)
18. **wb** (distributed White Board)
19. **zmtpl** (ZeroMQ Message Transport Protocol 1.0)

Για την επιλογή **–y**, οι συνηθισμένοι τύποι σύνδεσης είναι:

- ✓ **EN10MB**

- ✓ **IEEE802_11**
- ✓ **IEEE802_11_RADIO**

Η επιλογή **–z**, χρησιμοποιείται σε συνδυασμό με τις επιλογές **–C** και **–G** και οι εντολές που μπορεί να εκτελέσει, είναι για παράδειγμα η **gzip**, η οποία θα συμπιέσει το κάθε αρχείο εγγραφής χρησιμοποιώντας αυτή την εφαρμογή.

Η επιλογή **–Z** μπορεί να χρησιμοποιηθεί μόνο από τον root, ειδάλλως τίθεται αυτόματα ο τρέχων χρήστης.

4.2.7 tcpflow

Το **tcpflow** είναι εργαλείο το οποίο λαμβάνει δεδομένα που μεταδόθηκαν ως μέρος μιας TCP σύνδεσης. Από τον Simson Garfinkel και τρέχει σε Linux.

Αποθηκεύει τα δεδομένα σε μορφή αναγνώσιμη από εργαλεία όπως το **Wireshark**.

Η σύνταξη της εντολής είναι:

tcpflow [options] [expression]

–b *n*	Μέγιστος *αριθμός bytes* ανά ροή για αποθήκευση.
–c	Τυπώνει μόνο στην οθόνη. Δεν δημιουργεί αρχεία.
–C	Τυπώνει μόνο στην οθόνη, αλλά χωρίς την κεφαλίδα source/dest.
–d *n*	*Επίπεδο* debug. Προεπιλογή είναι το 1.
–e	Τυπώνει κάθε ροή με εναλλακτικά χρώματα.
–f *n*	Μέγιστος *αριθμός περιγραφέων* αρχείων για χρήση.
–i *inter*	*Interface* στο οποίο θα ακούει.
–p	Δεν χρησιμοποιεί την αδιάκριτη λειτουργία.
–r *file*	Διαβάζει τα πακέτα από *αρχείο* tcpdump.
–s	Αντικαθιστά τους μη-εκτυπώσιμους χαρακτήρες με τον χαρακτήρα “**.**”.
–v	Verbose που ισοδυναμεί με την επιλογή **–d 10**.
expression	Έκφραση φιλτραρίσματος όπως στο tcpdump.

4.2.8 tcptrace

Το **tcptrace** είναι εργαλείο ανάλυσης dump αρχείων TCP πακέτων. Μπορεί να τρέξει σε Unix, Solaris και Windows.

Δέχεται σαν είσοδο tcpdump αρχεία από διάφορα δημοφιλή προγράμματα σύλληψης πακέτων, όπως snort, tcpdump, WinDump και Wireshark και παράγει μια συνοπτική παρουσίαση των συνδέσεων.

–A*n*	Μέσα *n* τεμάχια για τα γραφήματα throughput. Προεπιλογή τα 10.
–b	Περιεκτική έξοδος.
–B*n*	Αναλύει τον αριθμό του πρώτου τεμαχίου. Προεπιλογή το 1.
–c	Αγνοεί μη ολοκληρωμένες συνδέσεις.
–C	Παράγει πολύχρωμα σχέδια.
–d	Τυπώνει πληροφορίες περί debug.
–D	Τυπώνει σε δεκαδικό.

–e	Εξάγει το περιεχόμενο κάθε TCP ροής σε αρχείο.
–E*n*	Αναλύει τον αριθμό του τελευταίου τεμαχίου. Προεπιλογή τελευταίο στο αρχείο.
–f*expr*	Έξοδος με χρήση *φίλτρου*.
–F	Δημιουργεί γραφήματα των μεγεθών των τεμαχίων.
–G	Δημιουργεί όλων των ειδών τα γραφήματα.
–i*n*	Αγνοεί την σύνδεση με αριθμό *n*.
–l	Μακρά έξοδος.
–L	Δημιουργεί γραφήματα χρονογραμμής.
–M	Παράγει μονόχρωμα σχέδια.
–n	Δεν μεταφράζει ονόματα host και υπηρεσιών. Πιο γρήγορο.
–N	Δημιουργεί τα γραφήματα OWIN (Outstanding Data Graph).
–o*n[-m]*	Επιτρέπει την σύνδεση με αριθμό *n* ή με εύρος αριθμών *n-m*. Το *n* μπορεί να αφορά αρχείο κι έτσι να διαβάζει την λίστα από εκεί.
–O*file*	Κρατάει τα αντιστοιχισμένα πακέτα στο δοσμένο tcpdump *αρχείο*.
–p	Τυπώνει ολόκληρο το περιεχόμενο ενός πακέτου.
–P	Τυπώνει το περιεχόμενο ενός πακέτου για επιλεγμένες συνδέσεις.
–r	Τυπώνει τα **RTT (Rount-Trip Time)** στατιστικά.
–R	Δημιουργεί γραφήματα για τα δείγματα RTT.
–s	Χρησιμοποιεί σύντομα ονόματα.
–S	Δημιουργεί γραφήματα για την ακολουθία του χρόνου.
–t	Μαρκάρει τον αριθμό των πακέτων ως ένδειξη προόδου.
–T	Δημιουργεί γραφήματα για το throughput.
–u	Εκτελεί ανάλυση UDP.
–w	Τυπώνει διάφορα προειδοποιητικά μηνύματα.
–X	Τυπώνει σε δεκαεξαδικό.
–y	Παραλείπει τα σημεία του στιγμιαίου throughput από το γράφημα του throughput.
–zx	Σχεδιάζει τον άξονα του χρόνου από το 0 αντί με την ώρα του ρολογιού.
–zy	Σχεδιάζει αριθμούς ακολουθίας από το 0. Για γραφήματα ακολουθίας μόνο.
–zxy	Σχεδιάζει και τους δύο άξονες από το 0.
–Z	Κρατάει τους χρόνους των δειγμάτων RTT σε αρχεία.

Η επιλογή **–d**, αν γραφτεί πολλαπλές φορές, θα δώσει περισσότερες πληροφορίες για το debug του προγράμματος.

Για την επιλογή **–f**, η σύνταξη του φίλτρου καθώς και οι μεταβλητές που μπορούν να χρησιμοποιηθούν, φαίνονται στην επιλογή **–hfilter**.

Οι επιλογές **–n** και **–o**, ο αριθμός αφορά συνδέσεις με αρίθμηση όπως εμφανίζονται στην έξοδο και μπορούν να μπουν πολλαπλές τιμές.

Για την επιλογή **–s**, ένα παράδειγμα είναι η χρήση του ονόματος "**picard**", αντί για ολόκληρο το όνομα της λίστας "**picard.cs.ohiou.edu**".

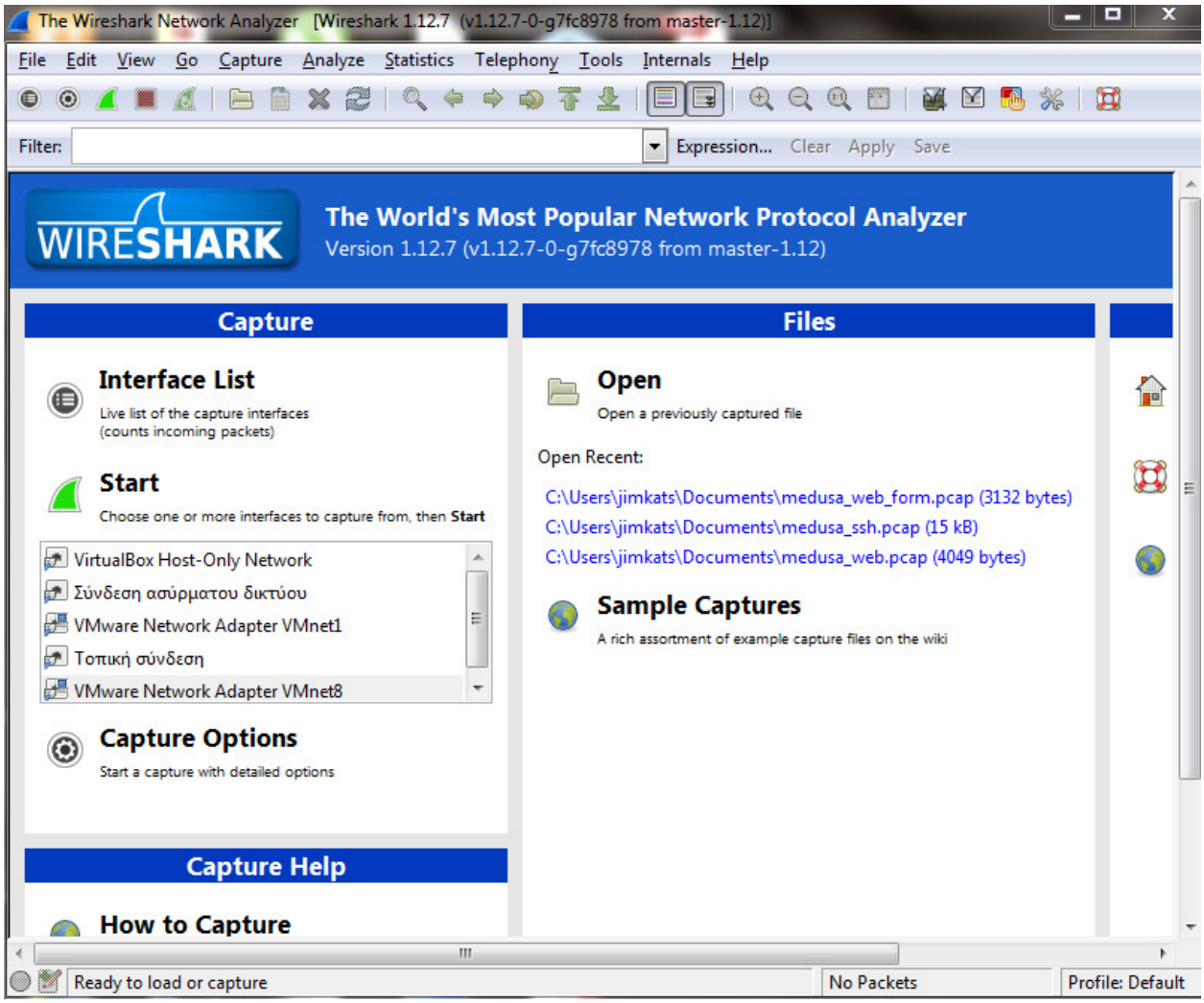
4.2.9 Wireshark

Το **Wireshark** είναι εργαλείο ανάλυσης δικτυακών πρωτοκόλλων και τρέχει στα περισσότερα λειτουργικά συστήματα, όπως Windows, Linux, OS X, BSD και Solaris. Μέχρι και το 2006 ήταν γνωστό ως **Ethereal**.

Όπως και το tcpdump, έτσι και το Wireshark χρησιμοποιεί την βιβλιοθήκη **libcap** και αντίστοιχα την **Winpcap** για τα Windows, για την δυνατότητα σύλληψης των πακέτων.

Στα Unix συστήματα, η διανομή του Wireshark περιλαμβάνει και μερικά εργαλεία που εκτελούνται σε γραμμή εντολών, κάνοντας διάφορες λειτουργίες. Συγκεκριμένα πρόκειται για:

- **capinfos** → Τυπώνει πληροφορίες για τα αρχεία σύλληψης.
- **dftest** → Δείχνει τον δυαδικό κώδικα ενός φίλτρου. Για debug.
- **dumpcap** → Κρατάει και εμφανίζει την δικτυακή κίνηση.
- **editcap** → Επεξεργάζεται και μεταφράζει την μορφή των αρχείων σύλληψης.
- **idl2wrs** → Παράγει C κώδικα για plugin από αρχείο CORBA IDL.
- **mergecap** → Ενώνει δύο ή περισσότερα αρχεία σύλληψης σε ένα.
- **randpkt** → Γεννήτρια τυχαίου πακέτου.
- **rawshark** → Κρατάει και αναλύει καθαρά δεδομένα pcap.
- **reordercap** → Ταξινομεί το αρχείο εισόδου ανά timestamp και το αποθηκεύει αλλού.
- **text2pcap** → Δημιουργεί αρχείο σύλληψης με βάση το ASCII hexdump των πακέτων.
- **tshark** → Διαβάζει και αναλύει την δικτυακή κίνηση.
- **wireshark-filter** → Σύνταξη φίλτρου του Wireshark.
- **wireshark** → Μέσω αλληλεπίδρασης κρατάει και αναλύει την δικτυακή κίνηση.



Εικόνα 4.3: Αρχική οθόνη Wireshark

Στα Windows, γίνεται χρήση του γραφικού περιβάλλοντος του, όπου μπορεί κανείς να παρακολουθεί την δικτυακή κίνηση και να διαβάζει αρχεία σύλληψης πακέτων με ευκατανόητο τρόπο και να φιλτράρει εύκολα αυτό που θέλει.

Συγκεκριμένα, όταν ανοίγει κανείς το Wireshark, βλέπει την κεντρική σελίδα όπου του εμφανίζονται τέσσερις ενότητες: **Capture**, **Capture Help**, **Files**, **Online**. Στο **Capture** μπορεί να δει την λίστα με τα δικτυακά interfaces του υπολογιστή και να ξεκινήσει την σύλληψη πακέτων, αλλάζοντας οποιαδήποτε ρύθμιση θέλει, ενώ στο **Files** μπορεί να ανοίξει αρχείο σύλληψης και να χρησιμοποιήσει έτοιμα παραδείγματα πακέτων.

Πατώντας στο Interface List στο Capture, εμφανίζονται τα interfaces με ονόματα, διευθύνσεις IP και λεπτομέρειες, στις οποίες αναφέρονται χαρακτηριστικά του interface και στατιστικά της χρήσης του.

Επιλέγοντας ένα interface από την λίστα και πατώντας Start, ξεκινάει να καταγράφει τα πακέτα που στέλνονται από και προς το συγκεκριμένο interface και ταυτόχρονα τα εμφανίζει. Σε εφτά στήλες βλέπουμε για το κάθε πακέτο:

- **No.** → Αύξων αριθμός πακέτου από την έναρξη της καταγραφής.
- **Time** → Χρόνος σε nanoseconds από την έναρξη της καταγραφής.

- **Source** → Διεύθυνση πηγής.
- **Destination** → Διεύθυνση προορισμού.
- **Protocol** → Πρωτόκολλο.
- **Length** → Μήκος πακέτου.
- **Info** → Πληροφορία για την ενέργεια του πακέτου.

Οι διευθύνσεις μπορεί να είναι είτε **IPv4** είτε **IPv6** μόνο σε κάποιες περιπτώσεις.

Ανάλογα με το πρωτόκολλο, οι αντίστοιχες εγγραφές χρωματίζονται διαφορετικά. Αυτό μπορεί να αλλάξει στο **View→Colorize Conversation→New Coloring Rule**… στο μενού στο πάνω μέρος.

Πατώντας πάνω σε μια ένα πακέτο, βλέπουμε πληροφορίες για τις κεφαλίδες, όπως τι δεδομένα περιέχουν και τι μήκος έχουν. Επίσης, κάτω από τις κεφαλίδες βλέπουμε το κύριο περιεχόμενο του πακέτου σε δεκαεξαδική μορφή και κάθε φορά που επιλέγουμε κάποια κεφαλίδα, αντίστοιχα από κάτω επισημαίνεται με μπλε χρώμα ποιο μέρος του περιεχομένου αναφέρεται.

Το μενού στο πάνω μέρος, υπάρχουν πολλές καρτέλες που βοηθάνε όχι μόνο στην ανάλυση πακέτων, αλλά και σε άλλα πράγματα, όπως στην εμφάνιση των κανόνων του firewall του υπολογιστή για όλα τα προϊόντα, μέσω του **Tools→Firewall ACL Rules**, όπως:

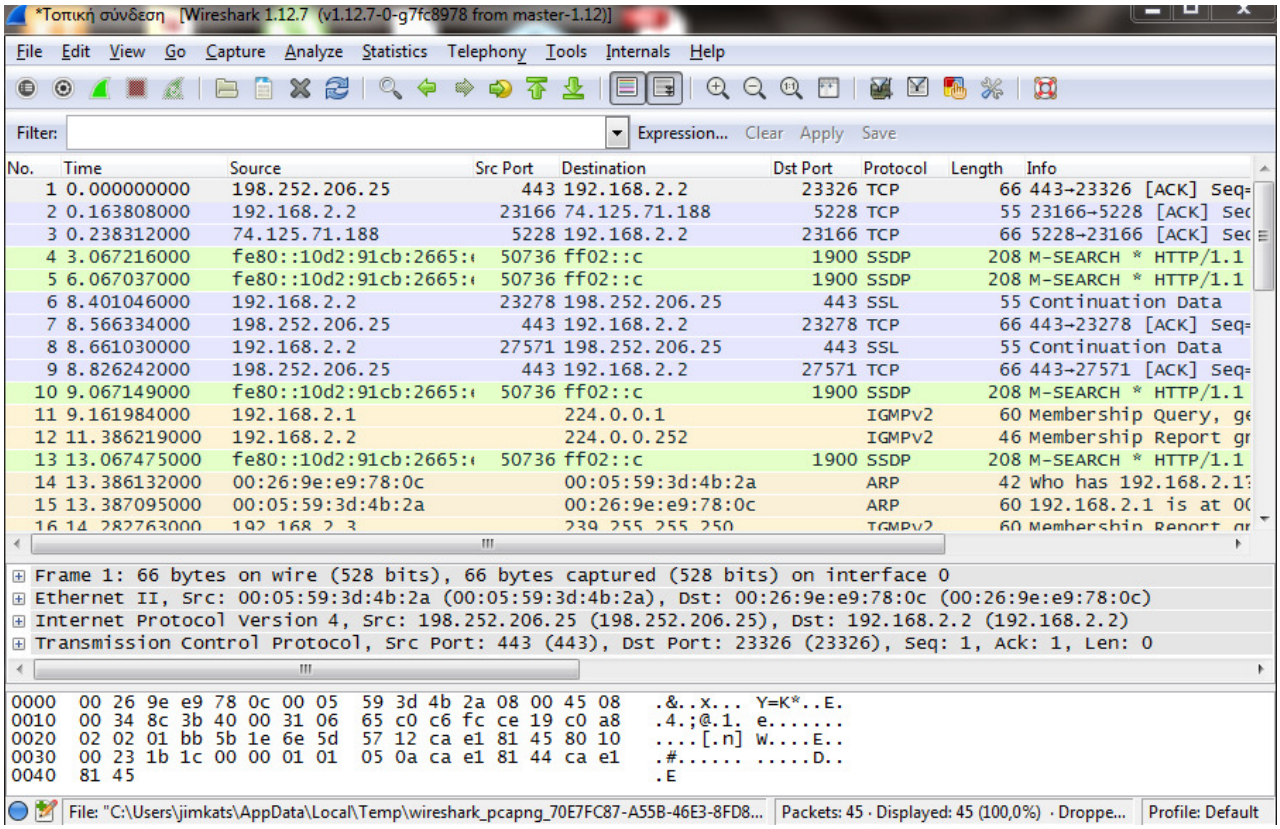
- **Cisco IOS**
- **Linux Netfilter (iptables)**
- **OpenBSD Packet Filter (pf)**
- **Windows Firewall (netsh)**

Μπορεί να γίνει ανάλυση ακόμη και πακέτων τηλεφωνίας και καταγραφή VoIP κλήσεων.

Κάτω από το μενού στο πάνω μέρος, υπάρχουν δύο μπάρες, η μπάρα διαχείρισης και η μπάρα φίλτρου.

Η μπάρα διαχείρισης περιέχει συντομεύσεις, όπως για την επιλογή interfaces, την έναρξη και διακοπή της σύλληψης πακέτων, άνοιγμα αρχείου και αποθήκευση σε αρχείο, αναζήτηση πακέτου και μετακίνηση με βάση τον αριθμό του, μεγέθυνση/σμίκρυνση στο παράθυρο των πακέτων και δημιουργία/επεξεργασία του φίλτρου.

Στην μπάρα φίλτρου μπορεί να συνταχθεί η έκφραση για το φίλτρο. Πατώντας στο Expression… εμφανίζεται σε ένα παράθυρο μια λίστα με όλα τα πρωτόκολλα και τις δικτυακές υπηρεσίες και ένας πίνακας με τις συνθήκες, όπου μόλις επιλεγεί κάτι, τότε μπορεί να προσδιοριστεί τιμή και εύρος για το εκάστοτε πεδίο πρωτοκόλλου.



Εικόνα 4.4: Παράδειγμα εμφάνισης πακέτων

5. Εγκληματολογική εξέταση εφαρμογών & συστήματος

Η εγκληματολογική εξέταση των εφαρμογών και των συστημάτων, είναι άλλο ένα σημαντικό κομμάτι επί του συνόλου της εγκληματολογικής έρευνας και ίσως και το πιο απαιτητικό.

Πιο συγκεκριμένα, οι εφαρμογές, είτε σαν απλά εργαλεία γραμμής εντολών, είτε σαν λογισμικά με γραφικό περιβάλλον, μπορούν να αποδειχθούν ιδιαίτερα επιβλαβή για ένα σύστημα, καθώς δεν είναι γνωστό τι περιέχει ο κώδικας μέσα. Ιδιαίτερα για τα Linux όπου όλα είναι ανοιχτός κώδικας κι έτσι ένα εργαλείο μπορεί να αναδιανεμηθεί με τροποποιημένο κώδικά ο οποίος να προκαλέσει υποκλοπή, απώλεια δεδομένων και τροποποίηση συστήματος.

Τα συστήματα έρχονται να ολοκληρώσουν την διαδικασία όσον αφορά τους υπολογιστές. Ως συστήματα αναφερόμαστε στα λειτουργικά συστήματα, όπου με τις ρυθμίσεις περιβάλλοντος, την ιεραρχική δομή που ακολουθείται στην εκτέλεση των εργασιών και την επικοινωνία του λειτουργικού με τους πόρους του υπολογιστή,

5.1 Μέθοδοι

Τα συστήματα δεν μπορούν να υπάρξουν χωρίς εργαλεία διαχείρισης και παρακολούθησης των, οπότε για κάθε λειτουργικό, η εκάστοτε εταιρία που το συντηρεί το συνοδεύει με αρκετά τέτοια εργαλεία, ώστε να μπορεί να κάνει την δουλειά του και ο απλός χρήστης.

5.1.1 at / schtasks

Η εντολή **at** των Windows εμφανίζει τις προγραμματισμένες εργασίες που έχουν δημιουργηθεί μέσω της ιδίας εντολής. Για την εμφάνιση όλων των προγραμματισμένων εργασιών των Windows και λοιπών προγραμμάτων, χρησιμοποιείται η εντολή **schtasks**.

Και οι δύο εντολές ανήκουν στην πρώτη έκδοση του προγραμματιστή εργασιών των Windows και ισχύουν σε Windows 2000 και XP.

Η σύνταξη της εντολής **at** είναι:

at [*computer*] [*ID*] [commands]

command	Ορίζει την *εντολή* που θα εκτελεστεί.
/delete [*id*]	Ακυρώνει όλες ή την *δοσμένη* προγραμματισμένη εργασία.
/every:*date*	Εκτελεί την εντολή κάθε δοσμένη *μέρα*.
/interactive	Η εργασία μπορεί να αλληλεπιδράσει με την επιφάνεια εργασίας του τρέχοντος χρήστη.
/next:*date*	Εκτελεί την εντολή την επόμενη δοσμένη *μέρα*.
time	Ορίζει την ώρα που θα εκτελεστεί η εντολή
/yes	Απαντά "Ναι" σε όλα τα ερωτήματα κατά την διαγραφή εργασιών.

Αν η εντολή εκτελεστεί σκέτη, θα εμφανίσει όλες τις προγραμματισμένες εργασίες.
Για τις εντολές /every και /next, η μέρα μπορεί να έχει μιας εκ των εξής μορφών:

- ✓ Μέρα της εβδομάδας με τις τιμές: **M, T, W, Th, F, S, Su**.
- ✓ Μέρα του μήνα με τιμές από **1 έως 31**.

Περισσότερες μέρες μπορούν να οριστούν χωρισμένες με κόμμα.
Αν παραλειφθεί η αναφορά της μέρας, θα χρησιμοποιηθεί η τρέχουσα ημέρα.
Η παράμετρος time έχει την γραφή *ώρα:λεπτά*, η ώρα σε 24ωρη γραφή.

Η σύνταξη της εντολής **schtasks** είναι:

schtasks [commands]

/change	Αλλάζει τις ιδιότητες της προγραμματισμένης εργασίας.
/create	Δημιουργεί μια νέα εργασία.
/delete	Διαγράφει όλες ή την δοσμένη εργασία.
/end	Διακόπτει την τρέχουσα εργασία.
/query	Εμφανίζει όλες τις εργασίες.
/run	Εκτελεί την εργασία που ορίζεται.
/showsid	Εμφανίζει το ID ασφαλείας που αντιστοιχεί στην δοσμένη εργασία.

5.1.2 auditpol

Το **auditpol** είναι ένα εργαλείο των Windows το οποίο προσδιορίζει την πολιτική ελέγχου λογαριασμών σε ένα σύστημα. Συγκεκριμένα, μπορεί να δημιουργεί, να επεξεργάζεται, να κρατάει back up και να αποθηκεύει τις πολιτικές ελέγχου οπουδήποτε και με λεπτομερή καταγραφή.

Το εργαλείο αυτό υπάρχει από τα Vista, το οποίο αντικαθιστούσε το **auditusr.exe** που υπήρχε από τα XP SP2.

Η σύνταξη της εντολής περιλαμβάνει και υποχρεωτική αναφορά των επιλογών και των παραμέτρων τους όπου απαιτείται:

auditpol [commands [options]]

- ✓ **/backup** → Αποθηκεύει την πολιτική ελέγχου σε αρχείο.
  - ➢ **/file :** Καθορίζει το όνομα του αρχείου.
- ✓ **/clear** → Διαγράφει την ισχύουσα πολιτική ελέγχου.
  - ➢ **/y :** Απενεργοποιεί την ερώτηση επιβεβαίωσης.
- ✓ **/get** → Εμφανίζει την τρέχουσα πολιτική ελέγχου.
  - ➢ **/category :** Θέτει την κατηγορία, είτε με GUID ή όνομα είτε με * για όλες.
  - ➢ **/option :** Ανάκτηση της πολιτικής για **CrashOnAuditFail**, **FullPrivilegeAuditing**, **AuditBaseObjects** ή **AuditBaseDirectories**.
  - ➢ **/r :** Εμφάνιση της εξόδου σε μορφή CSV.
  - ➢ **/sd :** Ανακτά την περιγραφή ασφαλείας που χρησιμοποιείται στην ανάθεση της πρόσβασης στην πολιτική ελέγχου.
  - ➢ **/subcategory :** Θέτει μια ή περισσότερες υποκατηγορίες.
  - ➢ **/user :** Η βασική αρχή ασφαλείας για την οποία υποβάλλεται ερώτημα για ανά χρήστη. Υποχρεωτικά μπαίνει και **/category** ή **/subcategory**. Εάν δεν τεθεί συγκεκριμένος χρήστης, τότε για όλο το σύστημα.
- ✓ **/list** → Εμφανίζει σε λίστα τις εγγραφές για τα επιλέξιμα στοιχεία πολιτικής.
  - ➢ **/category :** Τα ονόματα των κατηγοριών. Με την επιλογή **/v**, και το GUID.
  - ➢ **/subcategory :** Τα ονόματα των υποκατηγοριών. Με την επιλογή **/v**, και το GUID.
  - ➢ **/user :** Τα ονόματα των χρηστών. Με την επιλογή **/v**, και το SID.
- ✓ **/set** → Ορίζει την πολιτική ελέγχου.
  - ➢ **/category :** Θέτει την κατηγορία, είτε με GUID είτε με όνομα. Αν δεν τεθεί, τότε για όλο το σύστημα.
  - ➢ **/exclude :** Με το **/user**, απενεργοποιείται ο έλεγχος γι' αυτόν τον χρήστη. Δεν ισχύει για μέλη της τοπικής ομάδας διαχειριστών.
  - ➢ **/failure :** Καθορίζει την αποτυχία ελέγχου. Δεκτές οι παράμετροι enable για ενεργοποίηση και disable για απενεργοποίηση.
  - ➢ **/include :** Με το **/user**, δημιουργείται ο έλεγχος γι' αυτόν τον χρήστη. Δεν ισχύει για μέλη της τοπικής ομάδας διαχειριστών.
  - ➢ **/option :** Ορισμός της πολιτικής για **CrashOnAuditFail**, **FullPrivilegeAuditing**, **AuditBaseObjects** ή **AuditBaseDirectories**.

- **/subcategory :** Θέτει την υποκατηγορία, είτε με GUID είτε με όνομα. Αν δεν τεθεί, τότε για όλο το σύστημα.
- **/success :** Καθορίζει την επιτυχία ελέγχου. Προεπιλογή. Δεκτές οι παράμετροι enable για ενεργοποίηση και disable για απενεργοποίηση.
- **/sd :** Ορίζει την περιγραφή ασφαλείας για την ανάθεση της πρόσβασης στην πολιτική ελέγχου. Η περιγραφή πρέπει να καθορίζεται χρησιμοποιώντας SDDL και να έχει ένα DACL.
- **/user :** Η βασική αρχή ασφαλείας για την οποία ορίζεται η πολιτική ανά χρήστη.

✓ **/remove** → Καταργεί την πολιτική ελέγχου ανά χρήστη.
- **/allusers :** Διαγράφει την πολιτική για όλους τους χρήστες.
- **/user :** Διαγράφει την πολιτική για έναν χρήστη.

✓ **/restore** → Επαναφέρει την πολιτική ελέγχου από ένα αρχείο.
- **/file :** Ορίζει το αρχείο, το οποίο είτε θα έχει δημιουργηθεί από το **/backup**, είτε θα συμφωνεί συντακτικά με αυτή την μορφή του αρχείου.

✓ **/resourceSACL** → Ρυθμίζει τις παραμέτρους των καθολικών πόρων SACL.

Για την επιλογή **/user**, ο χρήστης ορίζεται είτε με το SID του είτε με το όνομα.

5.1.3 doskey

Το **DOSKEY** είναι εργαλείο των DOS και των Windows, το οποίο προσθέτει ιστορικό εντολών, λειτουργία μακροεντολών και βελτιωμένα χαρακτηριστικά επεξεργασίας στους command line interpreters.

Η χρήση της εντολής γίνεται ως εξής:

doskey [commands]

/exename=*exe_file*	Καθορισμός εκτελέσιμου *αρχείου*.
/history	Εμφάνιση του ιστορικού των εντολών που χρησιμοποιήθηκαν.
/insert	Καθορισμός εισαγωγής νέου κειμένου στο παλιό κείμενο.
/listsize=*μέγεθος*	Ορισμός του *μεγέθους* του buffer όπου θα αποθηκεύεται το ιστορικό των εντολών.
/macrofile=*exe_file*	Καθορισμός *αρχείου* μακροεντολών προς εγκατάσταση.
/macros	Εμφάνιση όλων των μακροεντολών Doskey.
/macros:all	Εμφάνιση όλων των μακροεντολών Doskey για όλα τα εκτελέσιμα αρχεία.
/macros:*exe_file*	Εμφάνιση όλων των μακροεντολών Doskey για το συγκεκριμένο *αρχείο* προς εκτέλεση.
/overstrike	Καθορισμός αντικατάστασης του παλιού κειμένου με το νέο.
/reinstall	Εγκατάσταση νέου αντιγράφου του Doskey.
macro_name=[text]	Καθορισμός ονόματος μακροεντολής που δημιουργείται. Το *κείμενο* καθορίζει τις εντολές που θα καταγραφούν.

Τα επιπλέον χαρακτηριστικά που προσθέτει το DOSKEY στο **cmd.exe** είναι:
- **Ανάκληση** των εντολών με τα πάνω και κάτω βέλη.
- **Διαγραφή** του **περιεχομένου** της γραμμής εντολών με το πλήκτρο ESC.

- **Εμφάνιση** ιστορικού εντολών σε παραθυράκι με το πλήκτρο F7.
- **Διαγραφή ιστορικού** εντολών με τον συνδυασμό πλήκτρων ALT+F7.
- **Αναζήτηση** στο ιστορικό εντολών με το πλήκτρο F8.
- **Επιλογή** εντολής με βάση τον *αριθμό* που έχει στο ιστορικό, με το πλήκτρο F9.
- **Διαγραφή ορισμών μακροεντολών** με τον συνδυασμό πλήκτρων ALT+F10.

5.1.4 dumpel

Το **dumpel** είναι εργαλείο της Microsoft και εμφανίζει σε ευανάγνωστη μορφή τα *δεκαεξαδικα* δεδομένα από τις καταγραφές γεγονότων των Windows.

Η σύνταξη της εντολής είναι:

dumpel [options] <*log-file*>

-b	Εμφανίζει το αρχείο backup. Με την επιλογή **–l** καθορίζεται το αρχείο.
-c	Χρησιμοποιεί κόμμα για τον διαχωρισμό των πεδίων.
-e *id*	Φιλτράρει για τα *γεγονότα* με το δοσμένο *ID*. Το μέγιστο 10 τίθενται.
-f *file*	*Αρχείο* εξόδου.
-format *x*	Ορίζει μορφή εξόδου.
-l *file*	Εμφανίζει το καθορισμένο *αρχείο καταγραφής*.
-m *event*	Φιλτράρει για τα γεγονότα με βάση το *όνομα*.
-ns	Δεν εμφανίζει τα strings.
-r	Βγάζει έξω τα γεγονότα που ορίζονται με την επιλογή **–m**.
-s *server*	Ο *server* στον οποίο βρίσκεται το αρχείο καταγραφής.
-t	Χρησιμοποιεί το TAB ως διαχωριστικό. Προεπιλογή το κενό διάστημα.

Για την επιλογή **–format**, η προεπιλεγμένη μορφή είναι η **dtTCISucs**, όπου:

- **t** : Χρόνος
- **d** : Ημέρα
- **T** : Τύπος γεγονότος
- **C** : Κατηγορία γεγονότος
- **I** : ID γεγονότος
- **S** : Πηγή γεγονότος
- **u** : Χρήστης
- **c** : Υπολογιστής
- **s** : Strings

5.1.5 finger

Το **finger** είναι εργαλείο της Microsoft, το οποίο εμφανίζει πληροφορίες για έναν χρήστη του συστήματος.

Η σύνταξη της εντολής είναι:

finger [-l] <*user*> @*host*

, όπου

- **-l** → Εμφανίζει πληροφορίες σε μορφή λίστας.
- **user** → Καθορισμός *χρήστη*. Όταν παραλείπετε, αφορά όλους τους χρήστες.
- **host** → Καθορισμός του απομακρυσμένου *υπολογιστή*.

5.1.6 last / lastb / lastlog / faillog

Και τα τέσσερα εργαλεία, υπάρχουν στα περισσότερα Unix συστήματα και εμφανίζουν τις τελευταίες συνδέσεις. Το καθ' ένα όμως εμφανίζει διαφορετικού είδους συνδέσεις, ανάλογα με την περίσταση.

Το **last** εμφανίζει τους τελευταία συνδεμένους χρήστες, όπως αυτές υπάρχουν στο αρχείο καταγραφής **/var/log/wtmp**, από όταν δημιουργήθηκε το αρχείο.

Το **lastb** εμφανίζει τις τελευταίες αποτυχημένες συνδέσεις, όπως αυτές υπάρχουν στο αρχείο καταγραφής **/var/log/btmp**, επίσης από όταν δημιουργήθηκε το αρχείο. Χρειάζεται άδεια διαχειριστή για να εκτελεστεί.

Η σύνταξη των εντολών είναι:

last [options] <*user*> <*tty*>
lastb [options] <*user*> <*tty*>

–*num* / **–n** *num*	Ορίζει πόσες *γραμμές* να εμφανιστούν.
–a	Εμφανίζει το όνομα του υπολογιστή.
–d	Μεταφράζει την διεύθυνση IP σε όνομα. Για απομακρυσμένες συνδέσεις.
–f *file*	Ορίζει την χρήση άλλου *αρχείου καταγραφής* αντί του προεπιλεγμένου.
–F	Τυπώνει ολόκληρους χρόνους για σύνδεση και αποσύνδεση.
–i	Εμφανίζει την διεύθυνση IP της απομακρυσμένης σύνδεσης.
–o	Διαβάζει παλαιού τύπου αρχείο **wtmp**, όπως γράφτηκε από **linux-libc5** εφαρμογές.
–R	Δεν εμφανίζει το πεδίο του ονόματος του υπολογιστή.
–t *time*	Εμφανίζει την κατάσταση των συνδέσεων του δοσμένου *χρόνου*.
–w	Εμφανίζει ολόκληρα τα ονόματα χρήστη και τομέα.
–x	Εμφανίζει τους τερματισμούς του συστήματος και τις αλλαγές του επιπέδου εκτέλεσης.

Και οι δύο εντολές, αν εκτελεστούν σκέτες θα εμφανίσουν τις αντίστοιχες τελευταίες συνδέσεις σε 5 στήλες:

- όνομα χρήστη
- όνομα TTY
- διεύθυνση σύνδεσης → IP ή hostname
- χρόνος σύνδεσης
- κατάσταση σύνδεσης

Αν κάποιος χρήστης είναι *συνδεδεμένος*, γράφει στην κατάσταση σύνδεσης το μήνυμα **still logged in**, *ειδάλλως* γράφει τι ώρα αποσυνδέθηκε και πόσο διήρκησε η σύνδεση. Συγκεκριμένα, η

διάρκεια της σύνδεσης αναγράφεται με την μορφή **(D+HH:MM)**, δηλαδή μέρες αν πρόκειται για πάνω από μία μέρα, ώρες και λεπτά.

Για την επιλογή **–t**, ο χρόνος έχει την μορφή *YYYYMMDDHHMMSS*, δηλαδή έτος, μήνας, μέρα, ώρα, λεπτά και δευτερόλεπτα.

Το **lastlog** εμφανίζει τις τελευταίες συνδέσεις όλων των χρηστών, όπως αυτές υπάρχουν στο αρχείο καταγραφής **/var/log/lastlog**.

Εμφανίζει το όνομα χρήστη, από ποια θύρα συνδέθηκε και τον χρόνο της τελευταίας σύνδεσης. Αν κάποιος χρήστης δεν συνδέθηκε ποτέ, εμφανίζεται το μήνυμα ****Never logged in****.

Η σύνταξη της εντολής είναι:

lastlog [options]

–b *n*	Εμφανίζει τις εγγραφές παλαιότερες από *n μέρες*.
–t *n*	Εμφανίζει τις πιο πρόσφατες εγγραφές από *n μέρες*.
–u *user*	Εμφανίζει τις εγγραφές για τους δοσμένους *χρήστες*.

Αν η εντολή εκτελεστεί σκέτη, θα εμφανιστεί ολόκληρη η λίστα των χρηστών και το πότε συνδέθηκαν τελευταία φορά, με την σειρά όπως είναι στο **/etc/passwd**.

Για την επιλογή **–u**, ο *χρήστης* μπορεί να δοθεί είτε με το *όνομα* του είτε με το *user ID*.

Επίσης, μπορεί να δοθεί και ως *εύρος user ID* με την χρήση:

- **min-max**
- **min-**
- **-max**

Το **faillog** εμφανίζει τις τελευταίες αποτυχημένες συνδέσεις για κάθε χρήστη του συστήματος, όπως αυτές υπάρχουν στο αρχείο καταγραφής **/var/log/faillog**.

Εμφανίζει το όνομα χρήστη, τις αποτυχίες, το μέγιστο των αποτυχιών, τον χρόνο της τελευταίας σύνδεσης και αν είναι συνδεδεμένος.

Η σύνταξη της εντολής είναι:

faillog [options]

–a	Εμφανίζει τις αποτυχημένες συνδέσεις όλων των χρηστών.
–l *n*	Κλειδώνει τον λογαριασμό για *n δευτερόλεπτα* μετά από αποτυχημένη σύνδεση.
–m *n*	Θέτει στους μετρητές των αποτυχημένων συνδέσεων το *μέγιστο n*.
–r	Επαναφέρει τους μετρητές στο 0.
–t *n*	Εμφανίζεις τις πιο πρόσφατες εγγραφές από *n μέρες*.
–u *user*	Εμφανίζει τις εγγραφές για τους δοσμένους *χρήστες*.

Για την επιλογή **–u**, ισχύει το ίδιο με την επιλογή **–u** της **lastlog**.

5.1.7 history

Το **history** είναι εργαλείο των Unix συστημάτων και εμφανίζει το ιστορικό των εντολών που δόθηκαν στο terminal. Δίνει πολλά πρόσθετα χαρακτηριστικά όπως το **DOSKEY** των Windows για την διατήρηση και την χρήση του ιστορικού.

Η σύνταξη της εντολής περιλαμβάνει προσδιοριστές και τροποποιητές:

history [designators] <*modifiers*>

Αν η εντολή εκτελεστεί μόνο με αριθμό, του στυλ **history** *n*, θα εμφανίσει τις τελευταίες n εντολές μαζί με την τρέχουσα.

Προσδιοριστές γεγονότος:

- **!***n* → Αναφέρει την εντολή με αριθμό *n*.
- **!-***n* → Αναφέρει την εντολή που απέχει *n* από την τρέχουσα.
- **!!** → Αναφέρει την τελευταία εντολή.
- **!***x* → Αναφέρει την πιο πρόσφατη εντολή που ξεκινάει με *x*.
- **!?***x*[**?**] → Αναφέρει την πιο πρόσφατη εντολή που περιλαμβάνει *x*.
- **!#** → Αναφέρει την εντολή που έχει γραφτεί μέχρι εκείνον τον προσδιοριστή.

Οι **τροποποιητές** μπαίνουν στο τέλος, προαιρετικά:

- ✓ **h** → Αφαιρεί το καταληκτικό στοιχείο filename, αφήνοντας μόνο το κεφάλι.
- ✓ **t** → Αφαιρεί όλα τα κυριεύοντα στοιχεία filename, αφήνοντας την ουρά.
- ✓ **r** → Αφαιρεί το πρόσθετο της μορφής **.xxx**, αφήνοντας την βάση.
- ✓ **e** → Αφαιρεί όλα τα πρόσθετα, εκτός του καταληκτικού.
- ✓ **p** → Τυπώνει την νέα εντολή, αλλά δεν την εκτελεί.
- ✓ **q** → Παραθέτει τις λέξεις υποκατάστασης, αποφεύγοντα περαιτέρω υποκατάσταση.
- ✓ **x** → Παραθέτει τις λέξεις υποκατάστασης, αλλά σπάει σε λέξεις στα κενά και νέες γραμμές.
- ✓ **s/***old***/***new***/** → Υποκαθιστά το *νέο* για το *παλιό*. Το διαχωριστικό μπορεί να αλλάζει.
- ✓ **%** → Επαναλαμβάνει την προηγούμενη υποκατάσταση.
- ✓ **g** → Εφαρμόζει τις αλλαγές σ' όλη την γραμμή γεγονότος.
- ✓ **G** → Εφαρμόζει τους '**s**' τροποποιητές μια φορά ανά λέξη στην γραμμή γεγονότος.

5.1.8 lsmod

Το **lsmod** είναι εργαλείο των Linux και εμφανίζει την τρέχουσα κατάσταση των μοντέλων του kernel.

Δεν δέχεται καμία επιλογή και εμφανίζει την κατάσταση των μοντέλων όπως αυτή φαίνεται στο αρχείο **/proc/modules**.

Συγκεκριμένα, εμφανίζει την λίστα σε τρεις στήλες:

1. **Module** → Όνομα του μοντέλου
2. **Size** → Μέγεθος σε bytes
3. **Used by** → Άλλα μοντέλα τα οποία το χρησιμοποιούν

5.1.9 modinfo

Το **modinfo** είναι εργαλείο των Linux κι Solaris και εμφανίζει πληροφορίες για τα μοντέλα του kernel.

Αν το δοθέν όνομα δεν είναι αρχείο, γίνεται αναζήτηση στον φάκελο **/lib/modules/*version***.

Η σύνταξη της εντολής είναι:

modinfo [options] <*module*>

–0	Χρήση του ASCII χαρακτήρα 0 για διαχωρισμό τιμών πεδίων, αντί για νέα γραμμή.
–a	Συντομογραφία για τον συντάκτη.
–d	Συντομογραφία για την περιγραφή.
–F *field*	Τυπώνει μόνο την τιμή του δοσμένου *πεδίου*, μια ανά γραμμή.
–k *kernel*	Δίνει πληροφορίες για έναν διαφορετικό kernel από τον τρέχων.
–l	Συντομογραφία για την άδεια.
–n	Συντομογραφία για το όνομα αρχείου.
–p	Συντομογραφία για την παράμετρο.

Οι επιλογές **–a**, **–d**, **–l**, **–n** και **–p** υπάρχουν για πιο εύκολη μετάβαση από την παλιά έκδοση του **modinfo**.

Για την επιλογή –F, μερικά πεδία τα οποία μπορεί να μην υπάρχουν σ' όλα τα modules, είναι:

1. **alias**
2. **author**
3. **depends**
4. **description**
5. **license**
6. **parm**

5.1.10 NTBackup

Το **NTBackup** είναι εργαλείο της Microsoft, το οποίο κρατάει backup των αρχείων και ταυτόχρονα καταγράφει σε log το ιστορικό των backup, δηλαδή πόσες φορές έγινε backup, ποια αρχεία έγιναν backup, πότε και πόσο κράτησε.

Υποστηρίζεται από τα Windows NT 4.0, είτε ως προεγκατεστημένο εργαλείο είτε ως ανεξάρτητο. Από τα Windows Vista και ύστερα, την θέση του πήρε το **Wbadmin**.

Η σύνταξη της εντολής είναι:

ntbackup [commands] <*@bks_file*>

/A	Κάνει επισύναψη. Μαζί με την εντολή **/G**, αλλά όχι με την **/P**.
/D "*descr***"**	Ορισμός *ταμπέλας* για κάθε σετ backup.
/DS "*serv***"**	Κάνει backup το directory service file του δοθέντος *Microsoft Exchange Server*.
/F "*file***"**	Διαδρομή και όνομα *αρχείου*. Να μην χρησιμοποιηθεί με τις εντολές **/G** και **/P**.
/G "*guid***"**	Γράφει από πάνω ή προσαρτά στον *δίσκο*.
/HC on | off	Χρησιμοποιεί συμπίεση υλικού, εάν είναι διαθέσιμη στον δίσκο.
/IS "*serv***"**	Κάνει backup το Information Store file του δοθέντος *Microsoft Exchange Server*.

/J "*job***"**	Προσδιορίζει το *όνομα* της *δουλειάς* που θα χρησιμοποιηθεί στο αρχείο καταγραφής.
/L *type*	Ορίζει τον *τύπο* του *αρχείου καταγραφής*.
/M *type*	Ορίζει τον *τύπο* του *backup*.
/N "*media***"**	Ορίζει το *όνομα* του νέου *αποθηκευτικού μέσου*. Να μην χρησιμοποιηθεί η **/A**.
/P "*pool***"**	Ορίζει την *λίστα* από όπου θα πάρει το *μέσο*. Χωρίς τις εντολές **/A**, **/G** και **/T**.
/R yes | no	Περιορίζει την πρόσβαση στο μέσο, μόνο στον ιδιοκτήτη και τους διαχειριστές.
/RS yes | no	Κάνει backup τα δεδομένα ενός απομακρυσμένου εξωτερικού μέσου.
/SNAP on | off	Ορίζει αν είναι ή όχι το backup σκιώδες αντίγραφο τόμου.
systemstate	Ορίζει το ότι θα γίνει backup των δεδομένων της κατάστασης του συστήματος.
/V yes | no	Επιβεβαιώνει τα δεδομένα μετά την ολοκλήρωση του backup.

Το *@bks_file* πρόκειται για **.bks** αρχείο, το οποίο περιέχει πληροφορίες για τα αρχεία και τους καταλόγους που θα γίνουνε backup. Δημιουργείται μέσω του γραφικού περιβάλλοντος του **Backup**.

Για την επιλογή **–L**, οι τύποι αρχείου καταγραφής είναι:

- **f** : Πλήρες.
- **n** : Τίποτα. Δεν θα δημιουργηθεί αρχείο.
- **s** : Περίληψη.

Για την επιλογή **–M**, οι τύποι backup είναι:

- **copy**
- **daily**
- **differential**
- **incremental**
- **normal**

5.1.11 ps

Το **ps** είναι εργαλείο των Unix συστημάτων, το οποίο εμφανίζει την κατάσταση των τρεχόντων διεργασιών. Οι τρέχουσες διεργασίες μπορούν να προβληθούν με γραφικό τρόπο και συγκεκριμένα με την μορφή δέντρου, με την εντολή **pstree**.

Η σύνταξη της εντολής είναι:

ps [options]

a	Όλες οι διεργασίες, μαζί με το **TTY**.
-a	Όλες οι διεργασίες, εκτός των πρώτων της συνεδρίας και του τερματικού.
-A | -e	Όλες οι διεργασίες.
c	Εμφάνιση πραγματικού ονόματος εντολής.
-c	Εμφάνιση διαφόρων πληροφοριών χρονοπρογραμματιστή.
-C *cmd*	Επιλογή με βάση το *όνομα* της *εντολής*.
--cols *n*	Ορισμός εύρους οθόνης.
--context	Εμφάνιση μορφής περιβάλλοντος ασφαλείας.
-d	Όλες οι διεργασίες, εκτός των πρώτων της συνεδρίας.

f	Εμφάνιση ιεραρχίας διεργασιών σε μορφή τέχνης ASCII.
-f	Έξοδος ολόκληρης μορφής. Συνδυάζεται με άλλες επιλογές για επιπλέον στήλες.
-g *rgid*	Επιλογή με βάση το *ID* ή το *όνομα* της αποτελεσματικής *ομάδας*.
-G *rgid*	Επιλογή με βάση το *ID* ή το *όνομα* της πραγματικής *ομάδας*.
-H	Εμφάνιση ιεραρχίας διεργασιών.
[**-**]**j**	Έξοδος μορφής ελέγχου εργασιών.
[**-**]**l**	Έξοδος μακράς μορφής.
[**-**]**m**	Εμφάνιση νημάτων μετά τις διεργασίες.
-M | **Z**	Προσθέτει στήλη για δεδομένα ασφάλειας.
n	Αριθμητική έξοδος για **WCHAN** και **USER**.
-N	Όλες οι διεργασίες, εκτός απ' αυτές που πληρούν τις προϋποθέσεις.
[**-**]**o**	Μορφή εξόδου καθορισμένη από τον χρήστη.
[**-**]**O**	Προφορτωμένο [**-**]**o** με περισσότερες στήλες.
[**-p**]*pid*	Επιλογή με βάση το *ID* της *διεργασίας*.
--ppid *pid*	Επιλογή με βάση το ID της γονικής διεργασίας.
r	Μόνο τις τρέχουσες διεργασίες.
--rows *n*	Ορισμός ύψους οθόνης.
s	Έξοδος μορφής σημάτων.
-[**s**]*sid*	Επιλογή με βάση το *ID* της *συνεδρίας*.
S	Σύνοψη πληροφοριών από νεκρές διεργασίες προς τις γονικές.
[**-**]**t** *tty*	Επιλογή με βάση το *TTY*.
T	Όλες οι διεργασίες του τρέχοντος τερματικού.
u	Έξοδος μορφής προσανατολισμένης προς χρήστη.
U | **-u** *user*	Επιλογή με βάση το *ID* ή το *όνομα* του αποτελεσματικού *χρήστη*.
-U *user*	Επιλογή με βάση το *ID* ή το *όνομα* του πραγματικού *χρήστη*.
v	Έξοδος μορφής εικονικής μνήμης.
[**-**]**w**	Ευρείας έξοδος. Διπλή χρήση της επιλογής, ορίζει άπειρο εύρος εξόδου.
x	Όλες οι διεργασίες με **TTY**.
X	Έξοδος μορφής καταχωρητών.
-y	Δεν δείχνει σημαίες, αντικαθιστά το **addr** με το **rss**. Χρησιμοποιείται με την επιλογή **–l**.

Για την επιλογή **n**, το **WCHAN** είναι το κανάλι αναμονής και το **USER** είναι το used & group ID.

5.1.12 regedit

Το **regedit** είναι εργαλείο της Microsoft με γραφικό περιβάλλον και χρησιμοποιείται για την προβολή και επεξεργασία της **registry** των Windows. Το αντίστοιχο εργαλείο γραμμής εντολών με τις ίδιες λειτουργίες, είναι το **reg**.

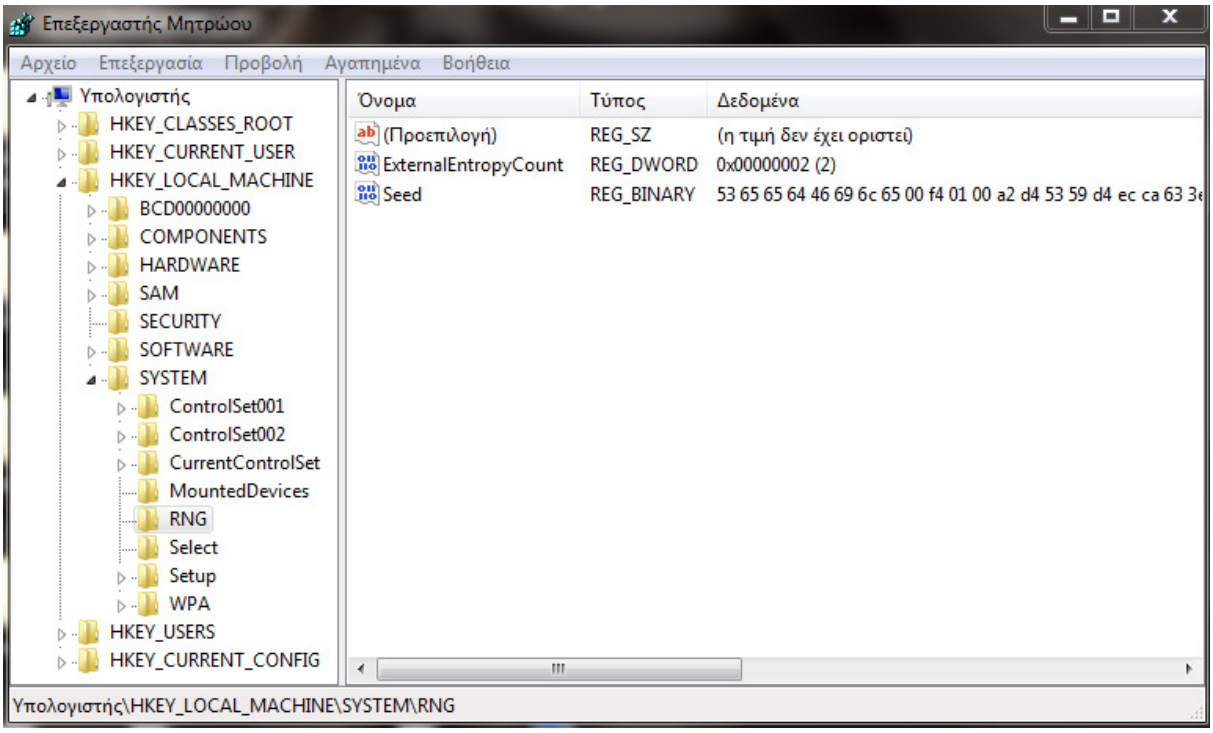
Η registry αποτελείται από πέντε φακέλους κλειδιών:

1. **HKEY_CLASSES_ROOT** → Συνδέσεις επεκτάσεων αρχείων με προγράμματα.
2. **HKEY_CURRENT_CONFIG** → Πληροφορίες υλικού υπολογιστή για εκκίνηση.

3. **HKEY_CURRENT_USER** → Ρυθμίσεις του τρέχοντος χρήστη.
4. **HKEY_LOCAL_MACHINE** → Ρυθμίσεις του υπολογιστή.
5. **HKEY_USERS** → Ριζικοί κατάλογοι όλων των χρηστών.

και τα κλειδιά είναι έξι τύπων:

- **REG_BINARY**
- **REG_DWORD**
- **REG_EXPAND_SZ**
- **REG_MULTI_SZ**
- **REG_SZ**
- **REG_FULL_RESOURCE_DESCRIPTOR**



Εικόνα 5.1: Επεξεργαστής μητρώου Windows

Στο κάτω μέρος του παραθύρου, εμφανίζεται η διαδρομή του κλειδιού που έχουμε επιλεγμένο.

Στο μενού **Επεξεργασία**, υπάρχουν οι δυνατότητες για δημιουργία κλειδιού με βάση τον εκάστοτε τύπο, την προβολής των δικαιωμάτων για κάθε φάκελο και η αναζήτηση με βάση τα κλειδιά, τις τιμές ή και τα δεδομένα.

Μπορεί να φορτωθεί το μητρώο ενός άλλου υπολογιστή στο δίκτυο, με την επιλογή **Αρχείο → Σύνδεση με το μητρώο δικτύου**, όπου εισάγετε το όνομα του υπολογιστή, ενώ μπορείτε να επιλέξετε τι συσκευή είναι και σε ποιά ομάδα εργασίας ανήκει.

5.1.13 strace

Το **strace** είναι εργαλείο των Linux, το οποίο αφορά διάγνωση και debugging των διεργασιών. Συγκεκριμένα, χρησιμοποιείται για παρακολούθηση των αλληλεπιδράσεων μεταξύ των διεργασιών

και του Linux kernel, όπως κλήσεις συστήματος και σήματα παραλαβής. Άλλα παρόμοια εργαλεία στα Unix είναι τα **dtrace**, **ktrace**, **ltrace**, **ptrace** και **truss**.

Η εντολή γράφεται ως εξής:

strace [options] <*command [arguments]*>

-a *n*	Ευθυγραμμίζει τις τιμές για την δοσμένη *στήλη*.
-c	Μετρά χρόνο, κλήσεις και λάθη για κάθε κλήση συστήματος και τυπώνει αναφορά.
-d	Εμφανίζει μερικές πληροφορίες για το debug του **strace**.
-D	Εκτελεί την διαδικασία ιχνηλάτη ως ανεξάρτητο εγγόνι και όχι ως γόνο.
-e *expr*	Έκφραση που ορίζει ποια γεγονότα να ιχνηλατήσει ή πως.
-E *var*	Αφαιρεί την *var* από τις μεταβλητές περιβάλλοντος πριν την εντολή.
-f	Ιχνηλατεί διεργασίες παιδιά καθώς δημιουργούνται από τρέχουσες διεργασίες ως αποτέλεσμα της κλήσης συστήματος fork.
-ff	Μαζί με την επιλογή **–o**, κάθε ιχνηλάτηση διεργασιών γράφεται στο *file.pid*.
-i	Τυπώνει τον δείκτη οδηγιών την στιγμή της κλήσης συστήματος.
-o *file*	Αποθηκεύει την έξοδο της ιχνηλάτησης στο δοσμένο *αρχείο*.
-p *pid*	Ιχνηλατεί την διεργασία με το δοσμένο *process ID*.
-q	Δεν εμφανίζει μηνύματα για ενσωμάτωση, ανεξαρτοποίηση, κ.τ.λ..
-r	Τυπώνει σχετικό timestamp στην εγγραφή κάθε συστήματος κλήσης.
-s *n*	Ορίζει το *μέγεθος* του string που θα τυπώνεται. Προεπιλογή το 32.
-S *x*	Ταξινομεί την έξοδο της επιλογής **–c** με βάση το δοσμένο *κριτήριο*.
-t	Προσθέτει τον χρόνο της μέρας στην αρχή κάθε γραμμής.
-tt	Ο χρόνος που προστίθεται, είναι σε μικροδευτερόλεπτα.
-ttt	Γράφεται η διαφορά χρόνου από το 1970.
-T	Δείχνει τον χρόνο που καταναλώθηκε στις κλήσεις συστήματος.
-u *user*	τρέχει την εντολή ως τον δοσμένο χρήστη ή ομάδα. Μόνο user & group IDs.
-v	Verbose.
-x	Τυπώνει όλα τα μη-ASCII strings σε δεκαεξαδική μορφή.
-xx	Τυπώνει όλα τα strings σε δεκαεξαδική μορφή.

Η επιλογή **–D**, μειώνει την εμφάνιση του **strace** κρατώντας το **tracee** ως απευθείας παιδί της κληθέντος διαδικασίας.

Για την επιλογή **–e**, η σύνταξη της έκφρασης είναι:

[*qualifier***=**][**!**]*value1*[**,***value2*]…

, όπου οι *qualifiers* είναι:

- **abbrev**
- **raw**
- **read**
- **signal**
- **trace**
- **verbose**
- **write**

Για την επιλογή **–ff**, το *pid* στο αρχείο είναι το ID της εκάστοτε διεργασίας.

Για την επιλογή **–q**, αυτό συμβαίνει όταν γίνεται ανακατεύθυνση εξόδου σε αρχείο και η εντολή τρέχει απευθείας αντί να ενσωματώνεται.

Για την επιλογή **–r**, αυτό καταγράφει την χρονική διαφορά μεταξύ της εκκίνησης διαδοχικών κλήσεων συστήματος.

Για την επιλογή **–S**, αποδεκτές τιμές είναι:

- **calls**
- **name**
- **nothing**
- **time** : Προεπιλογή

5.1.14 strings

Το **strings** είναι εργαλείο των Unix συστημάτων, το οποίο εκτυπώνει οτιδήποτε string υπάρχει μέσα σε δυαδικό αρχείο, όπως τα εκτελέσιμα.

Η σύνταξη της εντολής είναι:

strings [options] *file*

-a	Σαρώνει ολόκληρο το αρχείο, όχι μόνο τον τομέα δεδομένων.
-e=*y*	Επιλογή *y* χαρακτήρα και διαμέσου.
-f	Τυπώνει το όνομα του αρχείου πριν από κάθε string.
-n=*x*	Εντοπίζει και τυπώνει οποιαδήποτε ακολουθία που τελειώσει με κενό και έχει τουλάχιστον *x* χαρακτήρες. Από προεπιλογή είναι 4.
-o	Συντομογραφία για το **--radix=o**.
-t=*z*	Τυπώνει την τοποθεσία του string σε βάση 8, 10 ή 16 μέσω του *z*.
-T=*BFDNAME*	Προσδιορίζει την μορφή του δυαδικού αρχείου

Για την επιλογή **–e**, οι επιλογές είναι ανάμεσα σε:

- s = 7-bits
- S = 8 bits
- b, l = 16 bits
- B, L = 32 bits

Για την επιλογή **–t**, οι βάσεις μπορούν:

- o για βάση 8
- d για βάση 10
- x για βάση 16

5.1.15 tasklist

Η **tasklist** υπάρχει στα Windows και εμφανίζει μια λίστα με τις διεργασίες που τρέχουν στο σύστημα, είτε τοπικό είτε απομακρυσμένο. Η αντίστοιχη εντολή στα Linux είναι η **ps**.

Η σύνταξη της εντολής είναι:

tasklist [commands]

/FI *filter*	Εμφάνιση ενός συνόλου ενεργειών που ταιριάζουν με το *φίλτρο*.

/FO *μορφή*	Καθορισμός της *μορφής* εξόδου.
/NH	Δεν εμφανίζεται η κεφαλίδα στήλης στην έξοδο.
/M *[λειτουργική_μονάδα]*	Εμφάνιση σε λίστα των ενεργών διεργασιών που χρησιμοποιούν το όνομα **exe/dll**. Εάν δεν δοθεί η *λειτουργική μονάδα*, θα εμφανιστούν όλες οι λειτουργικές μονάδες.
/P *[password]*	Καθορισμός του *κωδικού* πρόσβασης για το καθορισμένο περιβάλλον χρήστη.
/S *system*	Καθορισμός του απομακρυσμένου *συστήματος* για σύνδεση.
/SVC	Εμφάνιση των υπηρεσιών που φιλοξενούνται σε κάθε διεργασία.
/U *[domain\] user*	Καθορισμός του περιβάλλοντος *χρήστη* υπό το οποίο πρέπει να εκτελεστεί η εντολή.
/V	Εμφάνιση λεπτομερών πληροφοριών για τις διεργασίες.

Αν η εντολή εκτελεστεί σκέτη, τότε θα εμφανιστεί μια λίστα ενεργών διεργασιών, κατά αύξοντα process ID. Επίσης, εμφανίζεται και η χρήση μνήμης κάθε διεργασίες σε KB.

Το φίλτρο της εντολής **/FI** μπορεί να είναι ένα από τα εξής:

Όνομα φίλτρου	Έγκυροι τελεστές	Έγκυρες τιμές
CPUTIME	eq, ne, gt, lt, ge, le	Χρόνος CPU με τη μορφή *ωω:λλ:δδ*.
IMAGENAME	eq, ne	Όνομα εικόνας.
MEMUSAGE	eq, ne, gt, lt, ge, le	Χρήση μνήμης σε *KB*.
MODULES	eq, ne	Όνομα DLL.
PID	eq, ne, gt, lt, ge, le	Τιμή PID.
SERVICES	eq, ne	Όνομα υπηρεσίας.
SESSION	eq, ne, gt, lt, ge, le	Αριθμός περιόδου λειτουργίας.
SESSIONNAME	eq, ne	Όνομα περιόδου λειτουργίας.
STATUS	eq, ne	Running | Not Responding | Unknown
USERNAME	eq, ne	Όνομα χρήστη σε διαμόρφωση *[domain\] user*.
WINDOWTITLE	eq, ne	Τίτλος παραθύρου.

Τα φίλτρα WINDOWTITLE και STATUS δεν υποστηρίζονται για απομακρυσμένο υπολογιστή.

Η εντολή **/NH**, ισχύει μόνο για τι μορφές TABLE και CSV.

5.1.16 top

Το **top** είναι εργαλείο των Unix συστημάτων, το οποίο έχει ίδιες λειτουργίες με το **ps**, αλλά εμφανίζει τις διεργασίες σε πραγματικό χρόνο. Ανάλογα εργαλεία είναι τα **atop** και **htop**.

Το εργαλείο αυτό είναι ιδιαίτερα χρήσιμο σε διαχειριστές συστημάτων, καθώς βοηθάει η ζωντανή προβολή των διεργασιών και των πόρων που χρησιμοποιούν, όπως ο **Task Manager** για τα Windows.

Με την απλή εκτέλεση της εντολής, εμφανίζονται στο terminal πληροφορίες για τους πόρους του υπολογιστή και μια λίστα με τις τρέχουσες διεργασίες, ταξινομημένη κατά ποσοστό χρήσης της CPU και ανανεώσιμη κάθε λίγα δευτερόλεπτα.

Συγκεκριμένα, η λίστα έχει από προεπιλογή τις εξής στήλες:

- **PID** → Το ID της διεργασίας.

- **USER** → Ο χρήστης υπό τον οποίο τρέχει την διεργασία.
- **PR** → Προτεραιότητα εργασίας.
- **NI** → Η ωραία τιμή της εργασίας.
- **VIRT** → Χρήση εικονικής μνήμης σε KB.
- **RES** → Χρήστη μη ανταλλαγμένης φυσικής μνήμης σε KB.
- **SHR** → Χρήση κοινής μνήμης σε KB.
- **S** → Κατάσταση της εργασίας, η οποία λαμβάνει τις εξής τιμές:
  - ✓ **D :** Αδιάκοπος ύπνος
  - ✓ **R :** Εκτελείται
  - ✓ **S :** Κοιμάται
  - ✓ **T :** Εντοπισμένη
  - ✓ **Z :** Ζόμπι
- **%CPU** → Ποσοστό χρήσης της CPU.
- **%MEM** → Ποσοστό χρήσης της RAM.
- **TIME+** → Συνολικός χρόνος χρήσης της CPU από όταν ξεκίνησε η εκτέλεση.
- **COMMAND** → Το όνομα της εντολής της διεργασίας.

Η σύνταξη της εντολής είναι:

top [options]

-a	Ταξινόμηση κατά χρήση μνήμης.
-b	Λειτουργία αποστολής εξόδου σε άλλα προγράμματα ή αρχεία.
-c	Εναλλαγή μεταξύ εμφάνισης γραμμής εντολών και ονόματος προγράμματος.
-d *t*	Ορισμός *χρονοκαθυστέρησης*.
-H	Εναλλαγή μεταξύ εμφάνισης όλων των νημάτων ή περίληψης των ανά διεργασία.
-i	Εναλλαγή μεταξύ εμφάνισης των αδρανών διεργασιών ή όχι.
-m	Αναφέρει την χρησιμοποιημένη φυσική μνήμη, αντί της εικονικής.
-M	Δείχνει τις μονάδες μέτρησης της μνήμης.
-n *n*	Δήλωση μέγιστου *αριθμού* επαναλήψεων.
-p *pid*	Παρακολούθηση μόνο των δοθέντων διεργασιών, με βάση το ID τους. Μέγιστο 20.
-s	Λειτουργία ασφαλείας, ακόμη και για τον χρήστη **root**.
-S	Εναλλαγή μεταξύ εμφάνισης συνολικού χρόνου χρήσης CPU ή όχι.
-u *uid*	Παρακολούθηση διεργασιών για χρήστη με βάση το *αποτελεσματικό user ID*.
-U *uid*	Παρακολούθηση διεργασιών για χρήστη με βάση το *user ID*.

Για την επιλογή **–d**, η *χρονοκαθυστέρηση* ορίζετε ως *ss.tt*, δηλαδή δευτερόλεπτα και δέκατα του δευτερολέπτου.

5.1.17 ver / uname

Η **ver** είναι εντολή των Windows και εμφανίζει την εσωτερική έκδοση του λειτουργικού συστήματος.

Η εντολή δεν δέχεται καμία παράμετρο και αν για παράδειγμα εκτελεστεί στα Windows 7, εμφανίζει το αποτέλεσμα:

Microsoft Windows [Έκδοση 6.1.7601]

Η **uname** είναι η αντίστοιχη εντολή στα Unix και μαζί με την έκδοση του λειτουργικού συστήματος, εμφανίζει και την έκδοση του kernel.

Σε αντίθεση με την **ver** που δεν δέχεται κανένα επιπλέον όρισμα, η **uname** μπορεί να δεχτεί τα εξής ορίσματα:

-a	Τυπώνει όλες τις πληροφορίες με την ακόλουθη σειρά, εκτός από τα **–p** και **–i** αν είναι άγνωστα.
-s	Τυπώνει το όνομα του kernel.
-n	Τυπώνει το hostname του δικτυακού κόμβου.
-r	Τυπώνει την έκδοση του kernel.
-v	Τυπώνει την ημερομηνία έκδοσης του kernel.
-m	Τυπώνει τον τύπο του επεξεργαστή.
-p	Το ίδιο με το **–m**.
-i	Τυπώνει την πλατφόρμα υλικού.
-o	Τυπώνει το λειτουργικό σύστημα.

5.1.18 w

Το **w** είναι εργαλείο των Unix συστημάτων, το οποίο εμφανίζει πληροφορίες για τους συνδεδεμένους χρήστες. Είναι συνδυασμός των **who**, **uptime** και **ps -a**.

Συγκεκριμένα, εμφανίζει τα στοιχεία σε εφτά στήλες:

1. **USER** → όνομα σύνδεσης χρήστη
2. **TTY** → κωδικό όνομα χρήστη στο terminal
3. **FROM** → απομακρυσμένος host από τον οποίον συνδέεται
4. **LOGIN@** → ημερομηνία σύνδεσης
5. **IDLE** → ανενεργός χρόνος
6. **JCPU** → συνολικός χρόνος εκτέλεσης διεργασιών στο terminal και των ενεργών εργασιών παρασκηνίου
7. **PCPU** → χρόνος εκτέλεσης της τρέχουσας διεργασίας
8. **WHAT** → τρέχουσα διεργασία που εκτελεί

Η σύνταξη της εντολής είναι:

w [options] <*user*>

-f	Εναλλάσσει την εμφάνιση του πεδίου **FROM**. Από προεπιλογή εμφανίζεται.
-h	Δεν εμφανίζει τις κεφαλίδες.
-l	Μακρά λίστα. Προεπιλογή.
-o	Εμφάνιση αποτελέσματος με το παλιό στυλ.
-s	Κοντή λίστα. Δεν εμφανίζονται τα πεδία **LOGIN@**, **JCPU** και **PCPU**.
-u	Αγνοεί το user ID των διεργασιών.
-V	Τυπώνει την έκδοση της εντολής.
user	Εμφανίζει τα στοιχεία μόνο για τον δοσμένο χρήστη.

Αν η εντολή εκτελεστεί σκέτη, εμφανίζει όλες τις πληροφορίες για όλους τους χρήστες.

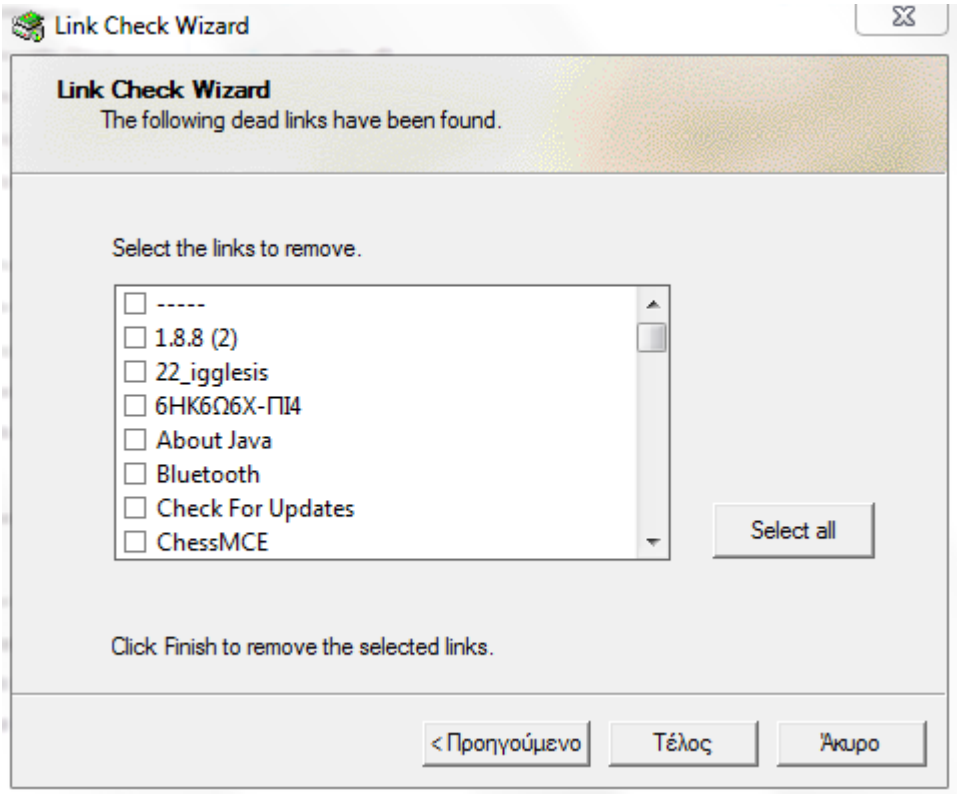
5.2 Εργαλεία

Τα εργαλεία διαχείρισης που συνοδεύουν τα λειτουργικά δεν αρκούν μερικές φορές για κάποιες λειτουργίες που θέλουμε, οπότε δημιουργήθηκαν εργαλεία και λογισμικά βασισμένα στα ίδια τα λειτουργικά και τις δυνατότητες που προσφέρουν, τις οποίες ο απλός χρήστης δεν μπορεί να εκμεταλλευτεί.

5.2.1 ChkLnks.exe

Το **ChkLnks.exe** είναι εργαλείο της Microsoft, μέρος του **NT Resource Kit**, το οποίο εντοπίζει καταστραμμένους συνδέσμους αρχείων. Αυτές οι καταστραμμένες συνδέσεις δημιουργούνται όταν διαγράφεται ένα αρχείο, αλλά όχι η συντόμευσή του.

Έχει γραφικό περιβάλλον, όπου αφού σου βρίσκει τους κατεστραμμένους συνδέσμους, σου δίνει την δυνατότητα να τους διαγράψεις μετά.



Εικόνα 5.2: ChkLnks.exe

Όταν εκτελείται το εργαλείο, εμφανίζει ένα μικρό παράθυρο με ονομασία **Link Check Wizard**, όπου περιγράφει στα αγγλικά με λίγα λόγια την λειτουργία του.

Στην συνέχεια πατάμε **Επόμενο**, όπου αρχίζει η αναζήτηση, η οποία μπορεί να διαρκέσει μερικά λεπτά.

Την ίδια στιγμή της αναζήτησης εμφανίζονται σταδιακά και τα αποτελέσματα της σε αλφαβητική σειρά.

Για τις πληροφορίες ενός κατεστραμμένου συνδέσμου, κάνουμε δεξί κλικ πάνω του και εμφανίζει σε άλλο παράθυρο:

- Όνομα συντόμευσης
- Μονοπάτι συντόμευσης
- Μονοπάτι αντιστοίχισης πραγματικού αρχείου
- Κατάσταση λάθους

5.2.2 chkrootkit

Το **chkrootkit**, είναι εργαλείο το οποίο αναζητά στο σύστημα για rootkits, δηλαδή για προγράμματα τα οποία εγκαθίστανται στο σύστημα με σκοπό να ανοίξουν διόδους σε εξωτερικό χρήστη για κακόβουλη χρήση. Υποστηρίζεται από τα περισσότερα Unix συστήματα, όπως Linux, OS X, Solaris και FreeBSD.

Δεν διαγράφει τα rootkits από το σύστημα, απλώς βοηθάει τον χρήστη να τα εντοπίσει και να τα αναλάβει ο ίδιος όπως θέλει. Για να εκτελεστεί, απαιτούνται δικαιώματα διαχειριστή.

Η σύνταξη της εντολής είναι:

chkrootkit [options] [test]

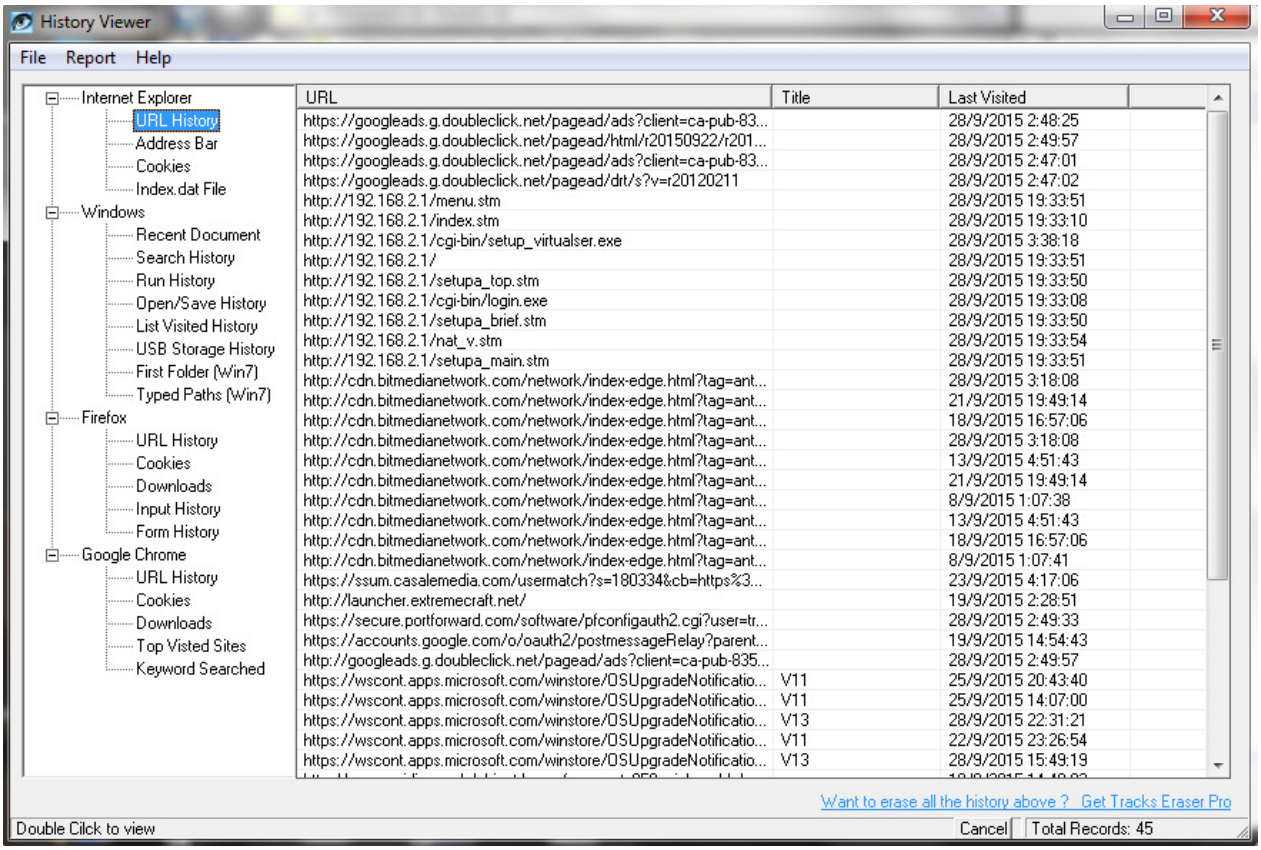
-d	Αποσφαλμάτωση
-e	Δεν λαμβάνει υπόψη γνωστά αρχεία / καταλόγους ως λανθασμένα θετικά.
-l	Δείχνει τα διαθέσιμα τεστ.
-n	Δεν λαμβάνει υπόψη του καταλόγους του **NFS**.
-p *dirs*	Διαδρομές για χρήση εξωτερικών εντολών.
-q	Ήσυχη λειτουργία.
-r *dir*	Χρησιμοποιεί τον *κατάλογο* ως ρίζα.
-x	Λειτουργία ειδικού.
-V	Πληροφορίες έκδοσης.

Αν η εντολή γραφτεί σκέτη, αρχίζει την σάρωση του συστήματος.

Για την επιλογή **–p**, οι πολλαπλές διαδρομές έχουν ως διαχωριστικό το σύμβολο **:**.

5.2.3 History Viewer

Το **History Viewer**, είναι εργαλείο που εμφανίζει το ιστορικό περιήγησης ενός χρήστη σε έναν υπολογιστή. Για το διαδίκτυο, εμφανίζει το ιστορικό περιήγησης όπως αυτό καταγράφεται σε **Internet Explorer**, **Mozilla Firefox** και **Google Chrome**. Υποστηρίζεται από Windows 98 μέχρι 7 και Windows Server 2008.



Εικόνα 5.3: History Viewer

Οι επιλογές πληροφοριών για κάθε πρόγραμμα, είναι οι εξής:

- **Internet Explorer**
  - *URL History*
  - *Address Bar*
  - *Cookies*
  - *Index.dat File*
- **Windows**
  - *Recent Document*
  - *Search History*
  - *Run History*
  - *Open/Save History*
  - *List Visited History*
  - *USB Storage History*
  - *First Folder (Win7)*
  - *Typed Paths (Win7)*
- **Firefox**
  - *URL History*
  - *Cookies*
  - *Downloads*
  - *Input History*
  - *Form History*
- **Google Chrome**

- *URL History*
- *Cookies*
- *Downloads*
- *Top Visited Sites*
- *Keyword Searched*

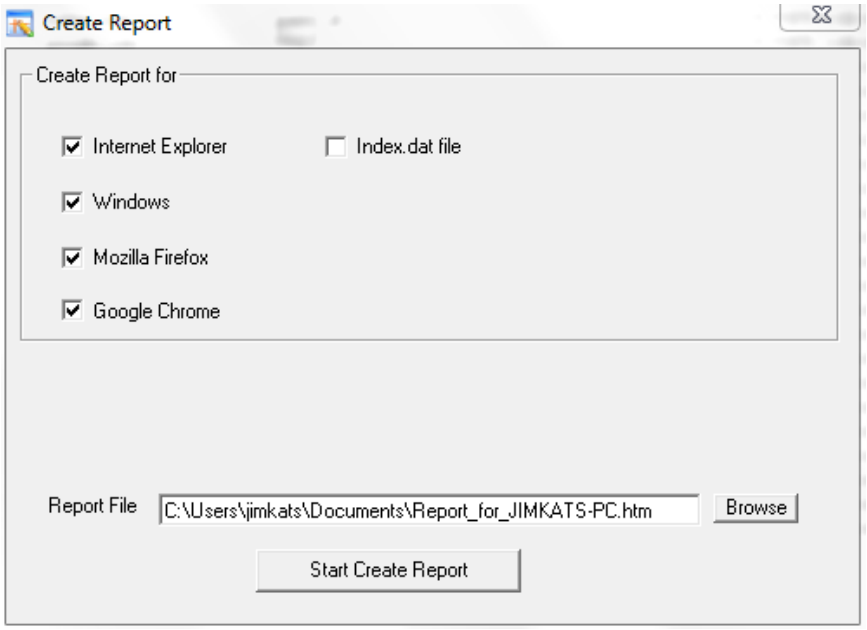
Για κάθε επιλογή, εμφανίζονται διαφορετικές πληροφορίες, όπως για τα **Cookies** όπου για τον Internet Explorer εμφανίζεται μόνο το link του site, ενώ για Chrome και Firefox εμφανίζεται επιπλέον και το όνομα της μεταβλητής για την οποία διατηρείται η πληροφορία.

Για τα **URL History**, εμφανίζεται το URL, ο τίτλος της σελίδας και η τελευταία επίσκεψη.

Για τα **Downloads**, εμφανίζεται το όνομα του αρχείου, η πηγή, πότε ξεκίνησε και πότε τελείωσε η λήψη.

Στο **Index.dat File**, πρέπει να επιλεγεί το αρχείο, καθώς δεν είναι μόνο ένα και έτσι πρέπει να φορτώνεται το κάθε ένα ξεχωριστά.

Υπάρχει η δυνατότητα δημιουργίας αναφοράς σε μορφή **HTML** μετά από επιλογή των αποτελεσμάτων που θέλουμε να εξαγάγουμε.



Εικόνα 5.4: History Viewer – Εξαγωγή αναφοράς

5.2.4 NTLast

Το **NTLast** είναι εργαλείο της Foundstone για Windows, το οποίο καταγράφει τις επιτυχημένες και αποτυχημένες συνδέσεις σε ένα σύστημα. Λειτουργεί μόνο αν είναι ενεργός ο έλεγχος συνδέσεων από το σύστημα.

Η σύνταξη της εντολής είναι:

ntlast [options]

–ad	Περιλαμβάνει εγγραφές μετά την μέρα/ώρα.
–bd	Περιλαμβάνει εγγραφές πριν την μέρα/ώρα.
–c	Συνοπτική έξοδος.
–csv	Έξοδος σε μορφή CSV.
–f	Τελευταίες αποτυχημένες συνδέσεις.
–file	Αρχείο **.evt** όπου βρίσκεται αποθηκευμένο το log.
–from *machine*	Τελευταίες συνδέσεις από *απομακρυσμένο υπολογιστή*.
–i	Τελευταίες διαδραστικές συνδέσεις.
–iis	Συνδέσεις του IIS 4.0 μόνο.
–l	Τελευταία επιτυχημένη σύνδεση.
–l:i	Τελευταία διαδραστική σύνδεση.
–l:r	Τελευταία απομακρυσμένη σύνδεση.
–m *machine*	Όνομα υπολογιστή που θα αναζητήσει.
–mil	Έξοδος ώρας σε στρατιωτική μορφή.
–n *n*	Τελευταίες *n* συνδέσεις.
–not *user*	Βγάζει εκτός αποτελέσματος τον *χρήστη*.
–null	Περιλαμβάνει τις κενές συνεδρίες.
–r	Τελευταίες απομακρυσμένες συνδέσεις.
–rt	Καθαρές ημερομηνίες/ώρες σε μορφή CSV.
–s	Τελευταίες επιτυχημένες συνδέσεις.
–u *user*	Συνδέσεις από τον *χρήστη*.
–v	Verbose. Δείχνει συνδέσεις, αποσυνδέσεις και διάρκεια.

Μπορεί να χρησιμοποιηθεί ο διακόπτης **/** αντί του **–**.

Οι επιλογές **–ad** και **–bd** μπορούν να συνδυαστούν για να βγει αποτέλεσμα για την ενδιάμεση περίοδο.

Το αρχείο log **.evt** συνήθως έχει την ονομασία **sec.evt** .

Οι συνδέσεις του IIS 4.0 φαίνονται μόνο μέσω της επιλογής **–iis** και όχι στα λοιπά αποτελέσματα.

Όταν το δοσμένο όνομα χρήστη είναι κενό, τότε αναφέρεται στην ανώνυμη σύνδεση.

Οι ώρες αναζήτησης χρησιμοποιούν την 24ωρη μορφή, για παράδειγμα **21/7/2015-14:0:0**.

Η χρήση της επιλογής **–u** χωρίς όνομα χρήστη, εμφανίζει λίστα με κενές συνδέσεις.

5.2.5 Pasco

Το **Pasco** είναι εργαλείο ανάλυσης των cookies που διατηρεί ο Internet Explorer, δημιουργία του Keith Jones.

Δεν βρίσκει αυτόματα τα αρχεία που απαιτεί, οπότε πρέπει πρώτα να τα βρούμε εμείς ώστε να μπορέσουμε να τα χρησιμοποιήσουμε.

Σύνταξη της εντολής:

pasco [options] *file*

-d	Επαναφέρει σβησμένες εγγραφές.
-t	Διαχωριστικό πεδίων. Από προεπιλογή το TAB.

5.2.6 pwdump

Είναι μια σειρά Windows εργαλείων που εμφανίζει τους κωδικούς των χρηστών ενός συστήματος, σε μορφή *LM* και *NTLM* hash που υπάγονται στο **System Account Manager (SAM)**.

Έχει βγει σε πολλές εκδόσεις από διάφορους προγραμματιστές και οι οποίες δεν έχουν τεράστιες διαφορές μεταξύ τους, απλώς προσθήκες και βελτιώσεις.

pwdump

Η πρώτη έκδοση του προγράμματος, η οποία παίρνει την βάση δεδομένων των χρηστών από το μητρώο και συγκεκριμένα από την θέση **HKEY_LOCAL_MACHINE\SECURITY\SAM\ Domains\Account\Users** και τους αποθηκεύει σε μορφή **smbpasswd** αρχείου που χρησιμοποιείται από το λογισμικό Samba και αναγνωρίζεται από όλα τα εργαλεία ελέγχου κωδικών ασφαλείας των Windows.

pwdump2

Αυτή η έκδοση παίρνει τα hashes των κωδικών από την βάση δεδομένων του SAM, ασχέτως αν είναι ενεργοποιημένο ή όχι το εργαλείο **Syskey**. Έχοντας την ίδια μορφή εξόδου με την πρώτη έκδοση, μπορεί να χρησιμοποιηθεί από τους διαχειριστές για έλεγχο αδύναμων κωδικών, αλλά και ως είσοδο σε εργαλεία σπασίματος κωδικών.

pwdump3 – pwdump3e

Σ' αυτή την έκδοση, η εκτέλεση του προγράμματος μπορεί να γίνει και δικτυακά, ώστε να γίνει η ανάκτηση των hashes από απομακρυσμένο υπολογιστή. Ταυτόχρονα η επόμενη έκδοση κρυπτογραφεί την ενέργεια αυτή ώστε να μην μπορεί να αναγνωστεί εύκολα από κάποιον άλλον στο δίκτυο. Συγκεκριμένα χρησιμοποιεί το πρωτόκολλο **Diffie-Hellman** για την δημιουργία κοινού κλειδιού και κάνει χρήση του **Windows Crypto API** για την προστασία των hashes.

pwdump4

Βελτίωση της τρίτης έκδοσης, με πιθανότητες το ένα να δουλεύει εκεί που δεν δουλεύει το άλλο.

pwdump5

Ανάλογη με την δεύτερη έκδοση, όπου αν είναι ενεργοποιημένο το **Syskey**, το πρόγραμμα ανακτά το κλειδί κρυπτογράφησης των 128 bit, το οποίο χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των hashes των κωδικών.

pwdump6

Αποτελεί τροποποίηση της τρίτης έκδοσης και έχει την δυνατότητα εξαγωγής των LM και NTLM hashes, ασχέτως αν είναι ενεργό το **Syskey**. Επίσης μπορεί να εμφανίζει το ιστορικό των κωδικών εάν είναι διαθέσιμο, δηλαδή ποιοι ήταν οι προηγούμενοι κωδικοί για τον ίδιο λογαριασμό. Σ' αυτή την έκδοση, η μετάδοση των δεδομένων δεν είναι κρυπτογραφημένη.

pwdump7

Η έβδομη έκδοση δουλεύει με δικό της οδηγό filesystem, έτσι ώστε οι χρήστες με δικαιώματα διαχειριστή να μπορούν να πάρουν απευθείας από τον δίσκο τις ομάδες μητρώου του SAM και του SYSTEM. Μόλις γίνει αυτό, θα ανακτηθεί το Syskey κλειδί από την ομάδα SYSTEM και θα χρησιμοποιηθεί για να αποκρυπτογραφηθούν τα hashes και ύστερα να αποθηκευτούν στο αρχείο μορφής pwdump.

6. Εγκληματολογία κινητών τηλεφώνων

Η εγκληματολογία των κινητών τηλεφώνων είναι ένας τομέας που τα τελευταία χρόνια εξελίσσεται ραγδαία, λόγω της ύπαρξης των smartphones, τα οποία λειτουργούν ως μίνι υπολογιστές κι έτσι διευρύνονται οι δυνατότητες και η χρησιμότητα τους από τα απλά κινητά τηλέφωνα. Αυτό οφείλεται κυρίως στο ότι τα λειτουργικά συστήματα που εμπεριέχονται στα smartphones, δίνουν την δυνατότητα δημιουργίας και διανομής εφαρμογών, γραμμένων από οποιονδήποτε είτε γνωρίζει προγραμματισμό είτε όχι. Έτσι, οι εφαρμογές που βρίσκει κανείς στα online καταστήματα, μπορεί να είναι επιβλαβή για το κινητό και για τον χρήστη.

Τα εργαλεία εγκληματολογικής ανάλυσης κινητών που υπάρχουν, είτε γίνεται από υπολογιστή είτε από τα ίδια τα κινητά, βρίσκουν και αποθηκεύουν όλο το περιεχόμενο ενός κινητού τηλεφώνου, δηλαδή:

- SMS / MMS
- Κλήσεις
- Κατάλογος επαφών
- Φωτογραφίες
- Βίντεο
- Πληροφορίες συσκευής
- Αρχεία εφαρμογών
- Αρχεία και ρυθμίσεις λειτουργικού συστήματος
- Λοιπά αρχεία (έγγραφα, σημειώσεις, κ.τ.λ.)

Τα περισσότερα εργαλεία είναι επί πληρωμή, όπως τα **Oxygen Forensic Suite**, **Lantern** 4**, Logicube CellXtract**, **MOBILedit!**, **Secure View 3** και άλλα. Υπάρχουν επίσης και open-source εργαλεία, όπως τα **iPhone Analyzer**, **Mobile Internal Acquisition Tool**, **TULP2G** και άλλα.

6.1 Foroboto

Το **Foroboto** είναι εργαλείο ανάκτησης δεδομένων και αρχείων από Android συσκευές και τρέχει μέσω γραμμής εντολών σε Windows και Unix συστήματα.

Πιο συγκεκριμένα, χρειάζεται για να λειτουργήσει και αυτοματοποιεί το εργαλείο **Android Debug Bridge** (**adb**), το οποίο αποτελεί μέρος του **Android SDK** και είναι υπεύθυνο για την δημιουργία σύνδεσης του υπολογιστή με την συσκευή, σε επίπεδο debug. Περιέχει διάφορες εντολές, οι οποίες αφορούν κυρίως την εμφάνιση διαφόρων πληροφοριών για την συσκευή, καθώς και την δυνατότητα ανάκτηση δεδομένων.

Όταν εκτελεστεί το εργαλείο, θα τυπώσει το εξής μήνυμα στην γραμμή εντολών:

```
Select the run level you wish to execute:
 1. Collect live information (Dumpstate + Logcat)
 2. Level 1 + System information
 3. Level 2 + Logical acquisition of the SD Card
 4. Level 3 + Logical acquisition of the Data directory
 5. Level 4 + Full logical acquisition (Common local directories)
Type in the collection level (1-5):
```

Δηλαδή ζητά από τον χρήστη να επιλέξει τι είδους ανάκτηση θέλει να κάνει. Τα **επίπεδα 1**, **2** και **3** δεν απαιτούν *πρόσβαση root* στην συσκευή, ενώ τα **επίπεδα 4** και **5** το απαιτούν.

Επίπεδο 1

Εκτελεί τις εντολές **Dumpstate** και **logcat**.
Παρέχει πολλές αναλυτικές πληροφορίες για την συσκευή σε σύντομο χρονικό διάστημα.

Επίπεδο 2

Εμφανίζει πληροφορίες για:

- **Mount points**
- **Δικτυακές συνδέσεις**
- **Ημερομηνία και ώρα**
- **Χρήση αποθηκευτικού χώρου**
- **Λίστα ανοιχτών αρχείων**
- **Χρονική διάρκεια λειτουργίας της συσκευής**

Παρέχει επιπρόσθετες πληροφορίες για την δικτύωση και τον αποθηκευτικό χώρο της συσκευής.

Επίπεδο 3

Αντιγράφει τα δεδομένα της **κάρτας SD** για τα οποία υπάρχει πρόσβαση.
Περισσότερα αρχεία μπορούν να ανακτηθούν με *πρόσβαση root*.

Επίπεδο 4

Αντιγράφει αρχεία από τον κατάλογο **/data/**.
Εκεί αποθηκεύονται τα δεδομένα των εφαρμογών και οι περισσότερες ρυθμίσεις.
Λόγω σφάλματος, δεν ανακτώνται όλες οι πληροφορίες από τον κατάλογο **/data/data**.

Επίπεδο 5

Ανακτά δεδομένα από τους εξής καταλόγους:

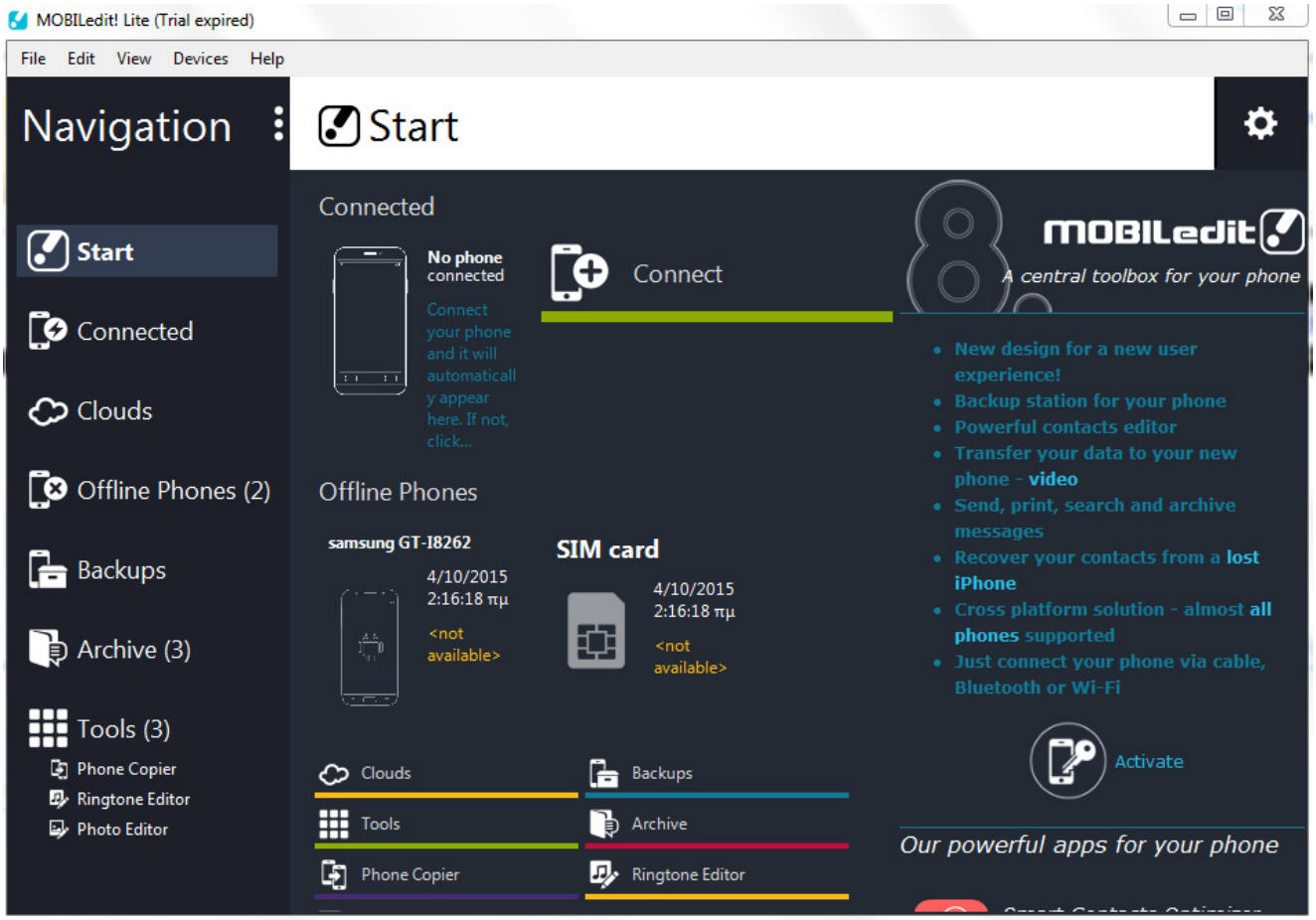
- ✓ **/cache**
- ✓ **/charger**
- ✓ **/config**
- ✓ **/d**
- ✓ **/etc**
- ✓ **/mnt**
- ✓ **/res**
- ✓ **/root**
- ✓ **/sbin**
- ✓ **/sys**
- ✓ **/system**
- ✓ **/tombstones**

Συλλέγει όλες τις πληροφορίες από τους πιο κοινούς καταλόγους της συσκευής.

6.2 MOBILedit!

Το **MOBILedit!** είναι λογισμικό ανάκτησης όλων των πληροφοριών και αρχείων ενός κινητού. Τρέχει μόνο σε Windows, είναι επί πληρωμή και είναι δημιουργία της COMPELSON Labs.

Το εύχρηστο γραφικό περιβάλλον, σε συνδυασμό με την υποστήριξη πολλών και διαφόρων κινητών συσκευών, κάνει το εργαλείο αρκετά χρήσιμο για τον οποιοδήποτε.



Εικόνα 6.1: Αρχική οθόνη MOBILedit!

Αφού εκτελεστεί το πρόγραμμα, εμφανίζεται στον χρήστη το κεντρικό παράθυρο στο οποίο μπορεί να επιλέξει ότι θέλει.

Για να ξεκινήσει, αρκεί να πατήσει το Connect στο κέντρο του παραθύρου και έπειτα επιλέγει τι θέλει να συνδέσει:

- **Τηλέφωνο**
- **Δικτυακό χώρο αποθήκευσης**
- **Αρχείο δεδομένων**
- **Αναγνώστης κάρτας SIM**

Ανάλογα με την επιλογή, βάζει μετά και τις αντίστοιχες ρυθμίσεις. Για παράδειγμα, για το τηλέφωνο επιλέγει τον τρόπο σύνδεσης:

- **USB**
- **WiFi (Android, iPhone)**
- **Bluetooth**
- **Υπέρυθρες**
- **Tethering**

Πριν γίνει η προσθήκη του τηλεφώνου, ζητά από τον χρήστη να κατεβάσει τους οδηγούς του κινητού σε περίπτωση που δεν υπάρχουν ήδη και να ενεργοποιήσει το USB Debugging από τις ρυθμίσεις του κινητού.

Αφού έχει γίνει η προσθήκη του τηλεφώνου, τώρα ο χρήστης μπορεί από το παράθυρο να επιλέξει την εκάστοτε κατηγορία πληροφοριών που θέλει να δει και αφού έχει φορτώσει πλήρως,

έχει την δυνατότητα να αποθηκεύσει τα δεδομένα στον υπολογιστή και να δημιουργήσει αναφορές με βάση αυτά, σε ευανάγνωστη μορφή.

7. Πολυεργαλεία εγκληματολογικής εξέτασης υπολογιστών

Συνήθως στις διάφορες υπηρεσίες που κάνουν χρήση εγκληματολογικών εργαλείων, προτιμώνται τα λογισμικά τα οποία είναι *πολυεργαλεία* ή «*σουίτες*» *εργαλείων*, δηλαδή κάνουν την δουλειά πολλών εργαλείων μαζί, σαν κι αυτών που αναφέρθηκαν στα προηγούμενα κεφάλαια. Από τα πιο γνωστά, είναι τα **EnCase**, **Forensic Toolkit** και **The Sleuth Kit**.

Επίσης, γίνεται συχνή χρήση και *λειτουργικών συστημάτων* ειδικά σχεδιασμένων για εγκληματολογικές αναλύσεις ή ασφάλεια δικτυακών συστημάτων, τα οποία παρομοίως συμπεριλαμβάνουν εργαλεία όπως τα από πάνω. Μερικά από τα πιο γνωστά είναι τα **Kali Linux**, **CAINE** και **SIFT**. Όλα ανήκουν στην κατηγορία των κατηγορία των Unix συστημάτων και ιδίως στην Linux οικογένεια, λόγω του open-source kernel.

7.1 Acct

Το **Acct** ή αλλιώς **GNU Accounting Utilities**, είναι πακέτο εργαλείων που καταγράφουν πληροφορίες και στατιστικά για τις συνδέσεις και την κίνηση των λογαριασμών ενός συστήματος.

Περιλαμβάνει έξι εργαλεία:

- **ac**
- **accton**
- **lastcomm**
- **sa**
- **dump-acct**
- **dump-utmp**

7.1.1 ac

Το **ac** τυπώνει στατιστικά για τους χρόνους σύνδεσης. Μπορεί να αναφέρει τον συνολικό χρόνο σύνδεσης σε δευτερόλεπτα ενός χρήστη ή μιας ομάδας χρηστών, με βάση τις εγγραφές στο **/var/log/wtmp** αρχείο.

Η εντολή γράφεται ως εξής:

ac [options]

-a	Τυπώνει μια εγγραφή για κάθε μέρα, αντί να μην τυπώνει για μέρες που δεν υπήρξε σύνδεση.
--compatibility	Συντομογραφία για τις επιλογές **--reboots**, **--supplants** και **--timewarps**.
--complain	Τυπώνει μήνυμα λάθους, άμα το **wtmp** αρχείο έχει πρόβλημα.

-d	Τυπώνει το σύνολο για κάθε μέρα, αντί για το συνολικό.
-f *file*	Διαβάζει τις καταγραφές από το δοσμένο *αρχείο*.
-p	Τυπώνει το σύνολο για κάθε χρήστη.
--print-zeros	Τυπώνει τον συνολικό χρόνο ακόμη κι όταν είναι μηδέν.
--reboots	Υπολογίζει τον συνολικό χρόνο ενός χρήστη, μέχρι την επανεκκίνηση του συστήματος.
--supplants	Υπολογίζει τον συνολικό χρόνο ενός χρήστη, μέχρι την επόμενη σύνδεση του.
--timewarps	Υπολογίζει τον συνολικό χρόνο ενός χρήστη, μέχρι την διαστρεβλωμένη ώρα του **wtmp** αρχείου.
--tw-leniency *n*	Θέτει τον χρόνο επιείκειας σε *δευτερόλεπτα* μεταξύ δύο εγγραφών.
--tw-suspicious *n*	Θέτει τον χρόνο σε *δευτερόλεπτα* μεταξύ δύο εγγραφών για να θεωρηθούν προβληματικές.
-y	Τυπώνει το έτος μαζί με τις ημερομηνίες.

Αν η εντολή εκτελεστεί σκέτη, εμφανίζει το συνολικό χρόνο από όλες τις συνδέσεις.

Για την επιλογή **--reboots**, το **ac** υπολογίζει τον χρόνο όχι μέχρι την διαδικασία κλεισίματος του υπολογιστή, αλλά μέχρι την στιγμή που έχει ανοίξει ο υπολογιστής πάλι.

Για την επιλογή **--supplants**, μερικές φορές δεν καταγράφεται η αποσύνδεση ενός χρήστη, όταν γίνεται από διαφορετικό τερματικό απ' αυτό που συνδέθηκε.

Για την επιλογή **--timewarps**, κάποιες φορές οι ώρες στις εγγραφές στο **wtmp** αρχείο πάνε πίσω κι έτσι ο υπολογισμός της συνολικής διάρκειας μπορεί να μην είναι σωστός.

Για την επιλογή **--tw-leniency**, αν γίνουν για παράδειγμα δύο συνδέσεις εντός του δοσμένου χρόνου επιείκειας, τότε η $2^{η}$ γράφεται $1^{η}$. Από προεπιλογή ο χρόνος είναι 1 δευτερόλεπτο.

Για την επιλογή **--tw-suspicious**, αν δύο εγγραφές απέχουν μεταξύ τους περισσότερο από τον δοσμένο χρόνο, τότε δεν αναγράφεται ο χρόνος των χρηστών. Αυτό μπορεί να συμβαίνει είτε γιατί το **wtmp** αρχείο έχει πρόβλημα, είτε γιατί ο υπολογιστής έχει να χρησιμοποιηθεί πολύ καιρό.

7.1.2 accton

Το **accton** ενεργοποιεί και απενεργοποιεί αντίστοιχα το acct για την καταγραφή των πληροφοριών και αποθηκεύει την πρόοδο σε αρχείο.

Η εντολή γράφεται ως εξής:

accton [**on/off**] <*file*>

Αν γραφτεί **accton on**, θα χρησιμοποιηθεί το προεπιλεγμένο αρχείο καταγραφής.

7.1.3 lastcomm

Το **lastcomm** εμφανίζει πληροφορίες για τις τελευταίες εντολές που εκτελέστηκαν.
Για κάθε εγγραφή, εμφανίζονται σε τέσσερις στήλες τα εξής:

- Όνομα της εντολής της διεργασίας.
- Σημαίες, όπως καταγράφονται από την ρουτίνα του συστήματος:
  - ✓ **C** → εντολή που εκτελέστηκε από τον υπερ-χρήστη.

- ✓ **D** → εντολή που εκτελέστηκε μετά από διχάλα, χωρίς επακόλουθη εκτέλεση.
- ✓ **F** → εντολή που τρέχει σε συμβατότητα **PDP-11**. Για **VAX** μόνο.
- ✓ **S** → εντολή που τερματίστηκε με την παραγωγή ενός αρχείου πυρήνα.
- ✓ **X** → εντολή που τερματίστηκε με το σήμα **SIGTERM**.

- ➢ Όνομα χρήστη που έτρεξε την διεργασία.
- ➢ Χρόνος που η διεργασία τερματίστηκε.

Η εντολή γράφεται ως εξής:

lastcomm [options] <*command* | *tty* | *user*>

--ahz *hz*	Ορίζει την τιμή του AHZ για να μπορεί να διαβάσει **acct** αρχεία άλλου μηχανήματος, με διαφορετικές αρχιτεκτονικές και εκδόσεις πυρήνα.
--command *cmd*	Εμφανίζει τις εγγραφές που αντιστοιχούν στο *όνομα εντολής*.
-f *file*	Διαβάζει από το *αρχείο* αντί από το αρχείο **acct**.
--forwards	Διαβάζει το αρχείο προς τα μπρος αντί προς τα πίσω.
-p	Δείχνει στατιστικά σελιδοποίησης.
--strict-match	Εμφανίζει τις εγγραφές που αντιστοιχούν με όλες τις παραμέτρους της εντολής.
--tty *name*	Εμφανίζει τις εγγραφές που αντιστοιχούν στο *tty όνομα*.
--user *name*	Εμφανίζει τις εγγραφές που αντιστοιχούν στο *όνομα χρήστη*.

Αν η εντολή εκτελεστεί σκέτη, θα εμφανιστούν πληροφορίες για όλες τις εντολές, όπως αυτές βρίσκονται στο αρχείο **acct**.

Για την επιλογή **--forwards**, γίνεται για να διαβάζει από διασωλήνωση και όχι για να κυνηγά. Αναφέρεται πριν την επιλογή **–f**.

7.1.4 sa

Το **sa** συνοψίζει πληροφορίες για τις εκτελεσμένες εντολές, όπως καταγράφηκαν από το αρχείο **acct**, συμπεριλαμβανομένου την χρήση της CPU και τις φορές που έχει κληθεί η εντολή.

Το αποτέλεσμα εμφανίζει σε στήλες με τις εξής πληροφορίες:

- ➢ **cpu** → Άθροισμα των χρόνων χρήστη και συστήματος, σε CPU δευτερόλεπτα.
- ➢ **re** → "Πραγματικός χρόνος" σε CPU δευτερόλεπτα.
- ➢ **k** → Μέση χρήση πυρήνα, σε μονάδες των 1000 CPU δευτερολέπτων.
- ➢ **avio** → Μέσος αριθμός I/O λειτουργιών ανά εκτέλεση.
- ➢ **tio** → Συνολικός αριθμός I/O λειτουργιών.
- ➢ **k*sec** → Ολοκληρωμένη αποθήκη CPU, σε μονάδες των 1000 δευτερολέπτων πυρήνα.
- ➢ **u** → Χρόνος CPU χρήστη σε δευτερόλεπτα CPU.
- ➢ **s** → Χρόνος συστήματος σε δευτερόλεπτα CPU.

Οι εντολές οι οποίες καλούνται μόνο μία φορά ή έχουν στο όνομα τους μη-εκτυπώσιμους χαρακτήρες, ταξινομούνται από το **sa** στην ομάδα ***other**.

Σε μερικά συστήματα, οι κεφαλίδες δεν φαίνονται και ενσωματώνονται μέσα στις τιμές. Επίσης, κάποιες επιλογές δεν υποστηρίζονται παντού, λόγω του ότι κάποιες πληροφορίες δεν καταγράφονται.

Η εντολή γράφεται ως εξής:

sa [options] <*file*>

-a	Δεν ταξινομεί τις εντολές της κατηγορίας ***other**.
-b	Ταξινομεί με βάση την διαίρεση της στήλης **cpu** με τον αριθμό των κλήσεων.
-c	Τυπώνει ποσοστά του συνολικού χρόνου για χρήστες, σύστημα και πραγματικό χρόνο.
-d	Ταξινομεί με βάση τον μέσο αριθμό I/O λειτουργιών του δίσκου.
-D	Ταξινομεί με βάση τον συνολικό αριθμό των I/O λειτουργιών του δίσκου.
-f	Θεωρεί θετικές όλες τις απαντήσεις για τις ερωτήσεις στην επιλογή **-v**.
-i	Δεν διαβάζει τις πληροφορίες στο **savacct**.
-j	Τυπώνει δευτερόλεπτα ανά κλήση, αντί για λεπτά ανά κατηγορία.
-k	Ταξινομεί με βάση την μέση χρήση μνήμης σε CPU χρόνο.
-K	Ταξινομεί με βάση την ολοκληρωτική CPU αποθήκη.
-l	Τυπώνει ξεχωριστές στήλες για χρόνους χρήστη και συστήματος.
-m	Τυπώνει τον αριθμό των διεργασιών και των CPU λεπτών για κάθε χρήστη.
-n	Ταξινομεί με βάση των αριθμό των κλήσεων. Προεπιλεγμένη ταξινόμηση.
-p	Τυπώνει τον αριθμό των σφαλμάτων σελίδας και των εναλλαγών. Σημαντικών και ασήμαντων.
-P	Το ίδιο με την επιλογή **–p**, διαιρούμενα με τον αριθμό των κλήσεων.
-r	Ταξινομεί αντίστροφα.
-s	Συγχωνεύει τα συνολικά δεδομένα στα αρχεία **savacct** και **usracct**.
-t	Τυπώνει την αναλογία πραγματικού χρόνου προς το σύνολο χρόνων χρήστη και συστήματος, για κάθε εγγραφή.
-u	Για κάθε εντολή, τυπώνει το user id και το όνομα της εντολής.
-v *n*	Εμφανίζει τις εντολές που εκτελέστηκαν το πολύ *n* φορές και περιμένουν απάντηση από το τερματικό.
--sort-real-time	Ταξινομεί με βάση τον "πραγματικό χρόνο" για κάθε εντολή.
--ahz *hz*	Ορίζει την τιμή του AHZ για να μπορεί να διαβάσει **acct** αρχεία άλλου μηχανήματος, με διαφορετικές αρχιτεκτονικές και εκδόσεις πυρήνα.

Για την επιλογή **–t**, εμφανίζει ***ignore*** αν το σύνολο των χρόνων χρήστη και συστήματος είναι πολύ μικρό για να αναφερθεί.

Η επιλογή **–u**, προσπερνάει όλες τις υπόλοιπες κι έτσι με το που τυπωθούν όλες εγγραφές, τερματίζεται η εκτέλεση.

Για την επιλογή **–v**, αν η απάντηση του τερματικού ξεκινάει με **y**, τοποθετεί την εντολή στην ομάδα ****junk****.

7.1.5 dump-acct / dump-utmp

Οι **dump-acct** και **dump-utmp** εμφανίζουν τα αντίστοιχα αρχεία καταγραφής σε ευανάγνωστη μορφή.

Για το **dump-acct**, το αρχείο είναι το **/var/log/account/paact**, ενώ για το **dump-utmp** είναι το **/var/log/wtmp**.

Τα δεδομένα που τυπώνονται, ορίζονται στις εξής στήλες:

- ✓ **ac_comm** : όνομα εκτελούμενου προγράμματος

- ✓ **ac_version** : έκδοση αρχείου μορφής **acct**
- ✓ **ac_utime** : χρόνος χρήστη
- ✓ **ac_stime** : χρόνος συστήματος
- ✓ **ac_etime** : παρερχόμενος χρόνος
- ✓ **ac_uid** : ID χρήστη
- ✓ **ac_gid** : ID ομάδας
- ✓ **ac_mem** : μέση χρήση μνήμης
- ✓ **ac_io** : αριθμός χαρακτήρων που μεταφέρθηκαν στο I/O
- ✓ **ac_pid** : ID διεργασίας
- ✓ **ac_ppid** : ID γόνου διεργασίας

Οι εντολές γράφονται ως εξής:

dump-acct [options] <*files*>
dump-utmp [options] <*files*>

--ahz *hz*	Ορίζει την τιμή του AHZ για να μπορεί να διαβάσει **acct** αρχεία άλλου μηχανήματος, με διαφορετικές αρχιτεκτονικές και εκδόσεις πυρήνα.
--byteswap	Εναλλάσσει τα bytes στην έξοδο της επιλογής **–R**.
--format	Ορίζει μορφή εξόδου με την επιλογή **–R**.
-n *n*	Περιορίζει τον αριθμό των *γραμμών* που θα εμφανιστούν.
-r	Διαβάζει το αρχείο προς τα πίσω, δηλαδή τυπώνει την τελευταία εγγραφή πρώτα.
-R	Εμφανίζει χύμα δεδομένα και όχι σε ευανάγνωστη μορφή.

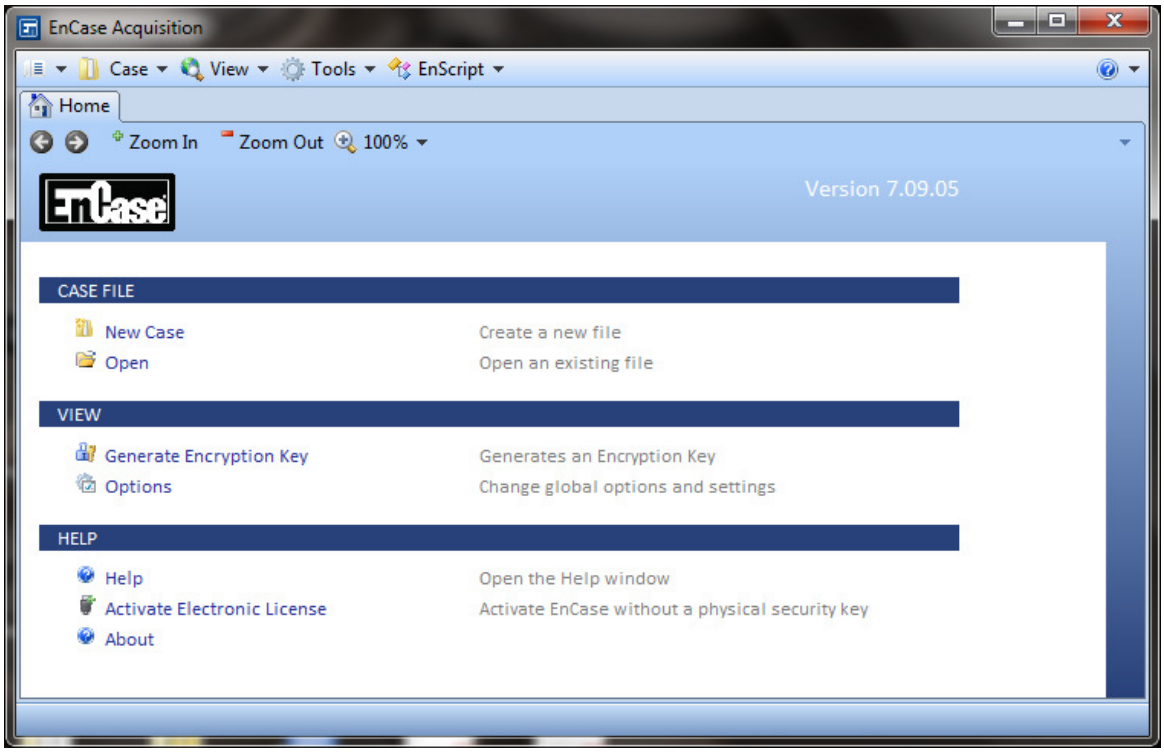
Η επιλογή **--ahz**, επηρεάζει το I/O, εκτός του αρχείου μορφής v3, το οποίο είναι σταθερό στο **AHZ=100**. Για μετατροπή ανάμεσα σε διαφορετικές τιμές AHZ, πρώτα μετατρέψτε την μορφή v3 με την παλιά τιμή AHZ και έπειτα μετατρέψτε στην επιθυμητή μορφή εξόδου με την νέα τιμή AHZ.

7.2 EnCase Forensic

Το **EnCase Forensic** της Guidance Software είναι ένα εγκληματολογικό πολυεργαλείο, το οποίο έχει την δυνατότητα εύρεσης, ανάκτησης και επεξεργασίας των αρχείων ενός μέσου αποθήκευσης. Τρέχει μόνο σε Windows και είναι εργαλείο επί πληρωμή, για το οποίο υπάρχουν ειδικά προγράμματα εκμάθησής του με πιστοποιήσεις, καθώς χρησιμοποιείται από τις περισσότερες υπηρεσίες ανά τον κόσμο. Η τρέχουσα έκδοση είναι η **7.10.05**.

Μερικά χαρακτηριστικά του EnCase είναι η:

- ❖ δυνατότητα δημιουργίας σεναρίων με την χρήση των APIs που περιλαμβάνει.
- ❖ δημιουργία images των μέσων αποθήκευσης σε μορφή **EnCase Evidence File Format**.
- ❖ ανάλυση κινητών τηλεφώνων με την χρήση πρόσθετων της εταιρίας, από την έκδοση 7.



Εικόνα 7.1: Αρχική οθόνη EnCase

Για να δημιουργήσει κανείς μια νέα υπόθεση, αρκεί μόνο να επιλέξει **Case → New Case** κι εκεί δηλώνει το όνομα της υπόθεσης. Οι διαδρομές αναγράφονται από κάτω και δημιουργούνται αυτόματα.

Αφού του ανοίξει την νέα υπόθεση, θα μπορεί να προσθέσει αποδεικτικά στοιχεία, να τα χειριστεί και να κλείσει την υπόθεση. τα αποδεικτικά στοιχεία που μπορεί να προσθέσει, είναι:

- **Local Device**
- **Network Preview**
- **Evidence File**
- **Raw Image**
- **Crossover Preview**

Στο **Local Device**, μπορούν να επιλεγούν τα εξής:

- Detect Tableau Hardware
- Only Show Write-blocked
- Detect Legacy FastBloc
- Enable DCO Removal
- Enable Physical Memory
- Enable Process Memory

Στο **Evidence File**, τα είδη αρχείων που υποστηρίζονται είναι:

- Legacy Evidence File → **.E01**
- Current Evidence File → **.Ex01**
- SafeBack File → **.001**
- VMware File → **.vmdk**

- Legacy Logical Evidence File → **.L01**
- Current Logical Evidence File → **.Lx01**
- Virtual PC File → **.vhd**

Το **EnScript**, είναι η μηχανή δημιουργίας των σεναρίων του EnCase και βρίσκει κανείς έτοιμα τα εξής σκριπτάκια:

- Case Analyzer
- Case Processor
- File Report
- ProcessorOptions
- ProcManLocalWebServer
- ProcManWebServer
- Remote Acquisition Monitor
- Sweep Enterprise

Αυτά τα σκριπτάκια μπορούν να τροποποιηθούν στις ανάγκες του καθ' ενός, καθώς και να δημιουργήσει καινούργια.

7.3 Forensic Toolkit

Το **Forensic Toolkit (FTK)** είναι πολυεργαλείο ανάλογο του EnCase, το οποίο επίσης έχει την δυνατότητα ανάκτησης διαγραμμένων e-mail. Είναι δημιουργία της Foundstone και ισχύει για Windows 95 και ύστερα.

Η τωρινή της έκδοση είναι η 2.0, υπάρχει από το 2000 και περιλαμβάνει 7 εντολές, οι οποίες είναι οι:

1. AFind
2. Audited
3. DACLchk
4. FileStat
5. HFind
6. Hunt
7. SFind

Σε όλες τις εντολές, μπορούν να χρησιμοποιηθούν ως διακόπτες είτε **/** είτε **–**.

7.3.1 AFind

Η **AFind** παρουσιάζει τα αρχεία με βάση την ώρα της τελευταίας προσπέλασης.

Το εργαλείο αυτό εμφανίζει το timestamp αυτό χωρίς να αλλοιώσει τα δεδομένα, σε αντίθεση με το δεξί κλικ που κάνουμε στο αρχείο για να δούμε τις ιδιότητες. Δίδεται η δυνατότητα αναζήτησης σε συγκεκριμένο χρονικό εύρος.

Η σύνταξη της εντολής είναι:

afind [options]

directory	Ο κατάλογος όπου θα αναζητήσει.
-a *d/m/y-h:m:s*	Αρχεία τα οποία προσπελάστηκαν μετά την ημερομηνία/ώρα.
-d *days*	Αρχεία που προσπελάστηκαν λιγότερο από χ μέρες.
-f *filename*	
-h *hours*	Αρχεία που προσπελάστηκαν λιγότερο από χ ώρες.
-m *minutes*	Αρχεία που προσπελάστηκαν λιγότερο από χ λεπτά.
-ns	Δεν περιλαμβάνει τους υποκαταλόγους.
-s *seconds*	Αρχεία που προσπελάστηκαν λιγότερο από χ δευτερόλεπτα.

7.3.2 DACLchk

Η **DACLchk** ελέγχει αν τα ACEs ενός αρχείου έχουν μπει με λάθος σειρά.

Αν μια ACE άρνησης πρόσβασης είναι μετά από μια ACE αποδοχής πρόσβασης, τότε θα είναι σαν να μην υπήρχε ποτέ άρνηση πρόσβασης. Αυτό θεωρείται τρύπα ασφαλείας.

Η σύνταξη της εντολής είναι:

daclchk [options]

directory	Ο κατάλογος όπου θα αναζητήσει.
-ns	Δεν περιλαμβάνει τους υποκαταλόγους.
-d	Εμφανίζει όλες τις ACEs.

Αν δεν μπει η επιλογή **–d**, τότε θα εμφανίσει μόνο τα αρχεία που έχουν τις ACEs με λάθος σειρά, δηλαδή αν έχουν άρνηση πρόσβασης, να μην βρίσκεται στην αρχή.

7.3.3 FileStat

Η **FileStat** εμφανίζει τις ιδιότητες ασφάλειας και αρχείου για αρχεία και καταλόγους.

Συγκεκριμένα εμφανίζει τα ACEs, τις ιδιότητες αρχείου ή καταλόγου και τις ροές δεδομένων του αρχείου.

Η σύνταξη της εντολής είναι:

filestat <*file* | *directory*>

Για τα αρχεία, στις ροές εκτός από την βασική ή τις εναλλακτικές, αν υπάρχουν, εμφανίζει και ροή δεδομένων για την κατηγορία ασφάλεια.

7.3.4 HFind

Η **HFind** αναζητά κρυμμένα αρχεία στον δίσκο.

Η σύνταξη της εντολής είναι:

hfind [options]

directory	Ο κατάλογος όπου θα αναζητήσει.
-ns	Δεν περιλαμβάνει τους υποκαταλόγους.

Αν η εντολή εκτελεστεί σκέτη, θα αναζητήσει στον τρέχων κατάλογο.

7.3.5 Hunt

Η **Hunt** εμφανίζει πληροφορίες για κοινόχρηστους πόρους και τους χρήστες ενός υπολογιστή στο δίκτυο.

Η σύνταξη της εντολής είναι:

hunt *computer*

Η χρήση της εντολής ενδείκνυται για να δείξει τι πληροφορίες εμφανίζει σε μια κενή συνεδρία, δηλαδή όταν κάποιος χρήστης συνδέεται σε ένα τοπικό σύστημα με όνομα χρήστη και κωδικό να είναι κενοί χαρακτήρες, όπου σημαίνει ότι ανήκει στην κατηγορία όλων των χρηστών, αλλά όχι στους εξουσιοδοτημένους.

7.3.6 SFind

Η **SFind** ψάχνει για εναλλακτικές ροές δεδομένων.

Η σύνταξη της εντολής είναι:

sfind [options]

directory	Ο κατάλογος όπου θα αναζητήσει.
-ns	Δεν περιλαμβάνει τους υποκαταλόγους.

Αν η εντολή εκτελεστεί σκέτη, θα αναζητήσει στον τρέχων κατάλογο.
Η εντολή εμφανίζει το όνομα της εναλλακτικής ροής και το μέγεθος σε byte.

7.4 Kali Linux

Τα **Kali Linux** είναι λειτουργικό σύστημα της Offensive Security, βασισμένο στην αρχιτεκτονική των Linux, το οποίο αποτελείται από πληθώρα εργαλείων για εγκληματολογική χρήση. Παλιότερα, τα Kali Linux ήταν γνωστά ως **Backtrack** και χαρακτηρίζονται ως δοκιμαστές διείσδυσης συστημάτων.

Εκτός από PC και Mac, μπορούν να στηριχθούν από συγκεκριμένα tablets και γενικά συστήματα με ARM αρχιτεκτονική, όπως το Raspberry Pi. Όσο εξελίσσονται, όλο και περισσότερα συστήματα τα υποστηρίζουν.

Εικόνα 7.2: Kali Linux

Λόγω του ότι τα εργαλεία που περιλαμβάνουν τα Kali Linux είναι πολλά, κάποια από τα οποία αναφέρονται σ' αυτή την πτυχιακή, θα αναφερθούν μόνο οι κατηγορίες των εργαλείων που υπάρχουν, μαζί με τις υποκατηγορίες τους.

Έτσι λοιπόν, στην έκδοση 2.0, υπάρχουν οι εξής κατηγορίες εργαλείων:

1. **Information Gathering**
    i. **DNS Analysis**
    ii. **IDS/IPS Identification**
    iii. **Live Host Identification**
    iv. **Network & Port Scanners**
    v. **OSINT Analysis**
    vi. **Route Analysis**
    vii. **SMB Analysis**
    viii. **SMTP Analysis**
    ix. **SNMP Analysis**
    x. **SSL Analysis**
2. **Vulnerability Analysis**
    i. **Cisco Tools**
    ii. **Fuzzing Tools**
    iii. **OpenVAS Scanner**
    iv. **Stress Testing**
    v. **VoIP Tools**
3. **Web Application Analysis**

   i. **CMS & Framework Identification**
   ii. **Web Application Proxies**
   iii. **Web Crawlers & Directory Bruteforce**
   iv. **Web Vulnerability Scanners**
4. **Database Assessment**
5. **Password Attacks**
   i. **Offline Attacks**
   ii. **Online Attacks**
   iii. **Passing the Hash tools**
   iv. **Password Profiling & Wordlists**
6. **Wireless Attacks**
   i. **802.11 Wireless Tools**
   ii. **Bluetooth Tools**
   iii. **Other Wireless Tools**
   iv. **RFID & NFC Tools**
   v. **Software Defined Radio**
7. **Reverse Engineering**
8. **Exploitation Tools**
9. **Sniffing & Spoofing**
   i. **Network Sniffers**
   ii. **Spoofing and MITM**
10. **Post Exploitation**
   i. **OS Backdoors**
   ii. **Tunneling & Exfiltration**
   iii. **Web Backdoors**
11. **Forensics**
   i. **Digital Forensics**
   ii. **Forensic Carving Tools**
   iii. **Forensic Imaging Tools**
   iv. **PDF Forensics Tools**
   v. **Sleuth Kit Suite**
12. **Reporting Tools**
13. **System Services**
   i. **BeFF**
   ii. **Dradis**
   iii. **OpenVas**

Εκτός από τα εξειδικευμένα εργαλεία ελέγχου ασφάλειας και εγκληματολογίας, τα Kali Linux περιλαμβάνουν και αρκετά εργαλεία για λοιπές χρήσεις, όπως το **Arduino IDE**, το **chirp**, το **Wireshark**, το **ipython** και το **Ophcrack**.

Την λίστα με τις κατηγορίες των εργαλείων, την βρίσκει κανείς στην καρτέλα Applications στο πάνω μέρος της οθόνης. Στα αριστερά της οθόνης, υπάρχει μια μπάρα με τα πιο συνηθισμένα εργαλεία για πιο γρήγορη πρόσβαση. Επίσης, ένα άλλο σημαντικό

χαρακτηριστικό, είναι η δυνατότητα *εγγραφής* της οθόνης και του ήχου μέσω ενός κουμπιού στο πάνω μέρος της οθόνης.

7.5 Sysinternals Suite

Το **Sysinternals Suite** είναι το σύνολο όλων των εργαλείων της Sysinternals που αποσκοπούν στην επίλυση προβλημάτων στα Windows. Μέσα σ' αυτά περιλαμβάνονται και πολλά εργαλεία που χρησιμοποιούνται για εγκληματολογική έρευνα, τα οποία θα δούμε παρακάτω. Τα περισσότερα εργαλεία τρέχουν σε command line και υποστηρίζονται από Windows XP & Server 2003 και άνω.

Τα εργαλεία αυτά μπορεί κανείς να τα βρει και ανεξάρτητα, ώστε να μην χρειάζεται να κατεβάζει ολόκληρο το σετ.

7.5.1 AccessChk

Το **AccessChk** εμφανίζει τα δικαιώματα χρηστών και ομάδων πάνω σε αρχεία, κλειδιά μητρώου, υπηρεσίες και άλλα.

Η σύνταξη της εντολής είναι περίπλοκη, καθώς αποτελείται από πολλές επιλογές:

accesschk [options] <*file, etc*>

-a *name*	Εμφανίζει ποιοι χρήστες και ομάδες έχουν συγκεκριμένα δικαιώματα. Το * είναι για όλα τα δικαιώματα του λογαριασμού των Windows.
-c *name*	Εμφανίζει τι δικαιώματα έχουν οι χρήστες σε συγκεκριμένες υπηρεσίες. Το * είναι για όλες τις υπηρεσίες.
-d	Επεξεργάζεται μόνο καταλόγους ή κλειδιά υψηλού επιπέδου.
-e	Δείχνει ρητά ορισμένα επίπεδα ακεραιότητας. Για Vista και άνω μόνο.
-f <*accounts*>	Αποκλείει τους ορισμένους λογαριασμούς από την έξοδο. Σε συνδυασμό με την επιλογή **–p** δείχνει ενδεικτικές πληροφορίες για τις διεργασίες μαζί με τις ομάδες και τα δικαιώματα.
-h *name*	Εμφανίζει τα κοινόχρηστα μέσα και τα δικαιώματα των χρηστών. Το * είναι για όλα τα κοινόχρηστα μέσα.
-i	Αγνοεί αντικείμενα με μόνο κληροδοτημένες ACEs όταν αδειάζει ολόκληρες ACLs. Χρησιμοποιείται μόνο μαζί με την επιλογή **–l**.
-k *name*	Εμφανίζει τα δικαιώματα των χρηστών στα κλειδιά του μητρώου. Για παράδειγμα *HKLM\SYSTEM*.
-l	Εμφανίζει πλήρη περιγραφή ασφαλείας για τους χρήστες.
-n	Δείχνει τα αντικείμενα που δεν έχουν κανένα δικαίωμα.
-o	Δείχνει τον τύπο των αντικειμένων του Διαχειριστή Αντικειμένων.
-p *name*	Εμφανίζει τα δικαιώματα των χρηστών στις διεργασίες. Το * είναι για όλες τις διεργασίες. Σε συνδυασμό με την επιλογή **–t** εμφανίζει τα νήματα.
-q	Παραλείπει τις πρώτες γραμμές της εξόδου με τις πληροφορίες του εργαλείου.
-r	Δείχνει μόνο τα αντικείμενα με δικαιώματα ανάγνωσης.
-s	Αναδρομική αναζήτηση.
-t <*object*>	Φίλτρο για αντικείμενα, όπως ''section''.
-u	Παραλείπει τα λάθη από την έξοδο.
-v	Verbose. Περιλαμβάνει τον βαθμό ακεραιότητας των Windows Vista.

-w	Δείχνει τα αντικείμενα που έχουν δικαίωμα εγγραφής.

Το *file* μπορεί να είναι επίσης κατάλογος, κλειδί μητρώου, υπηρεσία, διεργασία και αντικείμενο.

7.5.2 AccessEnum

Το **AccessEnum** είναι εργαλείο με γραφικό περιβάλλον, το οποίο δείχνει τα δικαιώματα εγγραφής και ανάγνωσης των χρηστών και ομάδων για εκάστοτε καταλόγους και κλειδιά μητρώου.
Για να εμφανίσει τα αποτελέσματα, το εργαλείο χρησιμοποιεί τα APIs ασφαλείας των Windows.

Απλό στην χρήση, απλώς επιλέγετε είτε τον κατάλογο αρχείων είτε τα κλειδιά μητρώου που θέλετε και πατάτε Scan για να δείτε τα αποτελέσματα σε 4 στήλες, την διαδρομή, το δικαίωμα την ανάγνωσης, το δικαίωμα της εγγραφής και ποιοι δεν έχουν κανένα δικαίωμα.

Κατάλληλο για να βρείτε τρύπες ασφαλείας στο σύστημα.

7.5.3 Autoruns

Το **Autoruns** παρουσιάζει τα προγράμματα που είναι ρυθμισμένα να φορτώνουν αυτόματα με το άνοιγμα του συστήματος και με την σύνδεση του χρήστη. Επίσης, εμφανίζει μια πλήρη λίστα με τις τοποθεσίες σε μητρώο και αρχεία όπου οι εφαρμογές μπορούν να ρυθμιστούν για την αυτόματη εκκίνηση.
Το εργαλείο υπάρχει και σε command line, αλλά και με γραφικό περιβάλλον. Εμείς θα μιλήσουμε για το δεύτερο, καθώς είναι πιο εύχρηστο και ευανάγνωστο και θα μας βοηθήσει πιο πολύ στην έρευνα που διεξάγουμε.

Δείχνει οτιδήποτε πρόγραμμα και υπηρεσία είναι, είτε είναι της Microsoft είτε ανεξάρτητο. Μπορεί επίσης να δείξει τι φορτώνονται όταν ανοίγουν συγκεκριμένα προγράμματα των Windows, όπως τα codecs για το Windows Media Player και τα add-ons για τον Internet Explorer.

Με το που ανοίγει το **Autoruns**, κατευθείαν εμφανίζονται όλα τα προγράμματα και στοιχεία που φορτώνονται αυτόματα. Έξι στήλες εμφανίζονται στα αποτελέσματα:

1. το όνομα της εγγραφής
2. η περιγραφή της
3. ο εκδότης
4. η διαδρομή του αρχείου
5. η ημερομηνία δημιουργίας του αρχείου
6. η αξιολόγηση της VirusTotal για το κατά πόσο θεωρείτο επιβλαβές το αρχείο

Επίσης, τις εγγραφές τις ταξινομεί αλφαβητικά μόνο και ανάλογα με την τοποθεσία, οπότε είναι πιο εύκολο να βρεθεί κάτι. Και εκτός από το να εμφανίζει όλες τις εγγραφές μαζί, μπορεί να τις εμφανίσει σε ξεχωριστές καρτέλες, ανάλογα με τον τύπο του αρχείου, δηλαδή:

- AppInit
- Boot Execute

- Codecs
- Drivers
- Explorer
- Image Hijacks
- Internet Explorer
- KnownDLLs
- Logon
- LSA Providers
- Network Providers
- Print Monitors
- Scheduled Tasks
- Services
- Sidebar Gadgets
- Winlogon
- Winsock Providers
- WMI

Τα αποτελέσματα μπορούν να αποθηκευτούν σε αρχεία με επέκταση **.arn** ώστε να φορτωθούν μετά και να συγκριθούν με άλλα αποτελέσματα.

7.5.4 EFSDump

Το **EFSDump** δείχνει ποιοι λογαριασμοί έχουν πρόσβαση σε κρυπτογραφημένα αρχεία.

Χρησιμοποιεί το API *QueryUsersOnEncryptedFile*, το οποίο δημιουργήθηκε για να εξυπηρετεί τους χρήστες, καθώς στα Windows 2000 εμφανίστηκε για πρώτη φορά το Encrypting File System, το οποίο χρησιμοποιείται για την προστασία των ευαίσθητων δεδομένων των χρηστών.

Η σύνταξη της εντολής είναι:

efsdump [options] <*file* | *directory*>

-s	Αναδρομική αναζήτηση στους υποκαταλόγους.
-q	Δεν εμφανίζει τα μηνύματα λάθους.

7.5.5 FindLinks

Το **FindLinks** εμφανίζει τον δείκτη ενός αρχείου και εναλλακτικές διαδρομές, δηλαδή συντομεύσεις που υπάρχουν στο ίδιο partition.

Δεν είναι απαραίτητο οι συντομεύσεις να έχουν τον ίδιο ακριβώς τίτλο με το αρχικό αρχείο, καθώς αρκεί να συμπεριλαμβάνεται ο τίτλος μέσα στο όνομα αρχείου.

Η σύνταξη της εντολής είναι:

findlinks <*file*>

7.5.6 ListDLLs

Το **ListDLLs** εμφανίζει τα DLLs, τα οποία χρησιμοποιούνται σε διεργασίες. Μπορεί να δείξει τα DLLs που χρησιμοποιούν συγκεκριμένες διεργασίες ή και το αντίστροφο, δηλαδή τις διεργασίες που χρησιμοποιούν ένα συγκεκριμένο DLL.

Η σύνταξη της εντολής είναι:

listdlls [options] [process | pid]

-d *dllname*	Δείχνει μόνο τις διεργασίες που έχουν φορτώσει το συγκεκριμένο DLL.
-r	Επισημαίνει τα DLLs που μετακινήθηκαν διότι δεν φορτώθηκαν από την βασική τους διεύθυνση.
-u	Εμφανίζει μόνο τα DLLs που δεν έχουν ψηφιακή υπογραφή.
-v	Εμφανίζει τις πληροφορίες έκδοσης των DLL.

Η εντολή μπορεί να δεχτεί είτε το όνομα του DLL είτε το όνομα ή το id της διεργασίας, όχι και τα δύο.

7.5.7 LogonSessions

Το **LogonSessions** εμφανίζει τις ενεργές συνεδρίες του συστήματος, καθώς επίσης και τις διεργασίες που τρέχουν σε κάθε συνεδρία.

Η σύνταξη της εντολής είναι:

logonsessions [-p]

Αν η εντολή εκτελεστεί σκέτη, θα εμφανίσει διάφορες πληροφορίες για τις ενεργές συνεδρίες, όπως τον αριθμό της, το όνομα του χρήστη, το Sid και την ώρα σύνδεσης.

Με την επιλογή –p, εμφανίζονται οι ίδιες πληροφορίες και επιπροσθέτως μια λίστα με τις διεργασίες που τρέχουν σε κάθε συνεδρία και συγκεκριμένα το Pid και το όνομα της διεργασίας.

7.5.8 NTFSInfo

Το **NTFSInfo** εμφανίζει πληροφορίες για τους NTFS τόμους του συστήματος, όπως επίσης και για τον MFT.

Το εργαλείο δουλεύει για όλες τις εκδόσεις του NTFS, αλλά στο NTFS των Windows 2000, υπάρχουν διαφορετικά αρχεία μεταδεδομένων τα οποία δεν μπορεί να διαβάσει το εργαλείο.

Η σύνταξη της εντολής είναι:

ntfsinfo <*drive letter*>

Στο αποτέλεσμα φαίνονται 4 ενότητες πληροφοριών:

- **Volume Size**, για συνολικό και ελεύθερο χώρο σε MB, καθώς επίσης και πλήθος clusters και sectors.
- **Allocation Size**, για μέγεθος σε bytes των sector και cluster.
- **MFT Information**, για μέγεθος του πίνακα MFT και της ζώνης MFT, καθώς και από ποια clusters ξεκινάνε.
- **Meta-Data files**, για τα αρχεία μεταδεδομένων, όπως το $boot.

Κάποιες πληροφορίες μπορεί να μην εμφανίζονται, ανάλογα με το σύστημα και την έκδοση του NTFS.

7.5.9 Process Explorer

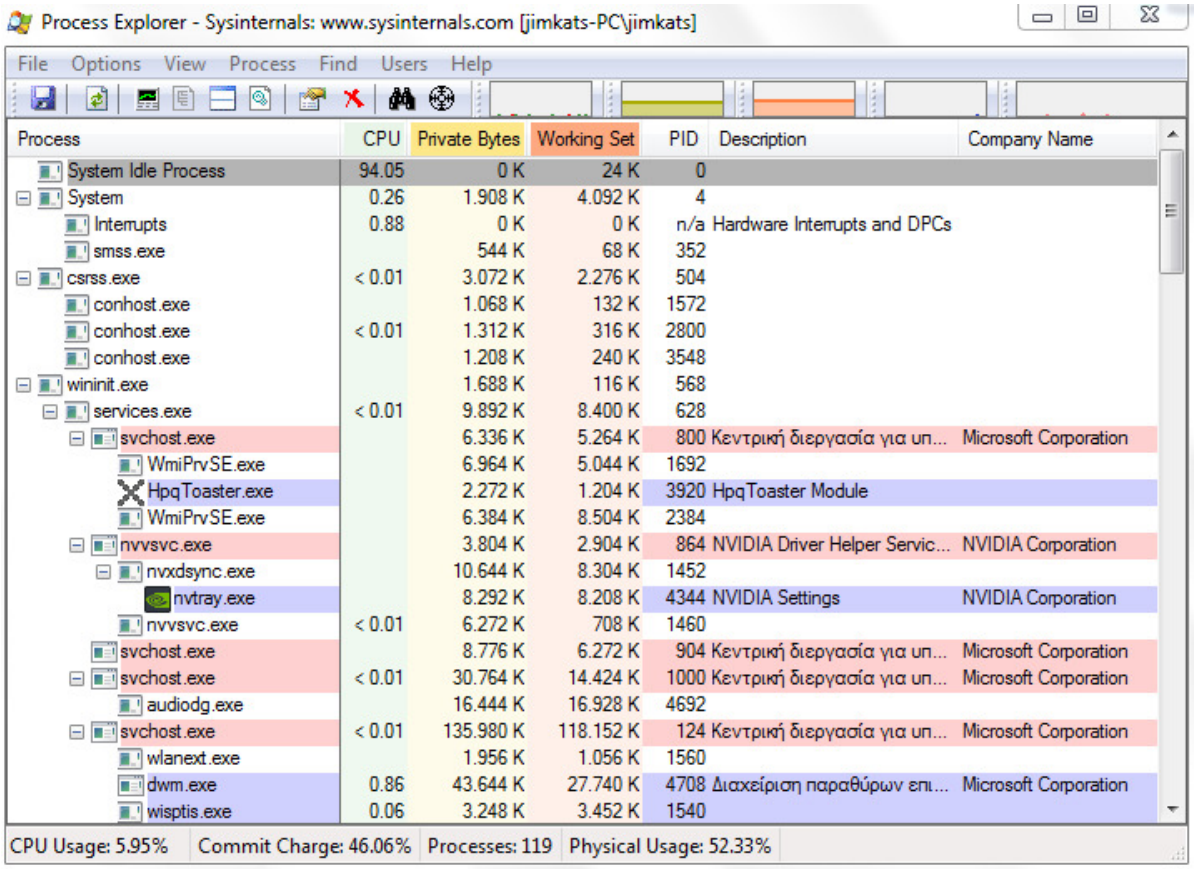
Το **Process Explorer** δείχνει ποιές διεργασίες είναι ανοιχτές, ποια αρχεία των διεργασιών εκτελούνται, ποια κλειδιά του μητρώου είναι ανοιχτά και άλλα. Γενικά δίνει πολύ περισσότερες πληροφορίες για τις διεργασίες από ότι ο Task Manager και ταυτόχρονα λειτουργεί όπως ο Task Manager, δηλαδή παύση και εκκίνηση διεργασιών και υπηρεσιών.

Μέσω γραφικού περιβάλλοντος μπορεί κανείς να δει γραφήματα με live καταγραφή χρήσης CPU και RAM, να δει διάφορες πληροφορίες για κάθε διεργασία, όπως τα νήματα που χρησιμοποιεί, τον βαθμό επικινδυνότητας από την VirusTotal, εκτυπώσιμα strings που υπάρχουν στο αρχείο και άλλα πολλά.

Πιο αναλυτικά, όταν ανοίγει κανείς τον Process Explorer, βλέπει 7 στήλες:

- **Process**, το όνομα της διεργασίας.
- **CPU**, το ποσοστό που καταναλώνει από την χρησιμοποιημένη CPU την στιγμή εκείνη.
- **Private Bytes**, η μνήμη που χρησιμοποιεί από το σύστημα σε bytes.
- **Working Set**, η συνολική μνήμη RAM που χρησιμοποιεί.
- **PID**, το Process ID.
- **Description**, περιγραφή της διεργασίας.
- **Company Name**, το όνομα της εταιρίας που έχει δημιουργήσει το αρχείο.

Στο κάτω μέρος του παραθύρου μας δείχνει σε ποσοστά την χρήση CPU και RAM, καθώς επίσης και το πλήθος των διεργασιών που τρέχουν εκείνη την στιγμή.



Εικόνα 7.3: Process Explorer

Όταν κάνουμε δεξί κλικ σε μια διεργασία, βλέπουμε το ίδιο ακριβώς μενού όπως στον Task Manager. Στις ιδιότητες βλέπουμε πολλές χρήσιμες πληροφορίες σε συνολικά 11 καρτέλες:

- **Image**, όπως οι γενικές ιδιότητες ενός αρχείου συστήματος και της συντόμευσης της.
- **Performance**, πληροφορίες χρήσης CPU, RAM και εικονικής μνήμης.
- **Performance Graph**, τα ίδια σχεδόν σε γραφήματα.
- **Disk and Network**, το I/O της διεργασίας σε δίκτυο και δίσκο.
- **GPU Graph**, γραφήματα χρήσης της GPU και της μνήμης της.
- **Services**, οι υπηρεσίες που συνδέονται με την διεργασία.
- **Threads**, τα νήματα που χρησιμοποιούνται και μερικές πληροφορίες γι' αυτά.
- **TCP/IP**, οι δικτυακές συνδέσεις της διεργασίας.
- **Security**, πληροφορίες για την ασφάλεια του συστήματος.
- **Environment**, πληροφορίες για το περιβάλλον του συστήματος, όπως η αρχιτεκτονική.
- **Strings**, τα εκτυπώσιμα strings της διεργασίας.

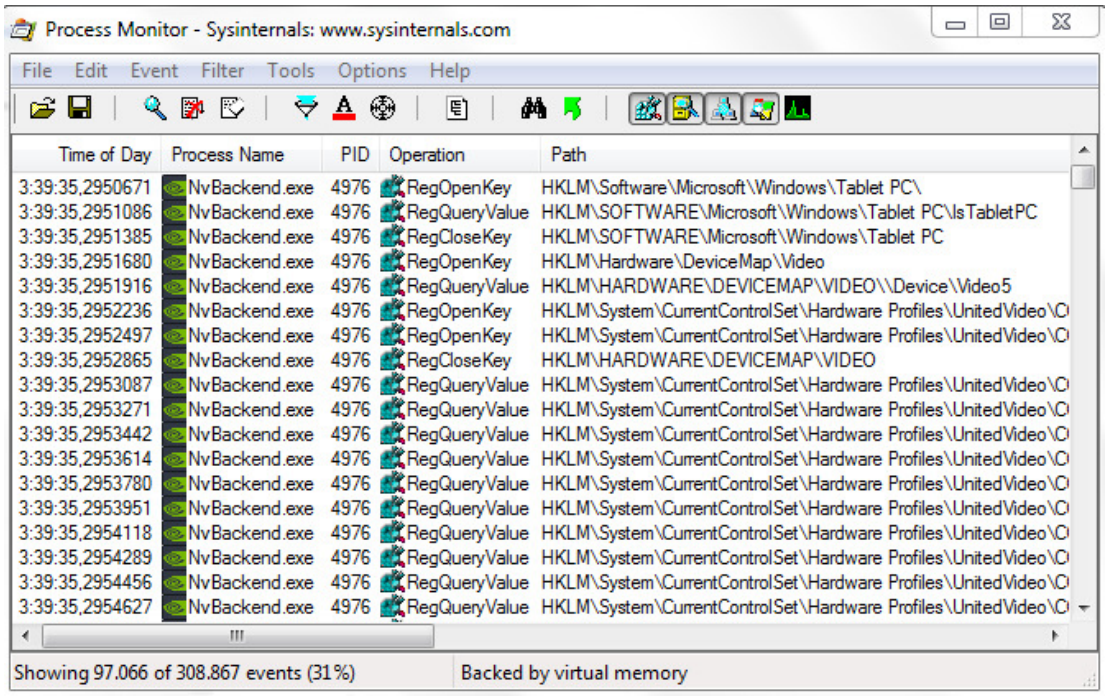
7.5.10 Process Monitor

Το **Process Monitor** καταγράφει και εμφανίζει σε πραγματικό χρόνο όλη την δραστηριότητα του συστήματος, δηλαδή οποιαδήποτε γεγονότα συμβαίνουν και ότι αλλαγές γίνονται στο σύστημα και στο μητρώο. Το πρόγραμμα αυτό αποτελεί τον συνδυασμό του **FileMon** και του **Regmon**.

Μέσω ενός γραφικού περιβάλλοντος παρόμοιο με αυτό του Process Explorer, ο χρήστης με ευκολία μπορεί να δει ποιές διεργασίες κάνουν τι ενέργεια σε ποιό μέρος του μητρώου, κάποια συνοπτικά στατιστικά και διάφορες πληροφορίες.

Πιο αναλυτικά, με το που τρέχει η εφαρμογή, εμφανίζονται οι εξής στήλες:

- **Time of Day**, η χρονική στιγμή όπου έγινε η σύλληψη του γεγονότος.
- **Process Name**, το όνομα της διεργασίας.
- **PID**, το ID της διεργασίας.
- **Operation**, η λειτουργία που εκτελεί.
- **Path**, η διαδρομή στην οποία εκτελείται η λειτουργία.
- **Result**, η κατάσταση του αποτελέσματος της λειτουργίας.
- **Detail**, πληροφορίες σχετικά με την λειτουργία.



Εικόνα 7.4: Process Monitor

Στην πάνω μπάρα, υπάρχουν επιλογές όπως διαχείριση της διαδικασίας σύλληψης διεργασιών, αναζήτηση και φιλτράρισμα των εγγραφών.

Με δεξί κλικ πάνω στην μπάρα των στηλών, μπορεί κανείς να επιλέξει ποιες στήλες να εμφανίζονται.

Με διπλό κλικ πάνω σε μια εγγραφή, εμφανίζονται οι ιδιότητες της όπου αναφέρονται πολλά στοιχεία για την διεργασία και την ενέργεια της

7.5.11 PsTools

Το **PsTools** είναι ένα σετ εργαλείων. Περιέχει διάφορα εργαλεία τα οποία βρίσκουν διάφορες πληροφορίες, όπως τους συνδεμένους χρήστες - τοπικά ή απομακρυσμένα -, τις τρέχουσες διεργασίες, το περιεχόμενο των αρχείων καταγραφής συμβάντων, κ.α..

Παρακάτω θα δούμε τα εργαλεία που μας δίνουν χρήσιμες πληροφορίες για την έρευνα μας.

7.5.11.1 PsFile

Το **PsFile** δείχνει ποιά αρχεία έχουν ανοιχτεί απομακρυσμένα στον υπολογιστή όπου βρισκόμαστε. Ταυτόχρονα δίνει την δυνατότητα να κλείσουμε αυτά τα αρχεία.

Η σύνταξη της εντολής είναι:

psfile [\\computer] [id | path] [options]

-c	Κλείνει τα αρχεία που έχουν προσδιοριστεί από το ID ή την διαδρομή.
-p *pass*	Προσδιορίζει τον κωδικό για την χρήστη. Εάν παραλειφθεί, θα ζητηθεί να γραφτεί ο κωδικός στα κρυφά.
-u *user*	Προσδιορίζει όνομα χρήστη για την σύνδεση σε απομακρυσμένο υπολογιστή.

Εάν η εντολή γραφτεί σκέτη, δηλαδή **psfile**, θα δείξει τα αρχεία που είναι ανοιχτά στο τοπικό σύστημα.

Για ενέργειες σε άλλον υπολογιστή του δικτύου, αρκεί να προσδιοριστεί στο *computer*.

7.5.11.2 PsGetSid

Το **PsGetSid** μεταφράζει τα SIDs, τα οποία είναι τα Security IDs, στο εμφανιζόμενο όνομα και αντιστρόφως. Η εντολή μπορεί να λειτουργήσει και λειτουργήσει εκτός από το τοπικό σύστημα και να δείξει τα SIDs και τα ονόματα τους όπως ισχύουν σε άλλους υπολογιστές που ενεργοί στο δίκτυο.

Η σύνταξη της εντολής είναι:

psgetsid [\\computer | computer | @file] [options] [account | sid]

-p *pass*	Ορίζει τον κωδικό για τον χρήστη. Εάν παραλειφθεί, θα ζητηθεί να γραφτεί ο κωδικός στα κρυφά.
-u *user*	Ορίζει το όνομα χρήστη για την σύνδεση σε απομακρυσμένο υπολογιστή.

Εάν η εντολή γραφτεί σκέτη, θα εμφανιστεί το SID του τοπικού συστήματος.

Για να εκτελεστεί η εντολή σε άλλον υπολογιστή στο δίκτυο, μπαίνει το *computer*. Εάν πρόκειται για όλους τους υπολογιστές του δικτύου, μπαίνει το *. Εάν πρόκειται για συγκεκριμένους υπολογιστές, χρησιμοποιείται το *@file*, το οποίο παραπέμπει σε αρχείο όπου είναι καταχωρημένα τα ονόματα των υπολογιστών στους οποίους θα γίνει η σύνδεση.

Εάν επιζητείται το SID ενός λογαριασμού, γράφουμε **psgetsid** *account*, ενώ αν θέλουμε το όνομα του λογαριασμού για ένα συγκεκριμένο SID, γράφουμε **psgetsid** *sid*.

7.5.11.3 PsInfo

Το **PsInfo** παρουσιάζει τις πληροφορίες είτε του τοπικού είτε ενός απομακρυσμένου συστήματος.

Η σύνταξη της εντολής είναι:

psinfo [\\computer | computer | @file] [options] [filter]

-c	Τυπώνει το αποτέλεσμα σε μορφή CSV.
-d	Εμφανίζει πληροφορίες για τον τόμο του δίσκου.
-h	Εμφανίζει τις εγκατεστημένες επείγουσες διορθώσεις του λειτουργικού.
-p *pass*	Ορίζει τον κωδικό για τον χρήστη. Εάν παραλειφθεί, θα ζητηθεί να γραφτεί ο κωδικός στα κρυφά.
-s	Εμφανίζει όλες τις εγκατεστημένες εφαρμογές στο λειτουργικό σύστημα.
-t	Αλλάζει τον διαχωριστικό χαρακτήρα για την επιλογή **–c**, όπου από προεπιλογή είναι το κόμμα.
-u *user*	Ορίζει το όνομα χρήστη για την σύνδεση σε απομακρυσμένο υπολογιστή.

Η **PsInfo** μπορεί να χειριστεί με τον ίδιο τρόπο όπως η **PsGetId** όσον αφορά το τοπικό και τα απομακρυσμένα συστήματα.

Το φίλτρο που μπαίνει στο τέλος της εντολής, δείχνει μεμονωμένες πληροφορίες και όχι όλες τις πληροφορίες απ' αυτές που δείχνει από προεπιλογή.

7.5.11.4 PsLoggedOn

Το **PsLoggedOn** εμφανίζει τους χρήστες που είναι συνδεδεμένους σε ένα τοπικό ή απομακρυσμένο σύστημα. Δείχνει επίσης τους χρήστες που είναι συνδεδεμένοι απομακρυσμένα σε ένα σύστημα και την ώρα που συνδέθηκαν.

Η σύνταξη της εντολή είναι:

psloggedon [options] [\\computer | username]

-l	Εμφανίζει μόνο τις τοπικές συνδέσεις.
-x	Δεν εμφανίζει τους χρόνους που πραγματοποιήθηκαν οι συνδέσεις.

Με την χρήση ενός ονόματος υπολογιστή, θα δούμε ποιοι είναι συνδεδεμένοι σ' αυτό τον υπολογιστή.

Με την χρήση ενός ονόματος χρήστη, θα δούμε αν είναι συνδεδεμένος και σε ποιόν υπολογιστή.

Το **PsLoggedOn**, όσον αφορά τους τοπικούς χρήστες, για να δείξει ποιοι είναι, σαρώνει τα SID που βρίσκονται στο HKEY_USERS στο μητρώο, όπου στην ουσία είναι οι ενεργές συνεδρίες και από εκεί εξάγει τα ονόματα τους. Για τους απομακρυσμένους χρήστες, γίνεται χρήση του API του **NetSessionEnum**.

7.5.11.5 PsLogList

Το **PsLogList** εμφανίζει το ιστορικό καταγραφής γεγονότων είτε τοπικού είτε απομακρυσμένου συστήματος. Το ίδιο πράγμα δηλαδή όπως η Προβολή Συμβάντων των Windows, αλλά σε πιο εύχρηστη και ευανάγνωστη μορφή.

Η σύνταξη της εντολής είναι:

psloglist [\\computer | @file [-u user] [-p pass]] [options] *eventlog*

-a *mm/dd/yy*	Εμφανίζει καταγραφές μετά από ορισμένη ημερομηνία.
-b *mm/dd/yy*	Εμφανίζει καταγραφές πριν από ορισμένη ημερομηνία.
-c	Καθαρίζει το event log μετά την εμφάνιση.
-d *n*	Εμφανίζει καταγραφές από τις προηγούμενες *n* μέρες.
-e *ID*	Εξαιρεί γεγονότα με συγκεκριμένο *ID* ή *IDs*. Το μέγιστο 10.
-f filter	Φιλτράρει τύπου γεγονότων με βάση το string.
-h *n*	Εμφανίζει καταγραφές από τις προηγούμενες *n* ώρες.
-i *ID*	Εμφανίζει γεγονότα με συγκεκριμένο ID ή IDs. Το μέγιστο 10.
-l *file*	Παρουσιάζει τις καταγραφές από το ορισμένο αρχείο καταγραφής.
-m *n*	Εμφανίζει καταγραφές από τα προηγούμενα *n* λεπτά.
-n *n*	Εμφανίζει τις τελευταίες *n* καταγραφές.
-o *source*	Εμφανίζει καταγραφές από την ορισμένη πηγή ή πηγές γεγονότων.
-p *pass*	Ορίζει τον κωδικό για τον χρήστη. Εάν παραλειφθεί, θα ζητηθεί να γραφτεί ο κωδικός στα κρυφά.
-q *source*	Παραλείπει καταγραφές από την ορισμένη πηγή ή πηγές γεγονότων.
-r	Εμφανίζει τις καταγραφές με αύξουσα σειρά.
-s	Τυπώνει τις καταγραφές γραμμή-γραμμή.
-t	Ορίζει χαρακτήρα για διαχωριστικό. Από προεπιλογή είναι το κόμμα.
-u *user*	Ορίζει το όνομα χρήστη για την σύνδεση σε απομακρυσμένο υπολογιστή.
-w	Αναμένει για καινούργια γεγονότα και ύστερα τα παρουσιάζει. Μόνο για το τοπικό σύστημα.
-x	Εμφανίζει εκτεταμένα δεδομένα.

Η **PsLogList** μπορεί να χειριστεί με τον ίδιο τρόπο όπως τα προηγούμενα εργαλεία όσον αφορά το τοπικό και τα απομακρυσμένα συστήματα.

Στο **–f**, το φίλτρο μπορεί να είναι για παράδειγμα w ώστε να εξαιρεθούν οι προειδοποιήσεις.

Για όλες τις επιλογές, εκτός της **–r**, οι καταγραφές παρουσιάζονται με φθίνουσα σειρά.

Η επιλογή **–s** είναι κατάλληλη όταν θέλουμε να εξάγουμε τα δεδομένα σε υπολογιστικό φύλλο ή όταν θέλουμε να κάνουμε αναζήτηση με κάποιο ειδικό εργαλείο.

7.5.11.6 PsService

Το **PsService** εμφανίζει τις υπηρεσίες και μπορεί και να τις χειριστεί, δηλαδή να τις εκκινήσει, να τις σταματήσει και να τις επανεκκινήσει.

Η σύνταξη της εντολής είναι:

psservice [\\computer [-u user] [-p pass] [commands] [options]

config *svc*	Εμφανίζει την ρύθμιση της δοσμένης υπηρεσίας.

cont *svc*	Επαναφέρει μια σταματημένη υπηρεσία.
depend *svc*	Παρουσιάζει σε λίστα τις υπηρεσίες που εξαρτώνται από την δοσμένη.
find *svc* [*all*]	Αναζητά στο δίκτυο την δοσμένη υπηρεσία. Από προεπιλογή, αναζητά ενεργές παρουσίες την υπηρεσίας, ενώ με την επιλογή *all* αναζητά και τις ανενεργές.
pause *svc*	Κάνει παύση την ενεργή υπηρεσία που έχει δοθεί.
query	Εμφανίζει πληροφορίες για όλες τις υπηρεσίες.
query *svc*	Εμφανίζει πληροφορίες για την δοσμένη υπηρεσία.
query –g *group*	Εμφανίζει υπηρεσίες που ανήκουν σε συγκεκριμένη ομάδα.
query –t *type*	Εμφανίζει τις υπηρεσίες συγκεκριμένου τύπου.
query –s *state*	Εμφανίζει τις υπηρεσίες ανάλογα με την κατάσταση.
restart *svc*	Επανεκκινεί την δοσμένη υπηρεσία.
security *svc*	Αναφέρει τα δικαιώματα πρόσβασης της συγκεκριμένης υπηρεσίας.
setconfig *svc start-type*	Θέτει το τύπο εκκίνησης της συγκεκριμένης υπηρεσίας.
start *svc*	Εκκινεί την δοσμένη υπηρεσία.
stop *svc*	Σταματάει την δοσμένη υπηρεσία.
–p *pass*	Ορίζει τον κωδικό για τον χρήστη. Εάν παραλειφθεί, θα ζητηθεί να γραφτεί ο κωδικός στα κρυφά.
–u *user*	Ορίζει το όνομα χρήστη για την σύνδεση σε απομακρυσμένο υπολογιστή.

Η **PsService** μπορεί να χειριστεί με τον ίδιο τρόπο όπως τα προηγούμενα εργαλεία όσον αφορά το τοπικό και τα απομακρυσμένα συστήματα.

Για την εντολή **query –t**, οι τύποι που υπάρχουν είναι:

1. **driver**, για τους οδηγούς συσκευών.
2. **service**, για τις υπηρεσίες Win32. Προεπιλογή.
3. **interactive**, για τις διαδραστικές υπηρεσίες Win32.
4. **all**, για όλα τα παραπάνω.

Για την εντολή **query –s**, οι καταστάσεις που υπάρχουν είναι:

1. **active**, για τις ενεργές υπηρεσίες.
2. **inactive**, για τις ανενεργές υπηρεσίες.
3. **all**, και για τις δύο καταστάσεις. Προεπιλογή.

Για την εντολή **setconfig**, οι διαθέσιμοι τύποι εκκίνησης είναι:

1. **auto**, για αυτόματα.
2. **demand**, για μη-αυτόματα.
3. **disable**, για απενεργοποιημένη.

7.5.12 ShareEnum

Το **ShareEnum**, είναι εργαλείο με γραφικό περιβάλλον, το οποίο εμφανίζει τα κοινόχρηστα στοιχεία του υπολογιστή, τα οποία μπορεί να είναι κάποιοι φάκελοι στον δίσκο, ακόμη και εκτυπωτής που είναι συνδεδεμένος πάνω του και τι δικαιώματα έχουν οι χρήστε πάνω του.

Πιο συγκεκριμένα, αφού πρώτα επιλεγεί το domain και πατηθεί το **Refresh**, εμφανίζονται πληροφορίες σε 8 στήλες:

- **Share Path**, η διαδρομή με την οποία γίνεται κοινή χρήση στο δίκτυο.

- **Local Path**, η διαδρομή στο σύστημα μας.
- **Domain**, σε ποιο domain υπάγεται.
- **Type**, το είδος του κοινόχρηστου στοιχείου.
- **Everyone**, τα δικαιώματα που όλοι έχουν.
- **Other Read**, ποιοι έχουν δικαίωμα ανάγνωσης.
- **Other Write**, ποιοι έχουν δικαίωμα εγγραφής.
- **Deny**, ποιοι δεν έχουν δικαιώματα στα κοινόχρηστα στοιχεία.

Τα αποτελέσματα μπορούν να γίνουν εξαγωγή σε *.txt* αρχείο.

7.5.13 Sigcheck

Το **Sigcheck** δείχνει πληροφορίες για την έκδοση και την ψηφιακή υπογραφή ενός αρχείου. Επιπλέον δίνει την δυνατότητα ελέγχου του αρχείου στο VirusTotal.

Η σύνταξη της εντολής είναι:

sigcheck [options] <*file* | *directory*>

-a	Εμφανίζει περαιτέρω πληροφορίες έκδοσης. Η εντροπία είναι τα bits ανά byte πληροφορίας στο περιεχόμενο του αρχείου.
-c	Έξοδος σε μορφή CSV με κόμμα ως διαχωριστικό.
-ct	Έξοδος σε μορφή CSV με καρτέλες ως διαχωριστικά.
-d	Κρατάει το περιεχόμενο ενός αρχείου καταλόγου.
-e	Σαρώνει τα εκτελέσιμα αρχεία.
-f *catalog_file*	Κοιτάει την υπογραφή του δοθέντος αρχείου καταλόγου.
-h	Δείχνει τα hashes των αρχείων.
-i	Δείχνει το όνομα του καταλόγου και τους υπογράφοντες των αρχείων.
-l	Κοιτάει στα αρχικά αρχεία αντί των συντομεύσεων και των κόμβων καταλόγων.
-m	Κρατάει το μανιφέστο.
-n	Δείχνει μόνο τον αριθμό έκδοσης του αρχείου.
-q	Δεν εμφανίζει τις επικεφαλίδες στο αποτέλεσμα.
-r	Να μην ελέγξει για ανάκληση πιστοποιητικού.
-s	Ψάχνει αναδρομικά στους καταλόγους.
-t	Κρατάει τα περιεχόμενα συγκεκριμένου αποθηκευτικού χώρου πιστοποιητικών. * για όλους τους χώρους.
-tu	Κοιτάει στους αποθηκευτικούς χώρους του χρήστη. Από προεπιλογή κοιτάει στης μηχανής.
-u	Δείχνει τα αρχεία που είναι άγνωστα στο VirusTotal ή δεν έχουν μηδενική βαθμολογία, αλλιώς εμφανίζει μόνο τα μην υπογεγραμμένα αρχεία.
-v	Ερώτημα στο VirusTotal για malware βασισμένο στο hash του αρχείου. Τα αποτελέσματα μπορεί να μην είναι διαθέσιμα για τουλάχιστον πέντε λεπτά.
-vr[s]	Ανοίγει τις αναφορές για αρχεία με μη μηδενική βαθμολογία. Με την επιλογή **s** θα ανεβαίνουν στο VirusTotal αρχεία που δεν έχουν ελεγχθεί προηγουμένως.
-vt	Έλεγχος και αποδοχή των όρων χρήσης της υπηρεσίας του VirusTotal.

Το εργαλείο μπορεί να χρησιμοποιηθεί για έλεγχο και επαλήθευση των ψηφιακών υπογραφών των αρχείων του συστήματος, ώστε να βεβαιωθούμε ότι δεν υπάρχει κάποιο κακόβουλο λογισμικό ανάμεσα τους.

7.5.14 Streams

Το **Streams** δίνει την δυνατότητα εύρεσης εναλλακτικών ροών δεδομένων των αρχείων και των καταλόγων, οι οποίες εναλλακτικές ροές υποστηρίζονται από το NTFS.

Αυτές οι εναλλακτικές ροές δεν χρησιμοποιούνται από προεπιλογή, όμως μπορεί κανείς να τις χρησιμοποιήσει με την σύνταξη **file:stream**. Δημιουργούνται με την εντολή **echo message > example:stream**. Σε οποιαδήποτε περίπτωση, αυτά τα αρχεία φαίνονται άδεια και με μέγεθος *0 byte*. Ο μόνος τρόπος για να διαβάσει κανείς αυτά τα αρχεία, για τα οποία είναι γνωστά ότι χρησιμοποιούν εναλλακτικές ροές, είναι **more < example:stream**.

Η σύνταξη της εντολής Streams είναι απλή:

streams [options] <*file* | *directory*>

-d	Διαγράφει τις ροές.
-s	Αναζητά αναδρομικά στους υποκαταλόγους. Απαραίτητο και για τον ίδιο κατάλογο.

Η **Streams** μόνο εντοπίζει τα αρχεία που έχουν εναλλακτικές ροές. Για να τα διαβάσουμε αυτά τα αρχεία, όπως προαναφέραμε χρησιμοποιούμε την **more**.

7.5.15 Strings

Το **Strings** μπορεί να βρει Unicode ή ASCII strings με ελάχιστο μήκος τους 3 χαρακτήρες σε ένα δυαδικό αρχείο. Μπορεί να λειτουργήσει και σε Windows 95.

Η βασική του λειτουργία μοιάζει με την εντολή **strings** των Unix, όμως οι επιλογές διαφέρουν.

Η σύνταξη της εντολής είναι:

strings [options] <*file* | *directory*>

-a	Αναζήτηση μόνο για ASCII.
-b *bytes*	Πόσα bytes από το αρχείο να σαρώσει.
-f *offset*	Από ποιο όφσετ του αρχείου να αρχίσει να σαρώνει.
-n *length*	Ελάχιστο μήκος του string.
-o	Τυπώνει το όφσετ του αρχείου στο οποίο εντοπίστηκε το string.
-q	Χωρίς επικεφαλίδες.
-s	Αναδρομική αναζήτηση στους υποκαταλόγους.
-u	Αναζήτηση μόνο για Unicode.

Χωρίς τις επιλογές **–a** και **–u** η εντολή αναζητά και για Unicode και για ASCII.

7.5.16 TCPView

Το **TCPView** είναι εργαλείο με γραφικό περιβάλλον το οποίο εμφανίζει τις ενεργές συνδέσεις που τρέχουν από τις υπηρεσίες του υπολογιστή. Στην ουσία λειτουργεί όπως η netstat, αλλά με περισσότερες πληροφορίες.

Όταν κάποιος τρέχει το πρόγραμμα, βλέπει στα αποτελέσματα δώδεκα στήλες:

- **Process**, το όνομα της διεργασίας.
- **PID**, το ID της διεργασίας.
- **Protocol**, το πρωτόκολλο που χρησιμοποιείται στην μεταφορά των δεδομένων.
- **Local Address**, η διεύθυνση της πηγής.
- **Local Port**, η θύρα της πηγής.
- **Remote Address**, η διεύθυνση προορισμού.
- **Remote Port**, η θύρα προορισμού.
- **State**, η κατάσταση της σύνδεσης.
- **Sent Packets**, το πλήθος των πακέτων που στάλθηκαν.
- **Sent Bytes**, τα bytes που στάλθηκαν.
- **Rcvd Packets**, το πλήθος των ληφθέντων πακέτων.
- **Rcvd Bytes**, τα bytes που ελήφθησαν.

Στο κάτω μέρος του παραθύρου βλέπουμε το σύνολο των συνδέσεων, πόσες έχουν καθιερωθεί και άλλου είδους συνδέσεις.

Δίδεται η δυνατότητα μέσω του μενού να μην προβάλλονται οι μη εγκατεστημένες συνδέσεις και να αλλάζουμε τον ρυθμό ανανέωσης των πληροφοριών των συνδέσεων.

Επίσης, μπορούμε να δούμε πληροφορίες για έναν απομακρυσμένο host με το **whois** που υπάρχει στο μενού.

Οι πληροφορίες που παρουσιάζονται μπορούν να αποθηκευτούν σε αρχείο **.txt**.

7.6 The Sleuth Kit (TSK)

Το **TSK** είναι ένα σύνολο εργαλείων χρήσιμων για την εγκληματολογία μέσων αποθήκευσης. Αφορά τα Windows και τα Unix συστήματα.

Επειδή περιέχει εργαλεία γραμμής εντολών, συνήθως χρησιμοποιείται σε συνδυασμό με την επέκταση **Autopsy**, το οποίο προσφέρει περιβάλλον διεπαφής για τον χρήστη. Το **Autopsy** δεν περιέχεται μαζί με το **TSK** και πρέπει να ληφθεί ξεχωριστά.

Εκτελώντας κανείς το **Autopsy**, του εμφανίζει ένα μικρό παραθυράκι όπου επιλέγει για φόρτωμα ή δημιουργία νέας υπόθεσης.

Για την δημιουργία νέας υπόθεσης, δίδεται το όνομα της υπόθεσης και ο κατάλογος στον οποίο θα αποθηκεύονται τα αρχεία. Μετά δίδεται ο αριθμός της υπόθεσης και ο εξεταστής.

Έπειτα, πρέπει να επιλεγεί η πηγή των δεδομένων και αυτό γίνεται ανάμεσα σε τρείς τύπους πηγών:

1. **Image File** και συγκεκριμένα:

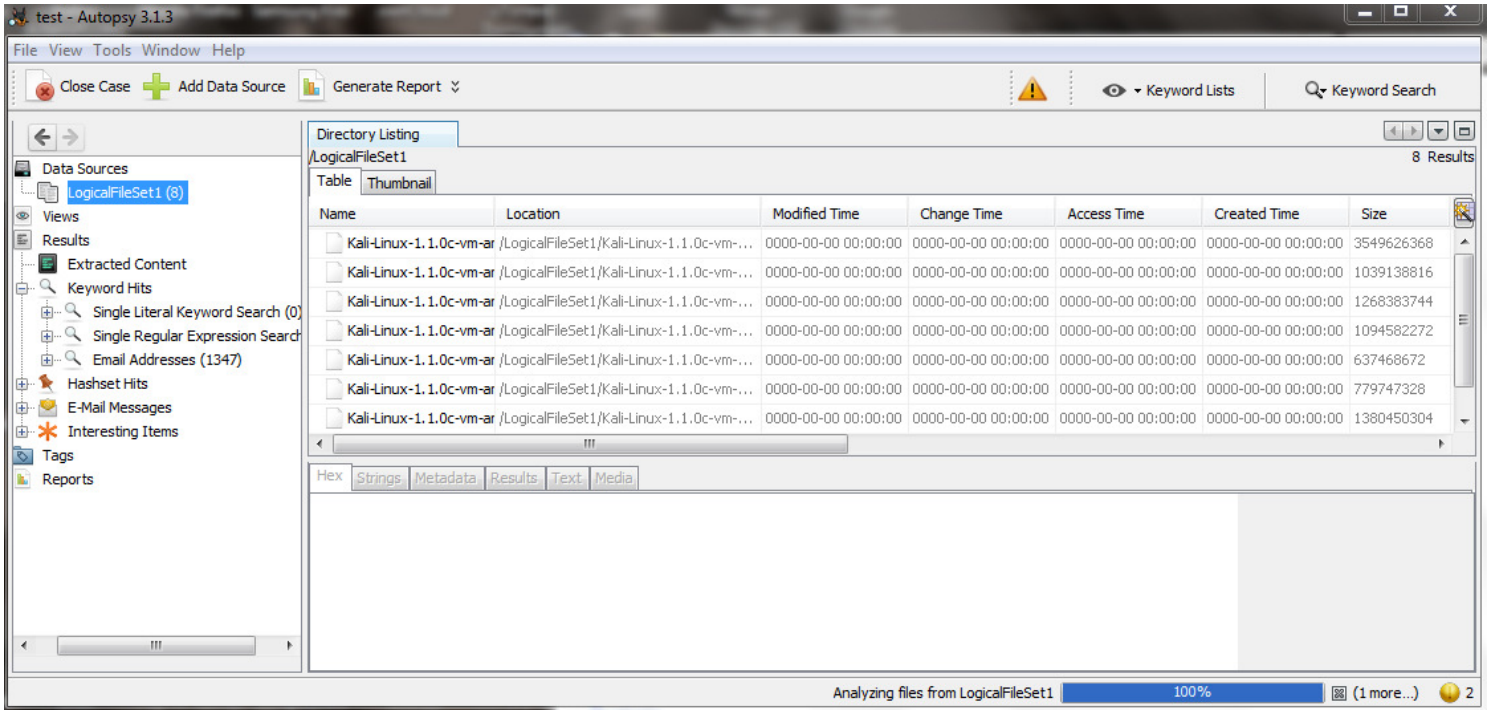
- **.001**
- **.aa**
- **.bin**
- **.dd**
- **.e01** (EnCase image)
- **.img**
- **.raw**

2. **Local Disk**, για τοπικό δίσκο ή διαμέρισμα.
3. **Logical Files**, για λοιπά αρχεία.

Στην συνέχεια, επιλέγονται τα είδη των εξετάσεων που θα γίνουν στις πηγές.

- **Recent Activity**
- **Hash Lookup**
- **File Type Identification**
- **Embedded File Extractor**
- **Exif Parser**
- **Keyword Search**
- **Email Parses**
- **Extension Mismatch Detector**
- **E01 Verifier**
- **Android Analyzer**
- **Interesting Files Identifier**
- **PhotoRec Carver**

Επίσης, δίνεται η επιλογή για κατεργασία του ελεύθερου χώρου.



Εικόνα 7.5: The Sleuth Kit

Μερικές από τις επιλογές και τα χαρακτηριστικά του Autopsy, είναι:

- ✓ Εγκατάσταση και διαχείριση των plugins, ακόμα και python plugins.
- ✓ Προβολή σε πλήρης οθόνη.
- ✓ Εμφάνιση στατιστικών για την χρήση των πηγών δεδομένων.
- ✓ Δημιουργία χρονοδιαγράμματος συμβάντων.
- ✓ Δημιουργία αναφοράς για συγκεκριμένες πληροφορίες ή για όλα τα αποτελέσματα.

Το **TSK** γενικά, περιλαμβάνει εργαλεία για διάφορους τομείς του υπολογιστή, όπως για τα ονόματα των αρχείων, τα μεταδεδομένα, το file system, τα images αρχεία, τον δίσκο και άλλα. Στην 4.2 έκδοση περιλαμβάνονται τα εξής εργαλεία:

blkcalc	Μετατρέπει μεταξύ μονάδων ελεύθερου και κανονικού δίσκου.
blkcat	Εξάγει τα περιεχόμενα ενός file system σε image δίσκου.
blkls	Καταγράφει τις μονάδες δεδομένων του δίσκου.
blkstat	Τυπώνει τις λεπτομέρειες μιας μονάδας δεδομένων file system, όπως μπλοκ ή τομέας.
fcat	Εμφανίζει τα περιεχόμενα ενός *αρχείου*.
ffind	Αναζητά το όνομα του αρχείου ή του καταλόγου, με την χρήση *inode*.
fls	Καταγράφει ονόματα αρχείων και καταλόγων ενός image δίσκου.
fsstat	Τυπώνει γενικές πληροφορίες του file system.
hfind	Αναζητά μια *τιμή hash* στην βάση δεδομένων των hashes.
icat	Εμφανίζει το περιεχόμενο ενός αρχείου, βασισμένο στο *inode*.
ifind	Βρίσκει την δομή μεταδεδομένων από μια *μονάδα δίσκου* ή ένα *όνομα αρχείου*.
ils	Τυπώνει τις πληροφορίες του inode.
img_cat	Εμφανίζει τα περιεχόμενα ενός *αρχείου image*.
img_stat	Τυπώνει πληροφορίες ενός *αρχείου image*.
istat	Τυπώνει πληροφορίες μιας δομής μεταδεδομένων, όπως ενός inode.
jcat	Εμφανίζει τα περιεχόμενα ενός μπλοκ στο ημερολόγιο του file system.
jls	Εμφανίζει τα περιεχόμενα του ημερολογίου του file system.
mactime	Δημιουργεί χρονοδιάγραμμα σε ASCII της δραστηριότητας του *αρχείου*.
mmcat	Τυπώνει τα περιεχόμενα ενός partition.
mmls	Εμφανίζει την κάτοψη ενός partition ενός συστήματος τόμου.
mmstat	Εμφανίζει πληροφορίες για το σύστημα τόμου.
tsk_comparedir	Συγκρίνει τα περιεχόμενα ενός καταλόγου με τα περιεχόμενα ενός image ή τοπικής συσκευής.
tsk_gettimes	Συλλέγει τις χρονοσφραγίδες από ένα image δίσκου σε απλό αρχείο.
tsk_loaddb	Φορτώνει τα μεταδεδομένα ενός image δίσκου σε βάση δεδομένων SQLite.
tsk_recover	Εξάγει τα αρχεία από ένα image σε τοπικό κατάλογο.

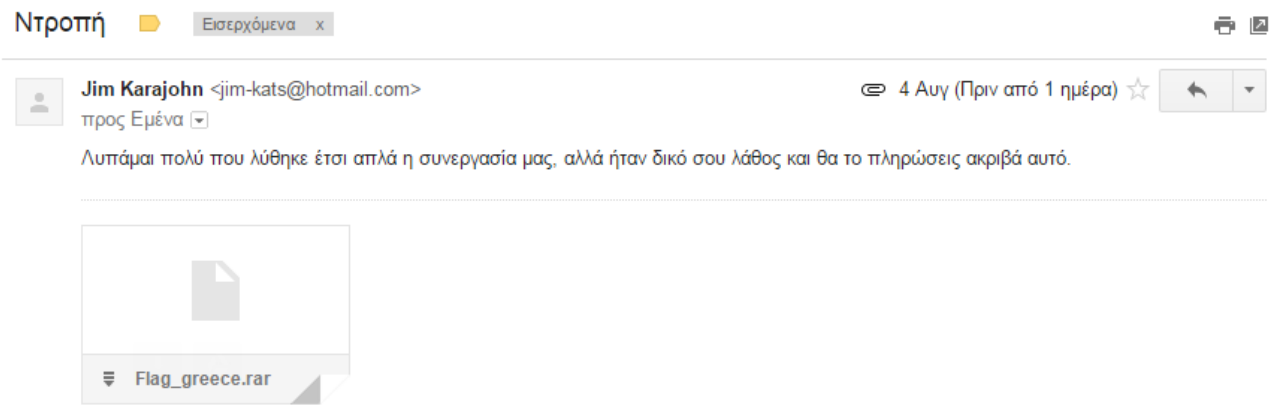
8. Σενάρια χρήσης εργαλείων

Αφού γνωρίσαμε και περιγράψαμε αρκετά από τα εργαλεία που χρησιμοποιούνται στις εγκληματολογικές έρευνες, ώρα να χρησιμοποιήσουμε μερικά από αυτά σε υποθετικά σενάρια εγκληματολογικών ερευνών, ώστε να κατανοήσουμε καλύτερα την χρησιμότητα και την αποτελεσματικότητα τους.

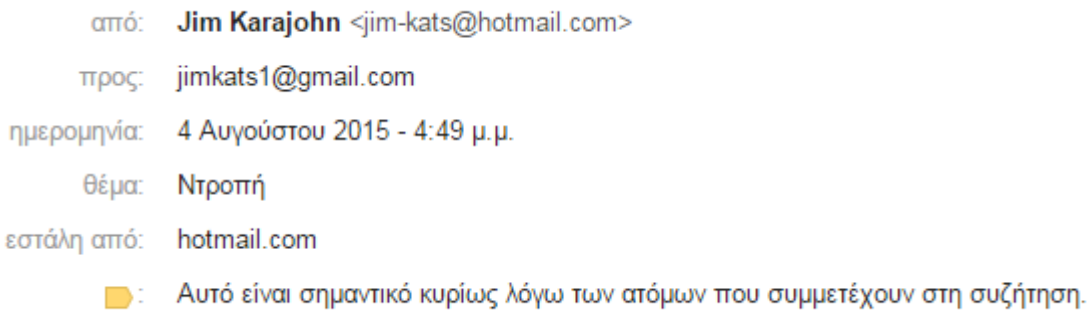
8.1. Σενάριο #1

Σ' αυτό το σενάριο, έχουμε δύο πρώην συνεργάτες οι οποίοι τα χάλασαν μεταξύ τους και ο ένας θέλει να εκδικηθεί τον άλλον καταστρέφοντας απομακρυσμένα τον υπολογιστή. Ή τουλάχιστον αυτό θα προσπαθήσει να κάνει.

Ξεκινάμε με το θύμα, το οποίο έλαβε email από τον δράστη το οποίο περιείχε ένα απειλητικό μήνυμα και ένα συνημμένο. Πιο συγκεκριμένα, το μήνυμα που ελήφθη είναι το εξής:



Εικόνα 8.1: Περιεχόμενο email



Εικόνα 8.2: Πληροφορίες email

Το θύμα έχει καταγγείλει το μήνυμα που έλαβε στις Αρχές ως απειλητικό. Για να αποδειχθεί ότι εστάλη το μήνυμα από τον πρώην συνεργάτη του, έρευνα στον υπολογιστή του πρέπει να γίνει.

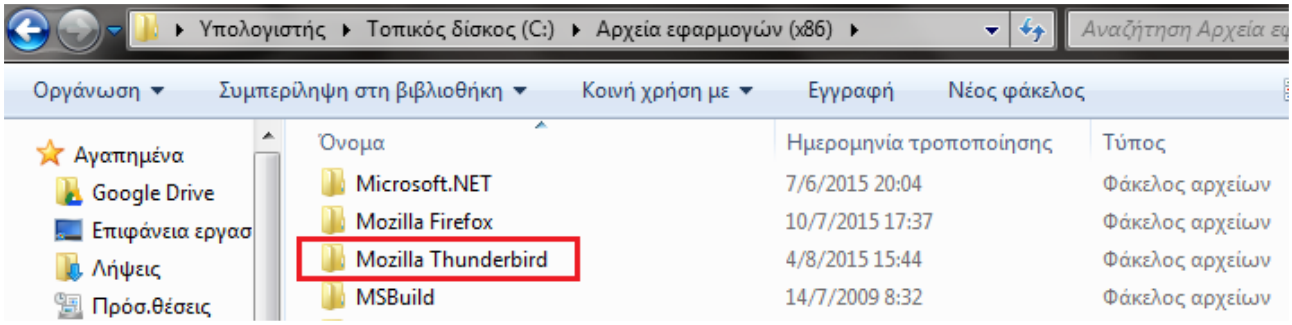
Πρώτα όμως, θα πάρουμε το checksum του συνημμένου αρχείου, για να μπορούμε να το συγκρίνουμε αργότερα με το αρχικό αρχείο.

```
C:\Windows\system32>cd \tools\FCIV

C:\tools\FCIV>fciv C:\Users\jimkats\Downloads\Flag_greece.rar
//
// File Checksum Integrity Verifier version 2.05.
//
e906d0960e4953dec69be9e110c5083b c:\users\jimkats\downloads\flag_greece.rar

C:\tools\FCIV>
```

Εικόνα 8.3: Υπολογισμός checksum

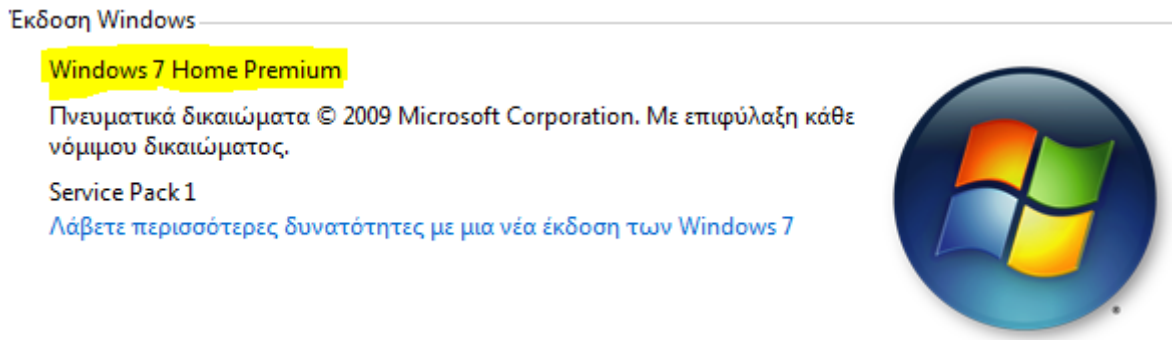
Όπως βλέπουμε, το checksum είναι: **e906d0960e4953dec69be9e110c5083b**

Στον υπολογιστή του υπόπτου, πρώτα πρέπει να ελέγξουμε αν έχει κάποιο email client. Σύμφωνα με μια γρήγορα αναζήτηση στα προγράμματα του υπολογιστή, βρήκαμε ότι έχει το **Thunderbird** της *Mozilla*.



Εικόνα 8.4: Θέση φακέλου Thunderbird

Αυτό θα μας βοηθήσει ώστε να ξέρουμε που να ψάξουμε για τα αρχεία της εφαρμογής όπου υπάρχουν αποθηκευμένα τα email που περιλαμβάνονται στον λογαριασμό του υπόπτου. Επίσης, από τις ιδιότητες του **Ο Υπολογιστής Μου**, βλέπουμε ότι το OS πρόκειται για **Windows 7**.

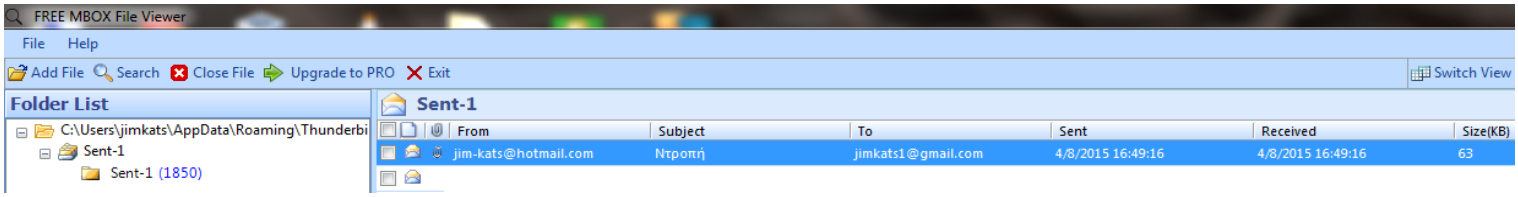


Εικόνα 8.5: Έκδοση λειτουργικού

Έτσι γνωρίζουμε που να ψάξουμε για τα αρχεία όπου βρίσκονται τα email του *Thunderbird*. Συγκεκριμένα, ο κατάλογος βρίσκεται στην θέση:

C:\Users\<user>\AppData\Roaming\Thunderbird\Profiles\<profile>\ImapMail

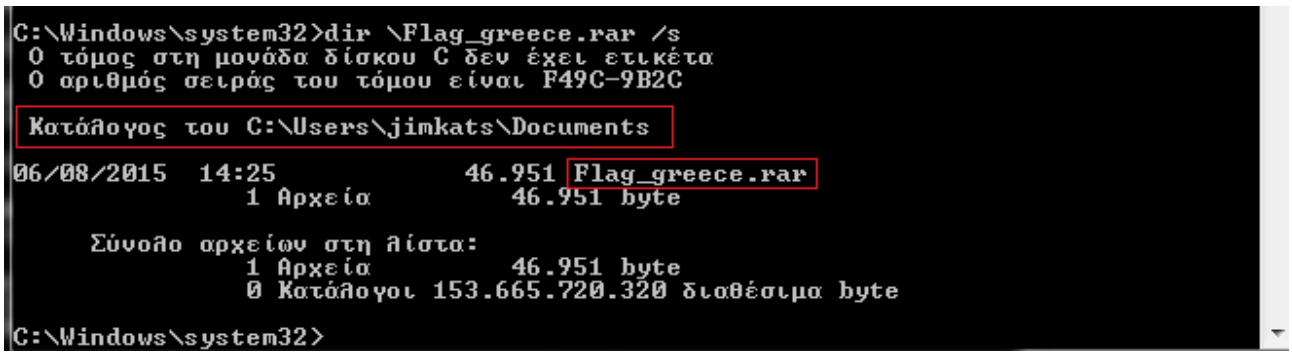
Για να διαβάσουμε τα αρχεία που πρέπει, θα χρησιμοποιήσουμε το **Free MBOX File Viewer**. Συγκεκριμένα, θα διαβάσουμε το αρχείο *Sent*. Επειδή όμως μπορεί να διαφοροποιούνται λίγο τα ονόματα ανάλογα με το πόσα μηνύματα υπάρχουν, στην προκειμένη περίπτωση θα διαβάσουμε το Sent-1, το οποίο είναι για τα πιο πρόσφατα εξερχόμενα.



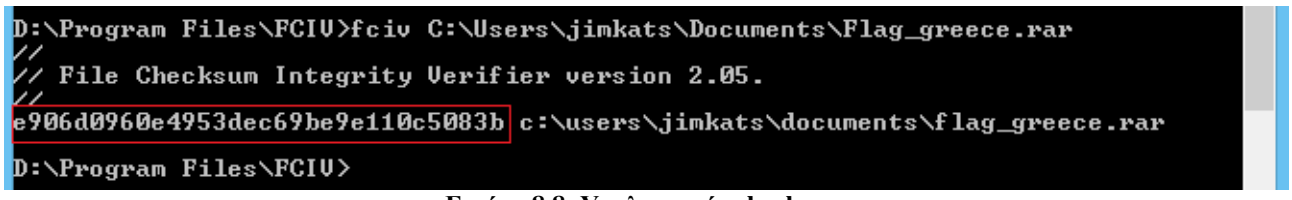
Εικόνα 8.6: FREE MBOX File Viewer

Όπως βλέπουμε στην από πάνω εικόνα, η ώρα αποστολής είναι προγενέστερη της ώρας παραλαβής του μηνύματος από το θύμα, οπότε αυτό το email είναι και το σωστό και όχι για παράδειγμα κάποιο που δεν ελήφθη ποτέ.

Τώρα, θα πρέπει να αναζητήσουμε το συνημμένο αρχείο στον υπολογιστή του δράστη, ώστε να πάρουμε το checksum και να το συγκρίνουμε με αυτό του αρχείου που ελήφθη, ώστε να βεβαιωθούμε ότι είναι τα ίδια και δεν τροποποιήθηκαν καθόλου στο ενδιάμεσο.



Εικόνα 8.7: Τοποθεσία Flag_greece.rar

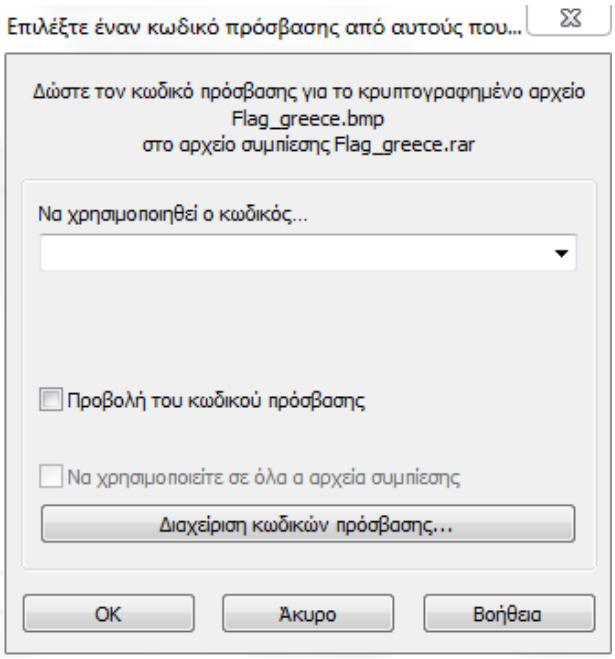


Εικόνα 8.8: Υπολογισμός checksum

Βλέπουμε ότι το αρχείο υπάρχει στον υπολογιστή, δηλαδή δεν έχει διαγραφεί και βρίσκεται στον κατάλογο **C:\Users\jimkats\Documents** και ότι το checksum του είναι **e906d0960e4953dec69be9e110c5083b** το οποίο είναι ακριβώς το ίδιο με το αρχείο που ελήφθη.

Έτσι τώρα μπορούμε να αρχίσουμε να αναλύουμε το αρχείο και να δούμε τι έχει μέσα και αν είναι απειλητικό για το θύμα.

Ας δοκιμάσουμε να αποσυμπιέσουμε το αρχείο.

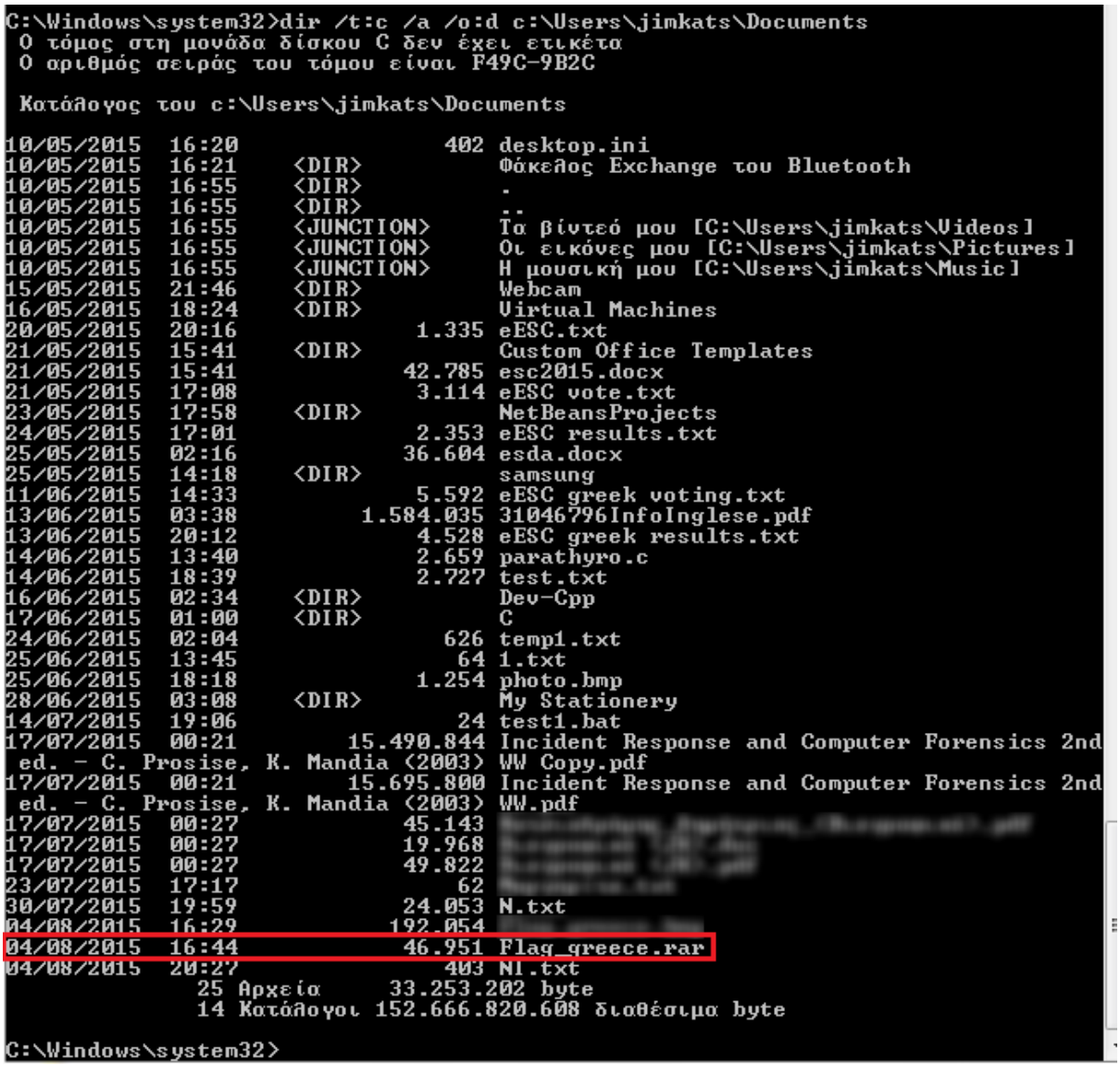


Εικόνα 8.9: Ασφαλισμένη αποσυμπίεση

Όπως φαίνεται, θέλει κωδικό για να αποσυμπιεστεί. Παρόλαυτα βλέπουμε ότι περιέχει ένα αρχείο εικόνας με το όνομα **Flag_greece.bmp**.

Τώρα πρέπει να βρούμε τον κωδικό αποσυμπίεσης. Υπάρχουν πολλά πιθανά μέρη όπου μπορεί να βρίσκεται ο κωδικός.

Ένας τρόπος είναι να δούμε στον κατάλογο όπου βρίσκεται το αρχείο, τους χρόνους δημιουργίας των υπολοίπων αρχείων, ώστε ανάλογα να δούμε εάν υπάρχει κοντά στην ώρα δημιουργίας του αρχείου άλλο αρχείο σχετικό.



Εικόνα 8.10: Προβολή timestamps

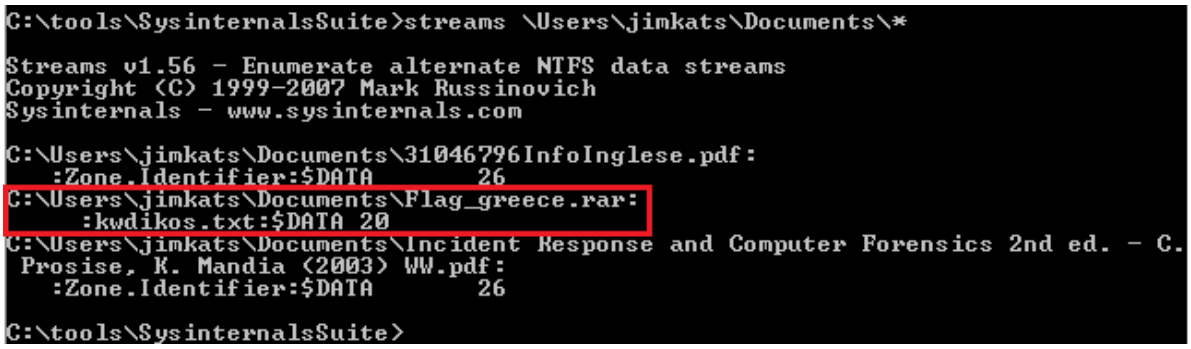
Συγκεκριμένα η εντολή που χρησιμοποιήσαμε για να δούμε τα timestamps δημιουργίας είναι:

dir /t:c /a /o:d C:\Users\<user>\Documents

όπου το **/t:c** για το timestamp δημιουργίας και το **/o:d** για ταξινόμηση κατά αύξων ημερομηνία.

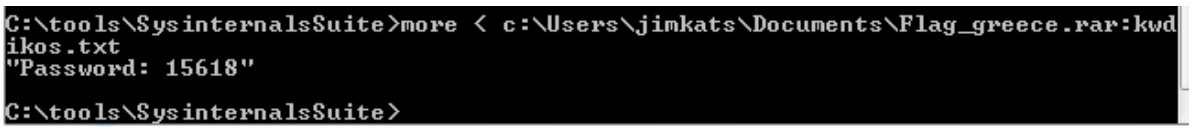
Με επισήμανση βλέπουμε το αρχικό αρχείο, ώστε να ξέρουμε που να κοιτάξουμε για άλλο αρχείο. Όπως φαίνεται, δεν υπάρχει άλλο αρχείο με κοντινή ώρα το οποίο να είναι ύποπτο.

Ένας άλλος τρόπος να βρούμε τον κωδικό, είναι να κοιτάξουμε για αρχεία με τυχόν εναλλακτικές ροές.



Εικόνα 8.11: Προβολή ADS

Συνολικά τρία αρχεία έχουν εναλλακτικές ροές, εκ των οποίων το δεύτερο φαίνεται ύποπτο, λόγο του ονόματος της εναλλακτικής ροής, το οποίο στην προκειμένη περίπτωση είναι **kwdikos.txt**.



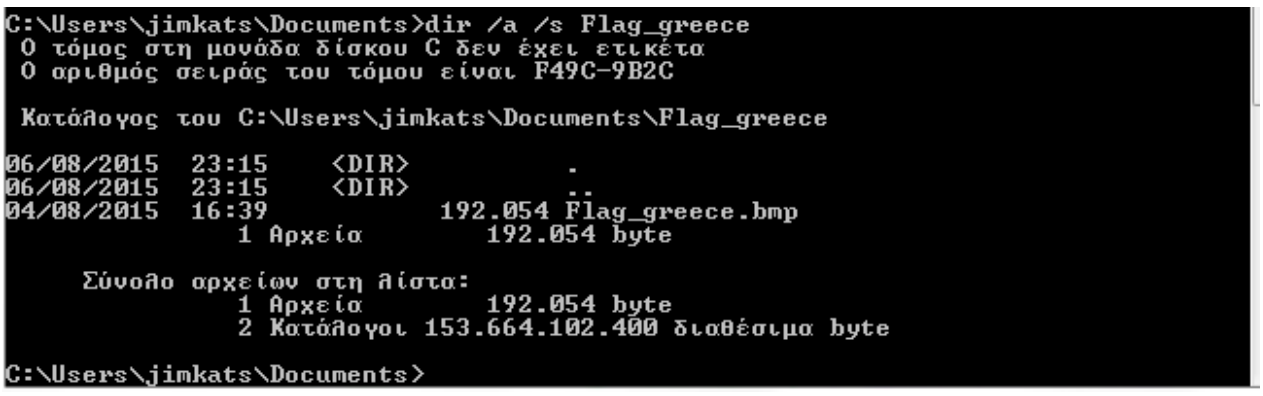
Εικόνα 8.12: Προβολή κωδικού

Για να διαβάσουμε την εναλλακτική ροή, τρέχουμε την εντολή:

more < c:\Users\<user>\Documents\Flag_greece.rar:kwdikos.txt

Κι έτσι βλέπουμε το περιεχόμενο "**Password: 15618**" κι έτσι καταλαβαίνουμε ότι το **15618** είναι ο κωδικός για να ξεκλειδώσουμε το αρχείο.

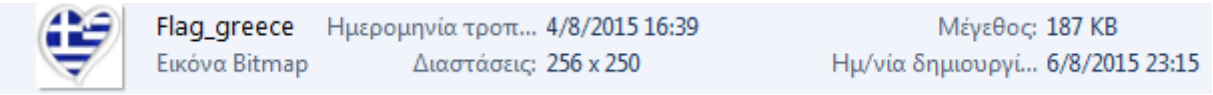
Αφού ξεκλειδώσαμε και αποσυμπιέσαμε το αρχείο σε φάκελο, τώρα μπορούμε να δούμε τι περιέχει.



Εικόνα 8.13: Περιεχόμενο αρχείου

Έτσι, επαληθεύουμε για πριν ότι υπάρχει μια εικόνα BMP, με το όνομα **Flag_greece.bmp**.

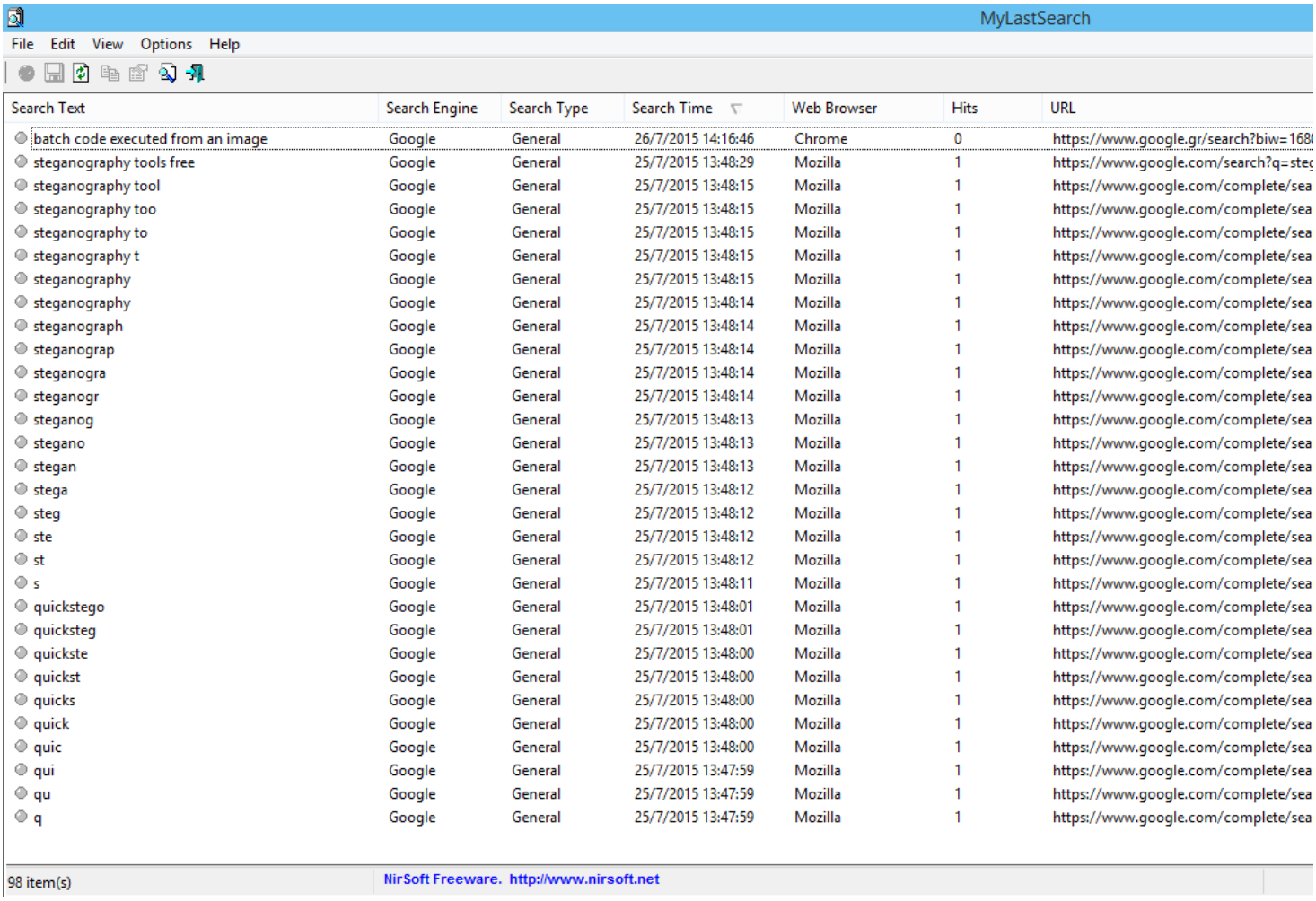
Αν δούμε την προεπισκόπηση της φωτογραφίας στον Explorer, θα δούμε ότι δεν συνάδει λογικά το μέγεθος του αρχείου της εικόνας με την ανάλυση της.



Εικόνα 8.14: Πληροφορίες εικόνας

Οπότε τώρα πρέπει να βρούμε εάν κρύβεται κάτι μέσα στην εικόνα και για να γίνει αυτό, πρέπει να μάθουμε τι εργαλείο στεγανογραφίας χρησιμοποίησε ο δράστης, καθώς κάθε εργαλείο στεγανογραφίας μπορεί να κρύψει με διαφορετικό τρόπο την κάθε πληροφορία, έτσι ώστε να μην μπορεί να βρεθεί απ' όλα τα αντίστοιχα εργαλεία.

Για αρχή θα ψάξουμε το ιστορικό αναζήτησης του στο Διαδίκτυο, μήπως υπάρχει ένδειξη ότι πήρε το εργαλείο ο δράστης από εκεί.



Εικόνα 8.15: MyLastSearch

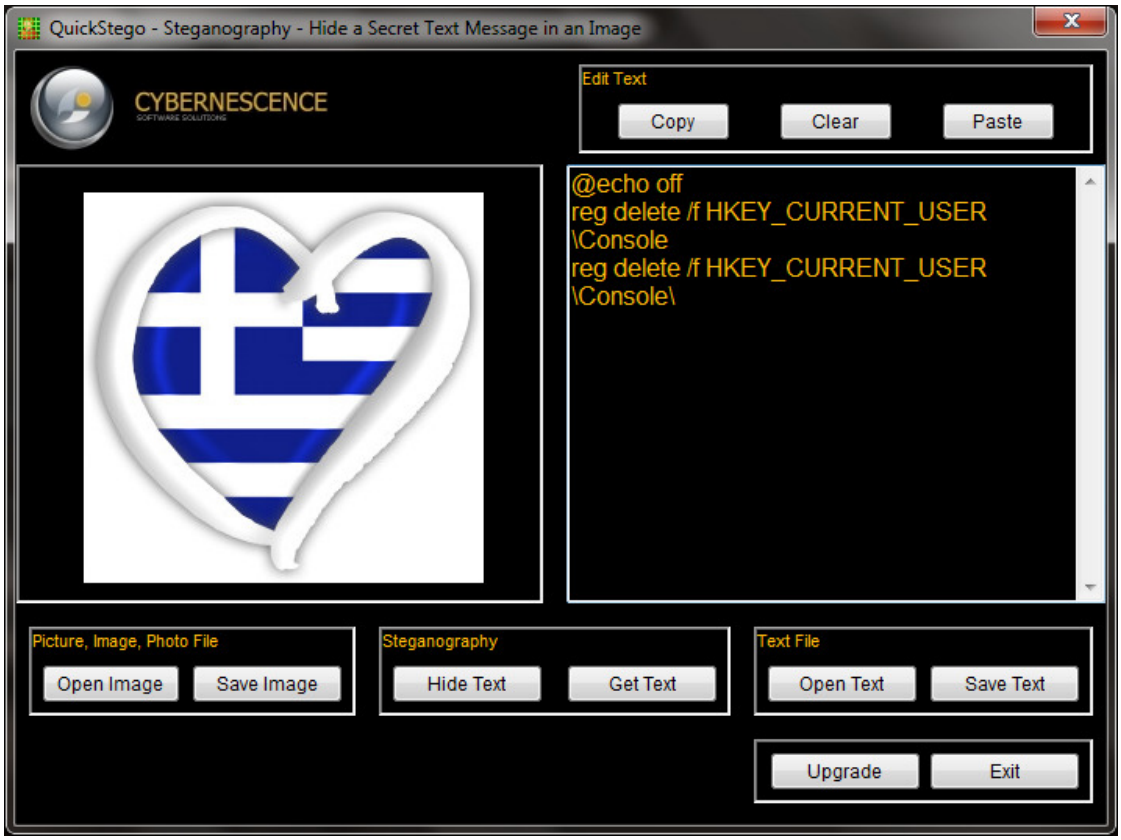
Χρησιμοποιώντας το **MyLastSearch**, βλέπουμε ότι έγινε αναζήτηση για δωρεάν εργαλεία στεγανογραφίας και για το **QuickStego**, το οποίο είναι εργαλείο στεγανογραφίας με δυνατότητα απόκρυψης και εμφάνισης κειμένου σε εικόνα.

Βέβαια, το ότι έγινε αναζήτηση του **QuickStego**, δεν σημαίνει απαραίτητα ότι το χρησιμοποίηση ο δράστης, οπότε πρέπει να επαληθεύσουμε ότι υπάρχει στον υπολογιστή και ένας τρόπος είναι να το βρούμε στην **registry** των Windows.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Comments	REG_SZ	Advanced Steganography & Privacy Software
DisplayIcon	REG_SZ	D:\Program Files (x86)\Quick Stego\QuickStego.exe
DisplayName	REG_SZ	Quick Stego 1.2
HelpLink	REG_SZ	http://QuickCrypto.com/
Inno Setup: App Path	REG_SZ	D:\Program Files (x86)\Quick Stego
Inno Setup: Deselected Tasks	REG_SZ	
Inno Setup: Icon Group	REG_SZ	(Default)
Inno Setup: Selected Tasks	REG_SZ	desktopicon,quicklaunchicon
Inno Setup: Setup Version	REG_SZ	5.2.3
Inno Setup: User	REG_SZ	[redacted]
InstallDate	REG_SZ	20150725
InstallLocation	REG_SZ	D:\Program Files (x86)\Quick Stego\
NoModify	REG_DWORD	0x00000001 (1)
NoRepair	REG_DWORD	0x00000001 (1)
Publisher	REG_SZ	Cybernescence Limited
QuietUninstallString	REG_SZ	"D:\Program Files (x86)\Quick Stego\unins000.exe" /SILENT
UninstallString	REG_SZ	"D:\Program Files (x86)\Quick Stego\unins000.exe"
URLInfoAbout	REG_SZ	http://Cybernescence.com/
URLUpdateInfo	REG_SZ	http://QuickCrypto.com/

Εικόνα 8.16: QuickStego στο μητρώο

Αναζητήσαμε στην registry για το **QuickStego** και αφού επιβεβαιώσαμε ότι υπάρχει στον υπολογιστή του δράστη, τώρα θα το χρησιμοποιήσουμε για να κάνουμε στεγανάλυση, δηλαδή να δούμε το κείμενο που μπορεί να έχει κρυφτεί μέσα στην εικόνα.



Εικόνα 8.17: Στεγανάλυση στο QuickStego

Βλέπουμε ότι το κείμενο που είναι κρυμμένο μέσα στην εικόνα, είναι το:

@echo off
reg delete /f HKEY_CURRENT_USER\Console
reg delete /f HKEY_CURRENT_USER\Console

Το "**@echo off**" υποδηλώνει ότι το κείμενο είναι κώδικας batch, δηλαδή κώδικας σεναρίου των Windows.

Οι δύο επόμενες εντολές δηλώνουν την διαγραφή δύο καταλόγων κλειδιών του μητρώου, χωρίς να ζητά την έγκριση του χρήστη.

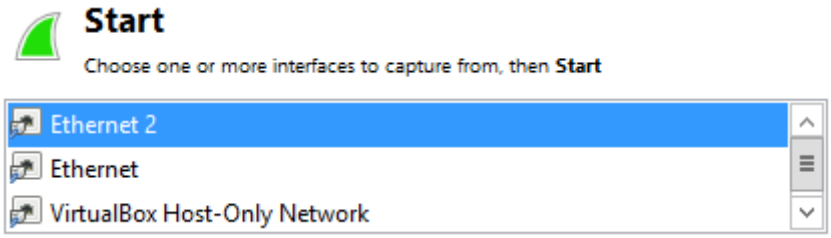
Στην πραγματικότητα, αυτός ο κώδικας ως έχει, δεν μπορεί να εκτελεστεί. Ακόμη και να μπορούσε, το αποτέλεσμα της διαγραφής αυτών των καταλόγων κλειδιών μητρώου, θα ήταν η εξαφάνιση εικονιδίων των Windows και μερικά κολλήματα του Explorer.

Αυτά τα στοιχεία, αρκούν για να αποφανθούμε ότι ο δράστης έχει κάνει απόπειρα πρόκλησης βλάβης στο υπολογιστικό σύστημα του θύματος.

8.2 Σενάριο #2

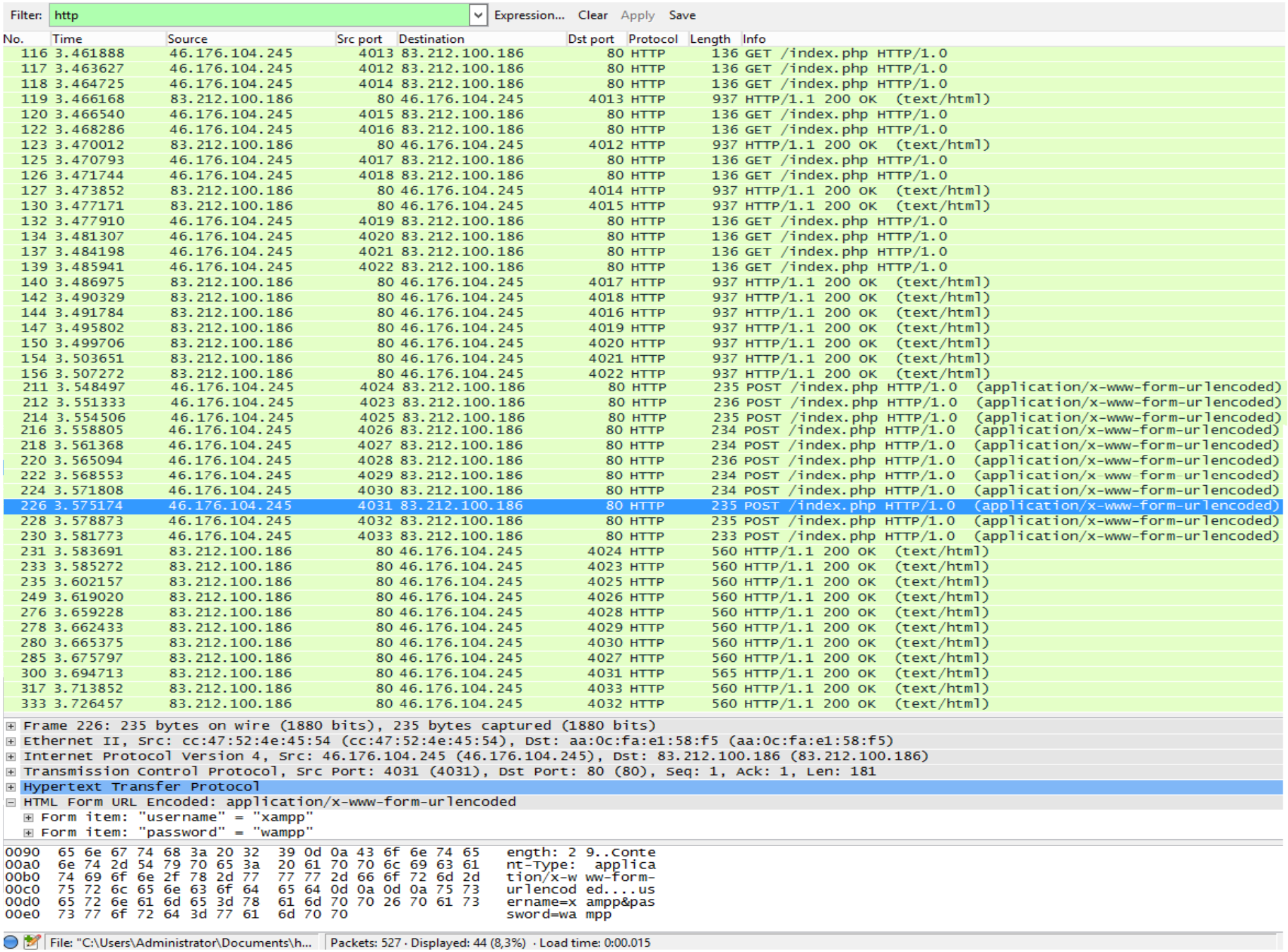
Σ' αυτό το σενάριο, θα γίνουμε μάρτυρες μια επίθεσης κωδικού σ' έναν server, η οποία μάλιστα είναι επιτυχής.

Πιο συγκεκριμένα, ο server έχει την διεύθυνση **83.212.100.186**, ο οποίος φιλοξενείται στην υπηρεσία σύννεφου Okeanos του GRNET και παρακολουθούμε μέσω **Wireshark** το interface **Ethernet 2** του server.



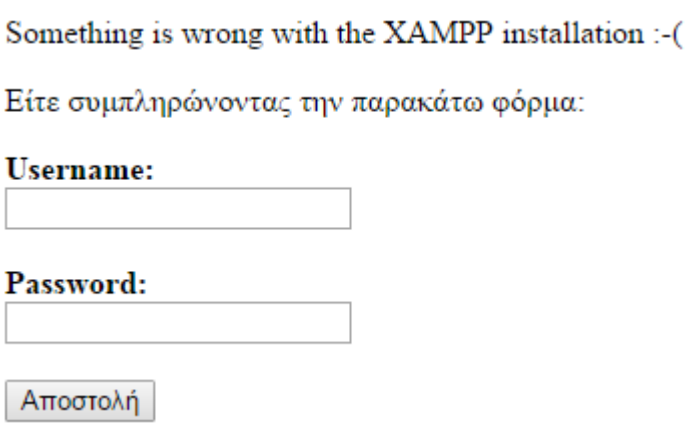
Εικόνα 8.18: Επιλογή interface

Στην επόμενη εικόνα βλέπουμε την καταγραφή του Wireshark της κίνησης στο interface Ethernet 2 του server για το πρωτόκολλο **HTTP**.


Filter: http
Expression... Clear Apply Save
No. Time Source Src port Destination Dst port Protocol Length Info
116 3.461888 46.176.104.245 4013 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
117 3.463627 46.176.104.245 4012 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
118 3.464725 46.176.104.245 4014 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
119 3.466168 83.212.100.186 80 46.176.104.245 4013 HTTP 937 HTTP/1.1 200 OK (text/html)
120 3.466540 46.176.104.245 4015 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
122 3.468286 46.176.104.245 4016 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
123 3.470012 83.212.100.186 80 46.176.104.245 4012 HTTP 937 HTTP/1.1 200 OK (text/html)
125 3.470793 46.176.104.245 4017 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
126 3.471744 46.176.104.245 4018 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
127 3.473852 83.212.100.186 80 46.176.104.245 4014 HTTP 937 HTTP/1.1 200 OK (text/html)
130 3.477171 83.212.100.186 80 46.176.104.245 4015 HTTP 937 HTTP/1.1 200 OK (text/html)
132 3.477910 46.176.104.245 4019 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
134 3.481307 46.176.104.245 4020 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
137 3.484198 46.176.104.245 4021 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
139 3.485941 46.176.104.245 4022 83.212.100.186 80 HTTP 136 GET /index.php HTTP/1.0
140 3.486975 83.212.100.186 80 46.176.104.245 4017 HTTP 937 HTTP/1.1 200 OK (text/html)
142 3.490329 83.212.100.186 80 46.176.104.245 4018 HTTP 937 HTTP/1.1 200 OK (text/html)
144 3.491784 83.212.100.186 80 46.176.104.245 4016 HTTP 937 HTTP/1.1 200 OK (text/html)
147 3.495802 83.212.100.186 80 46.176.104.245 4019 HTTP 937 HTTP/1.1 200 OK (text/html)
150 3.499706 83.212.100.186 80 46.176.104.245 4020 HTTP 937 HTTP/1.1 200 OK (text/html)
154 3.503651 83.212.100.186 80 46.176.104.245 4021 HTTP 937 HTTP/1.1 200 OK (text/html)
156 3.507272 83.212.100.186 80 46.176.104.245 4022 HTTP 937 HTTP/1.1 200 OK (text/html)
211 3.548497 46.176.104.245 4024 83.212.100.186 80 HTTP 235 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
212 3.551333 46.176.104.245 4023 83.212.100.186 80 HTTP 236 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
214 3.554506 46.176.104.245 4025 83.212.100.186 80 HTTP 235 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
216 3.558805 46.176.104.245 4026 83.212.100.186 80 HTTP 234 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
218 3.561368 46.176.104.245 4027 83.212.100.186 80 HTTP 234 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
220 3.565094 46.176.104.245 4028 83.212.100.186 80 HTTP 236 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
222 3.568553 46.176.104.245 4029 83.212.100.186 80 HTTP 234 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
224 3.571808 46.176.104.245 4030 83.212.100.186 80 HTTP 234 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
226 3.575174 46.176.104.245 4031 83.212.100.186 80 HTTP 235 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
228 3.578873 46.176.104.245 4032 83.212.100.186 80 HTTP 235 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
230 3.581773 46.176.104.245 4033 83.212.100.186 80 HTTP 233 POST /index.php HTTP/1.0 (application/x-www-form-urlencoded)
231 3.583691 83.212.100.186 80 46.176.104.245 4024 HTTP 560 HTTP/1.1 200 OK (text/html)
233 3.585272 83.212.100.186 80 46.176.104.245 4023 HTTP 560 HTTP/1.1 200 OK (text/html)
235 3.602157 83.212.100.186 80 46.176.104.245 4025 HTTP 560 HTTP/1.1 200 OK (text/html)
249 3.619020 83.212.100.186 80 46.176.104.245 4026 HTTP 560 HTTP/1.1 200 OK (text/html)
276 3.659228 83.212.100.186 80 46.176.104.245 4028 HTTP 560 HTTP/1.1 200 OK (text/html)
278 3.662433 83.212.100.186 80 46.176.104.245 4029 HTTP 560 HTTP/1.1 200 OK (text/html)
280 3.665375 83.212.100.186 80 46.176.104.245 4030 HTTP 560 HTTP/1.1 200 OK (text/html)
285 3.675797 83.212.100.186 80 46.176.104.245 4027 HTTP 560 HTTP/1.1 200 OK (text/html)
300 3.694713 83.212.100.186 80 46.176.104.245 4031 HTTP 565 HTTP/1.1 200 OK (text/html)
317 3.713852 83.212.100.186 80 46.176.104.245 4033 HTTP 560 HTTP/1.1 200 OK (text/html)
333 3.726457 83.212.100.186 80 46.176.104.245 4032 HTTP 560 HTTP/1.1 200 OK (text/html)
Frame 226: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
Ethernet II, Src: cc:47:52:4e:45:54 (cc:47:52:4e:45:54), Dst: aa:0c:fa:e1:58:f5 (aa:0c:fa:e1:58:f5)
Internet Protocol Version 4, Src: 46.176.104.245 (46.176.104.245), Dst: 83.212.100.186 (83.212.100.186)
Transmission Control Protocol, Src Port: 4031 (4031), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 181
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "xampp"
Form item: "password" = "wampp"
0090 65 6e 67 74 68 3a 20 32 39 0d 0a 43 6f 6e 74 65 ength: 2 9..Conte
00a0 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 nt-Type: applica
00b0 74 69 6f 6e 2f 78 2d 77 77 2d 66 6f 72 6d 2d tion/x-w ww-form-
00c0 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 0d 0a 75 73 urlencod ed....us
00d0 65 72 6e 61 6d 65 3d 78 61 6d 70 70 26 70 61 73 ername=x ampp&pas
00e0 73 77 6f 72 64 3d 77 61 6d 70 70 sword=wa mpp
File: "C:\Users\Administrator\Documents\h...
Packets: 527 · Displayed: 44 (8,3%) · Load time: 0:00.015

Βλέπουμε ότι ο server λαμβάνει πολλαπλά αιτήματα από τον υπολογιστή με διεύθυνση **46.176.104.245** στη μέθοδο **GET** στην αρχή και μετά έντεκα συνεχή στη μέθοδο **POST**, με την θύρα της πηγής να αυξάνεται κάθε φορά κατά ένα και να απαντάει ο server κανονικά και στα έντεκα. Τα είκοσι δύο αυτά πακέτα ενέργησαν σε χρονικό διάστημα *0,2 δευτερολέπτων* περίπου.

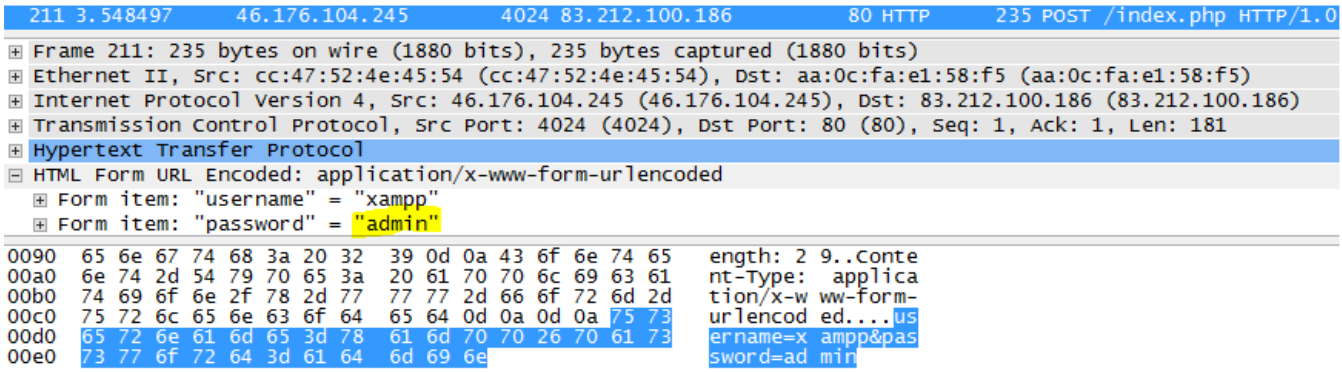
Και τα έντεκα πακέτα χρησιμοποιούν την διαδικτυακή φόρμα συμπλήρωσης στοιχείων του server, όπως φαίνεται στην παρακάτω εικόνα.



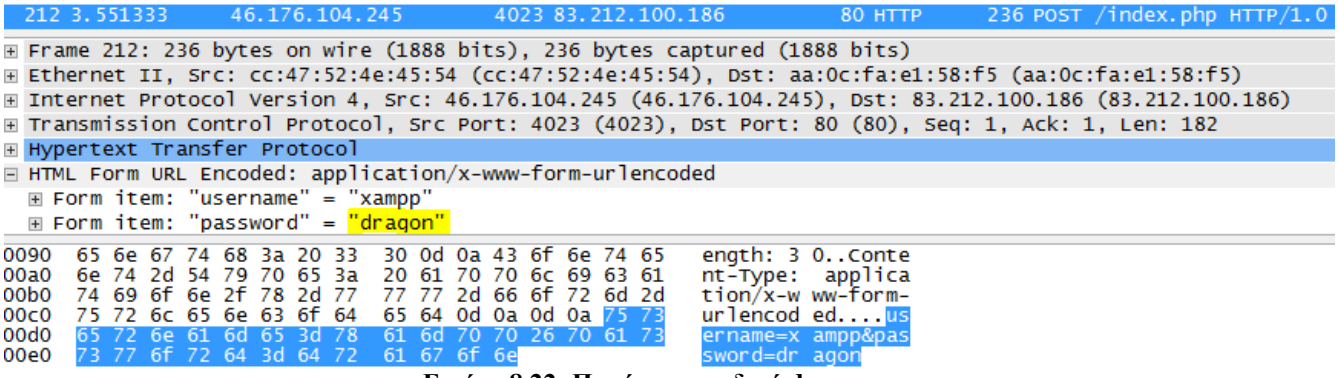
Εικόνα 8.20: Φόρμα σύνδεσης

Επίσης, ένα άλλο κοινό που έχουν τα πακέτα, είναι ότι χρησιμοποιούνε το ίδιο όνομα χρήστη και συγκεκριμένα το **xampp**.

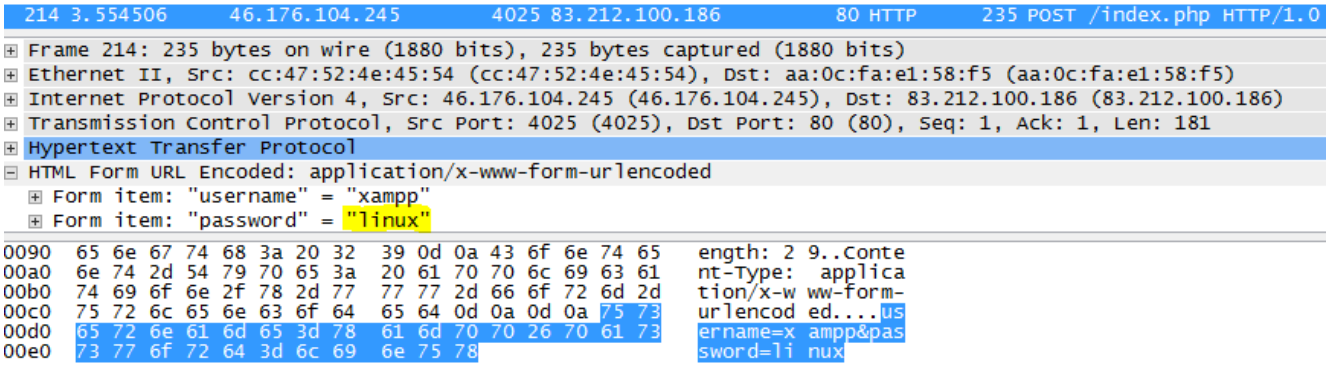
Παρακάτω φαίνονται τα στοιχεία σύνδεσης που περιλαμβάνει κάθε πακέτο.



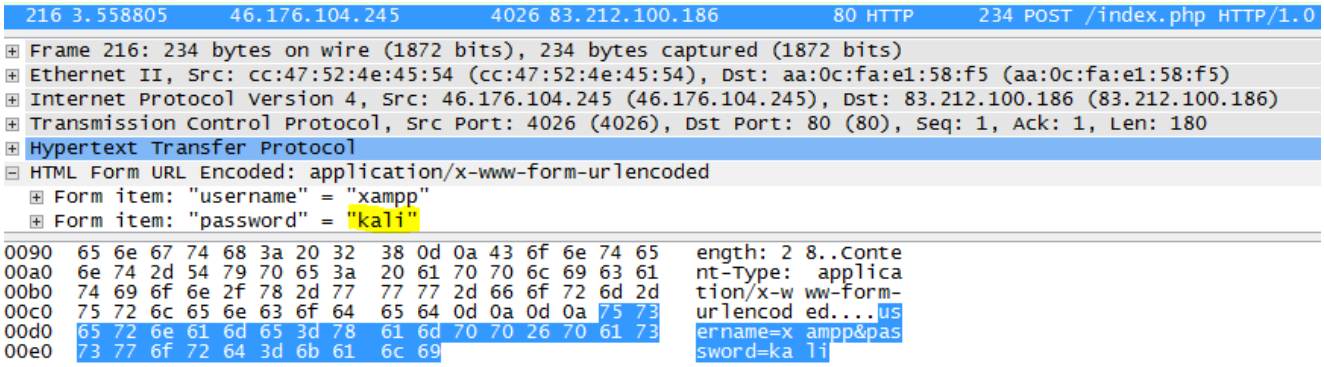
Εικόνα 8.21: Πακέτο με κωδικό admin



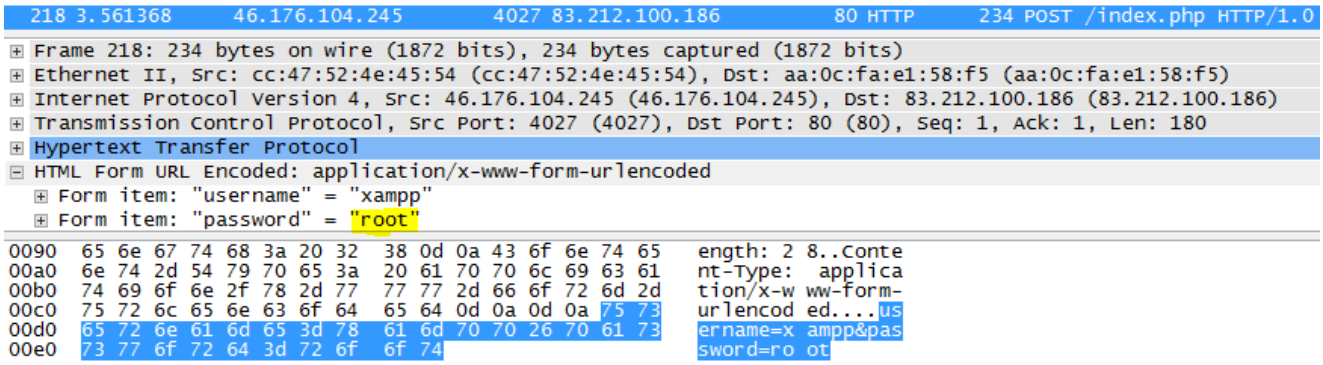
Εικόνα 8.22: Πακέτο με κωδικό dragon



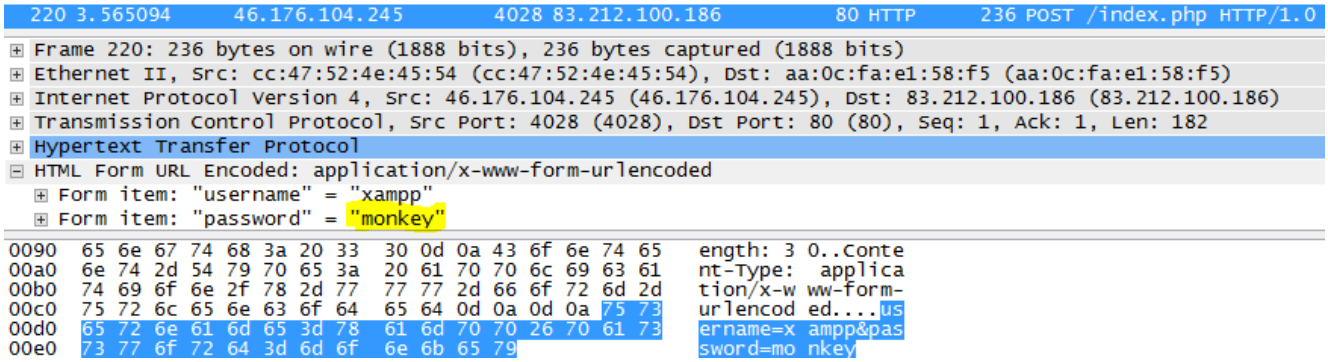
Εικόνα 8.23: Πακέτο με κωδικό linux



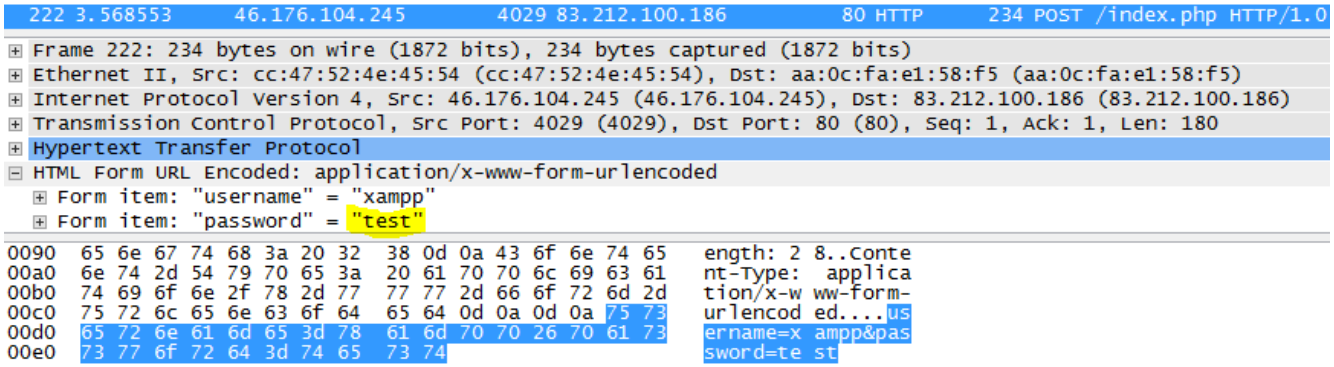
Εικόνα 8.24: Πακέτο με κωδικό kali



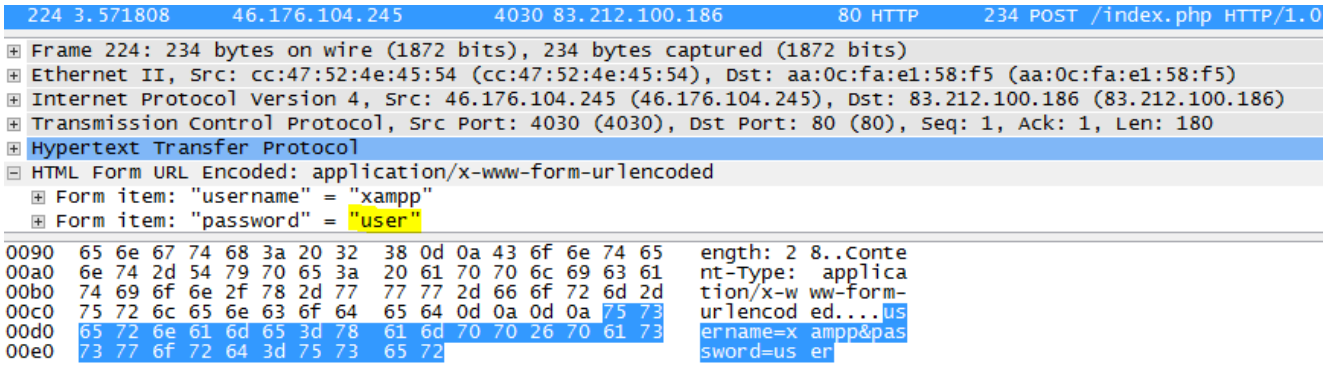
Εικόνα 8.25: Πακέτο με κωδικό root



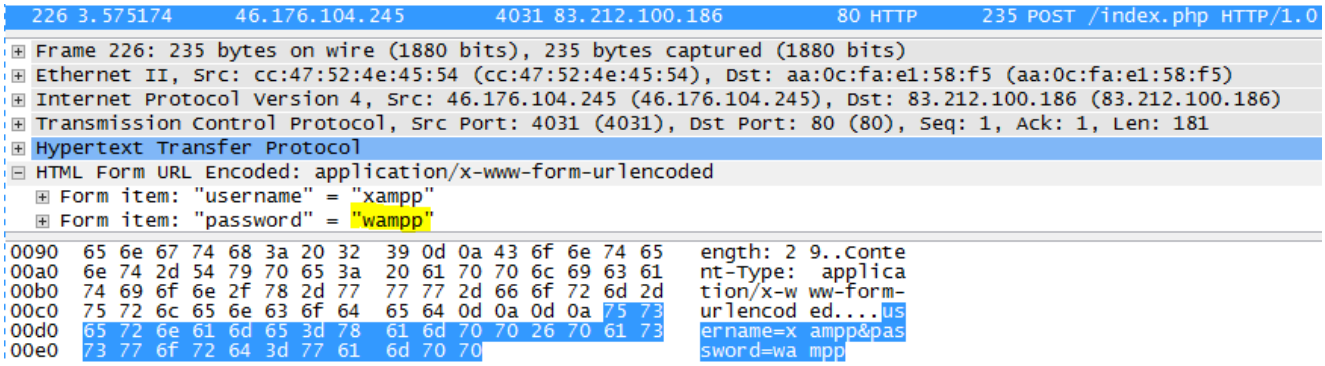
Εικόνα 8.27: Πακέτο με κωδικό monkey



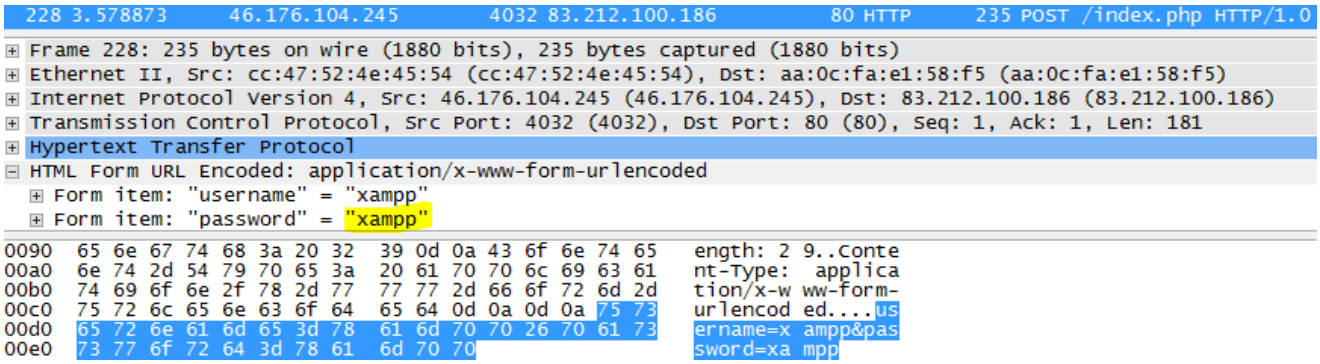
Εικόνα 8.28: Πακέτο με κωδικό test



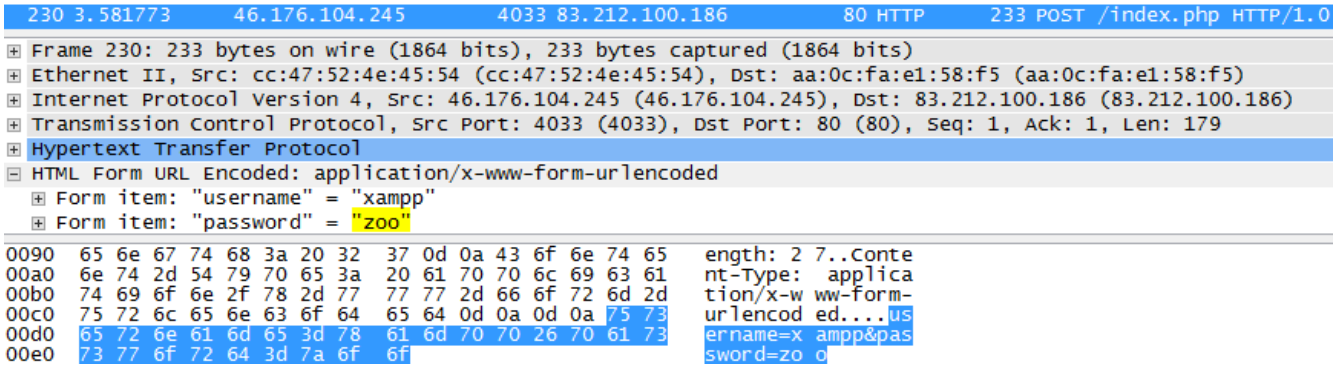
Εικόνα 8.29: Πακέτο με κωδικό user



Εικόνα 8.30: Πακέτο με κωδικό wampp

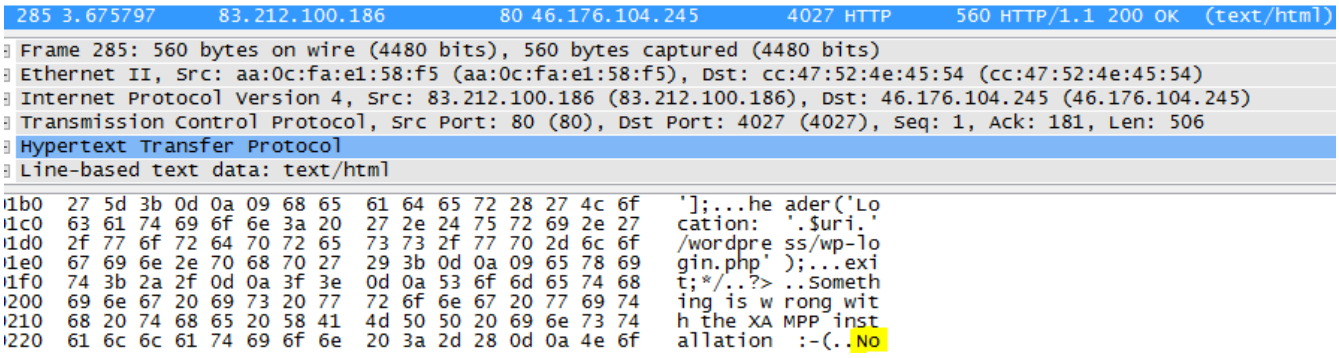


Εικόνα 8.31: Πακέτο με κωδικό xampp



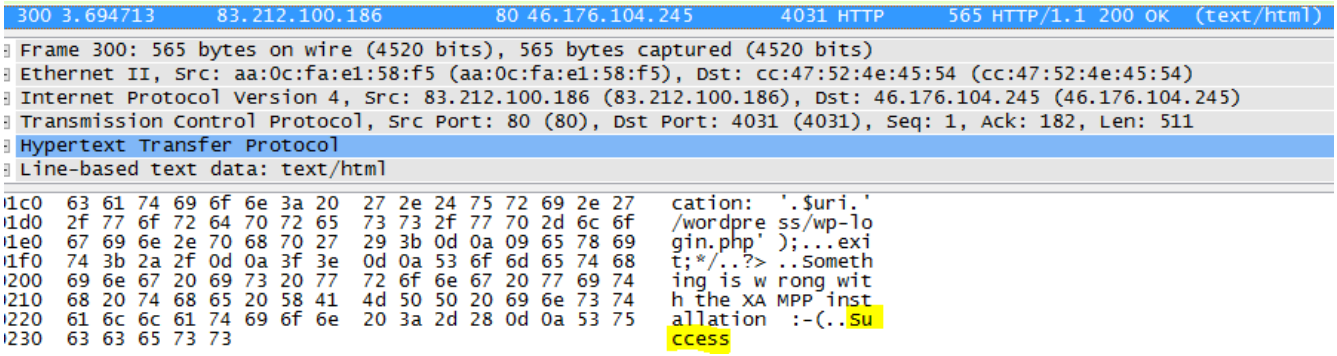
Εικόνα 8.32: Πακέτο με κωδικό zoo

Η επόμενη εικόνα μας δείχνει την απάντηση του server σε όσα πακέτα έστελναν *λάθος* κωδικό χρήστη, η οποία είναι "**No**".



Εικόνα 8.33: Η απάντηση για λάθος

Η επόμενη εικόνα μας δείχνει την απάντηση του server για το πακέτο που έστειλε τον *σωστό* κωδικό χρήστη, η οποία είναι "**Success**".

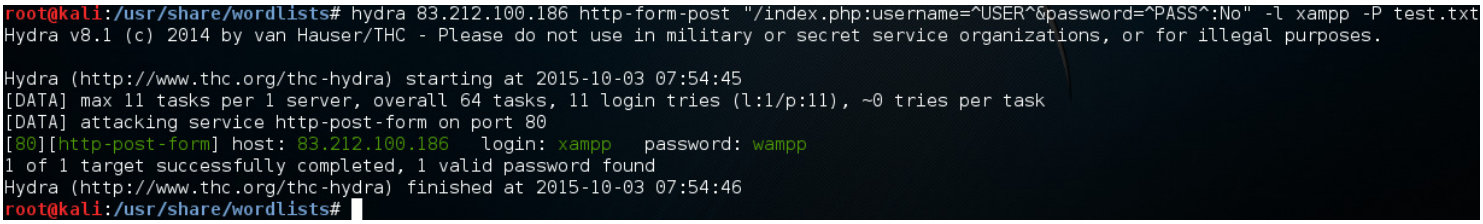


Εικόνα 8.34: Η απάντηση για σωστό

Αν συγκρίνουμε την **θύρα προορισμού**, δηλαδή την **4031** με τις θύρες πηγής των έντεκα πακέτων, θα δούμε ότι ταιριάζει με το **πακέτο 226**, το οποίο έχει στείλει τον κωδικό "**wampp**", ο οποίος είναι όντως ο σωστός.

Με βάση τα ανωτέρω, το ότι δηλαδή σε πολύ σύντομο χρονικό διάστημα εστάλησαν από την ίδια πηγή 11 αιτήματα πρόσβασης, με ίδιο όνομα χρήστη, θα μπορούσαμε να πούμε με βεβαιότητα ότι ο server έχει δεχθεί **επίθεση σπασίματος κωδικού**.

Η επίθεση πραγματοποιήθηκε με το εργαλείο **Hydra** στα **Kali Linux** και χρησιμοποιήθηκε ένα αυτοδημιούργητο αρχείο με κωδικούς.



Εικόνα 8.35: Η εντολή επίθεσης

Συγκεκριμένα, η εντολή που χρησιμοποιήθηκε για να πραγματοποιηθεί η επίθεση στον server, είναι:

hydra 83.212.100.186 http-form-post
"/index.php:username=^USER^&password=^PASS^:No" -l xampp -P test.txt

, όπου:

- ✓ **83.212.100.186**, η διεύθυνση του host στον οποίον θα γίνει η επίθεση.
- ✓ **http-form-post**, για την χρήση φόρμας με την μέθοδο POST.
- ✓ **/index.php**, για το αρχείο όπου βρίσκεται η φόρμα.
- ✓ **:username=^USER^&password=^PASS^**, για τις παραμέτρους της φόρμας.

- ✓ **:No**, για το μήνυμα που επιστρέφει ο server σε περίπτωση αποτυχίας σύνδεσης.
- ✓ **-l xampp**, για να τεθεί το όνομα χρήστη.
- ✓ **-P test.txt**, για να τεθεί το αρχείο με τους κωδικούς.

9. Πίνακας μεταφράσεων ξενικών όρων

Αγγλικά ←→Ελληνικά	
Access control entry (**ACE**)	Εγγραφή ελέγχου πρόσβασης
Access control list (**ACL**)	Λίστα ελέγχου πρόσβασης
Application programming interface (**API**)	Διεπαφή προγραμματισμού εφαρμογών
Backup	Αντίγραφο ασφαλείας
Cache	Κρυφή μνήμη
Checksum	Άθροισμα ελέγχου
Client	Πελάτης
Command line	Γραμμή εντολών
Debug	Αποσφαλμάτωση
Debugger	Αποσφαλματωτής
Dynamic-link library (**DLL**)	Βιβλιοθήκη δυναμικής σύνδεσης
Event log	Αρχείο καταγραφής συμβάντων
File system	Σύστημα αρχείων
Gateway	Πύλη
Hash	Κατακερματισμός
Host	Υπολογιστής
Input / Output (**I/O**)	Είσοδος / Έξοδος
Interface	Διεπαφή
Kernel	Πυρήνας
Malware	Κακόβουλο λογισμικό
Mode	Λειτουργία
Open-source	Ανοιχτού κώδικα
Operating system (**OS**)	Λειτουργικό σύστημα
Partition	Διαμέρισμα
Payload	Ωφέλιμο φορτίο
Plugin	Πρόσθετο
Registry	Μητρώο
Regular expression	Κανονική έκφραση
Server	Εξυπηρετητής
Stateful	Γεμάτο από καταστάσεις
String	Συμβολοσειρά
Symbolic link (**symlink**)	Συμβολική σύνδεση
Task manager	Διαχείρισης εργασιών
Third-party	Τρίτης πλευράς
Throughput	Διεκπεραίωση
Timestamp	Χρονική σήμανση
Verbose	Με πολλές πληροφορίες
Virtual machine (**VM**)	Εικονική μηχανή

10. Βιβλιογραφία

1. **"Το νομικό πλαίσιο των τηλεπικοινωνιών"**, Θανάσης Ξηρός - Θάλεια Ζ. Εμίρη, Εκδόσεις ΣΑΚΚΟΥΛΑ, 2003

2. **"Incident Response & Computer Forensics"**, Second Edition, Kevin Mandia - Chris Posise - Matt Pepe, McGraw-Hill, 2003

3. **"How to use Forensic Toolkit v2.0 on Windows NT 4.0 Server"**, Maarten van Essen - Landis ICT Services & Consultancy, SANS Institute, 2002

11. Σύνδεσμοι

1. **Βικιπαίδια:**
   http://el.wikipedia.org

2. **e-crimenews: Computer Forensics:**
   http://www.e-crime.gr/p/video.html

3. **Wikipedia:**
   http://en.wikipedia.org

4. **e-crimenews: Νομοθεσία:**
   http://www.e-crime.gr/p/links.html

5. **Νομοθεσία για τα προσωπικά – Ελλάδα:**
   http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal

6. **Terminal Vs. Shell – Super User:**
   http://superuser.com/questions/231005/terminal-vs-shell

7. **Linux man pages:**
   http://linux.die.net/man

8. **Netstat command:**
   http://pcsupport.about.com/od/commandlinereference/p/netstat-command.htm

9. **Microsoft TechNet: Resources for IT Professionals:**
   http://technet.microsoft.com

10. **Microsoft:**
    http://www.microsoft.com

11. **Apple Developer:**

http://developer.apple.com

12. ls command:
http://linuxcommand.org/man_pages/ls1.html

13. File types In Linux/Unix explained in detail. – The Linux Juggernaut:
http://www.linuxnix.com/2010/02/file-types-in-linux.html

14. Intel Security:
http://www.mcafee.com

15. last and lastb command:
http://www.computerhope.com/unix/last.htm

16. w command:
http://linux.about.com/library/cmd/blcmdl1_w.htm

17. ForensicsWiki:
http://forensicswiki.org

18. Accounting Utilities Manual:
http://www.gnu.org/software/acct/manual/accounting.html

19. The Sleuth Kit commands – SleuthKitWiki:
http://wiki.sleuthkit.org/index.php?title=The_Sleuth_Kit_commands

20. FileList:
http://www.jam-software.com/filelist/

21. File Scavenger:
http://www.quetek.com/prod02.htm

22. Rifiuti2:
http://abelcheung.github.io/rifiuti2/

23. Rifiuti2 manpage:
http://manpages.ubuntu.com/manpages/utopic/man1/rifiuti2.1.html

24. arpspoof:
http://su2.info/doc/arpspoof.php

25. TCPDUMP manpage:
http://www.tcpdump.org/tcpdump_man.html

26. TCPDUMP manpage (OpenBSD):
http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man8/tcpdump.8

27. WinDump:
http://www.winpcap.org/windump

28. TCPTRACE manual:
http://www.tcptrace.org/tcptrace-manual/manual/index.html

29. Wireshark – Command Line Manual Pages:
http://www.wireshark.org/docs/man-pages/

30. UNIXhelp for Users – University of Edinburgh:
http://unixhelp.ed.ac.uk

31. Lehman College:
http://www.lehman.cuny.edu

32. Windows password crackers – recovery, auditing and PWDUMP tools:
http://passwords.openwall.net/microsoft-windows-nt-2000-xp-2003-vista-7

33. Foroboto: Εργαλείο Ανάκτησης Δεδομένων σε Android | OSarena:
http://osarena.net/foroboto-ergaleio-anaktisis-dedomenon-se-android