ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ & ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Digital Forensics: Case Studies** **Ψηφιακή Εγκληματολογία: Μελέτη Πραγματικών Σεναρίων**
Ονοματεπώνυμο Φοιτητή	**Αποστολόπουλος Δημήτριος**
Πατρώνυμο	**Πέτρος**
Αριθμός Μητρώου	**MTE 1102**
Επιβλέπων	**Ξενάκης Χρήστος, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2013**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω όσους με βοήθησαν και μου συμπαραστάθηκαν κατά τη διάρκεια αυτής της επίπονης προσπάθειας. Ένα μεγάλο ευχαριστώ στους καθηγητές μου, που μου έδωσαν τα εφόδια για να αναπτυχθώ στην πανεπιστημιακή κοινότητα και να επιτύχω τους στόχους μου. Μεγάλο ευχαριστώ επίσης στους φίλους μου, χωρίς τους οποίους δε θα ήμουν ο άνθρωπος που είμαι τώρα. Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου, που όλα αυτά τα χρόνια μου συμπαραστέκονται ηθικά και οικονομικά και διαμορφώνουν γύρω μου ένα άνετο περιβάλλον, μέσα στο οποίο μπορώ να εργαστώ και να επεκτείνω τις γνώσεις μου.

Περίληψη

Η Ψηφιακή Εγκληματολογία είναι ένας κλάδος της εγκληματολογικής επιστήμης που αφορά τη χρήση της ψηφιακής πληροφορίας, η οποία παράγεται, αποθηκεύεται και μεταδίδεται από υπολογιστές, ως πηγή αποδείξεων σε έρευνες και νομικές διαδικασίες. Η απάτη με υπολογιστή και γενικότερα τα ψηφιακά εγκλήματα αυξάνονται μέρα με τη μέρα, ευτυχώς όμως η συντριπτική πλειοψηφία των ενεργειών σε ένα υπολογιστή αφήνουν ίχνη, επιτρέποντας έτσι στους ερευνητές να αποκτήσουν ουσιώδεις αποδείξεις, να λύσουν εγκληματικές υποθέσεις ή ακόμα και να αποτρέψουν κάποια εγκλήματα. Η Ψηφιακή Εγκληματολογία υπάρχει από τότε που οι υπολογιστές αποθήκευαν δεδομένα που θα μπορούσαν να χρησιμοποιηθούν ως αποδείξεις. Για πολλά χρόνια, οι κυβερνητικές υπηρεσίες διενεργούσαν την ψηφιακή εγκληματολογική έρευνα, όμως τα τελευταία χρόνια έχει γίνει κοινή πρακτική και στον ιδιωτικό τομέα.

Το πρώτο κεφάλαιο της συγκεκριμένης πτυχιακής παρέχει μια επισκόπηση των ειδών Ψηφιακής Εγκληματολογίας. Το δεύτερο κεφάλαιο αναφέρεται στο έγκλημα με υπολογιστή και το τρίτο αφορά τη νομοθεσία. Το τέταρτο κεφάλαιο αφορά την Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας. Τα κεφάλαια πέντε και έξι αναφέρονται στις μεθοδολογίες και στα διαθέσιμα εργαλεία Ψηφιακής Εγκληματολογίας. Τέλος, το κεφάλαιο επτά περιλαμβάνει σενάρια - υποθέσεις και μεθόδους διαλεύκανσης αυτών με τη χρήση εργαλείων Ψηφιακής Εγκληματολογίας.

Abstract

Digital Forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings. Computer fraud and digital crimes are growing day by day. Fortunately though, the vast majority of computer activities leave definite traces, allowing investigators to obtain essential evidence, solve criminal cases and prevent crimes. Digital forensics has existed for as long as computers have stored data that could be used as evidence. For many years, forensics investigation was performed primarily by government agencies, but has become common in the commercial sector over the past several years.

The first chapter of this thesis provides a brief overview of digital and mobile forensics. The second chapter refers to computer crime and the third chapter is about legislation concerning digital forensics. The fourth chapter is about Computer Security Incident Response Team. The chapters five and six refer to forensic methodologies and available tools. Finally, the chapter seven contains actual case scenarios using digital forensics methodologies and tools.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

1 Εισαγωγή

1.1 Ψηφιακή Εγκληματολογία

Η **Εγκληματολογική Επιστήμη** (Forensic Science), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής.

Πατέρας της εγκληματολογικής επιστήμης θεωρείται ο Αρχιμήδης (287-212 π.Χ.). Η παράδοση αναφέρει ότι κατάφερε να αποδείξει ότι το στεφάνι του βασιλιά των Συρακουσών Ιέρωνα δεν ήταν χρυσό, με βάση την αρχή της άνωσης που πρώτος αυτός διατύπωσε. Την διαπίστωση αυτή την έκανε στο λουτρό του, από την υπερχείλιση του νερού που εκτόπιζε το σώμα του. Μάλιστα βγήκε τρέχοντας στους δρόμους φωνάζοντας το περίφημο «εύρηκα». Μετά τον Αρχιμήδη, η πρώτη γνωστή εφαρμογή της εγκληματολογικής επιστήμης πραγματοποιήθηκε από έναν Άραβα μηχανικό, τον 7ο αιώνα, ο οποίος χρησιμοποιούσε τα δαχτυλικά αποτυπώματα για να αποδείξει την ταυτοπροσωπία δανειστών και δανειοληπτών. [1]

Τον ίδιο αιώνα, τα δαχτυλικά αποτυπώματα χρησιμοποιήθηκαν και από τους Κινέζους. Συστηματική εφαρμογή της εγκληματολογικής επιστήμης στον ευρωπαϊκό χώρο παρατηρείται αρχικά τον 16ο αιώνα, όταν η ιατρική επιστήμη άρχισε να χρησιμοποιεί τις γνώσεις της για τον προσδιορισμό της αιτίας θανάτου, σε περιπτώσεις ανθρωποκτονιών. Από τον 18ο αιώνα και άλλες επιστήμες, όπως η φυσική και χημεία, άρχισαν να χρησιμοποιούνται στην διερεύνηση των εγκλημάτων. Στους αιώνες που ακολούθησαν η εγκληματολογική επιστήμη εδραιώθηκε στον τομέας της διερεύνησης του εγκλήματος. Σήμερα η έρευνα του συνόλου των εγκλημάτων, στηρίζεται κατά μεγάλο ποσοστό στην εγκληματολογική επιστήμη.

Η **Ψηφιακή Εγκληματολογία** (Digital Forensics), είναι «η επιστήμη που ασχολείται με την συλλογή, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό». Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή.

Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα του κατηγορουμένου.

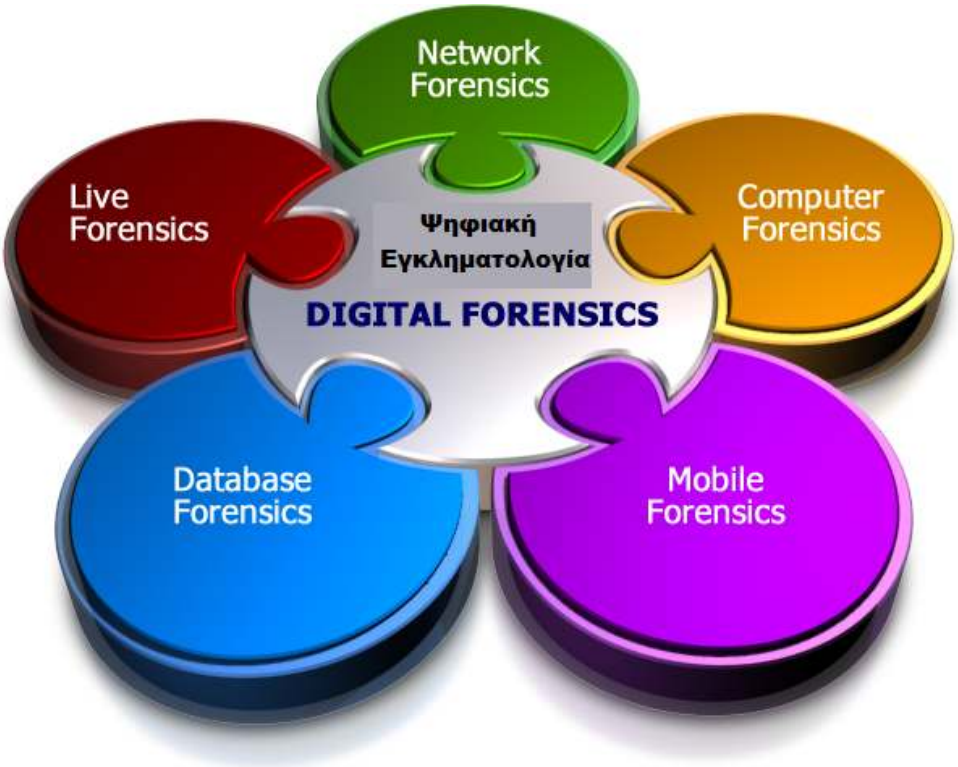
1.2 Ψηφιακή Εγκληματολογία σε Κινητές Συσκευές

Η Ψηφιακή Εγκληματολογία σε κινητές συσκευές (mobile forensics) είναι ένας κλάδος της Ψηφιακής Εγκληματολογίας που σχετίζεται με την ανάκτηση ψηφιακών αποδείξεων ή δεδομένων από μια κινητή συσκευή. Ο όρος κινητή συσκευή δεν περιλαμβάνει μόνο κινητά τηλέφωνα, αλλά όλες εκείνες τις συσκευές που έχουν εσωτερική μνήμη και δυνατότητες επικοινωνίας, όπως τα PDAs και τα tablets. Αν και η εμπλοκή των κινητών συσκευών σε εγκληματικές πράξεις ήταν ευρέως αναγνωρισμένη εδώ και χρόνια, η ψηφιακή έρευνα κινητών συσκευών μετρά μόνο λίγα χρόνια ζωής. [2]

Οι διαφορές των κινητών, ειδικά τα πιο νέα μοντέλα, με τους υπολογιστές οδήγησαν στην ανάγκη δημιουργίας ενός κλάδου έρευνας, γιατί οι τεχνικές της Ψηφιακή Εγκληματολογίας δεν ήταν αρκετές. Οι κινητές συσκευές μπορούν να αποθηκεύουν πολλών ειδών προσωπικά στοιχεία, όπως επαφές,

φωτογραφίες, βίντεο, SMS, MMS, email, πληροφορίες περιήγησης στο Διαδίκτυο(web browsing), πληροφορίες θέσης και μηνύματα κοινωνικής δικτύωσης.

Η τεχνικές Ψηφιακής Εγκληματολογίας σε υπολογιστές, σε κινητές συσκευές και η νομοθεσία είναι μόνο μερικά κομμάτια του παζλ της Ψηφιακής Εγκληματολογικής Επιστήμης.



Εικόνα 1. Συνιστώσες της Ψηφιακής Εγκληματολογίας

1.3 Διαδικασία Έρευνας

Η ηλεκτρονική έρευνα ενός εγκλήματος διαφέρει σημαντικά από την «παραδοσιακή έρευνα» που αναζητά απτά στοιχεία. Ο ηλεκτρονικός ερευνητής δεν αναζητά σε κάποιο συρτάρι ή σε κάποιο χώρο αλλά σε ηλεκτρονικούς φακέλους, αρχεία, αποθηκευτικά μέσα, υπολογιστικά συστήματα.

Τα *ψηφιακά αποδεικτικά* στοιχεία που συλλέγονται θεωρούνται ιδιαιτέρως ευαίσθητα, γι' αυτό σημαντικό κομμάτι της ηλεκτρονικής έρευνας αποτελεί η διατήρησή τους και η διασφάλιση τη μη αλλοίωσής τους.

Η ηλεκτρονική έρευνα ενός εγκλήματος, πρέπει να διεξάγεται σύμφωνα με την ισχύουσα κατά περίπτωση νομοθεσία, καθώς πολλές αμφιβολίες δημιουργούνται για την επάρκεια των γνώσεων ενός ερευνητή και για το αν η ανάλυση και διατήρηση των στοιχείων ακολουθεί τις προβλεπόμενες διαδικασίες. Κατά συνέπεια, πολλές φορές παρατηρείται το φαινόμενο σε μία δίκη να αμφισβητείται είτε η έρευνα, είτε να κατάσχονται οι πληροφορίες, επειδή δεν υφίσταται ειδικό νομοθετικό πλαίσιο στην περίπτωση των ερευνών στον κυβερνοχώρο.

Κατά τη διεξαγωγή μιας έρευνας, είναι σημαντικό να μην παραβιάζεται η ιδιωτικότητα του ατόμου. Κατόπιν τούτου, απαιτείται συνήθως ένταλμα που θα πρέπει να καθορίζει με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν και ακόμα και αν ο ερευνητής θεωρεί ότι μπορεί να αντλήσει στοιχεία και

από άλλα εκτός των παραπάνω αντικείμενα, τα στοιχεία αυτά δεν θα έχουν αποδεικτική αξία στη δικαστική αίθουσα.

Η ηλεκτρονική εγκληματολογική έρευνα πρέπει να πραγματοποιείται βάσει των κάτωθι αρχών:

- Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται σε υπολογιστή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
- Χρήση αρχέτυπων δεδομένων από τρίτο άτομο, κατόπιν εξουσιοδότησης.
- Δημιουργία ιστορικού ελέγχου των διαδικασιών.
- Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών.

Συνοψίζοντας τα παραπάνω:

1) **Συλλογή**: Περιλαμβάνει τις διαδικασίες και τις μεθόδους καταγραφής της φυσικής σκηνής του εγκλήματος καθώς και της απόλυτα πιστής αντιγραφής της πρωτότυπης ψηφιακής απόδειξης χρησιμοποιώντας τυποποιημένες και αποδεκτές πρακτικές.
2) **Διατήρηση**: Περιλαμβάνει ενέργειες απομόνωσης, προστασίας και συντήρησης της κατάστασης της φυσικής και της ψηφιακής απόδειξης, όπως είναι για παράδειγμα η παρεμπόδιση των ανθρώπων από τη χρήση των ψηφιακών συσκευών και η απαγόρευση άλλων ηλεκτρομαγνητικών συσκευών να χρησιμοποιούνται πέρα από μια συγκεκριμένη ακτίνα.
3) **Ανάλυση**: Σε αυτή τη φάση προσδιορίζεται η σημαντικότητα των συλλεγμένων δεδομένων και βγαίνουν συμπεράσματα που βασίζονται στις αποδείξεις που βρέθηκαν.
4) **Παρουσίαση**: Στο τέλος της έρευνας, τα στοιχεία καταγράφονται και παρουσιάζονται στους εντολείς. Ο ειδικός θα πρέπει να παρουσιάσει τα ευρήματα του σε μια καθαρή, περιεκτική, δομημένη και σαφή αναφορά στην οποία θα εξηγεί όλα τα συμπεράσματα στα οποία έχει καταλήξει.

1.4 Ψηφιακές Αποδείξεις και Δεδομένα

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή. [1] Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή, διαχωρίζοντάς τις σε:

- **Ψηφιακές αποδείξεις (digital evidence):** Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.
- **Αντικείμενα δεδομένων (data objects):** Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.
- **Φυσικά αντικείμενα (physical items):** Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
- **Γνήσιες ψηφιακές αποδείξεις (original digital evidence):** Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.
- **Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence):** Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
- **Αντίγραφο (copy):** Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

Οι ψηφιακές αποδείξεις μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, palmtop, κινητό τηλέφωνο κ.α., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs, DVDs, κάρτες μνήμης κ.α.

Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διαφόρων εργαλείων και μεθόδων. Ο ερευνητής, λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα.

Οι ψηφιακές αποδείξεις αποτελούνται από ψηφιακά δεδομένα (digital data). Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε μεταβλητά δεδομένα (volatile data) και σε διαρκή δεδομένα (persistent data). Τα μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν σταματήσει η τροφοδοσία του υπολογιστή με ρεύμα, αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση. Τα διαρκή δεδομένα είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως οδηγοί USB, CDs και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται, όταν τερματιστεί η λειτουργία του υπολογιστή ή γίνει επανεκκίνηση.

2 Ηλεκτρονικό Έγκλημα

2.1 Εισαγωγή

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison (1994) προσδιόρισε το ηλεκτρονικό έγκλημα ως *«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της»*. Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: *e-crime, cybercrime, computer-crime, internet related crime και hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα*, *δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop κλπ. Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί:

- Να αποτελεί τον στόχο κάποιας επίθεσης. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.

- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

2.2 Μορφές Ηλεκτρονικού Εγκλήματος

Σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως [1]:

1) **Κακόβουλες εισβολές σε δίκτυα (hacking και cracking):** Η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο υπολογιστών. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλέσει ζημιά ή να αποκομίσει οικονομικό όφελος αναφέρεται ως χάκερ (hacker) ενώ σε αντίθετη περίπτωση ως κράκερ (cracker).
2) **Επιθέσεις Άρνησης Εξυπηρέτησης:** Αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με τη διακοπή λειτουργίας μιας κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό.
3) **Κακόβουλο λογισμικό:** Είναι προγράμματα Ηλεκτρονικού Υπολογιστή (Η/Υ) που δημιουργούνται με σκοπό να προκαλέσουν ζημιά σε Η/Υ ή να εισχωρήσουν σε ένα Η/Υ για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τρεις βασικές κατηγορίες: Ιούς, (viruses), σκουλήκια (worms) και Δούρειους ίππους (Trojan Horses).
4) **Ανεπιθύμητη Αλληλογραφία (Spamming):** Είναι η χρήση οποιοδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιοδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό, από αυτόν που το λαμβάνει.
5) **Επιθέσεις σε δικτυακούς τόπους (sites):** Αποσκοπούν στην αλλοίωση τον περιεχομένου ενός δικτυακού τόπου, κατά τρόπο χιουμοριστικό, προπαγανδιστικό ή και προσβλητικό.
6) **Ηλεκτρονικό ψάρεμα (Phishing):** Με το phishing ή "ηλεκτρονικό ψάρεμα" επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κλπ. προκειμένου να χρησιμοποιηθούν σ' άλλες παράνομες δραστηριότητες. Οι επιθέσεις αυτές στηρίζονται στην εξαπάτηση του θύματος με διάφορους τρόπους και μεθόδους όπως π.χ., την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο. Μια από τις τεχνικές που χρησιμοποιείται είναι το social engineering.
7) **Πειρατεία λογισμικού:** Αναφέρεται στην αναπαραγωγή και/ή διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.
8) **Απάτη στο Διαδίκτυο:** Αποτελεί την ηλεκτρονική έκφανση της συμβατικής μορφής της απάτης. Μπορεί να συντελεστεί με διάφορους τρόπους και μεθόδους. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλλοντας Νιγηριανές Επιστολές ή ενημέρωση για κέρδη στο Ισπανικό Λόττο. Επίσης πολλές απάτες πραγματοποιούνται με τη χρήση πιστωτικών καρτών.

9) **Κλοπή ταυτότητας (identity theft):** Η υποκλοπή στοιχείων ταυτότητας ανυποψίαστων ατόμων και η χρήση τους για παράνομες δραστηριότητες.
10) **Ξέπλυμα χρήματος:** Η προσπάθεια εξαφάνισης χρήματος που προέρχεται από παράνομες δραστηριότητες . Χαρακτηριστικό παράδειγμα αποτελεί η αγορά μέσω του Διαδικτύου ασυνήθιστα μεγάλων ποσοτήτων αγαθών.
11) **Διακίνηση παιδικού πορνογραφικού υλικού:** Αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων.
12) **Διαδικτυακή τρομοκρατία:** Αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μιας τρομοκρατικής επίθεσης.
13) **Επιθέσεις παρενόχλησης (cyberbullying):** Είναι μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.α.

3 Νομοθεσία και Κρατικός Μηχανισμός

3.1 Δικονομία

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος πρέπει να συμβαδίζει με τους ισχύοντες κατά περίπτωση νόμους και κανονισμούς. Νομικοί προβληματισμοί προκύπτουν σχετικά με την έρευνα και κατάσχεση των ψηφιακών αποδείξεων, κατά πόσο δηλαδή οι γνώσεις ενός ερευνητή είναι επαρκείς για τη διεκπεραίωση μιας έρευνας σε ένα Η/Υ και αν η ανάλυση και διατήρηση των αποδείξεων γίνεται σύμφωνα με τις προβλεπόμενες διαδικασίες.

Σε μια δίκη αρχικά τίθεται υπό αμφισβήτηση η έρευνα και η κατάσχεση πληροφοριών. Σύμφωνα με το άρθρο 253 Κ.Π.Δ μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακούργημα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να βεβαιωθεί ή να διευκολυνθεί η διάπραξη του εγκλήματος, η ανακάλυψη των δραστών κ.λ.π. Επιπλέον κατά τη διεξαγωγή μιας έρευνας πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπέρμετρου. Επειδή δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για τις έρευνες στον κυβερνοχώρο, οι ανωτέρω διατάξεις εφαρμόζονται αναλογικά και στις περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχτηκαν.

Κατά τη διεξαγωγή μιας έρευνας, το βασικό αγαθό, που διακυβεύεται, είναι η ιδιωτικότητα του ατόμου. Το Αμερικανικό Σύνταγμα απαιτεί την ύπαρξη εντάλματος για τη διεξαγωγή έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αιτία ότι διαπράχθηκε έγκλημα. Το ένταλμα θα πρέπει να καθορίζει, επακριβώς το μέρος και τα αντικείμενα που μπορούν να ερευνηθούν. Για παράδειγμα, εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει στο χώρο. Αν το πράξει, έστω κι αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο γιατί παραβιάστηκε το ένταλμα.

Το δεύτερο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχεία σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για τη διεκπεραίωση μιας ηλεκτρονικής έρευνας. Ο μεγαλύτερος προβληματισμός έγκειται στα χρησιμοποιούμενα από τον ερευνητή εργαλεία λογισμικού. Ο ερευνητής, απλά γνωρίζει τη χρήση ενός

εργαλείου λογισμικού. Δεν μπορεί να έχει πρόσβαση στον πηγαίο κώδικα και έτσι δεν γνωρίζει τι εργασίες επιτελεί το λογισμικό.

Πώς λοιπόν μπορεί να βεβαιώσει ότι τα ψηφιακά δεδομένα, που συλλέχθηκαν, αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορούμενου; Έως σήμερα, δεν υπάρχει απόφαση δικαστηρίου που να απέρριψε την επιστημονική άποψη ενός ερευνητή, τέτοιο ενδεχόμενο, όμως δεν αποκλείεται να συμβεί στο μέλλον από τη στιγμή που τα εργαλεία λογισμικού εξελίσσονται και γίνονται όλο και πιο πολύπλοκα.

Το τρίτο και τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξετασθεί (π.χ. ενός σκληρού δίσκου) δημιουργώντας ακριβές αντίγραφο. Τα δικαστή- ρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο. Ωστόσο, πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την άρτια διατήρησή του.

Οι ψηφιακές πληροφορίες μπορούν να επηρεαστούν από μαγνητικά πεδία, καιρικές συν- θήκες κ.ά. Για παράδειγμα, στη υπόθεση Ohio v. Cook, ο κατηγορούμενος προέβαλλε μια σειρά από ισχυρισμούς έναντι της μη ορθής συλλογής και διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωσή τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θέση. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά τη διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών.

3.2 Τομέας Εξέτασης Ψηφιακών Πειστηρίων

Στο Εργαστήριο Δικαστικής Γραφολογίας λειτουργεί και ο Τομέας Εξέτασης Ψηφιακών πειστηρίων (Π.Δ. 223/16-7-2003). Ο τομέας δομήθηκε πάνω στον πυρήνα δύο ειδικών που εξέταζαν τις προκηρύξεις διάφορων οργανώσεων, όταν αυτές άρχισαν να χρησιμοποιούν Η/Υ.

Αντικείμενα εργασίας του τομέα σήμερα είναι:

- αναγνώσεις και συγκρίσεις ψηφιακών δεδομένων ή αρχείων ευρισκομένων σε ψηφιακούς χώρους Η/Υ ή σε περιφερειακά αυτών συστήματα.
- περί της γνησιότητας ψηφιακού υλικού-λογισμικού.
- επί κινητών τηλεφώνων ή άλλων ηλεκτρονικών συσκευών, οι οποίες περιέχουν ή αποθηκεύουν ψηφιακά δεδομένα.
- αναγνώσεις δεδομένων επί μαγνητικών ταινιών πιστωτικών ή άλλων καρτών, καθώς και εξετάσεις επί άλλων σύγχρονων μέσων ψηφιακής αποθήκευσης δεδομένων σε ηλεκτρονικό κύκλωμα ή άλλης μορφής ψηφιακό χώρο.

Παράλληλα ο τομέας παρέχει τεχνική συνδρομή σε διαδικασίες κατάσχεσης, μεταφοράς, αποθήκευσης και αποστολής των ψηφιακών πειστηρίων, που σχετίζονται με εγκληματική δραστηριότητα. Επιπλέον τηρεί αρχείο διενεργούμενων εργαστηριακών εξετάσεων, καθώς και συλλογές ψηφιακών πειστηρίων, λογισμικών και συσκευών ψηφιακής αποθήκευσης, προς υποβοήθηση των συγκριτικών εν γένει εξετάσεων.

3.3 Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Η ελληνική αστυνομία εδώ και χρόνια οργανώνεται και εξελίσσεται σύμφωνα με το πρότυπο του βρετανικού Computer Crime Unit και των τμημάτων των Cyber Crime στις αστυνομίες ολόκληρου του κόσμου. Πιο συγκεκριμένα με το Π.Δ 100/2004 ιδρύθηκε η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, υπαγόμενο στη Διεύθυνση Ασφάλειας Αττικής/ Υποδιεύθυνση Δίωξης Οικονομικών Εγκλημάτων & Αρχαιοκαπηλίας & Ηθών. [4]

Η εν λόγω Υπηρεσία έχει ως αρμοδιότητες τη δίωξη εγκλημάτων που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού, όπως επίσης και την επί 24ωρου έρευνα του Διαδικτύου προς διαπίστωση εγκληματικών πράξεων που τελούνται στη Χώρα. Αποτελείται από εξειδικευμένα στελέχη της Ελληνικής Αστυνομίας, επιλαμβάνονται υποθέσεων σε όλη την επικράτεια, ενώ παράλληλα συνεργάζεται με αντίστοιχες Υπηρεσίες του εξωτερικού.

Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων που ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.
- Το Τμήμα Προστασίας Ανηλίκων που ασχολείται με τα εγκλήματα που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων που ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, που ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

Πρόκειται για καθαρόαιμο επιχειρησιακό τμήμα που ασχολείται με ευρεία γκάμα υποθέσεων, όπως:

- Παραχάραξη πιστωτικών καρτών.
- Παραποίηση ηλεκτρονικών σελίδων στο Διαδίκτυο.
- Διάπραξη εγκλημάτων, όπως πορνογραφία και παιδοφιλία, μέσω του Διαδικτύου.
- Παραβάσεις τηλεφωνικών δικτύων.
- Οικονομικές απάτες μέσω υπολογιστών, όπως παράνομη μεταφορά χρημάτων.
- Δυσφημήσεις προσώπων μέσω του Διαδικτύου.

Σύμφωνα με τα όσα αναφέρει σχετικά ο επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος κ. Σφακιανάκης Ε., «κατά τη διάρκεια του 2006 δεχθήκαμε περίπου 400 καταγγελίες από πολίτες που αφορούσαν κυρίως περιπτώσεις απάτης μέσω Διαδικτύου με τη μέθοδο των απατηλών e-mail μηνυμάτων. Στο πρώτο εξάμηνο του 2007 οι καταγγελίες έχουν ήδη ξεπεράσει τις 400. Παράλληλα έχουν εξιχνιαστεί και αρκετές υποθέσεις όπως, οικονομικές απάτες, πλαστογραφήσεις πτυχίων, επιθέσεις ελλήνων χάκερ, υποθέσεις παιδεραστίας κ.λ.π ».

3.4 Ομάδα Δράσης για την Ψηφιακή Ασφάλεια

Το Υπουργείο Οικονομίας & Οικονομικών στο πλαίσιο της Ψηφιακής Στρατηγικής 2006-2013 προχώρησε στη σύσταση Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness & Response to Threats) ή D.A.R.T, όπως ανακοίνωσε στις 14-06-2007 ο ίδιος ο Υπουργός Οικονομίας και Οικονομικών. Βασικός σκοπός της Ομάδας είναι η πρόληψη και αντιμετώπιση των πάσης φύσεως ψηφιακών κινδύνων που μπορούν να απειλήσουν τους έλληνες πολίτες του κυβερνοχώρου. Στόχος η ενίσχυση της εμπιστοσύνης του κοινού των χρηστών στα νέα μέσα. [5]

Η Ομάδα D.A.R.T συντονίζεται από τον ειδικό γραμματέα Ψηφιακού Σχεδιασμού του Υπουργείου Οικονομίας και Οικονομικών, ενώ συμμετέχουν, εκπρόσωποι της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ), της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε), της Δίωξης

Ηλεκτρονικού Εγκλήματος του Υπουργείου Δημοσίας Τάξης κ.λ.π. Ακόμη στην Ομάδα συμμετέχουν ειδικοί εμπειρογνώμονες της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού. Στους σκοπούς της Ομάδας περιλαμβάνονται επίσης η ενημέρωση, η πρόληψη, καθώς και η ανταλλαγή τεχνογνωσίας για την αντιμετώπιση κινδύνων.

Η Ομάδα δραστηριοποιείται σε τρεις πυλώνες. Ο πρώτος είναι αυτός της πρόληψης των ψηφιακών κινδύνων από πολίτες, επιχειρήσεις και δημόσιους φορείς. Στο επίπεδο της πρόληψης, η D.A.R.T προτείνει πρακτικά μέτρα για την αποφυγή ψηφιακών κινδύνων, αναπτύσσει τεχνικές αξιολόγησης και πρόβλεψης πιθανών ψηφιακών απειλών, παρακολουθεί την εξάπλωση ψηφιακών κινδύνων και τους τρόπους έγκαιρης αντιμετώπισής τους.

Στο πλαίσιο του δεύτερου πυλώνα, της ενημέρωσης δηλαδή για ψηφιακούς κινδύνους, η Ομάδα λειτουργεί ως κεντρικό σημείο για την ενημέρωση πολιτών και επιχειρήσεων, αναφορικά με ζητήματα αντιμετώπισης ψηφιακών κινδύνων και απειλών, αξιοποιώντας κάθε πρόσφορο μέσο. Ακόμη, ενημερώνει και παρέχει πληροφόρηση σχετικά με ζητήματα ψηφιακής ασφαλείας στο κοινό, σε δημόσιους, ιδιωτικούς και ανεξάρτητους φορείς που δραστηριοποιούνται σε θέματα τεχνολογιών πληροφορικής και επικοινωνιών, με στόχο την ευαισθητοποίηση και τη συνειδητοποίηση των ψηφιακών κινδύνων ,και επιμελείται τη συλλογή και τη διάχυση πληροφοριών μέσα από πολλαπλά δίκτυα για την αύξηση της συνειδητοποίησης των ζητημάτων ψηφιακής ασφαλείας.

Στον τρίτο πυλώνα, αυτόν της ανταλλαγής τεχνογνωσίας, η Ομάδα συνεργάζεται με οργανώσεις και φορείς, διευκολύνει την επικοινωνία μεταξύ εμπειρογνωμόνων στους τομείς της ασφαλείας συστημάτων, αναπτύσσει δεσμούς με ερευνητικούς οργανισμούς και συμμετέχει σε ερευνητικές δραστηριότητες, καθώς και σε εγχώρια και διεθνή forum, αναθέτει έρευνες και συντονίζει παρουσίαση μελετών αναφορικά με την ασφάλεια συστημάτων και την προστασία των πολιτών, επιχειρήσεων και του κράτους από ψηφιακούς κινδύνους ενώ συνεργάζεται με διεθνείς και εγχώριους φορείς του δημόσιου ή ιδιωτικού φορέα προκειμένου να εξασφαλιστεί η προστασία των δικαιωμάτων των πολιτών έναντι κακόβουλων απειλών.

Σύμφωνα με το portal που έχει δημιουργήσει η Ομάδα, αρμόδιες αρχές για να προστατέψουν και να βοηθήσουν τον πολίτη είναι: α) η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), β) η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) και γ) το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος.

Η Α.Δ.Α.Ε είναι ανεξάρτητη αρχή που έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλον τρόπο, καθώς και την ασφάλεια των δικτύων και πληροφοριών [6]. Η Ε.Ε.Τ.Τ είναι επίσης ανεξάρτητη αρχή η οποία αποτελεί τον εθνικό ρυθμιστή που ελέγχει και εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και Διαδικτύου, καθώς και την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.[7]

3.5 Ευρώπη και Ηλεκτρονικό Έγκλημα

Η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος στον Ευρωπαϊκό χώρο, πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης, το 1976 στο Στρασβούργο, στις εργασίες του Συνεδρίου για τις Εγκληματολογικές Πλευρές του Οικονομικού Εγκλήματος. Ήταν η πρώτη φορά που παρουσιάστηκαν οι μορφές του ηλεκτρονικού εγκλήματος, συμπεριλαμβανόμενης και της απάτης.

Το 1986, συστήθηκε μια επιτροπή από το Ευρωπαϊκό Συμβούλιο, η οποία εξέτασε την ισχύουσα νομοθεσία στα κράτη-μέλη, τα δε συμπεράσματά της συμπεριλήφθησαν στη Σύσταση του 1989, η οποία

όριζε εγκληματικές πράξεις, όπως απάτη και πλαστογραφία με ηλεκτρονικούς υπολογιστές, καταστροφή δεδομένων και λογισμικού, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη αναπαραγωγή λογισμικού κ.ά. Επίσης, η Σύσταση αυτή περιελάμβανε και μια σειρά από Οδηγίες (μη υποχρεωτικές) προς τα κράτη-μέλη, σχετικά με τη μεθοδολογία θέσπισης νομοθετικών κειμένων για το ηλεκτρονικό έγκλημα.

Οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο ξεκίνησαν το 1997, όταν συστήθηκε μια επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα, που αναπτύσσεται και συνεχών διευρύνεται στον κυβερνοχώρο. Αν και αρχικά η περαίωση των εργασιών της επιτροπής, είχε προσδιοριστεί για το 1999, τα ιδιαίτερα προβλήματα που συνάντησαν τα μέλη της, έθεσαν νέα προθεσμία το έτος 2000.

Τελικά, το κείμενο της «Σύμβασης για το Έγκλημα στον Κυβερνοχώρο», υπογράφηκε στις 23-11-2001, στη Βουδαπέστη, από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου . Στη Σύμβαση, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

- για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ, τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.
- για τα αδικήματα που σχετίζονται με τους υπολογιστές, όπως η απάτη με Η/Υ και πλαστογραφία.
- για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
- για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επιπρόσθετα περιλαμβάνονται ρυθμίσεις για τη συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων, καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγεται το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η εν λόγω Σύμβαση έχει χαρακτηρισθεί από πολλούς ως το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή Ένωση και έχει ήδη υπογραφεί από 33 κράτη συμπεριλαμβανομένων των ΗΠΑ, Καναδά, Ν. Αφρική και Ιαπωνία. Φυσικά δεν λείπουν οι επικριτές της.

Παράλληλα υπάρχουν και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του ηλεκτρονικού εγκλήματος. Ενδεικτικά αναφέρουμε τα ακόλουθα που ισχύουν στην Ευρωπαϊκή Ένωση:

1) Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
2) Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
3) Το Ψήφισμα 97/C70/01 του Συμβουλίου και το άρθρο 2 της Σύμβασης της Europol (ν. 2605/1998).
4) Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
5) Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση

διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

6) Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
7) Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
8) Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

3.6 Ισχύουσα Κατάσταση στην Ελλάδα

Στην ελληνική έννομη τάξη, νομοθεσία ειδική για θέματα Διαδικτύου που να ρυθμίζει τη συμπεριφορά των χρηστών του δεν υπάρχει. Ο όρος 'ηλεκτρονικό έγκλημα' δεν αναφέρεται πουθενά στο ελληνικό δίκαιο. Οι παραβάσεις που διαπιστώνονται για αδικήματα που διαπράττονται μέσω Διαδικτύου τιμωρούνται σύμφωνα με τη νομοθεσία της κλασικής μορφής τέλεσης των αδικημάτων αυτών. Ισχύουν νόμοι για εγκλήματα που διαπράττονται με Η/Υ (1805/1988), για την προστασία προσωπικών δεδομένων από τη χρήση των τηλεπικοινωνιών (2867/2000, ο οποίος αντικατέστησε τον 2246/1994), την προστασία προσωπικών δεδομένων κατά τη χρήση του Διαδικτύου (2774/1999, σε συνδυασμό με 2472/1997), την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας (2225/1994, σε συνδυασμό με 3115/2003) κ.λ.π. Επιπρόσθετα ειδικότερες διατάξεις για θέματα που σχετίζονται με το ηλεκτρονικό έγκλημα περιλαμβάνονται στο Π.Δ. 131/2003, το οποίο θεσπίσθηκε σε εφαρμογή κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο και αναφέρεται στην "ανεπιθύμητη αλληλογραφία" και στην ευθύνη των παρόχων υπηρεσιών Διαδικτύου για πράξεις των χρηστών τους.

Ειδικά ο Ν. 1805/1988, τροποποίησε - συμπλήρωσε τις σχετικές διατάξεις του Π.Κ, που αφορούν τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. Πιο συγκεκριμένα προστέθηκαν τέσσερα εμβόλιμα άρθρα:

- εδαφ.β΄ στο άρθρο 13 περ.γ΄ (που περιγράφεται η έννοια του εγγράφου)
- 370β
- 370γ
- 386α

Φυσικά όταν καταρτιζόταν ο νόμος αυτός, το Διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη κατάρτισης ειδικότερης νομοθεσίας. Ανεξάρτητα όμως από το εάν ο Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής, το βέβαιο είναι ότι δεν επαρκεί να καλύψει τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του Διαδικτύου.

Απ' την άλλη έχει υποστηριχθεί η άποψη ότι δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομικό κενό στο Διαδίκτυο, διότι αναλογικά το κοινό δίκαιο μπορεί να εφαρμοστεί και στο χώρο του Διαδικτύου. Η άποψη αυτή βέβαια είναι εμφανώς εσφαλμένη, καθότι στον ποινικό τουλάχιστο χώρο, δεν ισχύει η αρχή της αναλογίας.

Στο βαθμό, λοιπόν, που τα προβλεπόμενα εγκλήματα (άρθρα 370β, 370γ, 386α) διαπράττονται και σε περιβάλλον Διαδικτύου, τότε τα άρθρα αυτά εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

Τα εγκλήματα του κυβερνοχώρου τελούνται με απαραίτητη προϋπόθεση τη χρήση τηλεπικοινωνιών, σταθερής ή κινητής τηλεφωνίας (Υπηρεσίες WAP). Ο Ν. 2246/1994 ψηφίστηκε για την οργάνωση και εν γένει λειτουργία του τομέα τηλεπικοινωνιών και ρυθμίζει θέματα σχετικά με το Διαδίκτυο. Προσδιορίζει συγκεκριμένα ότι φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι τα φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού.

Σύμφωνα με το άρθρο 2 παρ. 3 Ν.2246/1994 συνιστάται η Εθνική Επιτροπή Τηλεπικοινωνιών, η οποία έχει τεχνικές, νομικές και προανακριτικές αρμοδιότητες, γνωμοδοτεί για την έκδοση των κωδίκων δεοντολογίας, επιβάλλει διοικητικά πρόστιμα, και ελέγχει γενικώς την ομαλή και ορθή λειτουργία του τομέα τηλεπικοινωνιών. Σύμφωνα με το Ν. 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) προβλέπονται ποινικές κυρώσεις για όποιον προβαίνει σε διασύνδεση αρχείων χωρίς να τη γνωστοποιήσει στην αρμόδια αρχή και για όποιον χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών, ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο.

Αυτή είναι μία γενική διάταξη, που αποσκοπεί πράγματι στην προστασία προσωπικών δεδομένων, αλλά δεν καλύπτει τα γνήσια εγκλήματα κυβερνοχώρου, αφού η διασύνδεση αρχείων ή η επέμβαση σε δεδομένα, ή η διάδοση δεδομένων, η επεξεργασία και ανακοίνωσή τους μπορεί να πραγματοποιηθεί και χωρίς τη βούληση και γνώση του κατόχου ηλεκτρονικού υπολογιστή ή του χρήστη του Διαδικτύου. Για παράδειγμα, ένας κατευθυνόμενος από το δράστη ηλεκτρονικός "ιός" (virus) προσβάλλει το σύστημα και χρησιμοποιεί όλες τις ηλεκτρονικές διευθύνσεις (e-mail) φίλων, γνωστών του κ.λπ., που έχει αποθηκεύσει ο ανυποψίαστος κάτοχος και χρήστης του Διαδικτύου, προκειμένου να αποστείλει ο δράστης σε αυτούς ευαίσθητα προσωπικά δεδομένα.

Η χρήση συγκεκριμένων κωδίκων για τη μετατροπή δεδομένων με σκοπό την ανάγνωσή τους αποσκοπεί στην προστασία των δεδομένων αυτών. Με την κρυπτογραφία αποτρέπεται δηλαδή η πρόσβαση σε δεδομένα από μη εξουσιοδοτημένα πρόσωπα. Προς τούτο έχει διαμορφωθεί ένας ιδιαίτερος επιστημονικός κλάδος, η διαχείριση ασφάλειας δικτύων (network security administration).

Σύμφωνα με το άρθρο 1 του Ν. 2225/1994 ιδρύεται η Εθνική Επιτροπή Προστασίας Απορρήτου των Επικοινωνιών, της οποίας αποστολή είναι και η προστασία του απορρήτου της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης. Υπό τις προϋποθέσεις του Ν. 2225/1994 είναι δυνατή η παρακολούθηση ανταλλαγής ηλεκτρονικής αλληλογραφίας (e-mail). Για παράδειγμα, ο Α εκβιάζει τον Β με την αποστολή e-mail, ο Β καταγγέλλει το περιστατικό στην αστυνομία και η αστυνομία ζητά από τον πάροχο (Internet Service Provider) να παρακολουθήσει την ανταλλαγή e-mail. Ο πάροχος δεν δικαιούται να επικαλεστεί το απόρρητο των επικοινωνιών. Έχει τεθεί σε ισχύ η Απόφαση 165/2011,ΦΕΚ Β' 2715/17-11-2011, από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε), που αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για τη Διασφάλισή του Απορρήτου των Ηλεκτρονικών Επικοινωνιών. Αναλυτικότερα τον ισχύον νομοθετικό πλαίσιο στην Ελλάδα στο Παράρτημα Β.

Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων Διεθνών Οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων. Και οι τρεις παραπάνω Διεθνείς Οργανισμοί έχουν ασχοληθεί με το έγκλημα στον Κυβερνοχώρο. Σχετική όμως Σύμβαση καταρτίσθηκε μόνο στα πλαίσια του Συμβουλίου της Ευρώπης.

4 Computer Security Incident Response Team

4.1 Εισαγωγή

Απόλυτη ασφάλεια στο χώρο της πληροφορικής δεν υπάρχει. Συνεπώς όσο καλά προστατευμένο και να θεωρείται ένα δίκτυο υπολογιστών, κάποια στιγμή θα υπάρξει μια παραβίαση ασφαλείας. Αυτό μπορεί να οφείλεται είτε στο ότι οι γνώσεις του υπεύθυνου ασφαλείας είναι πεπερασμένες είτε γιατί το είδος της επίθεσης ή ο τρόπος εμφανίζεται για πρώτη φορά (zero day attack).

Η αντιμετώπιση περιστατικών είναι μια οργανωμένη προσέγγιση για να υπάρχει δυνατότητα διαχείρισης μιας επίθεσης ή μια παραβίαση ασφαλείας (γνωστό και ως περιστατικό). Ο σκοπός είναι να διαχειριστούμε την κατάσταση με τέτοιο τρόπο, έτσι ώστε να περιορίσουμε τη ζημιά, το χρόνο αποκατάστασης και το κόστος. Ένα σχέδιο αντιμετώπισης περιστατικών δεν μπορεί να θεωρείται πλήρες αν δεν περιλαμβάνει μια πολιτική στην οποία να ορίζεται ρητά τι είναι ένα περιστατικό και να παρέχει μια αναλυτική διαδικασία για την αντιμετώπισή του όταν προκύψει.

Τέτοια περιστατικά αναλαμβάνει η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Υπολογιστών κάθε εταιρείας ή εξωτερικοί συνεργάτες [8]. Η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Υπολογιστών (Computer Security Incident Response Team - CSIRT), είναι ένα σύνολο εξειδικευμένων ανθρώπων, οι οποίοι έχουν επιλεχθεί προσεκτικά, και σκοπός τους είναι να διαχειριστούν άμεσα, σωστά και αποτελεσματικά ένα περιστατικό, έτσι ώστε να περιοριστεί γρήγορα, να διερευνηθεί και να επιλυθεί [9]. Στη βιβλιογραφία η ομάδα αυτή εμφανίζεται και ως Computer Emergency Readiness Team (CERT). Η πρώτη εμφάνιση μιας τέτοιας ομάδας ήταν το Νοέμβριο του 1988, στο Πανεπιστήμιο Carnegie Mellon, η οποία συγκροτήθηκε για να αντιμετωπίσει το Morris Worm.

4.2 Μέλη της CSIRT

Το ποιος μπορεί να συμπεριληφθεί σε μια τέτοια ομάδα, εξαρτάται κυρίως από τις ανάγκες και τους πόρους της εκάστοτε εταιρείας. Παρακάτω ακολουθεί μια λίστα με τα πιθανά μέλη μιας ομάδας CSIRT:

- **Διοίκηση**: Είναι πολύ σημαντικό να υπάρχει κάποιο διοικητικό στέλεχος της εταιρείας. Είναι εκείνος που επικυρώνει την εξουσιοδότηση της ομάδας και παίρνει τις σημαντικές αποφάσεις ανάλογα με τα δεδομένα που θα του παρουσιάσουν τα υπόλοιπα μέλη αυτής.
- **Ασφάλεια Πληροφοριών**: Είναι τα άτομα εκείνα που έχουν εξειδικευτεί για διαχείριση ηλεκτρονικών περιστατικών. Από τα πιο σημαντικά μέλη της ομάδας γιατί είναι εκείνοι που θα εκτιμήσουν το μέγεθος της ζημιάς, θα την περιορίσουν, θα προτείνουν λύσεις για ανάκαμψη και τέλος θα κάνουν το πολύ σημαντικό κομμάτι της εγκληματολογικής έρευνας (forensics analysis).
- **IT**: Πολλές εταιρείες έχουν διαχωρίσει το τμήμα της ασφάλειας από το IT. Θα πρέπει να υπάρχει κάποιος από αυτό το τμήμα γιατί θα πρέπει να ενημερωθεί για τα δεδομένα της εταιρείας, ποια μπορούν να προσπελαστούν, ποια τμήματα του δικτύου θα είναι περιορισμένης πρόσβασης λόγω της έρευνας. Αν δεν υπάρχει κάποιος από αυτό το τμήμα, μπορεί να χαθούν πολύτιμες αποδείξεις, επειδή απλά ένας καλοπροαίρετος διαχειριστής εντόπισε μια κατεστραμμένη βάση δεδομένων και την αντικατέστησε με το αντίγραφο ασφαλείας.
- **Φυσική Ασφάλεια**: Αν στο περιστατικό υπάρχει άμεση επαφή με το σύστημα, είναι οι αρμόδιοι για να σε καθοδηγήσουν.

- **Νομικοί**: Παρέχουν στην ομάδα νομικές συμβουλές. Εξασφαλίζουν τη νομιμότητα κάθε απόδειξης που συλλέχθηκε, έτσι ώστε να έχει νομική βάση στο δικαστήριο. Επίσης παρέχει συμβουλές σε θέματα όπου το περιστατικό έχει να κάνει με πελάτες, μετόχους κ.α.
- **Διαχείριση Ανθρώπινων Πόρων**: Πολλά περιστατικά αφορούν εργαζόμενους της εταιρείας. Παρέχουν συμβουλές για την καλύτερη πρακτική διαχείρισης σε περιπτώσεις που εμπλέκονται εργαζόμενοι της εταιρείας. Βέβαια η συμμετοχή ενός ατόμου από το συγκεκριμένο τμήμα δικαιολογείται αφού έχει γίνει έρευνα και έχει αποδειχθεί ότι εμπλέκεται εργαζόμενος.
- **Δημόσιες Σχέσεις**: Η εικόνα κάθε εταιρείας είναι ένα πολύτιμο αγαθό. Όταν είναι δυνατό, οι περισσότερες εταιρείες προσπαθούν να αποσιωπήσουν μικρά περιστατικά. Άλλες φορές αυτό δεν είναι εφικτό και θα πρέπει η πληροφορία να διαρρεύσει στα ΜΜΕ. Ο ρόλος του συγκεκριμένου ατόμου θα είναι να επικοινωνεί με τους επικεφαλείς των ομάδων, να είναι το πρόσωπο της ομάδας στα ΜΜΕ ή/και να ενημερώνει τους μετόχους.

Δεν είναι υποχρεωμένη η εταιρεία να διαθέσει ένα άτομο από κάθε ειδικότητα. Όπως αναφέρθηκε και πριν, η δημιουργία της ομάδας είναι ανάλογη των δυνατοτήτων και αναγκών της εταιρείας. Θα πρέπει όμως να υπάρχουν τα κατάλληλα άτομα για να ανταποκριθούν στα θέματα που θα προκύψουν. Επίσης αν η εταιρία κρίνει ότι τα μέλη της δεν έχουν το κατάλληλο υπόβαθρο να ανταπεξέλθουν στο εκάστοτε περιστατικό, έχει τη δυνατότητα να προσλάβει και εξωτερικούς συνεργάτες.

Στην Ελλάδα κάθε εταιρεία μπορεί να έχει μια τέτοια ομάδα. Επίσημα υπάρχουν:

- Εθνική Υπηρεσίας Πληροφοριών (Ε.Υ.Π.).[10]
- Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness & Response to Threats – D.A.R.T).[5]
- AUTH-CERT Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.[11]

5 Μεθοδολογίες Έρευνας

5.1 Εισαγωγή

Η επιστήμη της πληροφορικής με τον ένα ή τον άλλο τρόπο, σχετίζεται με τις περισσότερες εγκληματικές έρευνες. Η εισαγγελική αρχή είναι δυνατόν να εκδώσει ένταλμα έρευνας του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών εγγράφων ατόμων που είναι ύποπτα για δολοφονία ή παιδική πορνογραφία. Ιδιωτικές εταιρείες, ελέγχουν τους προσωπικούς υπολογιστές των εργαζομένων τους, στοχεύοντας στην αποφυγή διαρροής εταιρικών μυστικών σε ανταγωνιστές. Απάτες εξακριβώνονται μέσα από τη συλλογή και ανάλυση στοιχείων από το πληροφοριακό σύστημα του υπό έρευνα οργανισμού. Έτσι λοιπόν δημιουργείται η ανάγκη τυποποίησης της συγκεκριμένης ερευνητικής διαδικασίας μέσα από μια κοινά αποδεκτή μεθοδολογία.

5.2 Διαδικασία Συλλογής Αποδεικτικών Στοιχείων

Η διαδικασία της ψηφιακής έρευνας σε ένα περαστικό, αποτελείται από τα παρακάτω βήματα:

- Απομόνωση του τόπου του εγκλήματος και είσοδος σε αυτό μόνο από εξουσιοδοτημένα άτομα.
- Προσδιορισμός μέσων εγγραφής των δεδομένων και φωτογράφηση ώστε να μπορεί να αποδειχθεί το φυσικό περιβάλλον και η κατάσταση των στοιχείων.
- Δημιουργία χώρων ασφάλισης των δεδομένων. Συνήθως χρησιμοποιείται κάποιο ασφαλές ντουλάπι.

- Κατάρτιση καταλόγου των στοιχείων που μπορεί να περιλαμβάνει: φορητούς ηλεκτρονικούς υπολογιστές, σκληρούς ή εξωτερικούς δίσκους, μέσα εγγραφής εφεδρικών αντιγράφων, DVD, CD κλπ., κλειδιά USB, υπολογιστές τσέπης, έξυπνα τηλέφωνα, ανάλυση δραστηριοτήτων δικτύου.
- Καταχώριση και ασφάλιση της ηλεκτρονικής εικόνας του δίσκου εγκληματολογικών δεδομένων.
- Δημιουργία φακέλου εγκληματολογικών αποδεικτικών στοιχείων, που δεν είναι δυνατόν να διαγραφούν ή να απομακρυνθούν, ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων και εργασία του υπευθύνου σε αντίγραφο ασφαλείας.
- Εξέταση των δεδομένων με το κατάλληλο λογισμικό ώστε να καταστούν αναγνώσιμα τα αναζητούμενα δεδομένα και χρήση π.χ. λέξεων κλειδιών για τον εντοπισμό δεδομένων σχετικών με την υπόθεση. Επιβαρυντικά και μη στοιχεία συλλέγονται και αποκρυπτογραφούνται αρχεία και σπάνε κωδικοί ασφαλείας.
- Αναζήτηση και άλλων πηγών άντλησης δεδομένων, όπως υποδεικνύει η πορεία της υπόθεσης.
- Στη συνέχεια συντάσσεται έκθεση στην οποία καταγράφεται κάθε στάδιο της ηλεκτρονικής εγκληματολογικής έρευνας με τα ευρήματα, η οποία υπογράφεται από τον πελάτη.
- Αν θεωρηθεί απαραίτητο, ο ερευνητής παρίσταται ως μάρτυρας στη δικαστική αίθουσα.

5.3 Απαιτήσεις

Ένα πληροφοριακό σύστημα μπορεί να θεωρηθεί το περιβάλλον στο οποίο διεξάγεται ένα ηλεκτρονικό έγκλημα. Κάτι αντίστοιχο με ένα δωμάτιο στο οποίο έχει γίνει ένα έγκλημα (π.χ. δολοφονία). Η μεθοδολογία ανεύρεσης ψηφιακών αποδεικτικών στοιχείων θα πρέπει να είναι πρακτική και να βασίζεται στη γενική διαδικασία συλλογής αποδεικτικών στοιχείων. Δεν θα πρέπει να επηρεάζεται από τις τεχνολογικές αλλαγές, αλλά θα πρέπει να προσαρμόζεται ανάλογα με τους περιορισμούς και τις ιδιαιτερότητες του περιστατικού και του περιβάλλοντος στο οποίο συνέβη. Το πιο σημαντικό όμως είναι ότι θα πρέπει να είναι καλά δομημένη με τέτοιο τρόπο έτσι ώστε να είναι δυνατή η τυποποίησή της με τη μορφή ενός ηλεκτρονικού εργαλείου.

Όσον αφορά τα ηλεκτρονικά ευρήματα θα πρέπει και εκείνα με τη σειρά τους να έχουν κάποια συγκεκριμένα χαρακτηριστικά για να γίνουν αποδεκτά, εφόσον το αποτέλεσμα της έρευνας μπορεί να χρησιμοποιηθεί για νομικές διαδικασίες:

- Αυθεντικότητα: Το στοιχείο το οποίο εξετάζεται προέρχεται από την πηγή Α και όχι από μια πηγή Β, άσχετη με το περιστατικό.
- Αξιοπιστία: Αναδεικνύει το ποσοστό εμπιστοσύνης που αποδίδουμε σε κάθε στοιχείο.
- Ακεραιότητα: Πολύ σημαντικός παράγοντας, ο οποίος ενδυναμώνει ή αποδυναμώνει μια δικαστική υπόθεση. (hash/image/hash FTK imager).
- Πληρότητα: Ο βαθμός ευρωστίας της ιστορίας που απορρέει από την εξέταση ενός στοιχείου. Δηλαδή αν οι πληροφορίες που εξάγονται από την έρευνα των στοιχείων αρκούν ή περιέχουν κενά τα οποία θα πρέπει να συμπληρωθούν από εξέταση άλλων στοιχείων.

5.4 Μοντέλο Διαδικασίας Διαχείρισης Περιστατικού (Incident Response Process Model - 2001)

Μια πρώτη απόπειρα μοντελοποίησης των διαδικασιών της Ψηφιακής Εγκληματολογίας είναι το μοντέλο της άμεσης ανάδρασης. Το μοντέλο αυτό επικεντρώνεται στον τρόπο με τον οποίο ένας οργανισμός πρέπει να αντιδράσει σε περιπτώσεις επιθέσεων ή καταχρήσεων του πληροφοριακού συστήματός του ώστε να τεκμηριώσει:

- ποιός είναι ο επιτιθέμενος
- στόχος επιτιθέμενου
- μέγεθος ζημιών
- συνέπειες
- κόστος
- τρόπους ανάκαμψης του συστήματος

Αν εξαιρέσουμε τη διαδικασία επιλογής της ομάδας, υπάρχουν ακόμη οκτώ βήματα στη διαδικασία διαχείρισης ενός περιστατικού:

1) **Προετοιμασία**: Χρέος των μελών της ομάδας είναι να ενημερώνονται πάντα για τα τελευταία περιστατικά ανά τον κόσμο και να εκπαιδεύονται συνεχώς σε νέες τεχνικές αντιμετώπισης περιστατικών.
2) **Αναγνώριση**: Η ομάδα αντιμετώπισης θα πρέπει να είναι σε θέση να αποφασίσει αν ένα γεγονός αποτελεί ένα περιστατικό ασφαλείας. Για αυτό το λόγο θα πρέπει να υπάρχουν σαφής ορισμοί για το τι στοιχειοθετεί ένα περιστατικό.
3) **Περιορισμός**: Η ομάδα μετά από έρευνα προσδιορίζει το μέγεθος του προβλήματος και το περιορίζει αποσυνδέοντας όλα τα προσβεβλημένα συστήματα για να αποτρέψει την εξάπλωση του κινδύνου.
4) **Αντιγραφή**: Στο βήμα αυτό δημιουργούνται αντίγραφα των προσβεβλημένων συστημάτων, έτσι ώστε η ανάλυση που ακολουθεί να γίνει στα αντίγραφα, για να μην αλλοιωθούν τα αποδεικτικά στοιχεία στα πρωτότυπα.
5) **Ανάλυση**: Με μεθόδους και εργαλεία (ψηφιακή εγκληματολογία) προσπαθούν να βρουν την αιτία που προκάλεσε το περιστατικό.
6) **Επίλυση**: Το αίτιο που προκάλεσε το περιστατικό μόλις εντοπιστεί, γίνονται όλες οι απαραίτητες ενέργειες για να απομακρυνθεί από το σύστημα.
7) **Ανάκαμψη**: Δεδομένα και λογισμικό επανέρχονται με τη χρήση «καθαρών» αντιγράφων ασφαλείας και τα συστήματα παρακολουθούνται για τυχόν αδυναμίες.
8) **Αναφορά** (**Ανάδραση**): Η ομάδα αναλύει και καταγράφει το περιστατικό και τον τρόπο που το διαχειρίστηκε. Έτσι μπορεί να κάνει προτάσεις για καλύτερη μελλοντική αντιμετώπιση και για να αποφευχθεί η επανάληψη. Αυτές οι προτάσεις θα πρέπει να ενσωματώνονται στην πολιτική ασφαλείας και οι εργαζόμενοι θα πρέπει να εκπαιδεύονται σύμφωνα με αυτές (awareness).

5.5 Ενοποιημένη Διαδικασία Ψηφιακής Έρευνας (Integrated Digital Investigation Process - 2003)

Τα συγκεκριμένο μοντέλα είναι ένα από τα πιο ολοκληρωμένα που έχει προτείνει η ακαδημαϊκή κοινότητα. Όπως είναι λογικό η μέθοδος αυτή έχει δανειστεί αρκετά πράγματα από τις προηγούμενες

μεθόδους. Πριν προχωρήσουμε στην ανάλυση της διαδικασίας, θα πρέπει να αποσαφηνίσουμε κάποιους όρους που χρησιμοποιούνται:

- Φυσικό περιβάλλον εγκλήματος: Ο χώρος και τα άτομα τα οποία διαχειρίζονται το υπολογιστικό σύστημα. Αποτελεί τον τόπο του εγκλήματος και πρέπει να ερευνηθεί με κλασσικές εγκληματολογικές τεχνικές.
- Ψηφιακή σκηνή εγκλήματος: Το περιβάλλον που δημιουργεί το υλικό, το λογισμικό και τα δεδομένα ενός μόνο υπολογιστή.
- Ψηφιακό περιβάλλον εγκλήματος: Το σύνολο των ψηφιακών σκηνών, δηλαδή το σύνολο των εμπλεκομένων υπολογιστών.

Η συγκεκριμένη διαδικασία χωρίζεται σε πέντε φάσεις:

1. **Φάση Ετοιμότητας:** Εξασφαλίζει ότι οι διαδικασίες και η υποδομή επαρκούν για σωστή και αποτελεσματική έρευνα. Χωρίζεται σε δυο μεγάλα τμήματα:
    i. Επιχειρησιακή Ετοιμότητα: Αφορά την εκπαίδευση των ερευνητών και τον εξοπλισμό τους με κατάλληλα εργαλεία ώστε να μπορούν να κάνουν αποτελεσματικά τη δουλειά τους. Επιπροσθέτως περιλαμβάνεται η οργανωτική δομή του εργαστηρίου, καθώς και ο διαρκής έλεγχος και ανανέωση του εξοπλισμού.
    ii. Ετοιμότητα Υποδομής: Αφορά την πληρότητα της ηλεκτρονικής υποδομής που έχουν στην κατοχή τους οι ερευνητές και το κατά πόσο τους βοηθά στο έργο τους.
2. **Φάση Ανάπτυξης**: Σκοπός της είναι να παρέχει ένα μηχανισμό. Έτσι ώστε το περιστατικό να καταγράφεται και να εξουσιοδοτούνται οι ερευνητές. Χωρίζεται και αυτό σε δυο τμήματα:
    i. *Φάση Αναγνώρισης και Ειδοποίησης*: Το περιστατικό εντοπίζεται, αναγνωρίζεται και ειδοποιείται η ομάδα αντιμετώπισης.
    ii. *Φάση Εξουσιοδότησης*: Η ομάδα επιβεβαιώνει την ύπαρξη του περιστατικού και εξασφαλίζει τη νόμιμη έγκριση για να διεξαχθεί η έρευνα.
3. **Φάση Έρευνας Φυσικού Περιβάλλοντος**: Σκοπός είναι να συγκεντρωθούν και αν αναλυθούν οι φυσικές αποδείξεις και να ανακατασκευαστούν οι πράξεις που έγιναν στη διάρκεια του ατυχήματος, σε ελεγχόμενες συνθήκες. Αποτελείται από 6 στάδια:
    i. Διατήρηση: Ο χώρος απομονώνεται και έτσι ώστε να διατηρηθεί όπως ακριβώς ήταν την ώρα του περιστατικού και το εξειδικευμένο προσωπικό να μπορεί να συλλέξει τις αποδείξεις χωρίς να έχουν αλλοιωθεί.
    ii. Επιτόπου Έρευνα: Ο ερευνητής περιδιαβαίνει το χώρο του περιστατικού και αναγνωρίζει φυσικές αποδείξεις.
    iii. Καταγραφή στοιχείων: Ο ερευνητής παίρνει φωτογραφίες του χώρου και καταγράφει λεπτομερώς τα στοιχεία μέσα σε αυτόν.
    iv. Λεπτομερής Έρευνα και Συλλογή Στοιχείων: Ενδελεχής έρευνα του χώρου, συλλογή στοιχείων καθώς και του υπολογιστικού συστήματος για τη διεξαγωγή της ψηφιακής έρευνας.
    v. Ανακατασκευή Περιστατικού: Οργάνωση των αποτελεσμάτων της έρευνας και χρησιμοποίησής τους για την ανάπτυξη μιας υπόθεσης / θεωρίας για το περιστατικό.
    vi. Παρουσίαση Ευρημάτων: Παρουσίαση των φυσικών και ψηφιακών αποδείξεων στην εκάστοτε εταιρεία ή στο δικαστήριο.

Εικόνα 2. Έρευνα φυσικού και ψηφιακού περιβάλλοντος

4. **Φάση Έρευνας Ψηφιακού Περιβάλλοντος**: Λαμβάνει χώρα αφού έχει τελειώσει το στάδιο της λεπτομερούς έρευνας της προηγούμενης φάσης. Ο σκοπός είναι η συλλογή και η ανάλυση των ψηφιακών αποδείξεων που αποκτήθηκαν από την προηγούμενη φάση. Αποτελείται και αυτή από έξι στάδια, παρόμοια με τα προηγούμενα, όμως επικεντρωνόμαστε στις ψηφιακές αποδείξεις αυτή τη φορά.
    i. Διατήρηση: Απομόνωση του υπολογιστικού συστήματος από τον υπόλοιπο περιβάλλον. Συγκεντρώνονται στοιχεία τα οποία θα χαθούν αν απενεργοποιηθεί, καταγράφονται οι χρήστες που είναι συνδεδεμένοι, το σύστημα αποσυνδέεται από το δίκτυο και απενεργοποιείται κατάλληλα. Δημιουργούνται αντίγραφα ασφαλείας με στόχο την μελλοντική επεξεργασία τους.
    ii. Επιτόπου Έρευνα: Συλλογή δεδομένων με μια πρώτη ανάλυση των αντιγράφων ασφαλείας.
    iii. Καταγραφή Στοιχείων: Ο ερευνητής καταγράφει τις ψηφιακές αποδείξεις που έχει συλλέξει και αναφέρει λεπτομερώς την προέλευση τους.
    iv. Λεπτομερής Έρευνα και Συλλογή Στοιχείων: Ενδελεχής έρευνα των ψηφιακών αποδείξεων με τη χρήση εξειδικευμένων εργαλείων. Προσπαθούμε με τη χρήση κατάλληλου λογισμικού να ανασύρουμε διαγραμμένα ή κατεστραμμένα αρχεία, καθώς και ημερομηνίες και αρχεία καταγραφής.
    v. Ανακατασκευή Περιστατικού: Οργάνωση των αποτελεσμάτων της ψηφιακής έρευνας και χρησιμοποίησής τους για την ανάπτυξη μιας υπόθεσης / θεωρίας για το περιστατικό.
    vi. Παρουσίαση Ευρημάτων: Παρουσίαση των ψηφιακών αποδείξεων στην ομάδα φυσικής έρευνας.

5. **Φάση Αναθεώρησης:** Μελετάται βήμα προς βήμα η διαδικασία, αξιολογείται και επισημαίνονται σημεία βελτίωσης. Είναι περισσότερο εσωτερική διεργασία.

5.6 DIGITAL FORENSICS RESEARCH WORKSHOP FRAMEWORK (2003)

Η ομάδα δημιουργίας του πλαισίου αποτελούνταν από ακαδημαϊκούς ερευνητές, μέλη ομάδων ασφάλειας πληροφοριακών συστημάτων ιδιωτικών οργανισμών και πολλούς χρήστες ηλεκτρονικών υπολογιστών οι οποίοι ενδιαφέρονταν για την επιστήμη της Ψηφιακής Εγκληματολογίας. Το πλαίσιο, το οποίο επισημοποιήθηκε το 2003 συνδυάζει όλες τις προηγούμενες μεθοδολογίες.

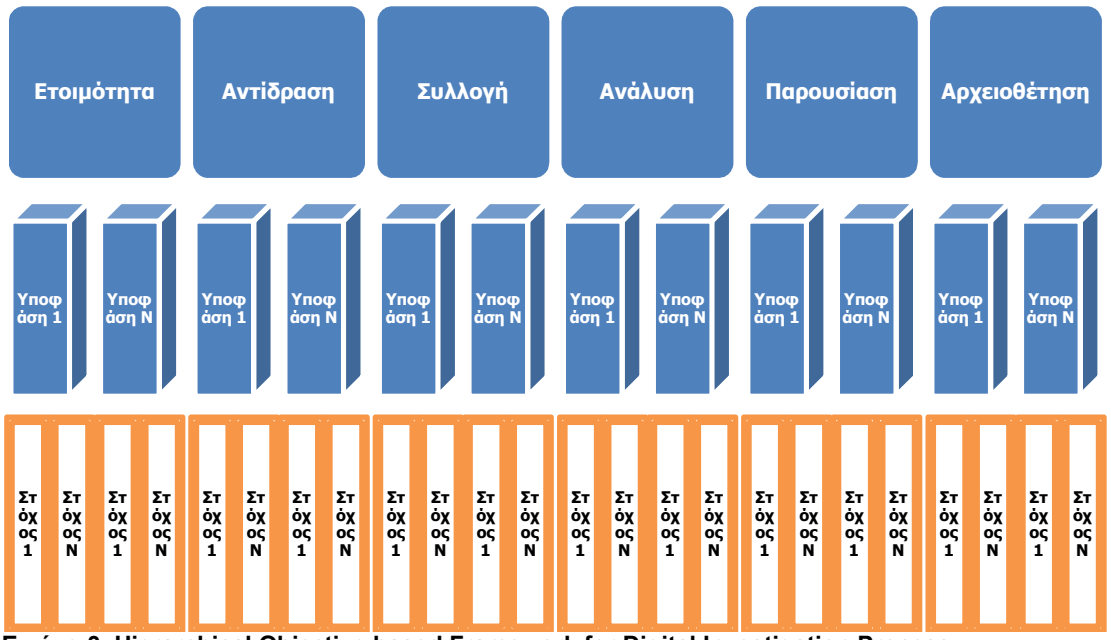
Αποτελείται από έξι κλάσεις, οι οποίες χωρίζονται σε στοιχεία. Στον παρακάτω πίνακα φαίνεται σχηματικά η μέθοδος, όπου οι τίτλοι των στηλών είναι οι κλάσεις και ακολουθούν τα στοιχεία. Τα στοιχεία με τα έντονα γράμματα είναι οι ενέργειες που θα πρέπει υποχρεωτικά να γίνουν για να θεωρηθεί η έρευνα επιτυχής και τα υπόλοιπα είναι συμπληρωματικές ενέργειες.

Αναγνώριση	Διαφύλαξη	Συλλογή	Διερεύνηση	Ανάλυση	Παρουσίαση
Ανίχνευση Περιστατικού	**Διαχείριση Περίπτωσης**	**Διαφύλαξη**	**Διαφύλαξη**	**Διαφύλαξη**	**Τεκμηρίωση**
Ανωμαλίες	**Chain of Custody**	**Αποδεκτές Μέθοδοι**	**Ιχνηλασιμότητα**	**Ιχνηλασιμότητα**	Κατάθεση Ειδικών
Παρακολούθηση Συστήματος	**Ορισμός Χρονικού Πλαισίου**	**Αποδεκτό Λογισμικό**	Τεχνικές Επικύρωσης	Στατιστική Ανάλυση	**Διαλεύκανση**
Audit Analysis	Τεχνολογίες Αντιγραφής	**Νομική Κάλυψη**	Ταυτοποίηση Προτύπου	Πρωτόκολλα	Προτεινόμενα Αντίμετρα
Παράπονα		Δειγματοληψία	Αποκάλυψη Κρυφών Στοιχείων	Εξόρυξη Γνώσης	
Profile Detection		Μείωση Όγκου Δεδομένων		Χωρική Ανάλυση	
Συνεντεύξεις		Τεχνικές Ανάκαμψης		Χρονική Ανάλυση	
		Συμπίεση Δεδομένων			

Πίνακας 1. DIGITAL FORENSICS RESEARCH WORKSHOP FRAMEWORK

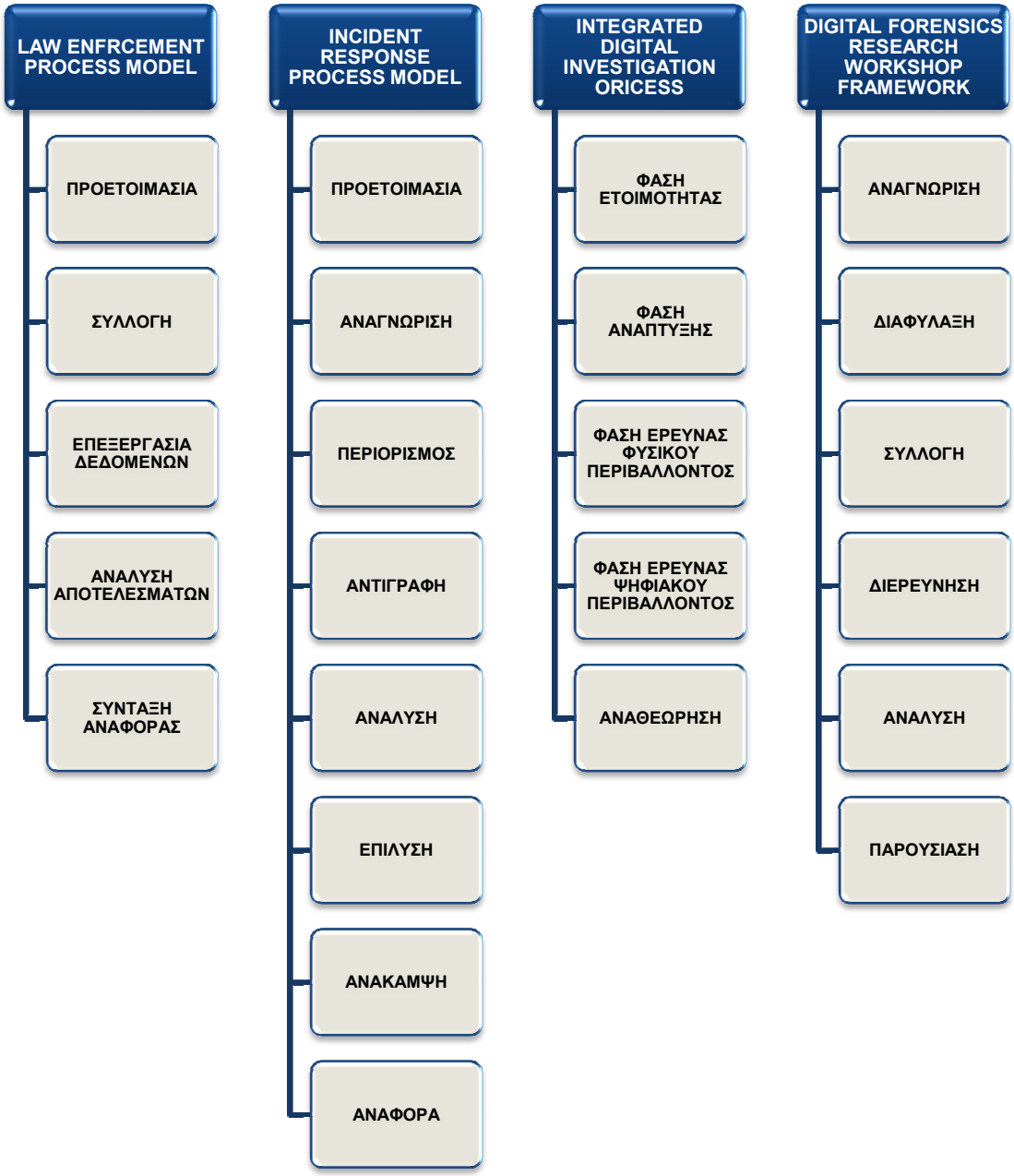
5.7 Hierarchical Objective based Framework for Digital Investigation Process (2004)

Η διαδικασία ιεράρχησης στόχων για ψηφιακές έρευνες δεν έχει να προσφέρει κάτι καινούριο. Η ιδέα είναι ότι διαιρεί κάθε φάση σε υποφάσεις, οι οποίες για να ολοκληρωθούν θα πρέπει να επιτευχθούν κάποιοι καλά ορισμένοι στόχοι. Η εκπλήρωση των στόχων σηματοδοτεί την μετάβαση από μια υποφάση σε μια άλλη. Η ολοκλήρωση όλων των υποφάσεων μιας φάσης σηματοδοτεί τη μετάβαση στην επόμενη φάση.



Εικόνα 3. Hierarchical Objective based Framework for Digital Investigation Process

5.8 Σύνοψη Μεθοδολογιών



Εικόνα 4. Συνοπτικός πίνακας των Μεθοδολογιών Ψηφιακής Εγκληματολογίας

6 Εργαλεία

Όπως αναφέρθηκε και στις προηγούμενες ενότητες, η προσπάθεια τυποποίησης μιας μεθοδολογίας έχει ως απώτερο σκοπό τη δημιουργία εργαλείων. Η ραγδαία εξέλιξη του κλάδου της Ψηφιακής Εγκληματολογίας είχε ως αποτέλεσμα και την ανάπτυξη πλήθους εργαλείων. Τα εργαλεία αυτά λειτουργούν τόσο σε περιβάλλον Windows (εμπορικά προϊόντα και ελεύθερου λογισμικού) όσο και σε περιβάλλον Linux (προϊόντα ανοιχτού - ελεύθερου λογισμικού).

Στόχος των εργαλείων είναι να ανακαλύψουν και να ανασύρουν διαγραμμένα ή κατεστραμμένα αρχεία από ένα σκληρό δίσκο και να αποκαλύψουν την ύπαρξη και το περιεχόμενο αρχείων τα οποία είτε είναι κρυμμένα (hidden files) είτε προστατεύονται με κωδικό πρόσβασης (password protected).

6.1 Εργαλεία Συλλογής Ψηφιακών Αποτυπωμάτων (Disk Imaging Tools)

Πολύ σημαντικό κομμάτι της Ψηφιακής Εγκληματολογίας είναι η συλλογή των ψηφιακών αποτυπωμάτων. Η λήψη αντιγράφων δηλαδή, από ένα σκληρό δίσκο, έτσι ώστε να τα επεξεργαστούμε στη συνέχεια. Η έρευνα δεν θα πρέπει να γίνεται επάνω στο αρχικό αποθηκευτικό μέσο, ώστε να προστατεύεται η ακεραιότητα των στοιχείων που βρίσκονται αποθηκευμένα σε αυτό. Η διαφύλαξη της ακεραιότητα των στοιχείων ίσως είναι ο σημαντικότερος παράγοντας, τον οποίο θα λάβει υπόψη του το δικαστήριο για να δεχθεί ως αξιόπιστα τα αποτελέσματα μιας έρευνας. Για παράδειγμα, το δικαστήριο θα μπορούσε να απορρίψει αποτελέσματα μιας έρευνας, τα οποία προέρχονται από αμφίβολες ή αναξιόπιστες πηγές ή από μια αποθηκευτική συσκευή, της οποίας η ακεραιότητα δεν διατηρήθηκε.

Για να διασφαλίζουμε την ακεραιότητα των δεδομένων και της πηγής, και ότι δεν έχει αλλαχθεί η αλλοιωθεί η αρχική πληροφορία, χρησιμοποιούμε της συναρτήσεις κατακερματισμού (hash functions). Τα περισσότερα εργαλεία χρησιμοποιούν την τεχνική hash/image/hash. Αρχικά το αποθηκευτικό μέσο το οποίο αποτελεί την πηγή της πληροφορίας, περνάει από μια hash function και το αποτέλεσμα αποθηκεύεται. Ακολουθεί η διαδικασία της δημιουργίας αντιγράφου (disk imaging) και στη συνέχεια το αντίγραφο περνάει από την ίδια hash function. Τέλος συγκρίνονται τα δυο αποτελέσματα των hash functions. Αν είναι ίδια, εξασφαλίζεται η ακεραιότητα και η αξιοπιστία τόσο της πηγής όσο και του αντιγράφου.

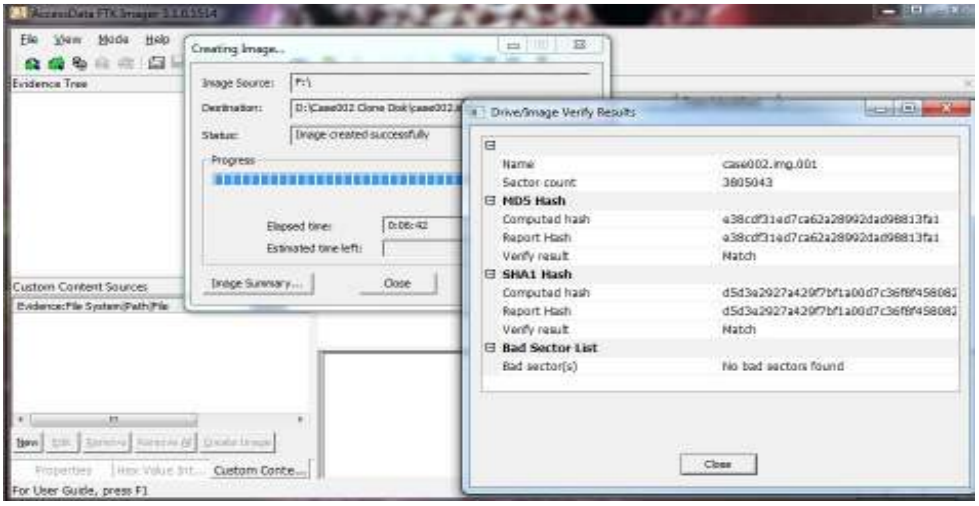
Εξαιτίας της σημαντικότητας της διαδικασίας συλλογής των ψηφιακών αποτυπωμάτων, κάθε εργαλείο disk imaging θα πρέπει να πληροί συγκεκριμένες προδιαγραφές:

- Κάθε εργαλείο θα πρέπει να φτιάχνει ένα ακριβές αντίγραφο του αρχικού αποθηκευτικού μέσου.
- Σε καμία περίπτωση δεν θα πρέπει να επιφέρει αλλοιώσεις στο αρχικό αποθηκευτικό μέσο.
- Θα πρέπει να καταγράφει σε αρχείο (log) τα σφάλματα.
- Το εργαλείο θα πρέπει να είναι σε θέση να πιστοποιήσει την ακεραιότητα ενός αντιγράφου (χρησιμοποιείται συνήθως η τεχνική hash/image/hash).

6.1.1 Εμπορικά Προϊόντα

FTK Imager:

Το FTK Imager είναι ένα εμπορικό εργαλείο που αναπτύχθηκε από την AccessData. Εξερευνεί τα περιεχόμενα αποθηκευτικών μέσων και δημιουργεί ακριβή αντίγραφά τους. Υποστηρίζει την ανάκτηση διαγραμμένων αρχείων. Για τη διασφάλιση της ακεραιότητας, το FTK Imager χρησιμοποιεί αλγορίθμους hashing, όπως ο MD5.[12]

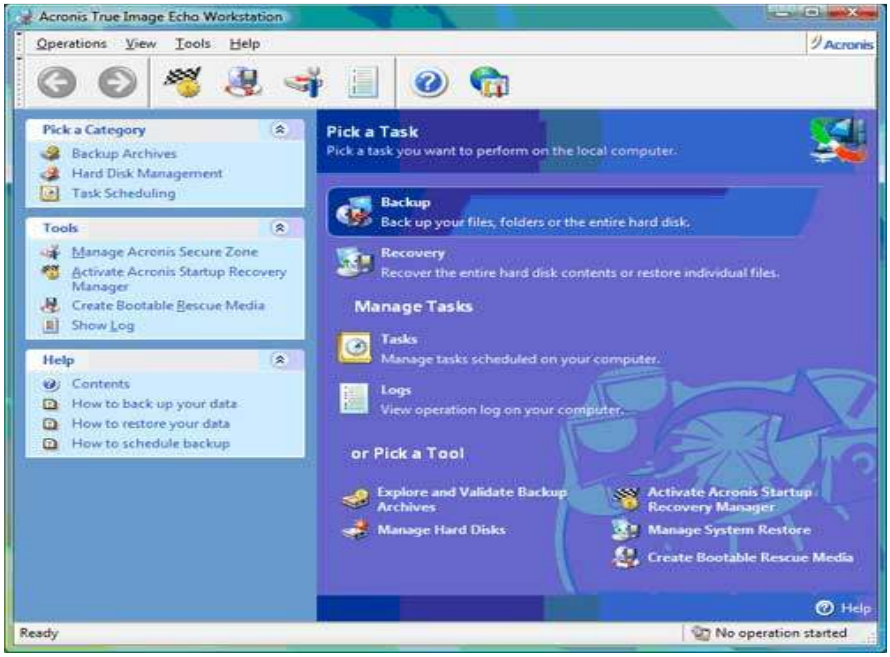


Εικόνα 5. Το περιβάλλον και οι λειτουργίες του FTK Imager

Acronis True Image:

Το TrueImage Echo Workstation παρέχεται από την εταιρίας Acronis και αποτελεί ένα από τα καλύτερα προγράμματα για επανάκτηση κατεστραμμένων τμημάτων του δίσκου αλλά και για την δημιουργία κλώνου αυτού.[13] Επίσης χρησιμοποιείται για την δημιουργία Back up των αρχείων αλλά και επαναφορά των διαγεγραμμένων αρχείων . Μπορεί να δουλέψει σε Window και Linux και με δεδομένα της μορφής :

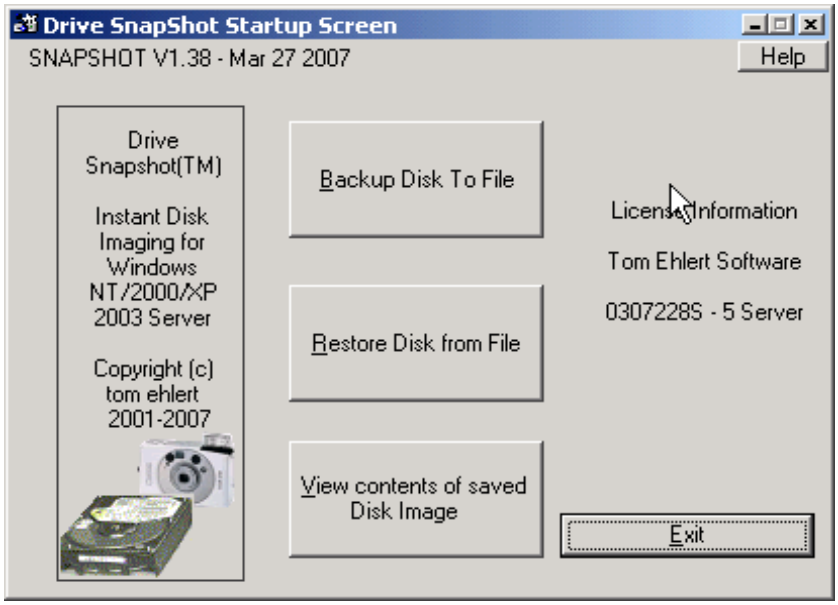
- FAT16/32
- NTFS
- Ext2/Ext3
- ReiserFS
- Linux SWAP
- DFS



Εικόνα 6. Το περιβάλλον του True Image

Drive Snapshot:

Το εργαλείο αυτό δημιουργεί ένα ακριβές αντίγραφο του συστήματος, συμπεριλαμβανομένου του λειτουργικού συστήματος, των εγκατεστημένων προγραμμάτων και των αποθηκευτικών μέσων.[14]



Εικόνα 7. Το περιβάλλον του Drive Snapshot

Total Recovery:

Εργαλείο με πολύ απλό interface, το οποίο δημιουργεί ακριβή αντίγραφα του συστήματος, τόσο του λειτουργικού όσο και των αποθηκευτικών μέσων.[15]

Εικόνα 8. Το περιβάλλον του Total Recovery

Genie Backup Manager:

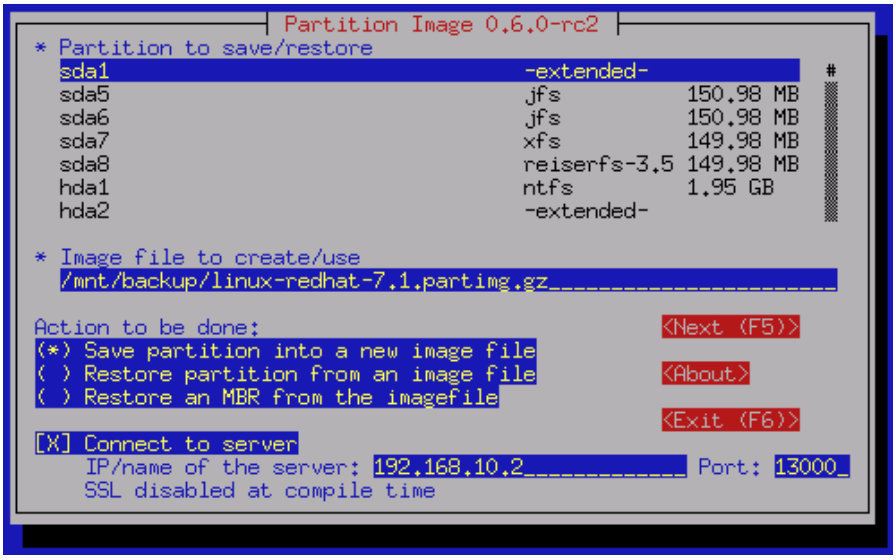
Ένα εργαλείο κλωνοποίησης αποθηκευτικών μέσων που λειτουργεί σε υπολογιστές, σε κινητά και σε PDA's.[16]

Εικόνα 9. Το περιβάλλον του Genie Backup Manager

6.1.2 Ελεύθερου Λογισμικού

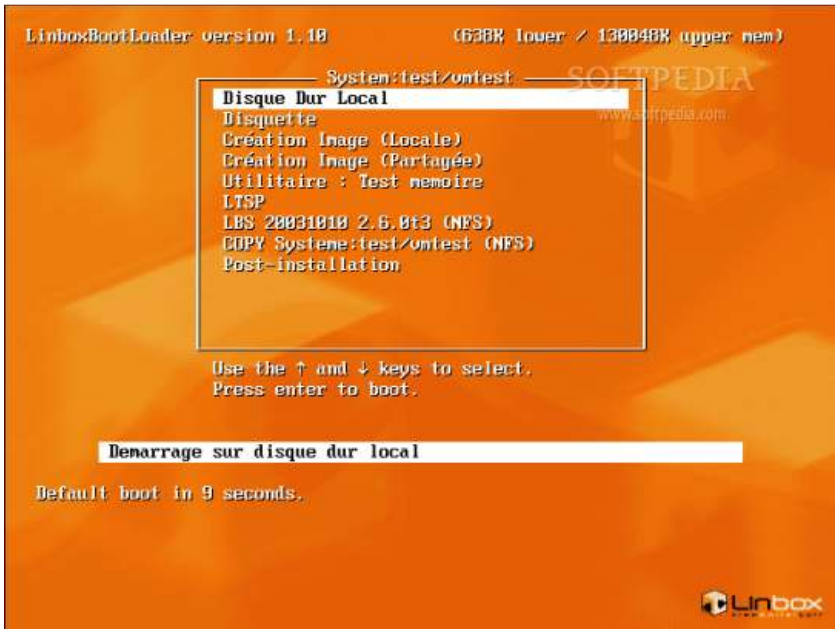
Linux Based:

- **Linux "dd":** Το Linux "dd" (Data Dumper) διατίθεται ελεύθερα και έχει τη δυνατότητα κατασκευής ακριβών αντιγράφων. Είναι τόσο δημοφιλές και για αυτό χρησιμοποιείται και σε σουίτες εργαλείων, όπως στο Helix 3. Υπάρχει σε πολλές εκδόσεις Linux. Η εντολή για να χρησιμοποιήσουμε το εργαλείο "dd" είναι η εξής: *dd if=<source> of=<target> bs=<byte size> conv=noerror* [17]
- **PartImage:** Διατίθεται ελεύθερα και έχει δυνατότητα κατασκευής ακριβών αντιγράφων αποθηκευτικού μέσου.[18]



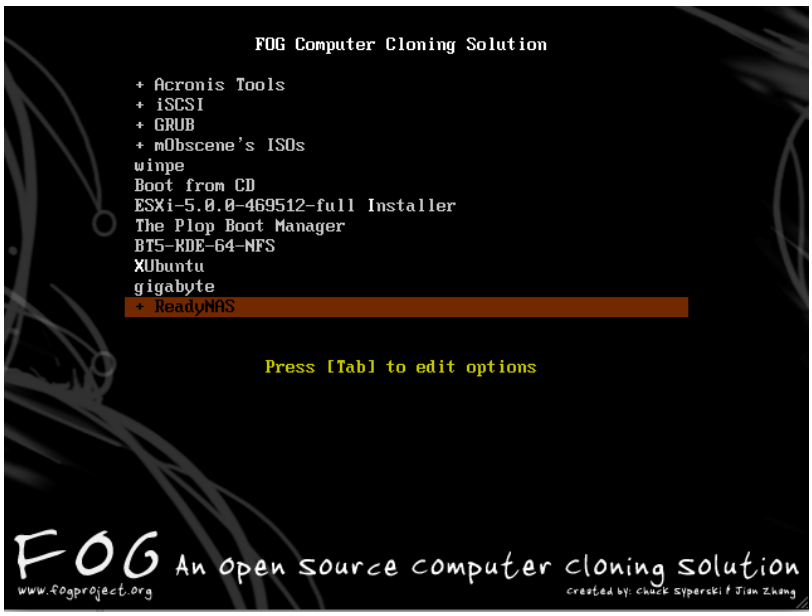
Εικόνα 10. Το περιβάλλον του PartImage

- **Linbox Rescue Server:** Επίσης ένα free εργαλείο disk imaging βασισμένο σε Linux.[19]



Εικόνα 11. Περιβάλλον του Linbox Rescue Server

- **FOG:** Εργαλείο disk imaging που παρέχεται δωρεάν με πολλές δυνατότητες, όπως δημιουργία κλώνων και παρακολούθησης δικτύου.[20]



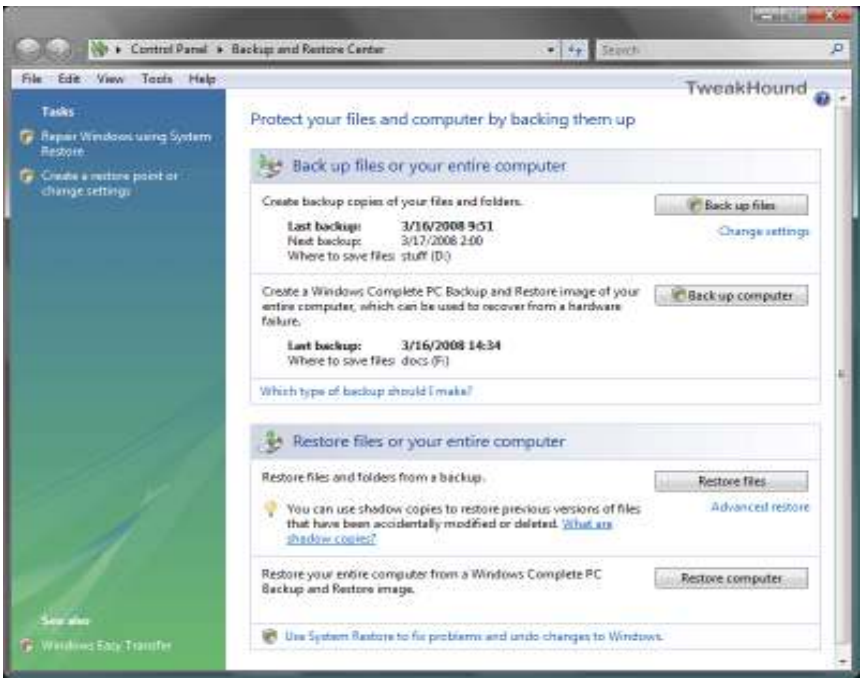
Εικόνα 12. Περιβάλλον του FOG

Windows Based:

- **DriveImage XML:** Το εργαλείο αυτό χρησιμοποιείται σε περιβάλλον windows και είναι πολύ απλό στη χρήση του. Διατίθεται δωρεάν για προσωπική χρήση.[21]

Εικόνα 13. Το περιβάλλον του DriveImage XML

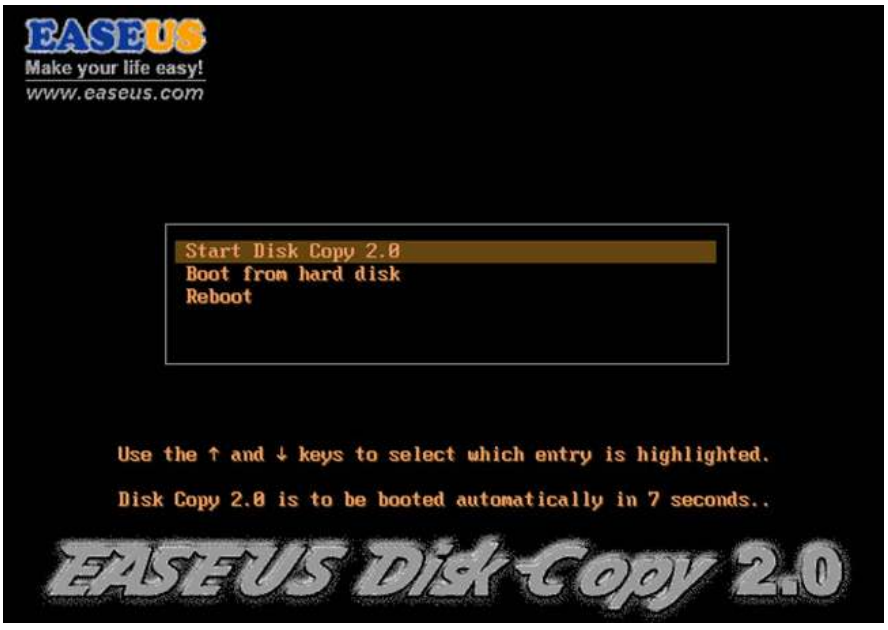
- **Windows Vista Ultimate Disk Imaging:** Στην έκδοση Ultimate των Windows Vista, υπάρχει ένα πλήρες εργαλεία κλωνοποίησης αποθηκευτικού μέσου.



Εικόνα 14. Το περιβάλλον του Disk Imaging εργαλείου των Windows Vista

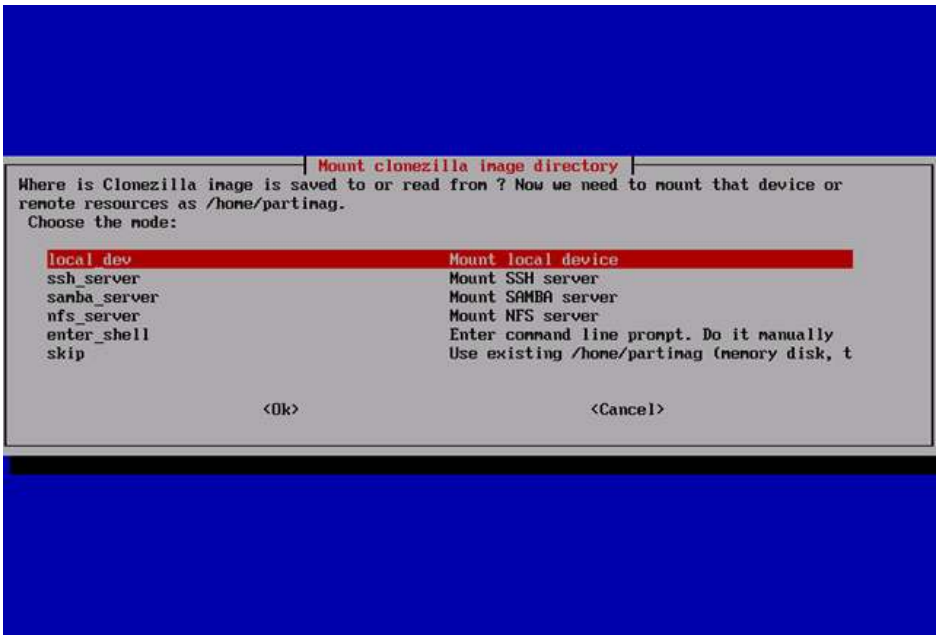
Boot CD:

- **EASUS Disk Copy:** Χρησιμοποιείται ανεξαρτήτων λειτουργικού συστήματος και υποστηρίζει κλωνοποίηση IDE, SATAI, SATAII, SCSI, Firewire και USB drives.[22]



Εικόνα 15. Το περιβάλλον του Easus Disk Copy

- **Clonezilla:** Το εργαλείο Clonezilla έρχεται σε δυο εκδόσεις. Μια "live" έκδοση με την οποία παίρνεις αντίγραφα του αποθηελυτικού μέσου ενός υπολογιστή, και μια "server" έκδοση, με την οποία είναι δυνατή η αντιγραφή πολλών αποθηκευτικών μέσων σε διαφορετικούς υπολογιστές.[23]



Εικόνα 16. Το περιβάλλον του Clonezilla

Mobile devices:

- **LiME:** Το LiME (πρώην DMD) είναι ένα Loadable Kernel Module (LKM), το οποίο επιτρέπει την απόκτηση ενός image της μνήμης RAM, Linux συσκευών, όπως τα Android κινητά τηλέφωνα. Το εργαλείο υποστηρίζει την απόκτηση του memory image τόσο στο file system της συσκευής όσο και μέσω δικτύου. Το LiME είναι μοναδικό γιατί είναι το πρώτο εργαλείο το οποίο επιτρέπει την πλήρη απόκτηση memory image Android συσκευών. Μειώνει επίσης την αλληλεπίδραση μεταξύ χρήστη και διεργασιών του kernel, επιτρέποντας έτσι την παραγωγή images τα οποία είναι αποδεκτά ως αποδείξεις σε εγκληματολογική έρευνα. [24]

6.2 Εργαλεία Ανάλυσης Ψηφιακών Αποτυπωμάτων (Forensics Analysis Tools)

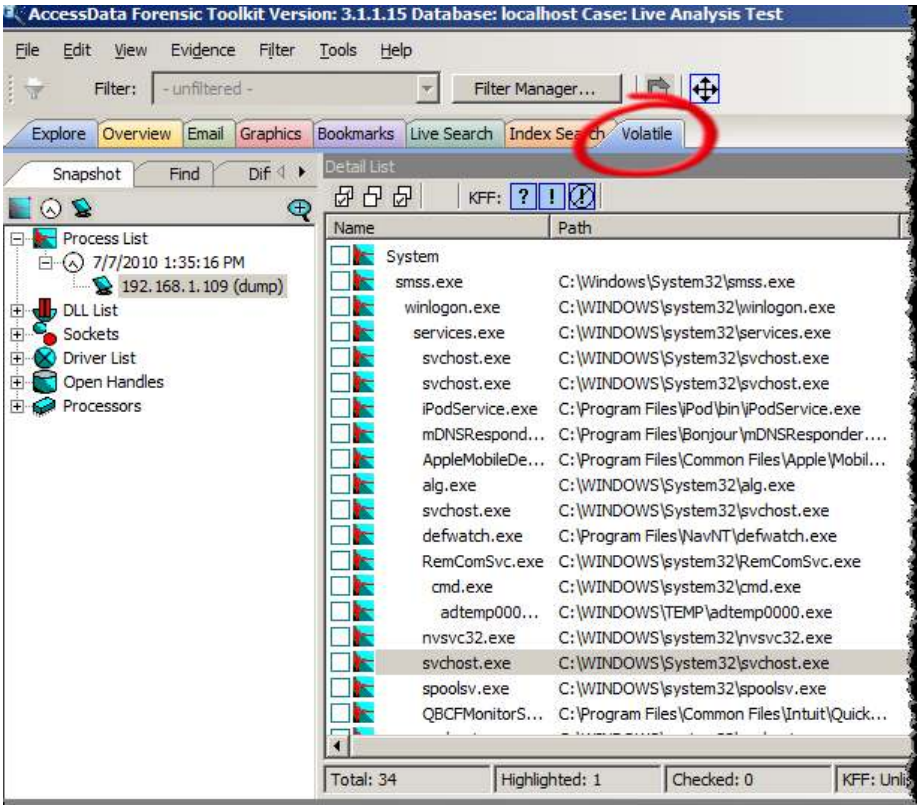
Τα εργαλεία αυτά δέχονται συνήθως δέχονται ως είσοδο ένα image αρχείο και το αναλύουν προσπαθώντας να ανακαλύψουν ευρήματα που θα βοηθήσουν τον αναλυτή να εντοπίσει αποδείξεις.

6.2.1 Εμπορικά Προϊόντα

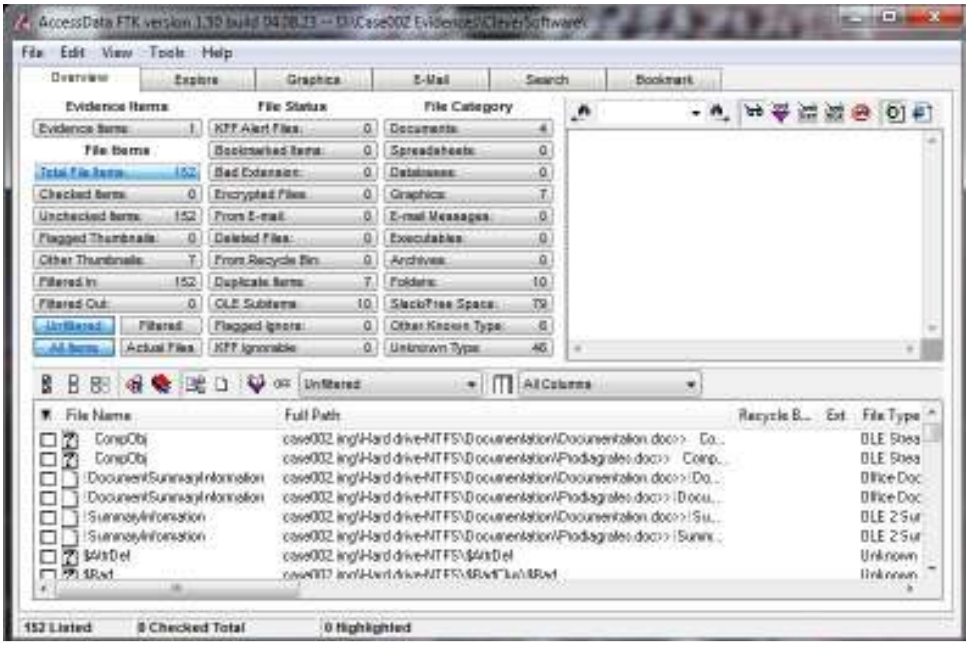
Forensic Toolkit:

Το Forensic Toolkit είναι ένα εμπορικό εργαλείο που αναπτύχθηκε από την AccessData. Δίνει τη δυνατότητα εύρεσης όλων των αρχείων μέσα σε μια αποθηκευτική συσκευή. Εμφανίζει κρυφά αρχεία, αρχεία κρυμμένα μέσα σε άλλα αρχεία, αρχεία μέσα σε εικόνες. Επίσης μπορεί να δώσει πληροφορίες για ηλεκτρονική αλληλογραφία και συνημμένα αρχεία, καθώς και για περιήγηση στο internet. Όχι μόνο ανακαλύπτει κρυμμένα αρχεία, αλλά παρέχει και κατάλληλο viewer για να δούμε τα περιεχόμενα. Επίσης

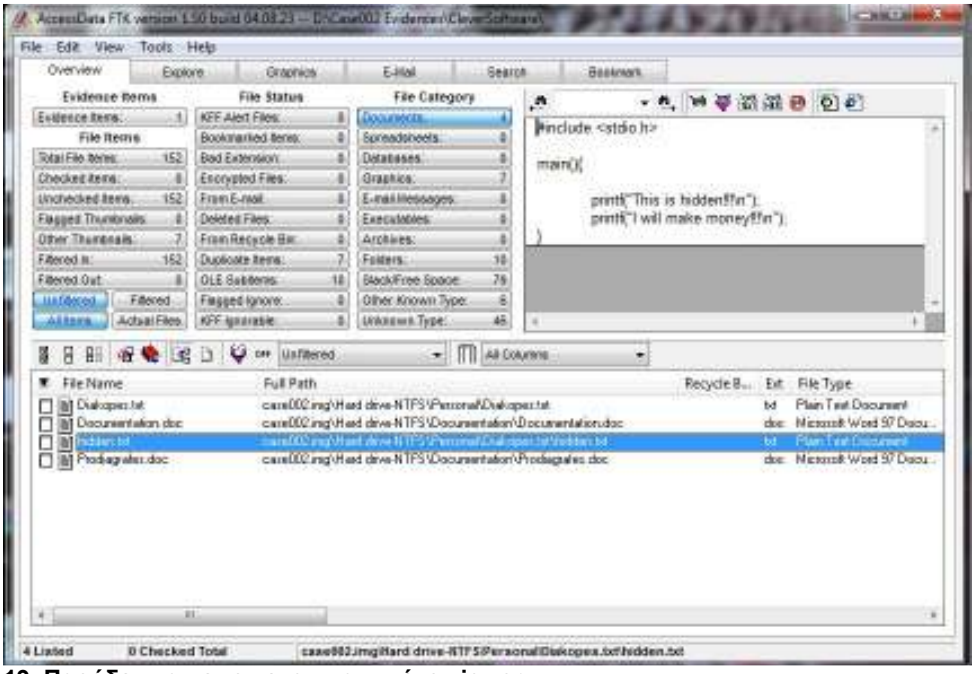
έχει τη δυνατότητα διατήρησης αρχείου καταγραφής (log) και bookmark σημαντικών αποδείξεων, ενώ τονίζει συμβάντα με πιθανό ενδιαφέρον. Παρακάτω φαίνεται η τελευταία έκδοση του εργαλείου και στη συνέχεια κάποιες εικόνες από την έκδοση του εργαλείου με την οποία εργαστήκαμε στα σενάρια.[12]



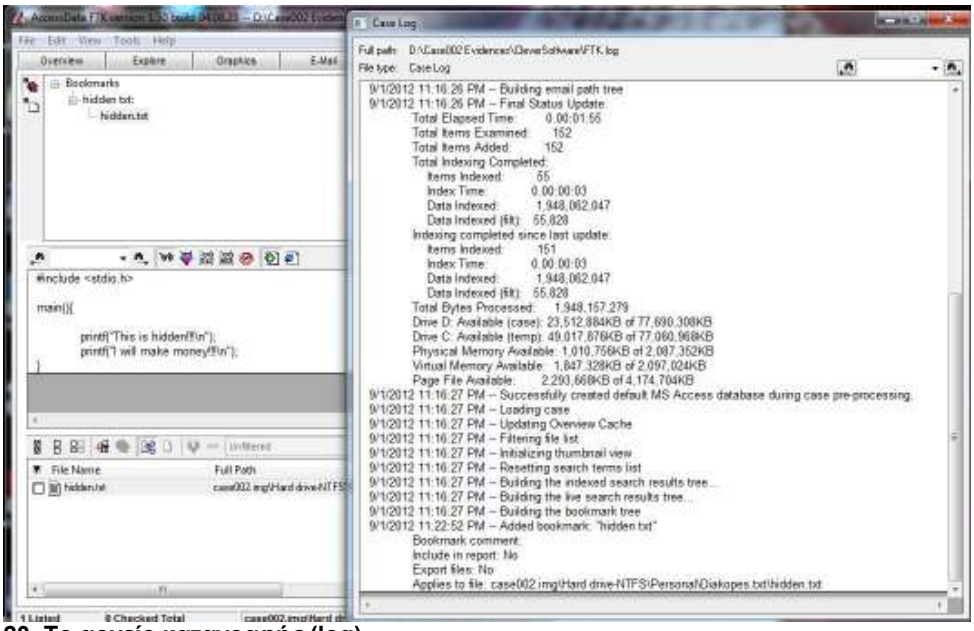
Εικόνα 17. Το περιβάλλον του FTK Analysis V3



Εικόνα 18. Το περιβάλλον του FTK Analysis V1.5



Εικόνα 19. Παράδειγμα με τον ενσωματωμένο viewer



Εικόνα 20. Το αρχείο καταγραφής (log)

EnCase v7:

Το Encase είναι ένα εμπορικό προϊόν, το οποίο αναπτύχθηκε από την Guidance Software και εισήχθη στην αγορά για πρώτη φορά το 1998. Πρόκειται ίσως για το πιο δημοφιλές εργαλείο στην περιοχή της Ψηφιακής Εγκληματολογίας και χρησιμοποιείται για την ανάλυση ψηφιακών αποδείξεων (για παράδειγμα σε αστικές / ποινικές έρευνες, τις έρευνες της δικαιοσύνης, τα δεδομένα της συμμόρφωσης). Το Encase είναι ένα πρόγραμμα μόλις 5-Mbyte γραμμένο σε C και προσφέρει ένα

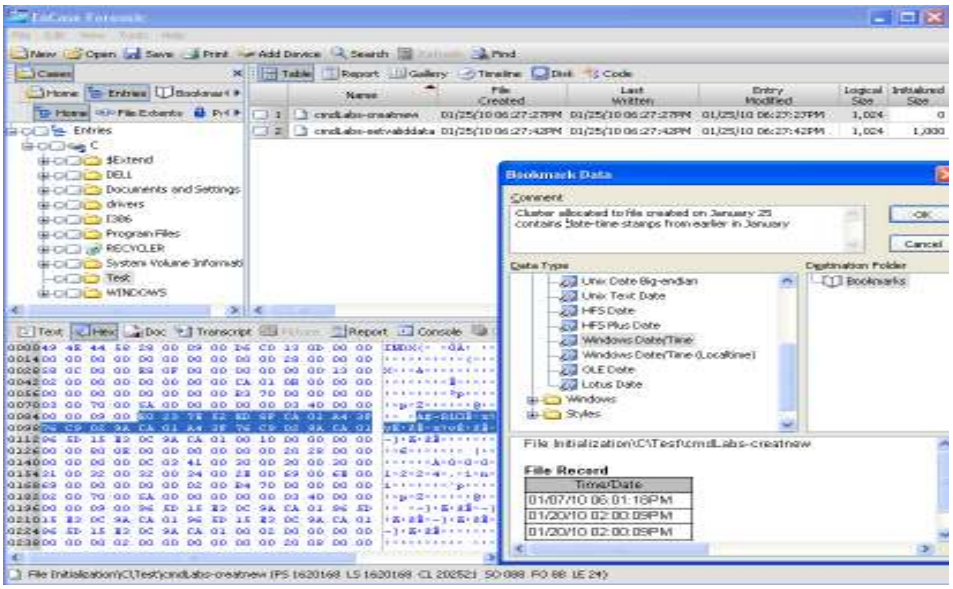
ολοκληρωμένο σύνολο εργαλείων εγκληματολογικών υπηρεσιών. Το λογισμικό είναι διαθέσιμο στις υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος αλλά και στις επιχειρήσεις.[25] Το Encase περιλαμβάνει λειτουργίες, όπως:

- Disk imaging
- Επικύρωση δεδομένων (data verification)
- Ανάλυση δεδομένων (data analysis)
- Ανάκτηση δεδομένων από μη ανατεθειμένες περιοχές του σκληρού δίσκου
- Παρουσίαση των ευρημάτων

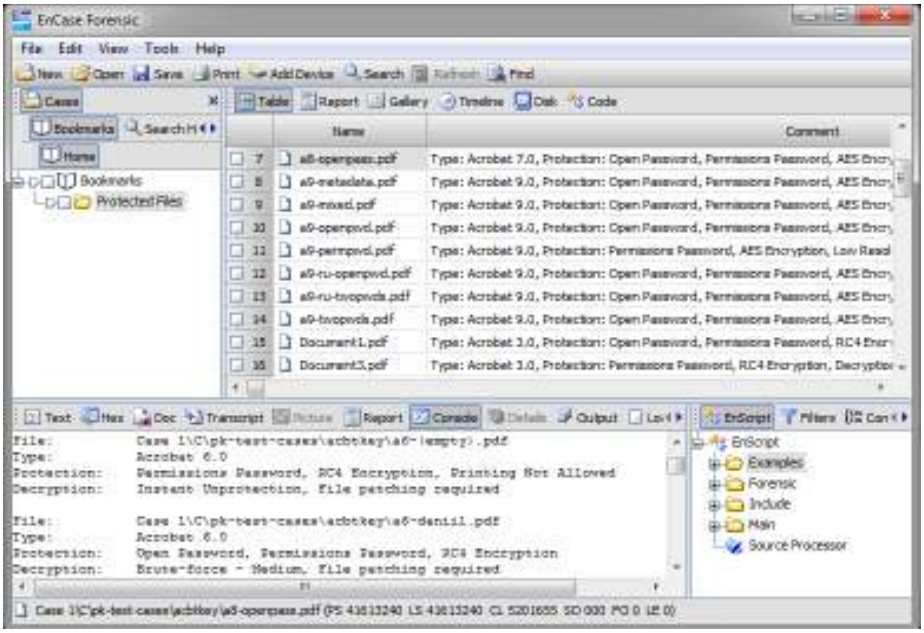
Το EnCase μπορεί να δουλέψει σε λειτουργικά Windows, Linux, Unix και Macintosh, και μπορεί να ανασύρει και να αναλύσει στοιχεία από αποθηκευτικά μέσα των παρακάτω τύπων: FAT12, FAT16, FAT32, NTFS, HFS, HFS+, CD, EXT2 (Linux) και UFS (UNIX). Ο υπολογιστής στον οποίο διεξάγεται η έρευνα ονομάζεται Subject, ενώ ο υπολογιστής στον οποίο εκτελείται το πρόγραμμα Storage.

Με το EnCase, οι ερευνητές αρχίσουν με την τοποθέτηση του σκληρό δίσκο του υπόπτου στον υπολογιστή που διεξάγει την έρευνα. Στη συνέχεια κάνει ένα bit-stream είδωλο του δίσκου. Η εικόνα-είδωλο του δίσκου τοποθετείται ως αρχείο μόνο για ανάγνωση των αποδεικτικών στοιχείων. Αυτό αποτρέπει τους ερευνητές από την τροποποίηση των δεδομένων και ως εκ τούτου δεν αναιρείται ως αποδεικτικό στοιχείο. Το αντίγραφο αυτό ονομάζεται Evidence File.

Στην προβολή αρχείων, το EnCase τα ταξινομεί με βάση διάφορα κριτήρια, όπως η επέκταση ή η χρονοσφραγίδα και μπορεί να αναλύσει τα αρχεία με βάση διαφορετικές μεθόδους που παρέχονται από το εργαλείο όπως, για παράδειγμα, η αναζήτηση για λέξεις κλειδιά ή η εξέταση αρχείων εικόνας ή ο έλεγχος διαγραμμένων αρχείων ή αδιάθετων περιοχών του σκληρού δίσκου . Οι χρήστες γενικά δεν μπορούν να δουν αυτές τις περιοχές του δίσκου μέσω μόνο του λειτουργικού συστήματος.



Εικόνα 21. Το περιβάλλον του Encase



Εικόνα 22. Δυνατότητες του Encase

Μια άλλη δημοφιλής μέθοδος ανάλυσης είναι η Signature Analysis, η οποία ελέγχει εάν η κατάληξη ενός αρχείου συμφωνεί με τον πραγματικό τύπο του αρχείου. Οι ερευνητές μπορούν να καθορίσουν αν ο χρήστης έχει προσπαθήσει να κρύψει τα στοιχεία από την ανίχνευση αλλάζοντας την επέκτασή του. Ελέγχονται επίσης τα Registry Files του υπολογιστή προκειμένου να ελεγχθούν τα προγράμματα που έχουν εγκατασταθεί, οι συσκευές που βρίσκονται συνδεδεμένες στο σύστημα και πληροφορίες για τους χρήστες. Προσφέρει επίσης μια EScript γλώσσα μακροεντολών που επιτρέπει στους προχωρημένους χρήστες την κατασκευή εργαλείων για την παροχή εξατομικευμένων λειτουργιών. Αφού ολοκληρωθεί ο έλεγχος, τα στοιχεία που προέκυψαν οργανώνονται σε μια αναφορά που ονομάζεται Final Report. Ο παρακάτω πίνακας παρουσιάζει μια τέτοια αναφορά.

Filename: teensex001.jpg
Full path: Toast C Drive\Windows\Temp Internet Files\...
Last Accessed: 05/05/02
Last Written: 01/19/02 03:48:44 PM
Logical File Size 12,493
Comment: This is a picture of pre-teen having sex.
Acquisition: EnCase version 3, zero errors
Acquisition Hash: 4CD90348D1C009D78E256
Verification Hash: 4CD90348D1C009D78E256
Drive Geometry: Total Size 8.8GB (10,002,825 Sectors)
Investigator's Name: Bob Private

Εικόνα 23. EnCase Final Report

Helix 3 και Helix 3 Pro:

Μια εξαιρετική προσπάθεια συλλογής και αξιοποίησης λογισμικού Ψηφιακής Εγκληματολογίας είναι αυτή της εταιρείας e-fense με το όνομα Helix3 (e-fense.com/helix).[26] Το Helix 3 μπορείτε να το κατεβάσετε δωρεάν, σε μορφή Live CD. Από εκεί και πέρα σας δίνονται οι εξής δυνατότητες:

Εικόνα 24. Επιλογές στο Helix3

Να εκκινήσετε τη σουίτα στα Windows. Μέσα από αυτό μπορείτε να αποκτήσετε πρόσβαση σε μια πληθώρα εργαλείων τα οποία θα διευκολύνουν το έργο σας. Βασικό μειονέκτημα αυτής της προσέγγισης είναι το ότι χρησιμοποιείται ένα live και συνεχώς μεταβαλλόμενο περιβάλλον (Live Analysis) για τη συλλογή και την ανάλυση των δεδομένων.

Εικόνα 25. Εκκίνηση υπολογιστή με boot Helix3

Δεύτερη επιλογή είναι να χρησιμοποιήσετε το CD για να εκκινήσετε με αυτό τον υπολογιστή σας. Το CD του Helix 3 υλοποιεί ένα παραμετροποιημένο λειτουργικό σύστημα βασισμένο στη διανομή

Ubuntu Linux, το οποίο περιέχει πολλά και χρήσιμα εργαλεία που θα βοηθήσουν το έργο σας. Βασικό πλεονέκτημα της συγκεκριμένης προσέγγισης είναι ότι λειτουργείτε σε μη μεταβαλλόμενο ή "νεκρό" περιβάλλον (Dead Analysis) το οποίο είναι το ενδεδειγμένο για έρευνες Ψηφιακής Εγκληματολογάις.

Το Helix 3 σε περιβάλλον Windows διαχωρίζει, μέσα από το γραφικό του περιβάλλον, το λογισμικό που ενσωματώνει, στις εξής κατηγορίες:

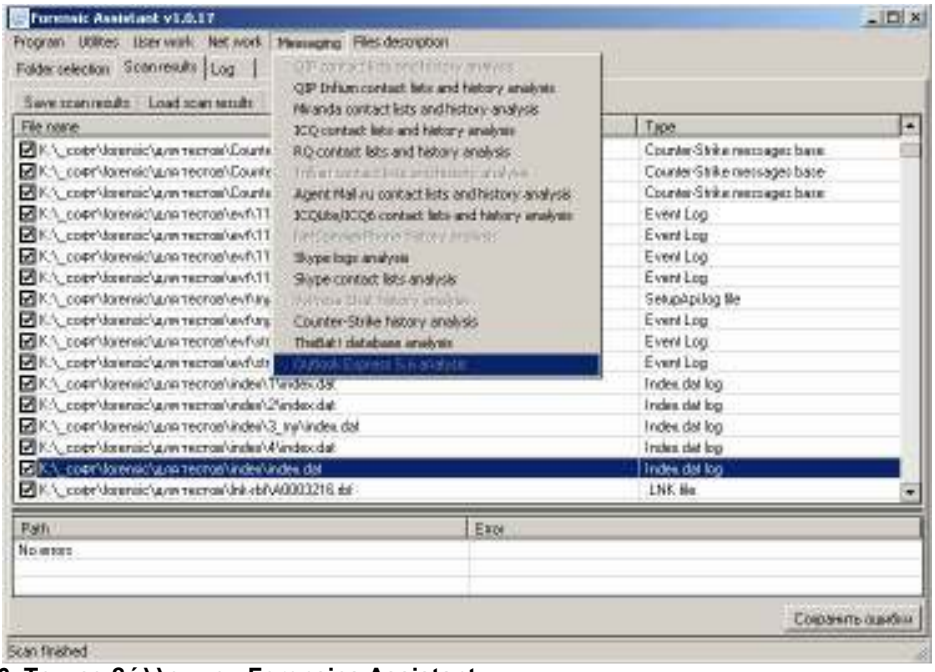
- System Information: Συγκεντρωτικά στοιχεία (drives, network, running processes κ.τ.λ.) για το προς εξέταση σύστημα.
- Live Acquisition: Σε αυτή την κατηγορία, μια πληθώρα εργαλείων όπως τα Helix Acquisition, FTK Imager, Winen και Mantech MDD μπορούν να χρησιμοποιηθούν για να πάρετε πιστά αντίγραφα (images) τόσο των σκληρών δίσκων όσο και της μνήμης του προς εξέταση συστήματος για περαιτέρω ανάλυση.
- Incident Response: Αυτή η κατηγορία περιλαμβάνει προγράμματα που θα σας επιτρέψουν τη συλλογή πολλών και χρήσιμων στοιχείων από το προς εξέταση σύστημα. Εργαλεία όπως τα WFT, FRU, IRCR2 και Nigilant32 έχουν πιο γενικό χαρακτήρα και θα συλλέξουν όσες περισσότερες πληροφορίες μπορούν από το σύστημα.
- Browse Contents: Μέσα από το γραφικό περιβάλλον του Helix3 μπορείτε να περιηγηθείτε στα αποθηκευμένα δεδομένα τού προς εξέταση συστήματος. Το Helix3 αυτόματα σας ενημερώνει για τις ημερομηνίες δημιουργίας, πρόσβασης και τροποποίησης αυτών των αρχείων καθώς και για την ακεραιότητά τους μέσω CRC και MD5 hashes.
- Scan for Pictures: Από τη συγκεκριμένη κατηγορία θα μπορέσετε να εντοπίσετε εύκολα εικόνες και φωτογραφίες που είναι αποθηκευμένες στον προς εξέταση υπολογιστή.
- Investigative Notes: Σε αυτήν την κατηγορία το Helix3 σας παρέχει ένα περιβάλλον στο οποίο μπορείτε να καταγράψετε την εξέλιξη της έρευνάς σας.

Σε περιβάλλον Linux το σύνολο του διαθέσιμου λογισμικού μπορείτε να τα βρείτε μέσω του βασικού μενού και της διαδρομής Applications > Forensics & IR. Τα βασικότερα εργαλεία που μπορείτε να χρησιμοποιήσετε, είναι τα Adepto, Autopsy, Linen και Retriever. Με αυτά θα μπορέσετε να πάρετε πιστά αντίγραφα των προς εξέταση δεδομένων, να τα αναλύσετε και να δημιουργήσετε τις κατάλληλες αναφορές.

Το σωστά διαμορφωμένο interface του, η πληθώρα των προγραμμάτων που περιέχει, η σωστή αρχειοθέτησή τους στις αντίστοιχες κατηγορίες και η δέσμευση της e-fense για υποστήριξη και ανανέωση του συγκεκριμένου Live CD καθιστούν το Helix 3 μια πολύ αξιόπιστη λύση.

Forensics Assistant:

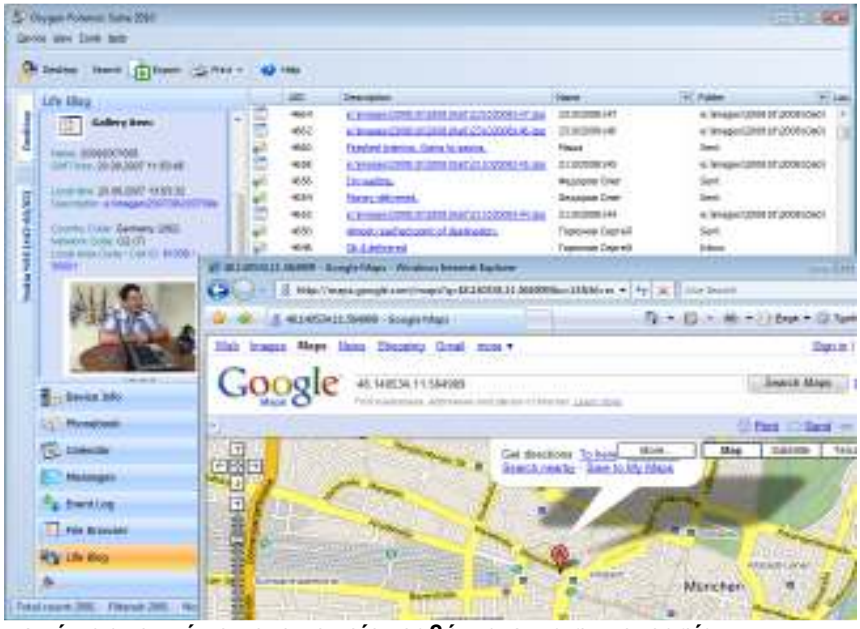
Το συγκεκριμένο εργαλείο δημιουργήθηκε για ειδικούς που εργάζονται σε κρατικές υπηρεσίες. Το πρόγραμμα βοηθά στην εύρεση και στην ανάλυση αποδείξεων μέσα από εγκατεστημένα προγράμματα, log files και αρχεία. Μπορεί να ανασύρει πληροφορίες επίσης από ICQ, messenger, Skype και Outlook. Επίσης μπορεί να ανασύρει και να αναλύσει τις κινήσεις του χρήστη στο internet, με τη βοήθεια των .dat αρχείων.[27]



Εικόνα 26. Το περιβάλλον του Forensics Assistant

Oxygen Forensics Suite:

Μια εργαλειοθήκη με πολλές δυνατότητες. Μπορεί να κάνει ανάλυση σε πολλών ειδών αρχεία, σε e-mail και σε περιηγητές. Μπορεί επίσης να αναλύσει κινητά τηλέφωνα ανεξαρτήτου λογισμικού (λειτουργεί σε iOS, Android, Blackberry, Windows mobile). ένα πολύ ενδιαφέρον χαρακτηριστικό του εργαλείου είναι ότι μπορεί να σαρώσει όλες τις φωτογραφίες και αν περιέχουν γεωγραφικές πληροφορίες να απεικονίσει κάθε μια στο μέρος στο οποίο τραβήχτηκε. Μπορεί επίσης να εξάγει στατιστικά στοιχεία ανάλογα με τα logs των κλήσεων.[28]



Εικόνα 27. Απεικόνιση του τόπου στον οποίο τραβήχτηκε μια φωτογραφία

Εικόνα 28. Στατιστικά στοιχεία επαφών

Netanalysis:

Λογισμικό το οποίο χρησιμοποιείται για ανάλυση ευρημάτων από ιστοσελίδες, cookies, κλπ. [29]

Internet Evidence Finder:

Χρησιμοποιείται για ανάκτηση ευρημάτων από δραστηριότητα στο διαδίκτυο. Ευκολο στη χρήση και αναλύει ευρήματα από κοινωνικά δίκτυα, instant messengers, web browsers κλπ.[30]

6.2.2 Ελεύθερου Λογισμικού

Backtrack:

Μια επίσης πολύ καλή προσπάθεια συλλογής και αξιοποίησης λογισμικού Ψηφιακής Εγκληματολογίας είναι η έκδοση Linux με το όνομα Backtrack. Το Backtrack μπορείτε να το κατεβάσετε δωρεάν, σε μορφή Live CD (backtrack-linux.org/downloads).[31]

Χρησιμοποιήστε το CD για να εκκινήσετε με αυτό τον υπολογιστή σας. Το CD του Backtrack υλοποιεί ένα παραμετροποιημένο λειτουργικό σύστημα βασισμένο στη διανομή Ubuntu Linux, το οποίο περιέχει πολλά και χρήσιμα εργαλεία που θα βοηθήσουν το έργο σας. Βασικό πλεονέκτημα της συγκεκριμένης προσέγγισης είναι ότι λειτουργείτε σε μη μεταβαλλόμενο ή "νεκρό" περιβάλλον (Dead Analysis) το οποίο είναι το ενδεδειγμένο για έρευνες Ψηφιακής Εγκληματολογίας.

Εικόνα 29. Προγράμματα για έρευνα στην ψηφιακή εγκληματολογία

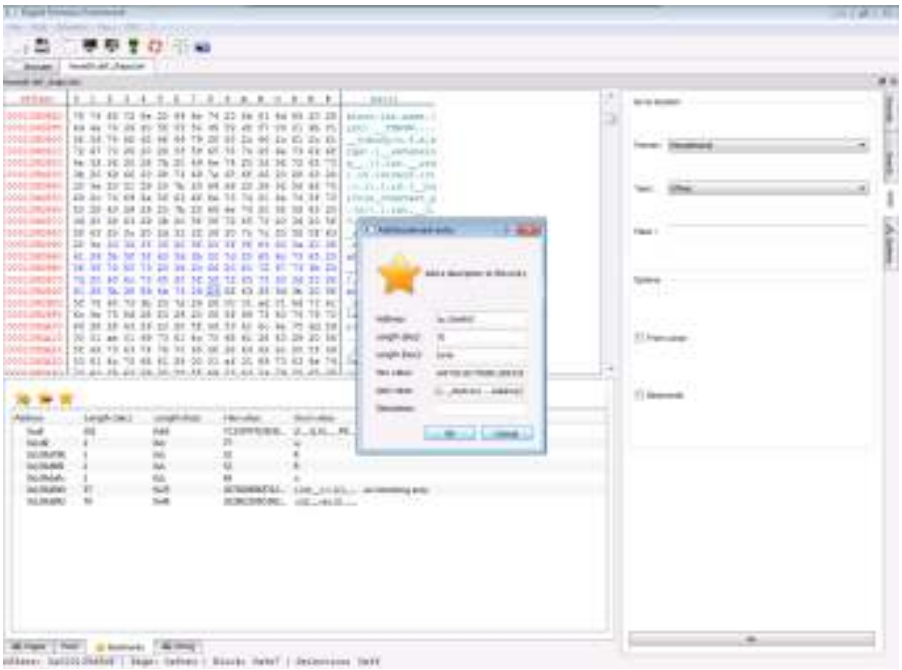
Διαθέσιμα προγράμματα:

1. **Anti Virus Forensic Tools**
   - chkrootkit
   - rkhunter
2. **Digital Anti Forensics**
   - truecrypt
3. **Digital Forensics**
   - hexedit
4. **Forensic Analysis Tools**
   - bulk_extractor
   - evtparse
   - exiftool
   - missidentify
   - mork
   - pref
   - PTK
   - readpst
   - reglookup
   - stegdetect
   - vinetto
5. **Forensic Carving Tools**
   - fatback
   - foremost
   - magicrescue
   - recoverjpeg
   - safecopy
   - scalpel
   - scrounge-ntfs
   - testdisk
6. **Forensic Hashing Tools**
   - hashdeep
   - md5deep
   - sha1deep
   - sha256deep
   - tigerdeep
   - whirlpooldeep
7. **Forensic Imaging Tools**
   - air
   - dc3dd
   - ddrescue
   - ewfaquire

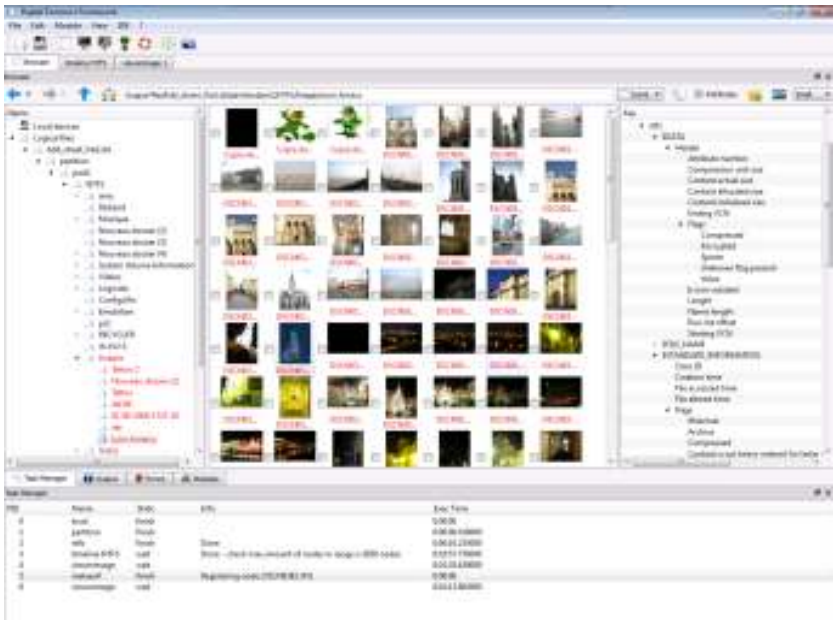
8. **Forensic Suites**
   - PTK
   - Setup Autopsy
   - Sleuthkit
9. **Network Forensics**
   - Driftnet
   - p0f
   - tcpreplay
   - Wireshark
   - Xplico
10. **Password Forensics Tools**
    - CmosPwd
    - fcrackzip
    - samdump
11. **PDF Forensic Tools**
    - pdfid
    - pdf-parser
    - peepdf
12. **RAM Forensics Tools**
    - pdfbook
    - pdgmail
    - PTK
    - Volatility

Digital Forensics Framework:

Το DFF είναι ταυτόχρονα ένα εργαλείο Ψηφιακής Εγκληματολογίας και μια πλατφόρμα ανάπτυξης εφαρμογών. Αποτελείται από εργαλεία, βιβλιοθήκες και διεπαφές χρηστών (user interfaces). Χρησιμοποιείται τόσο από ειδικούς ερευνητές όσο και για εκπαιδευτικό σκοπό. Είναι γραμμένο σε Python και C++ και χρησιμοποιεί μόνο τεχνολογίες ανοιχτού λογισμικού.[32]



Εικόνα 30. Το περιβάλλον του DFF



Εικόνα 31. Ανάλυση αποθηκευτικού μέσου και προβολή εικόνων

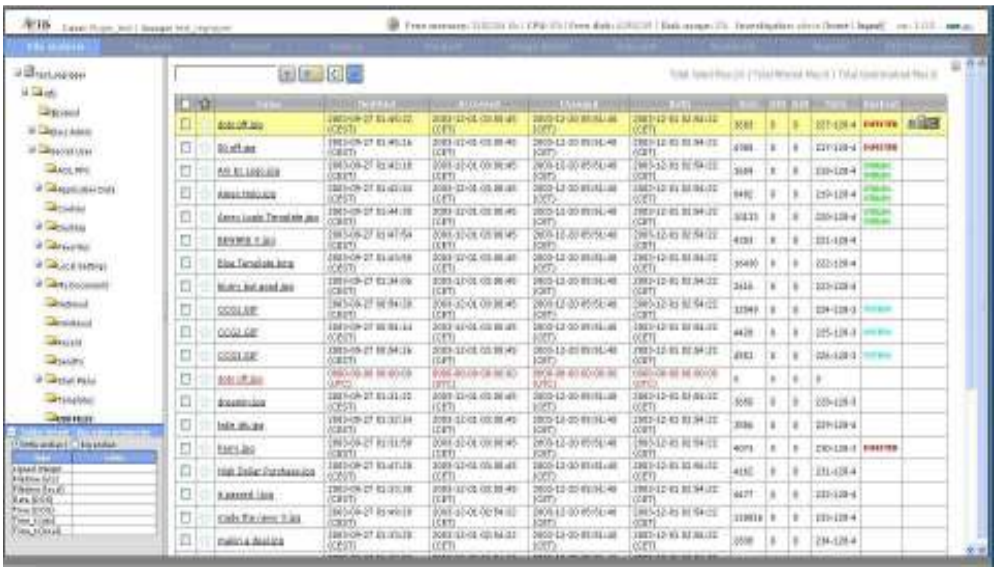
The Sleuth Kit:

Το TSK είναι μια σουίτα η οποία περιέχει βιβλιοθήκες και εργαλεία τόσο για Windows όσο και για Linux περιβάλλοντα. Γράφτηκε από τον ιδιωτικό ερευνητή Brian Carrier. Μπορεί να χρησιμοποιηθεί για ανάλυση και εξαγωγή ψηφιακών αποδείξεων από δεδομένα. Χρησιμοποιεί το Autopsy, το οποίο είναι το γραφικό περιβάλλον του TSK.[33]

Εικόνα 32. Η σουίτα TSK με το Autopsy

PTK Forensics:

Το εργαλείο αυτό είναι ένα πλαίσιο για τη χρησιμοποίηση των εργαλείων του The Sleuth Kit. Το PTK forensics είναι παραπάνω όμως δεν είναι μόνο ένα γραφικό περιβάλλον βασισμένο σε Ajax. Προσφέρει και άλλα χαρακτηριστικά όπως έρευνα, ανάλυση και διαχείριση πολύπλοκων ψηφιακών ερευνών και υποθέσεων.[34]



Εικόνα 33. Το γραφικό περιβάλλον του PTK Forensics

The Coroner's Toolkit:

Το Coroner's Toolkit είναι μια συλλογή από ελεύθερα εργαλεία. Χρησιμοποιείται κυρίως σε περιπτώσεις που πρέπει να ερευνηθεί η εισβολή σε έναν υπολογιστή. Το εργαλείο μπορεί να προσομοιώσει τις ενέργειες και τα βήματα του εισβολέα. Αυτό το επιτυγχάνει ελέγχοντας τους χρόνους πρόσβασης στα αρχεία τόσο του χρήστη όσο και του λειτουργικού συστήματος. Επίσης έχει δυνατότητα ανάκτησης διαγραμμένων αρχείων.[35]

SANS SIFT Workstation:

Πρόκειται για μια διανομή Linux σε VMWARE, η οποία αποτελεί πλήρες πακέτο για εγκληματολογική διερεύνηση σε ψηφιακά πειστήρια.[36]

CAINE:

Computer Aided INvestigative Environment. Πρόκειται για ανοικτό λογισμικό, το οποίο είναι μιά έκδοση live CD, με ενσωματωμένα εργαλεία για διερεύνηση ψηφιακών πειστηρίων. Περιλαμβάνει εργαλεία για συλλογή, ανάλυση και δημιουργία αναφορών.[37]

Lnx4n6:

Forensic boot CD που έχει δημιουργηθεί από την Βελγική αστυνομία (Federal Computer Crime Unit), βασισμένο σε Knoppix και περιέχει λογισμικό ανοικτού τύπου για διερεύνηση ψηφιακών πειστηρίων.[38]

PALADIN:

Δεν είναι ανοικτού τύπου αλλά είναι δωρεάν. Συλλογή πειστηρίων (Aquisition), ανάλυση και προεπισκίπηση (Preview). Ερχεται σε δύο εκδόσεις σε DVD και σε usb. Το δεύτερο πωλείται έναντι μικρού αντιτίμου. Δίνει έμφαση στην ευκολία χρήσης.[39]

SANTOKU:

Πρόκειται για διανομή Linux, προσαρμοσμένη κυρίως σε εξέταση κινητών τηλεφώνων. Περιλαμβάνει εργαλεία για εγκληματολογική εξέταση, flashing εργαλεία και εργαλεία για δημιουργία εγκληματολογικών αντιγράφων σε NAND. Περιλαμβάνει επίσης εργαλεία για διερεύνηση κακόβουλου λογισμικού σε κινητά και εργαλεία για έλεγχο του κινητού από πλευράς ασφαλείας.[40]

Forevid:

Ανοιχτό λογισμικό για την εγκληματολογική ανάλυση βίντεο προερχόμενο από CCTV και όχι μόνο. Υποστηρίζει ανάλυση βίντεο frame by frame, εξαγωγή στιγμιοτύπων, φίλτρα για βελτίωση εικόνας και άλλα εργαλεία, καθώς και βοήθεια στη δημιουργία αναφορών.[41]

7 Σενάρια

7.1 Βιομηχανική Κατασκοπεία

Εταιρική κατασκοπεία (Corporate Espionage) ή Βιομηχανική κατασκοπεία (Industrial Espionage). Η βιομηχανική κατασκοπία αρκείται σε μάνατζερ, τεχνικούς, developers και λοιπούς υπεράνω υποψίας παράγοντες με καθημερινή πρόσβαση σε απόρρητο περιεχόμενο. Οι πρακτικές της είναι ποικίλες και εξαιρετικά διαδεδομένες: κυβερνοεπιθέσεις, εσωτερική πληροφόρηση, διασπορά ψευδών πληροφοριών, αντιγραφή τεχνογνωσίας.

Πάνω από το 50% των κλοπών διεπράχθησαν από νυν ή πρώην υπαλλήλους. Κάποιες από τις κατηγορίες κλεμμένων πληροφοριών είναι:

- πληροφορίες τιμολόγησης
- πληροφορίες βιομηχανικής διαδικασίας
- πληροφορίες ανάπτυξης και προδιαγραφών προϊόντων
- πελατολόγιο
- αρχεία προσωπικού

Στο δικό μας σενάριο υπάρχουν δυο αντίπαλες εταιρείας λογισμικού, η εταιρεία Cleversoftware και η εταιρεία Stolensoftware. Η Cleversoftware είχε ανακοινώσει ότι την παραμονή της Πρωτοχρονιάς (31/12/2011) θα δώσει στην κυκλοφορία το νέο της προϊόν. Είχε ξοδέψει 150.000€ σε διαφημιστική καμπάνια και η διάρκεια σχεδίασης και ανάπτυξης του προϊόντος ήταν περίπου δυο χρόνια.

Ξαφνικά την παραμονή των Χριστουγέννων η αντίπαλη εταιρεία, η Stolensoftware, σε μια μικρή τελετή παρουσίασε το καινούριο της προϊόν, το οποίο ήταν παρόμοιο με το προϊόν που θα ανακοίνωνε η Cleversoftware. Όπως είναι λογικό πήρε το μεγαλύτερο κομμάτι της αγοράς, με τεράστια κέρδη και αντίστοιχα η Cleversoftware έχασε πολλά από το προϋπολογισθέντα κέρδη.

Ο Διευθύνων Σύμβουλος της Cleversoftware αμέσως κατάλαβε ότι η εταιρεία είχε πέσει θύμα επιχειρησιακής κατασκοπείας. Η πολιτική ασφαλείας και τα μέσα που την εφάρμοζαν ήταν τέτοια που η περίπτωση επίθεσης και υποκλοπής του λογισμικού ήταν σχεδόν απίθανη. Κατέληξε λοιπόν στο συμπέρασμα ότι η διαρροή ήταν εκ των έσω. Κάποιος υπάλληλος είχε εξαγορασθεί από την αντίπαλη εταιρεία. Πρόσβαση στον κώδικα είχαν μόνο ο ίδιος και τρεις developers. Ανέθεσε λοιπόν στο ιδιωτικό γραφείο ForTrust την υπόθεση, με σκοπό να βρουν αποδείξεις για την παράνομη πράξη, έτσι ώστε να είναι σε θέση να μηνύσει τον υπεύθυνο και την αντίπαλη εταιρεία για διαφυγόντα κέρδη.

Νομοθετικό πλαίσιο

Επιχειρηματικό απόρρητο είναι κάθε γεγονός που σχετίζεται με ορισμένη επιχείρηση, γνωστό μόνο σε στενά καθορισμένο κύκλο προσώπων υπόχρεων προς τήρηση μυστικότητας και το οποίο κατά τη βούληση του κυρίου της επιχειρήσεως πρέπει αν παραμείνει μυστικό λόγω υπάρξεως δικαιολογημένου οικονομικού συμφέροντος του προς τήρηση μυστικότητας.

- Νόμος 146/1914 «Περί αθεμίτου ανταγωνισμού» (ΦΕΚ Β' 16.12.1913-27.1.1914) Άρθρα 1, 16, 17 και 18.
- Νόμος 2190/1920 «Περί Ανώνυμων Εταιρειών» (ΦΕΚ Α' 37/30.3.1963) Άρθρο 22 Α.
- Νόμος 3190/1955 «Περί Εταιρειών Περιορισμένης Ευθύνης» (ΦΕΚ Α' 91/16.4.1955) Άρθρο 20.
- Αστικός Κώδικας Άρθρο 288, 741, 747.
- Ποινικός Κώδικας Άρθρο 370 Β.

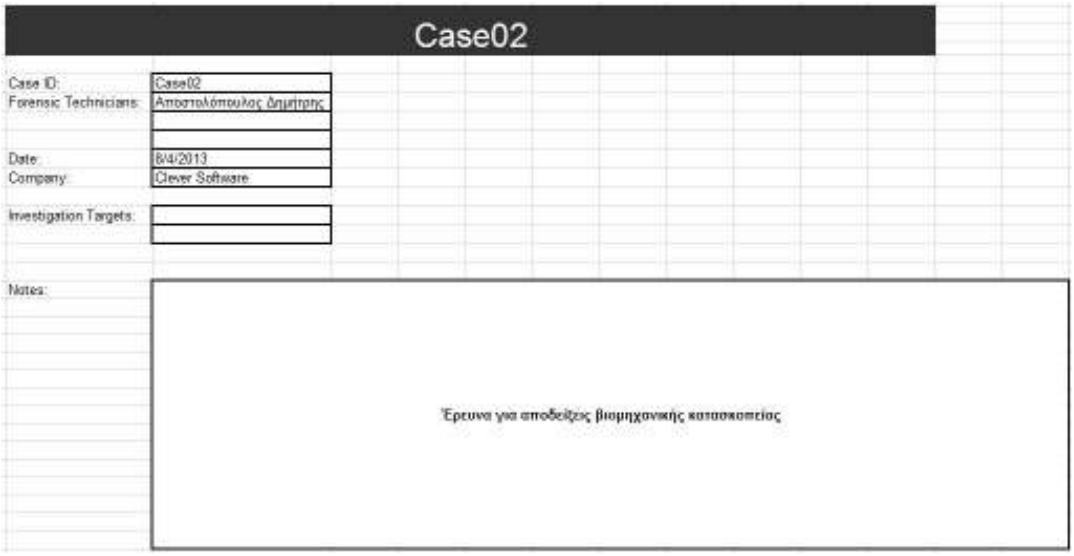
Διαδικασία έρευνας

Καταρχήν για να εξετάσουμε το χώρο του «εγκλήματος» και τα μηχανήματα, θα πρέπει να έχουμε γραπτή άδεια από τον ιδιοκτήτη και τους χρήστες. Ο ιδιοκτήτης μας εξουσιοδοτεί εγγράφως και μας ενημερώνει ότι οι χρήστες έχουν υπογράψει σύμβαση εχεμύθειας (Παράρτημα Α), στην οποία αναφέρεται ρητά ότι το υλικό και τα αποτελέσματα της Δραστηριότητας ανήκουν στην εταιρεία CleverSoftware. Ο ιδιοκτήτης της εταιρείας έχει δώσει μια εβδομάδα υποχρεωτική άδεια στους τρεις developers, έτσι ώστε η ομάδα της ForTrust να δουλέψει απερίσπαστη.

Κάθε ένα από τα τρία γραφεία στα οποία εργάζονταν οι developers σφραγίζονται και πρόσβαση σε αυτά έχουν μόνο οι Digital Forensics Experts της ForTrust. Την ίδια διαδικασία θα ακολουθήσουμε και για τα τρία γραφεία, εμείς όμως θα περιγράψουμε τη διαδικασία που ακολουθήσαμε στο γραφείου του κ. Άτιμου Περικλή, ο οποίος εκ των υστέρων αποδείχθηκε από τα ευρήματα της έρευνας, ότι ήταν ο υπαίτιος της διαρροής των πληροφοριών.

Τα ευρήματα της έρευνας είναι πολύ πιθανό να παρουσιαστούν στο δικαστήριο, οπότε για να γίνουν αποδεκτά θα πρέπει να ακολουθήσουμε μια συγκεκριμένη διαδικασία.

Η πρώτη φάση της έρευνας είναι να ασφαλίζουμε το χώρο και να εξασφαλίζουμε ότι κανένα μη εξουσιοδοτημένο άτομο δεν θα έχει πρόσβαση σε αυτό. Για την είσοδο και έξοδο στο χώρο έρευνας χρησιμοποιούμε ένα απλό αρχείο καταγραφής των ανθρώπων που εισέρχονται, το σκοπό, καθώς επίσης και το άτομο από το οποίο εξουσιοδοτήθηκαν.



Εικόνα 34. Αρχείο καταγραφής

Authorized By	Date Entry	Time Entry	Entry Reason	Full Name	Badge ID	Exit Time
Αποστολόπουλος Δημήτρης	8/4/2013	13:00	Crime Investigation	Αποστολόπουλος Δημήτρης	1	15:00

Εικόνα 35. Αρχείο καταγραφής εισερχομένων ατόμων

Θα πρέπει να φωτογραφήσουμε το χώρο και κάθε αντικείμενο μέσα σε αυτόν. Η μνήμη δεν είναι αποδεκτή απόδειξη στο δικαστήριο. Πρέπει να καταγραφούν όλα τα αντικείμενα στο χώρο λεπτομερώς και στη συνέχεια να εξάγουμε εκείνα τα αντικείμενα που θεωρούμε ότι θα μας βοηθήσουν στην έρευνα για να τα μεταφέρουμε στο εργαστήριο. Τοποθετούμε κάθε αντικείμενο (σκληρός δίσκος) σε ηλεκτροστατική σακούλα και το τοποθετούμε σε συγκεκριμένο κουτί. Τόσο η σακούλα όσο και του κουτί έχουν ID.

Evidence Technician: Αποστολόπουλος Δημήτρης

Evidence Catgegory	Tag ID	Bag ID	Time	Date	Collected By	Transport Box ID
Physical Hard Drive	1	1	13:30	8/4/2013	Αποστολόπουλος Δημήτρης	1

Εικόνα 36. Αρχείο καταγραφής των αντικειμένων προς μεταφορά

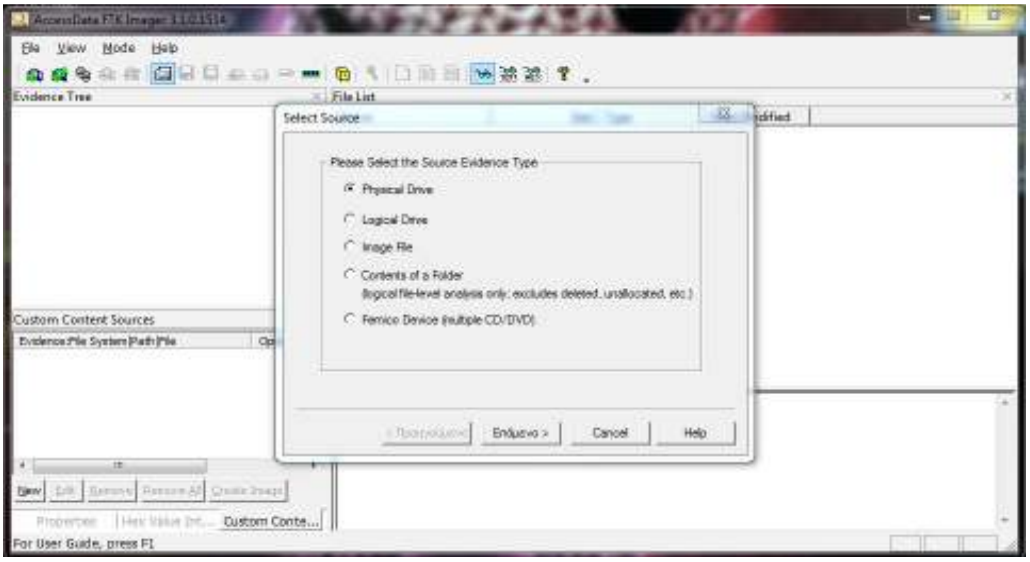
Τα αντικείμενα αυτά θα πρέπει να μεταφερθούν στο εργαστήριο από εξουσιοδοτημένο άτομο, με μεγάλη προσοχή.

Chain of Custody

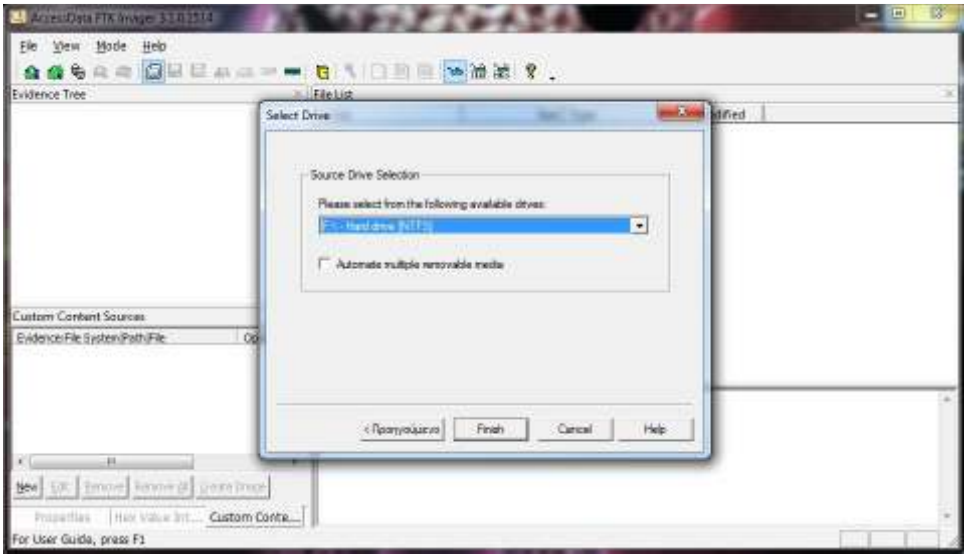
Name of Transporter	Current Location	Target Location	Reason for Transport	Box ID(s) in Transport	Released By	Date	Time	Arrival Signoff
Αποστολόπουλος Δημήτρης	Clever Software	Lab	Forensics Analysis	1	Αποστολόπουλος Δημήτρης	8/4/2013	15:05	
Αποστολόπουλος Δημήτρης	Lab	Court	Case Presentation	1	Αποστολόπουλος Δημήτρης	11/4/2013	10:00	

Εικόνα 37. Αρχείο καταγραφής μεταφοράς των αντικειμένων

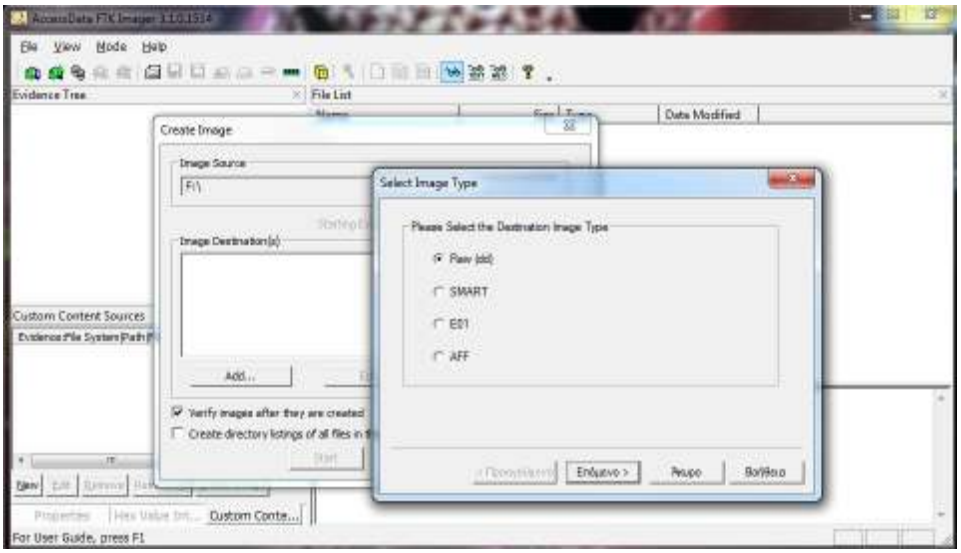
Στο εργαστήριο, στη φάση της ανάλυσης δε θα πρέπει να πειράξουμε το σκληρό δίσκο, γιατί αποτελεί αποδεικτικό στοιχείο και κάθε αλλαγή θα μπορούσε να καταστρέψει τη διαδικασία. Για το λόγο αυτό πρέπει να φτιάξουμε ένα κλώνο του σκληρού δίσκου για να εργαστούμε σε αυτόν. Έχουμε συνδέσει το σκληρό δίσκο στο σύστημά μας και με το εργαλείο FTK Imager δημιουργούμε ένα κλώνο του.



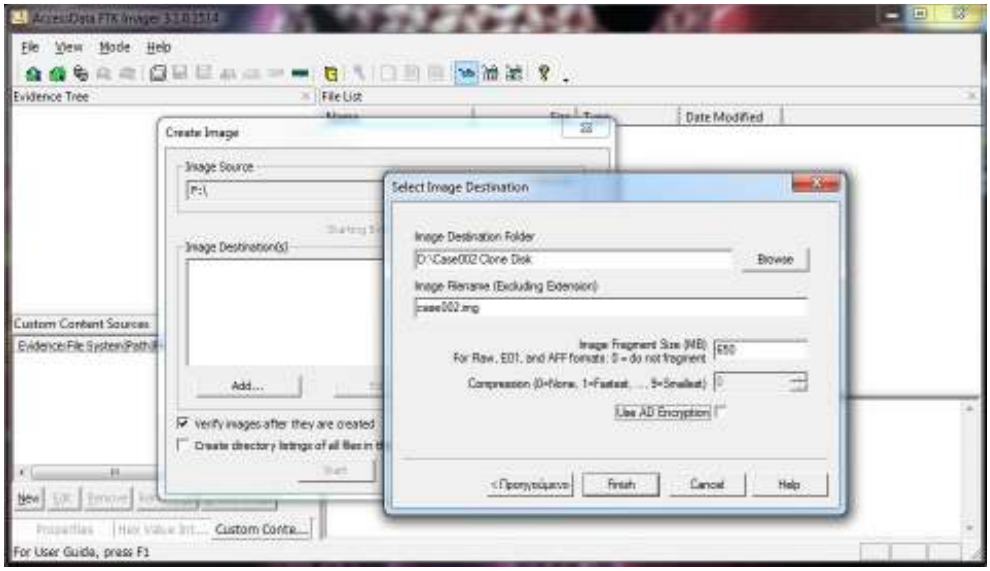
Εικόνα 38. Δημιουργία κλώνου_1



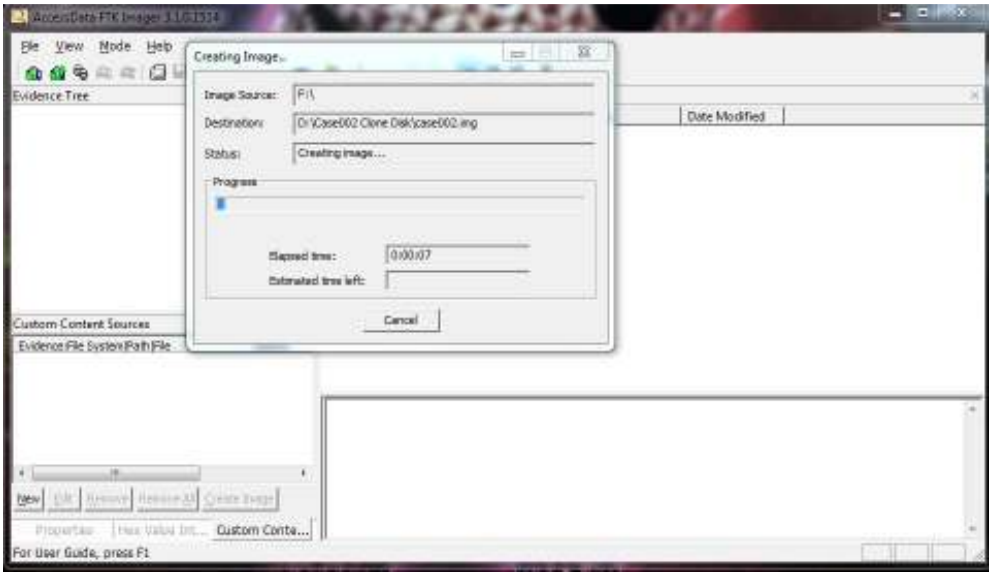
Εικόνα 39. Δημιουργία κλώνου_2



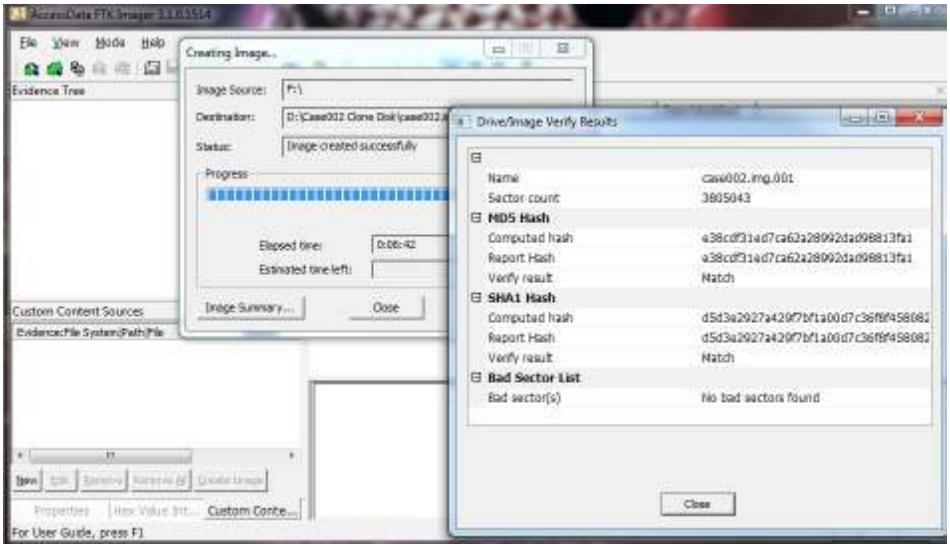
Εικόνα 40. Δημιουργία κλώνου_3



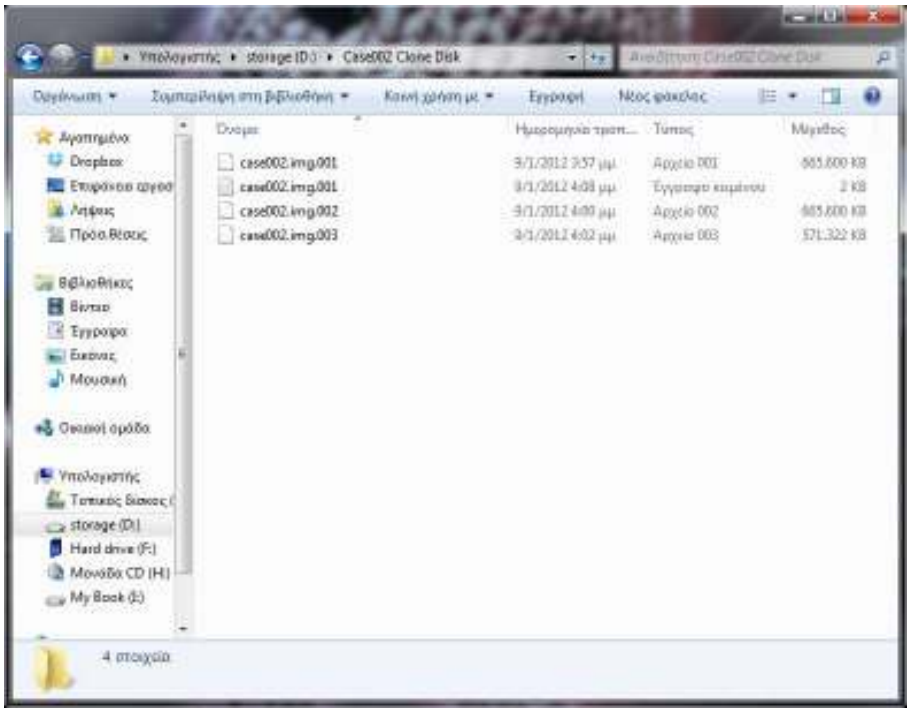
Εικόνα 41. Δημιουργία κλώνου_4



Εικόνα 42. Δημιουργία κλώνου_5



Εικόνα 43. Δημιουργία κλώνου_6



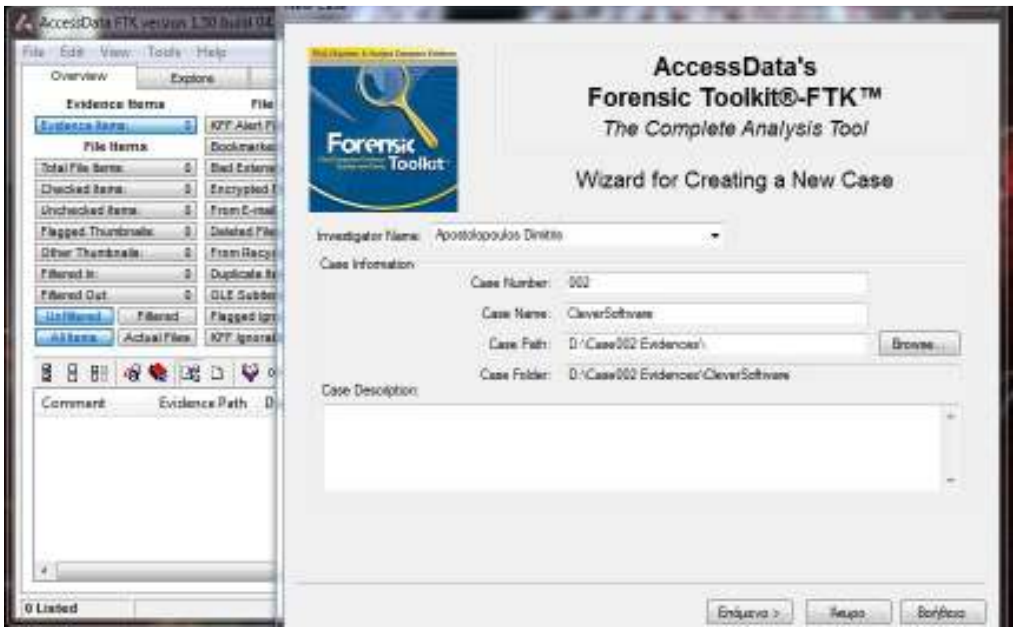
Εικόνα 44. Δημιουργία κλώνου_7

Τα περιεχόμενα του εγγράφου κειμένου case002.img.001 αντιγράφονται στο αρχείο καταγραφής ως αποδείξεις. Ολόκληρος ο φάκελος αντιγράφεται σε DVD για να αποφύγουμε κάποια αλλοίωση.

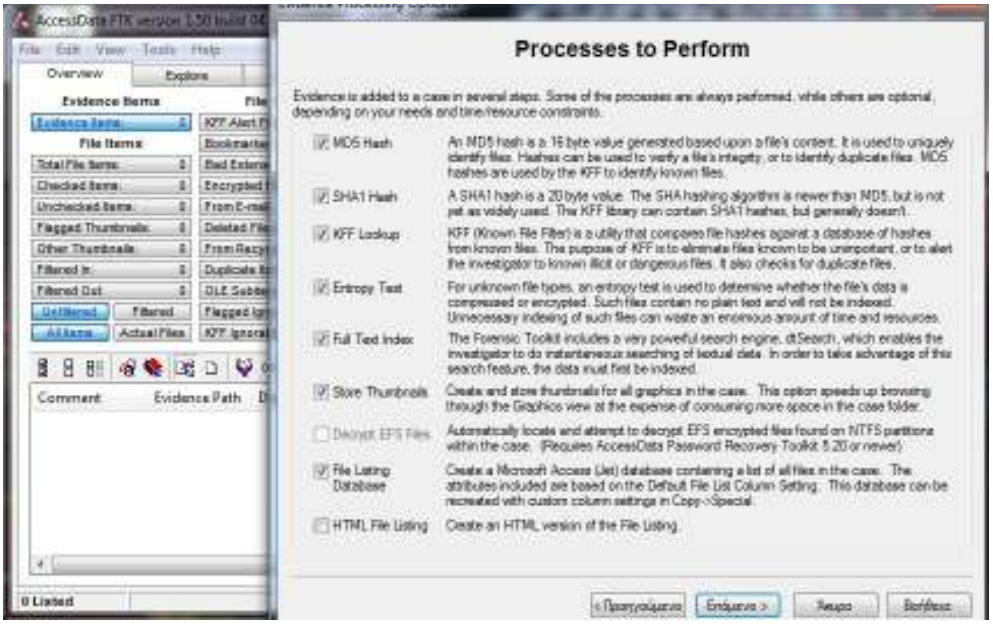
```
3707 9/4/2013 12:32:42 AM -- Updating Overview Cache
3708 9/4/2013 12:32:43 AM -- Filtering file list
3709 9/4/2013 12:32:43 AM -- Initializing thumbnail view
3710 9/4/2013 12:32:43 AM -- Resetting search terms list
3711 9/4/2013 12:32:43 AM -- Building the indexed search results tree...
3712 9/4/2013 12:32:43 AM -- Building the live search results tree...
3713 9/4/2013 12:32:43 AM -- Building the bookmark tree
3714 9/4/2013 12:36:34 AM -- Launched independent view of file\image01\Part_1\NONAME-NTFS\RECYCLER\S-1-5-21-1482476501-1292428093-1801674531-500\Oct10.009_02
3715 9/4/2013 12:36:36 AM -- Closed independent view of file image01\Part_1\NONAME-NTFS\RECYCLER\S-1-5-21-1482476501-1292428093-1801674531-500\Oct10.009_02
3716 9/4/2013 12:48:54 AM -- Added bookmark: "txt in jpg"
3717 Bookmark comment: Hidden txt file inside a jpg
3718 Include in report: Yes
3719 Export files: No
```

Εικόνα 45. Αρχείο καταγραφής ηλεκτρονικών αποδείξεων

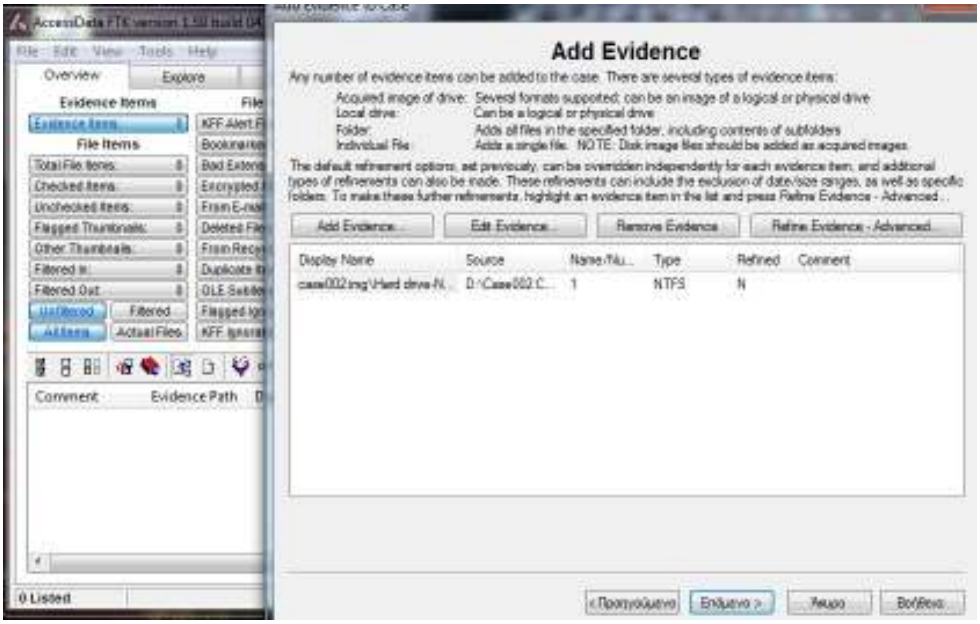
Μόλις ολοκληρωθεί η διαδικασία της αντιγραφής, ο δίσκος αποσυνδέεται από το σύστημά μας και τοποθετείται ξανά στην ηλεκτροστατική σακούλα του. Στη συνέχεια χρησιμοποιούμε το Forensics Toolkit για την ανάλυση των αντιγράφων.



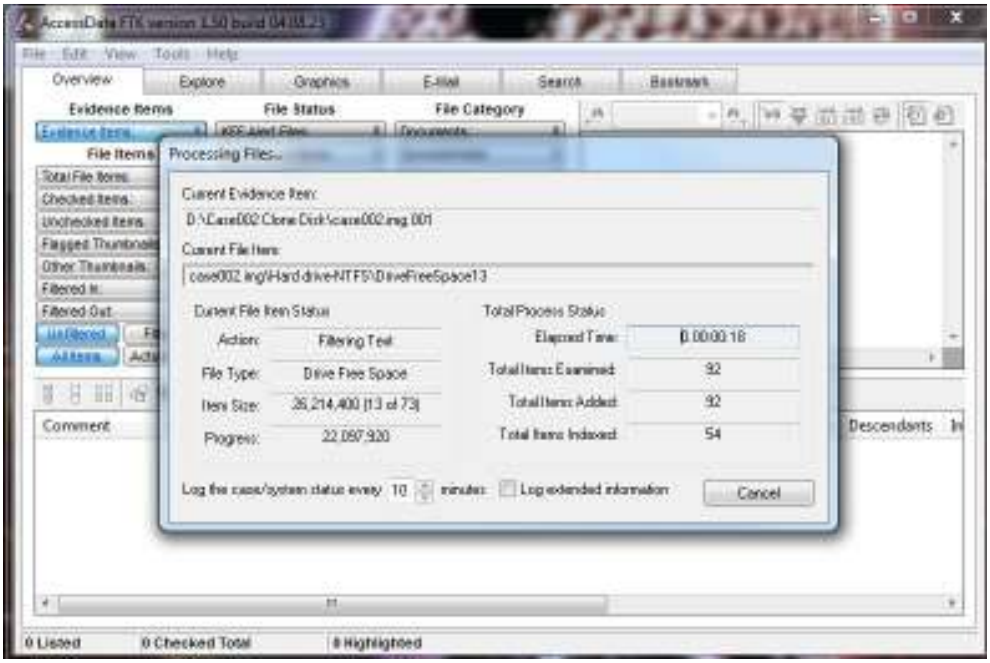
Εικόνα 46. Ανάλυση_1



Εικόνα 47. Ανάλυση_2

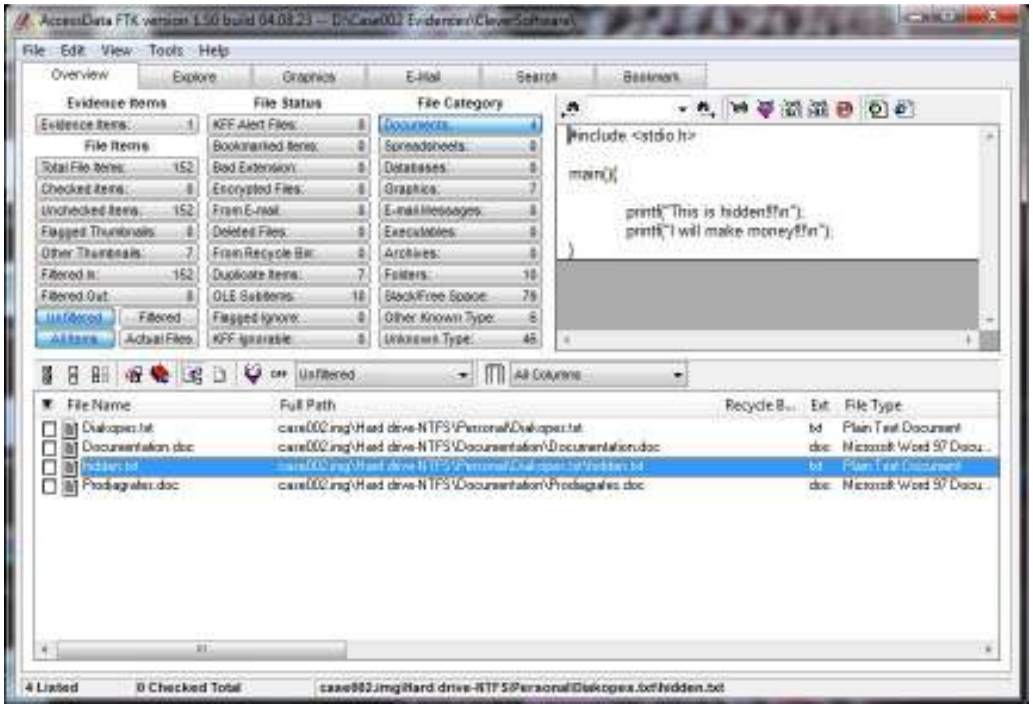


Εικόνα 48. Ανάλυση_3



Εικόνα 49. Ανάλυση_4

Στην παρακάτω εικόνα παρατηρούμε ότι το εργαλείο, αναγνώρισε ένα αρχείο κειμένου μέσα σε ένα άλλο. Και το κρυφό αρχείο, περιέχει κώδικα. Μπορούμε λοιπόν να συμπεράνουμε με ακρίβεια ότι αυτός ήταν ο τρόπος που ο συγκεκριμένος developer, «έβγαζε» κώδικα από την εταιρεία.



Εικόνα 50. Ανάλυση_5

Κάνουμε bookmark το συγκεκριμένο εύρημα και στη συνέχεια ανοίγουμε το log της εφαρμογής και αντιγράφουμε τα περιεχόμενά του στο αρχείο καταγραφής ως ηλεκτρονική απόδειξη. Τέλος παραδίδουμε στον υπεύθυνο της εταιρείας τα αποδεικτικά στοιχεία, το αρχείο καταγραφής της υπόθεσης και την αναφορά μας. Στο Παράρτημα Α υπάρχουν οι κινήσεις του κακόβουλου developer.

7.2 Ενδοεταιρική Αντιζηλία

Το σενάριο έχει να κάνει με ενδοεταιρική διαμάχη - αντιζηλία. Έχει ανατεθεί σε μια αρχιτεκτονική εταιρεία να μετασκευάσει αίθουσες ενιαίου λυκείου για τη δημιουργία εργαστηρίων φυσικών επιστημών, ηλεκτρονικών υπολογιστών και τεχνολογίας. Ανατέθηκε λοιπόν, σε μια ομάδα τριών αρχιτεκτόνων να κάνουν από μια μελέτη και εκείνη που θα κρινόταν ως η καλύτερη και η πιο συμφέρουσα οικονομικά θα περνούσε στη φάση της υλοποίησης. Αυτό σήμαινε κέρδη για την εταιρεία, bonus για τον υπεύθυνο αρχιτέκτονα και προαγωγή. Όπως είναι λογικό και οι τρεις αρχιτέκτονες ήθελαν να έχουν την καλύτερη μελέτη. ’Η στα πλαίσια του σεναρίου μας, η μελέτη των δυο να ήταν χειρότερη από του τρίτου.

Η αρχιτεκτονική εταιρεία επειδή ακριβώς είχε να κάνει με διαγωνισμούς δημοσίου έχει φροντίσει έτσι ώστε το πληροφοριακό της σύστημα να είναι αρκετά ασφαλές. Ο security officer έχει δημιουργήσει και υλοποιήσει μια πολιτική ασφαλείας στην οποία αναφέρονται μεταξύ άλλων:

- Clean desk policy.
- Password 10 χαρακτήρων το οποίο να περιέχει γράμματα, αριθμούς και σύμβολα.
- Αλλαγή του password κάθε 3 μήνες.
- Hybrid firewall (IPv4 και IPv6 κίνηση εσωτερική και εξωτερική).
- Antivirus σε κάθε υπολογιστή.
- Πολιτική backup στην οποία αναφέρεται ρητά ότι αντίγραφο ασφαλείας για κάθε υπολογιστή δημιουργείται κάθε Παρασκευή στις 19:00.
- Τα log files δεν αποθηκεύονται τοπικά σε κάθε υπολογιστή, αλλά υπάρχει κεντροποιημένο σύστημα ελέγχου.
- Κανείς δεν επιτρέπεται να έχει πρόσβαση στο χώρο εργασίας τις μη εργάσιμες μέρες και ώρες.

Οι ομάδα των αρχιτεκτόνων αποτελείται από τους εξής:

1) Περικλής Άτιμος
2) Θεόδωρος Τίμιος
3) Ανέστης Αδιάφορος

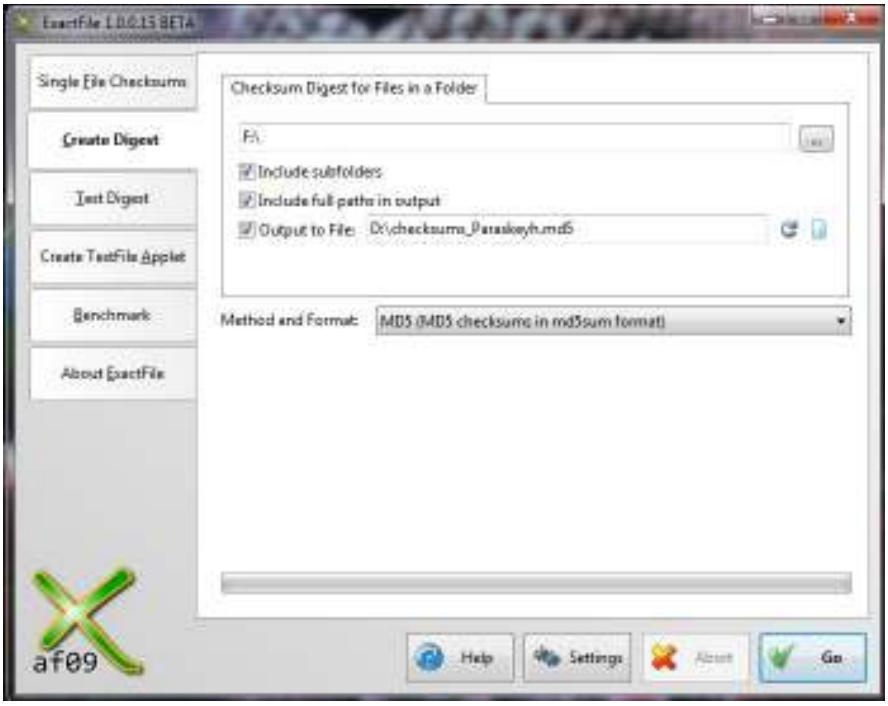
Ο κ. Άτιμος και ο κ. Τίμιος είναι άριστοι αρχιτέκτονες με μεταπτυχιακό και σχεδόν ισάξιοι. Ο κ. Αδιάφορος είναι ένα αρκετά καλός αρχιτέκτονας, αλλά σε καμία περίπτωση στο επίπεδο των άλλων 2. Ο κ. Άτιμος θέλει πάρα πολύ τη θέση και τα χρήματα. Γνωρίζοντας το επίπεδο γνώσεων και την ποιότητα δουλειάς των δυο συναδέλφων του, θεωρεί ότι απειλείται μόνο από τον κ. Τίμιο. Αποφασίζει λοιπόν να σαμποτάρει τη μελέτη του κ. Τίμιου, αλλάζοντας κάποια στοιχεία της, έτσι ώστε η δική του να είναι η καλύτερη.

Επί μια εβδομάδα οι τρεις αρχιτέκτονες εργάζονταν πυρετωδώς. Μέχρι την Παρασκευή ήταν η διορία παράδοσης της κάθε μελέτης, έτσι ώστε τη Δευτέρα να τις στείλουν πρωί πρωί στον υπεύθυνο αξιολόγησης.

Θα εξετάσουμε χωριστά τις ενέργειες των δυο αρχιτεκτόνων και στο τέλος θα αναλύσουμε τον τρόπο με τον οποίο η δολοπλοκία του κ. Άτιμου ανακαλύφθηκε.

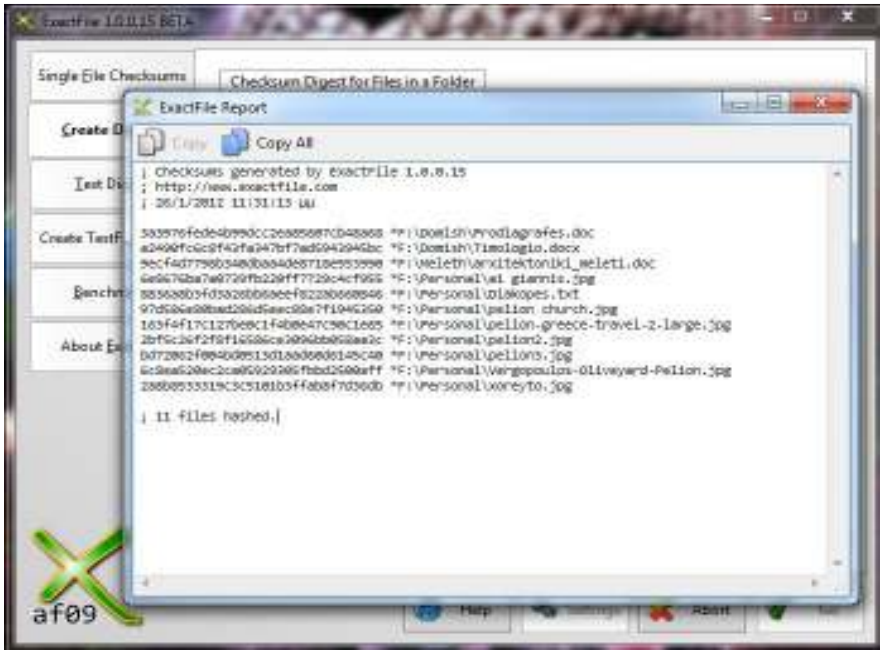
Ενέργειες κ. Τίμιου:

Ο κ. Τίμιος γνωρίζοντας ότι το θέμα της ασφάλειας των πληροφοριών είναι πολύ σημαντικό, είχε μελετήσει κάποια σχετικά άρθρα στο διαδίκτυο. Κάθε μέρα λοιπόν πριν κλείσει τον υπολογιστή στον οποίο εργαζόταν, αποθήκευε στο usb drive του ένα hash του σκληρού του υπολογιστή του. Είχε εγκαταστήσει το πρόγραμμα Exactfile, με το οποίο μπορούσε να δημιουργήσει μια hash τιμή, να την αποθηκεύσει σε usb drive και όποτε ήθελε να ελέγξει την ακεραιότητα των δεδομένων του, συγκρίνοντας την αποθηκευμένη hash τιμή με την επαναϋπολογισθείσα hash τιμή που του έδινε το πρόγραμμα. Αν οι δυο hash τιμές ταίριαζαν τότε η ακεραιότητα των δεδομένων ήταν εξασφαλισμένη. Αν όχι τότε τα δεδομένα είχαν αλλοιωθεί. Η λειτουργία του απλού αυτού προγράμματος, βασίζεται στις συναρτήσεις κατακερματισμού (hash functions). Η εισαγωγή δεδομένων σε μια τέτοια συνάρτηση έχει ως αποτέλεσμα μια τιμή. Αν έστω και ένας χαρακτήρας αλλάξει, αλλάζει όλη η τιμή.



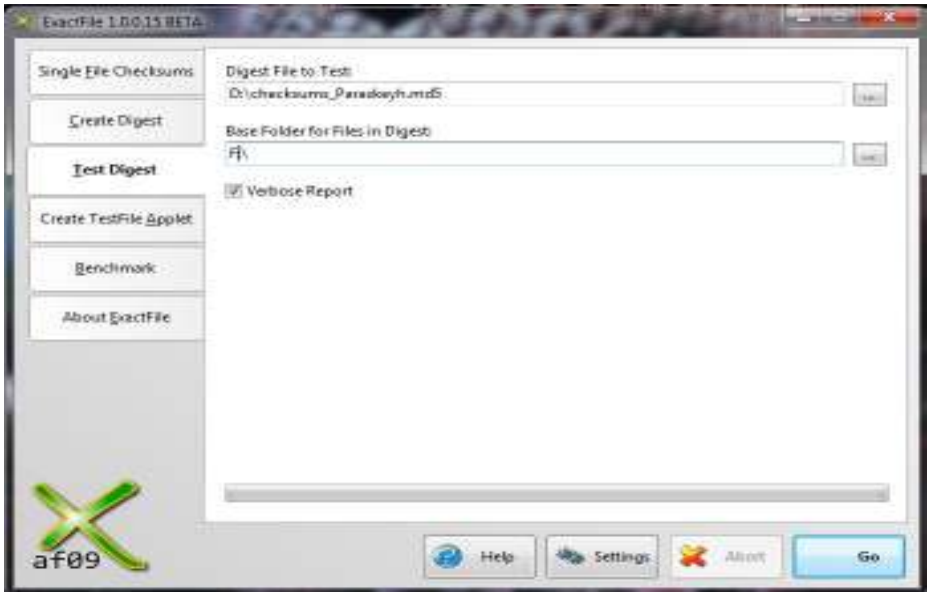
Εικόνα 51. Το περιβάλλον του Exactfile

Όπως κάθε μέρα έτσι και την Παρασκευή, ο κ. Τίμιος άνοιξε τον υπολογιστή του και χρησιμοποιώντας το πρόγραμμα Exactfile επιβεβαίωσε ότι τα δεδομένα του σκληρού δίσκου του ήταν ανέπαφα. Το απόγευμα μόλις τελείωσε τη μελέτη, πριν φύγει, χρησιμοποίησε το συγκεκριμένο πρόγραμμα και αποθήκευσε μια hash τιμή στο usb drive του.



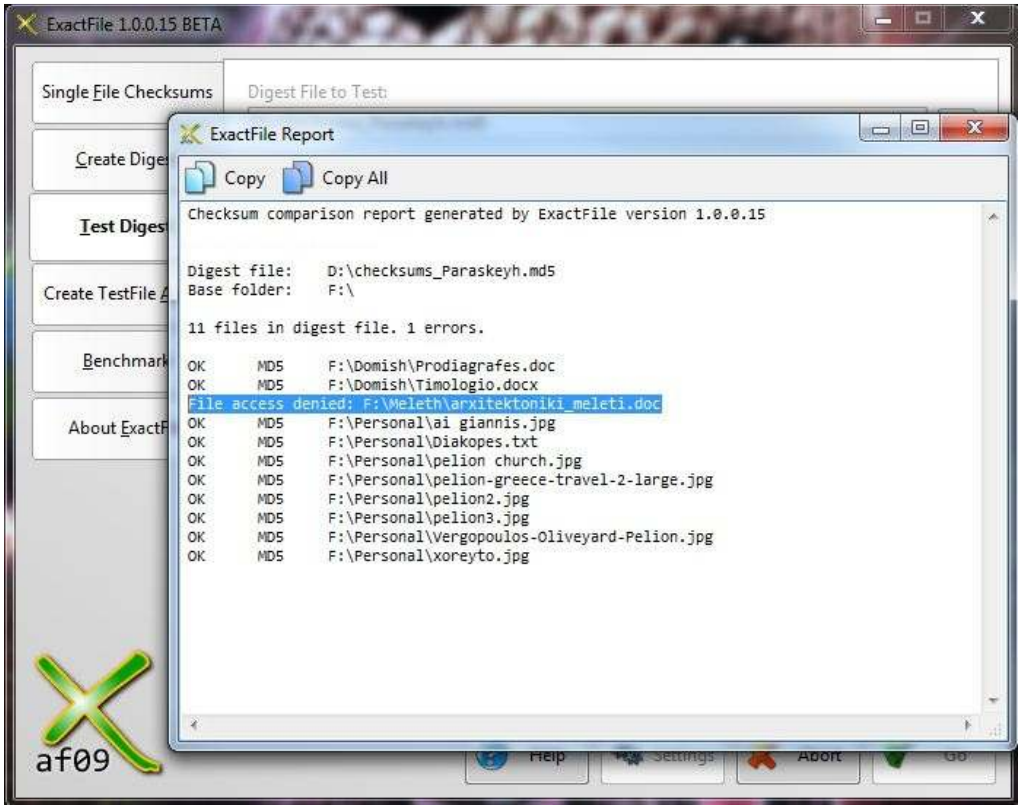
Εικόνα 52. Υπολογιστής κ. Τίμιου - Hash value Παρασκευής

Τη Δευτέρα επιστρέφοντας στο γραφείο του, πριν στείλει τη μελέτη του, χρησιμοποίησε πάλι το συγκεκριμένο πρόγραμμα.



Εικόνα 53. Έλεγχος hash value

Το αποτέλεσμα του ελέγχου αυτού έδειξε ότι κάποιο αρχείο είχε «πειραχθεί». Το μεγάλο πλεονέκτημα αυτού του προγράμματος είναι ότι επισημαίνει και ποιο ή ποια αρχεία έχουν αλλοιωθεί. Στη συγκεκριμένη περίπτωση το αρχείο ήταν το arxitektoniki_meleti.doc.



Εικόνα 54. Το αρχείο arxitetkoniki_meleti έχει τροποποιηθεί

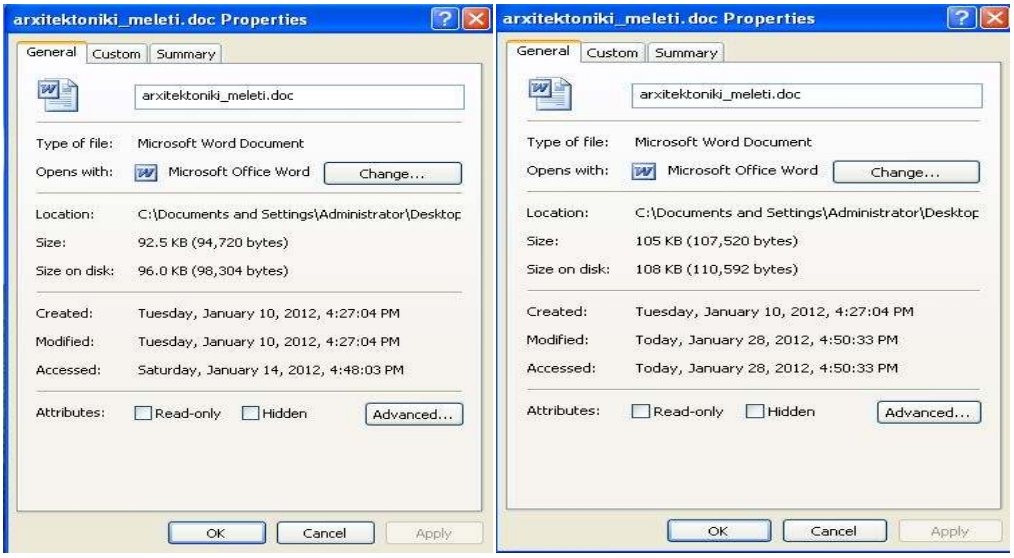
Ενέργειες κ. Άτιμου:

Ο κ. Άτιμος χρησιμοποιεί το **Kon Boot v1.1** που είναι αποθηκευμένο μέσα σε μια usb flash memory, και το οποίο δίνει τη δυνατότητα να εισέρθει στον υπολογιστή του κ. Τίμιου χωρίς τη χρήση κωδικού πρόσβασης.

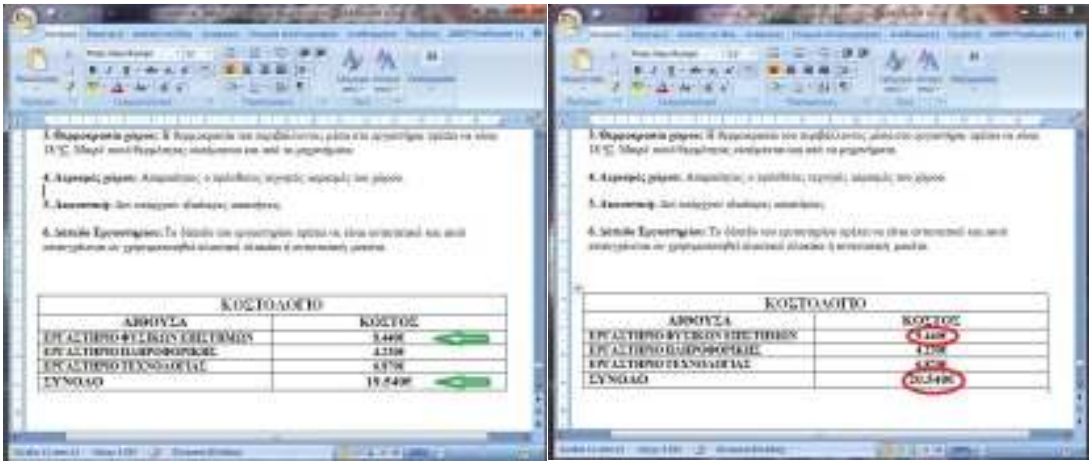
Εικόνα 55. Ο υπολογιστής του κ. Τίμιου είναι ασφαλισμένος με password

Εικόνα 56. Kon Boot v1.1 σε λειτουργία

Στη συνέχεια και αφού εντοπίσει το αρχείο με την αρχιτεκτονική μελέτη , διαβάζει από τα properties του εγγράφου τις ημερομηνίες και ώρες ώστε να τις επαναφέρει αργότερα και τέλος αλλάζει τα ποσά στους τελικούς πίνακες.

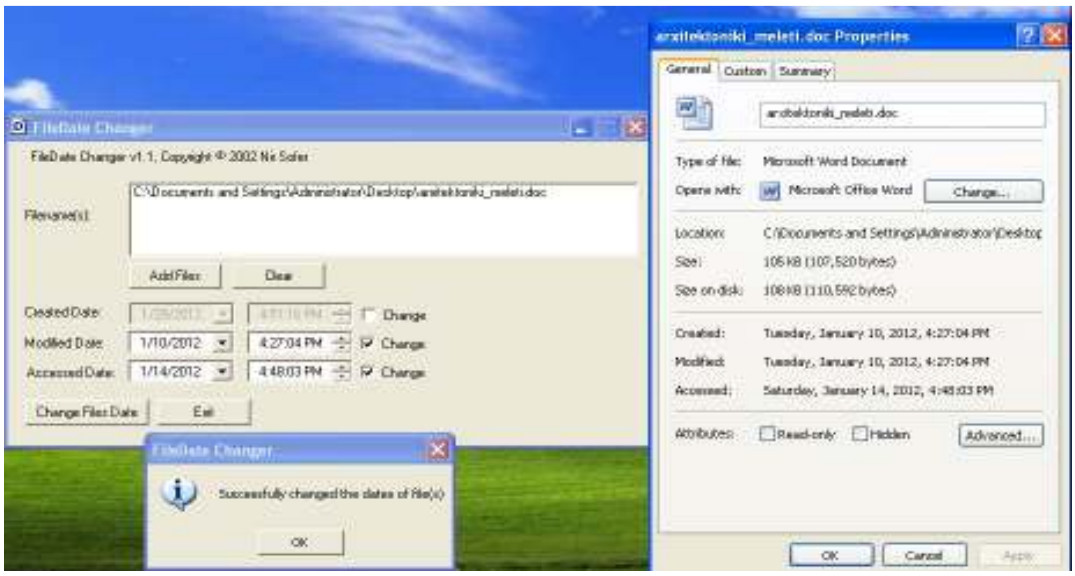


Εικόνα 57. Properties του αρχείου doc πριν και μετά τη μεταβολή



Εικόνα 58. Μεταβολή του αρχείου doc

Για να μην εντοπίσει όμως ο κ. Τίμιος ότι κάποιος μεταποίησε το αρχείο του, ο κ. Άτιμος με τη χρήση του **FileDateChanger** αλλάζει τις τιμές του Modified και του Accessed στις προηγούμενες.



Εικόνα 59. Επαναφορά των Modified και του Accessed Dates με το FileDateChanger

Ενέργειες κ. Τίμιου αφού εντόπισε την αλλοίωση:

Ο κ. Τίμιος γνωρίζοντας πολύ καλά την πολίτική ασφαλείας της εταιρείας, αμέσως επικοινώνησε με τον διαχειριστή και τον security officer και χρησιμοποιώντας το backup της Παρασκευής, κατάφερε να στείλει τη σωστή μελέτη.

Ενέργειες Security Officer:

Μετά την καταγγελία του κ. Τίμιου, ο υπεύθυνος ασφαλείας, επιβεβαίωσε την αλλοίωση του αρχείου μέσω της συνάρτησης κατακερματισμού και με τη βοήθεια του κ. Τίμιου εντόπισαν τις κακόβουλες αλλαγές στο κείμενο. Ο υπεύθυνος ζήτησε από τον διαχειριστή τα log files από την Παρασκευή μέχρι και τη Δευτέρα και εντόπισε μια επιτυχή προσπάθεια log on στον υπολογιστή του κ. Τίμιου το Σάββατο βράδυ στις 23:52. Συνεπώς κάποιος είχε καταρχήν, φυσική πρόσβαση στον

υπολογιστή του κ. Τίμιου και κατόπιν λογική πρόσβαση σε αυτόν. Επικοινώνησε με την εταιρεία φύλαξης και εντόπισε το φύλακα που εργαζόταν στην αρχιτεκτονική εταιρεία το Σάββατο. Έγινε καταγγελία στην Αστυνομία και μετά από τις απαραίτητες έρευνες αποδείχτηκε ότι ο φύλακας επέτρεψε έναντι αμοιβής στον κ. Άτιμο να εισέλθει στην εταιρεία το Σάββατο. Μετά από φυσική έρευνα στον υπολογιστή του κ. Τίμιου βρέθηκαν αποτυπώματα του κ. Άτιμου. Υπό το βάρος όλων αυτών των αποδείξεων ο κ. Άτιμος ομολόγησε ότι είχε αλλάξει κάποια από τα στοιχεία της μελέτης με σκοπό να κερδίσει σε αυτόν τον εσωτερικό διαγωνισμό.

7.3 «Απατημένη Σύζυγος»

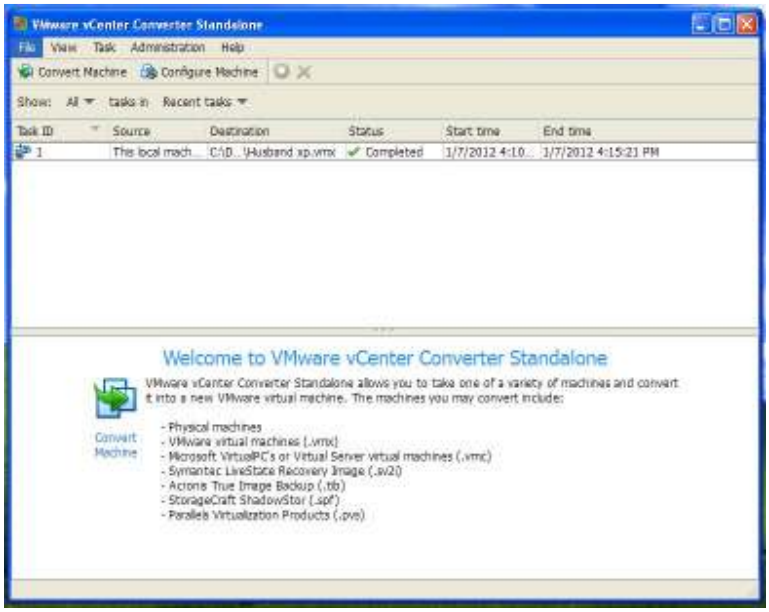
Υποθέτουμε ότι μια γυναίκα έρχεται σε εμάς (η κυρία Βάσω) και μας ζητάει να τη βοηθήσουμε σε ένα πρόβλημά της. Πιστεύει ότι ο σύζυγός της (ο Κύριος Αλέκος) την απατάει με κάποια άλλη γυναίκα. Μας παραδίδει τον προσωπικό του υπολογιστή και μας ζητάει να βρούμε σε αυτόν αποδείξεις για την απιστία του.

Διαδικασία έρευνας

Με τη χρήση του ***TrueImage Echo Workstation*** δημιουργώ ένα αντίγραφο (Clone) του υπό εξέταση υπολογιστή σε ένα διαφορετικό σκληρό δίσκο.

Εικόνα 60. Δημιουργία αντιγράφου του υπό εξέταση υπολογιστή

Στη συνέχεια δημιουργώ ένα τεστ περιβάλλον όμοιο με αυτό του υπολογιστή με τη βοήθεια του ***VMware vCenter Converter Standalone.***

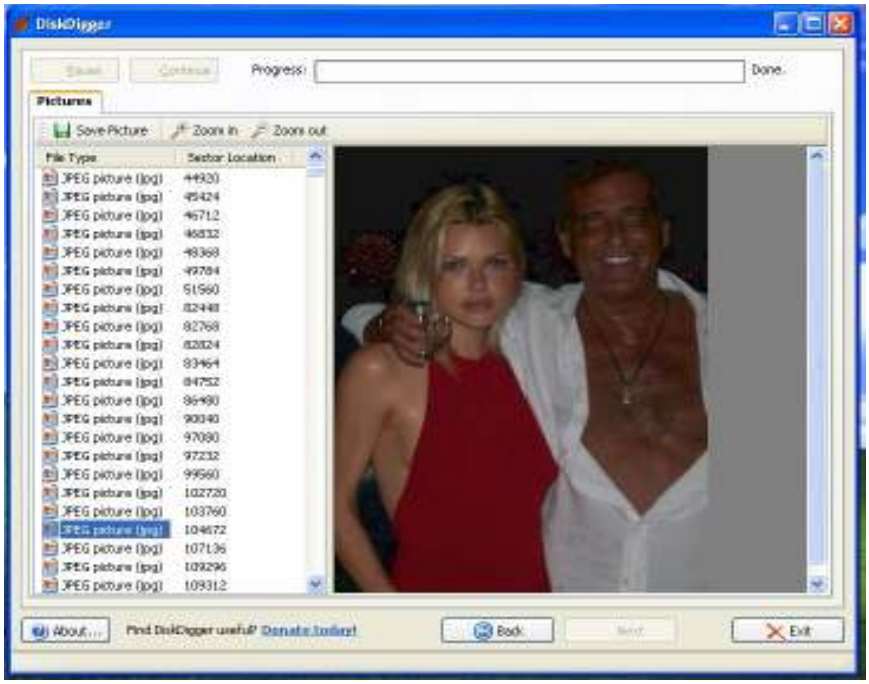


Εικόνα 61. Virtual Machine

Ο κλώνος του υπό εξέταση σκληρού δίσκου διατηρείται σε ξεχωριστό αυτόνομο δίσκο απομονωμένος από οποιαδήποτε εξωτερική αλλοίωση.

DiskDigger

Το **DiskDigger** είναι ένα free tool το οποίο παρέχει μια πρώτη εικόνα όλων των αρχείων του Σκληρού Δίσκου σε μια πρώτη και όχι πολύ προχωρημένη έρευνα για στοιχεία (συμπεριλαμβανομένων και των διαγεγραμμένων).

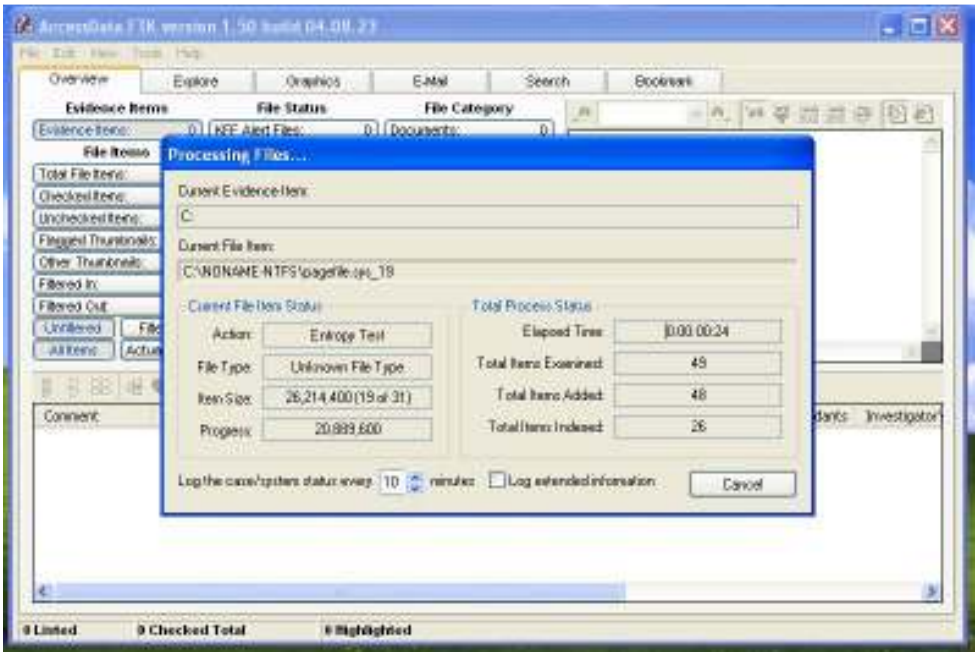


Εικόνα 62. Αποτελέσματα του Diskdigger

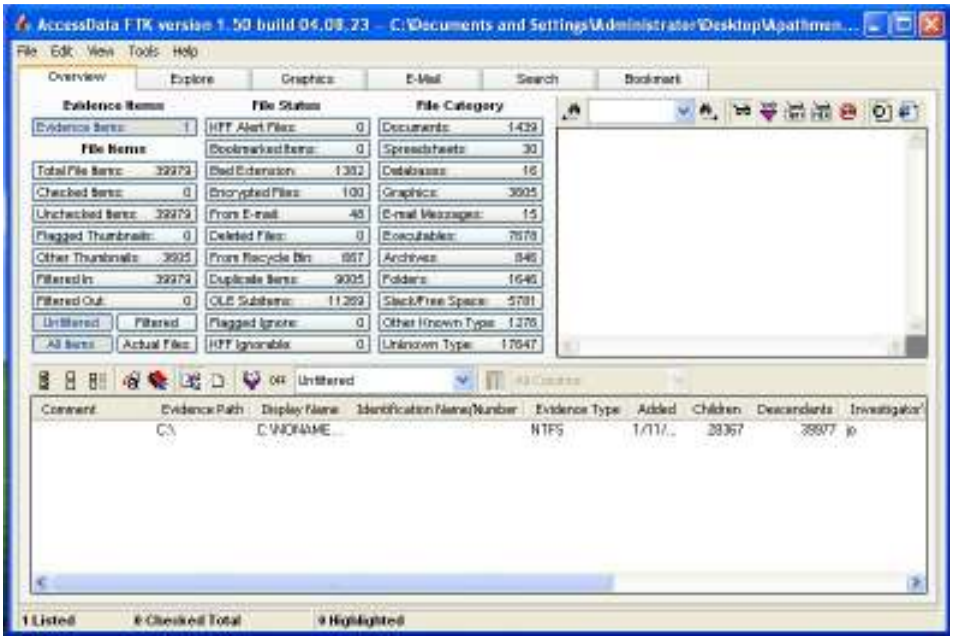
Αμέσως με την πρώτη αναζήτηση ανακαλύπτουμε διαγραμμένες φωτογραφίες που αποτελούν πειστήρια που αναζητούμε.

Forensic Toolkit

Για μία πιο προχωρημένη έρευνα ένα από τα καλύτερα εργαλεία του χώρου αποτελεί το **Forensic Toolkit της AccessData**. Για την έρευνα χρησιμοποιούμε τον κλώνο που δημιουργήσαμε με το ***TrueImage Echo Workstation.***

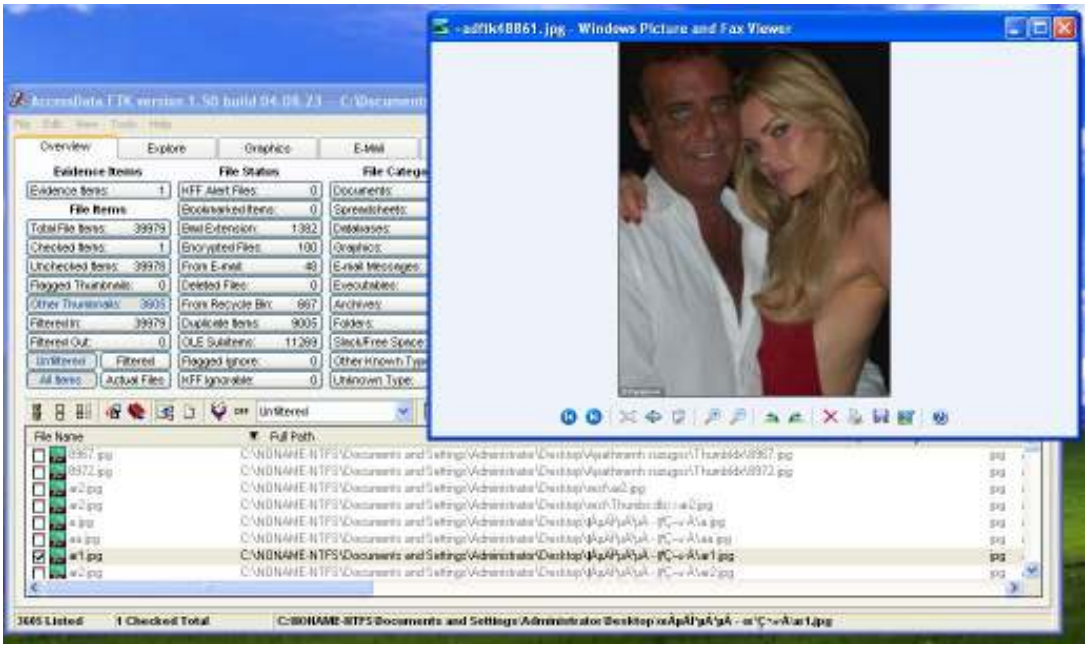


Εικόνα 63. Ανάλυση του image του υπό έρευνα υπολογιστή



Εικόνα 64. Αποτελέσματα έρευνας

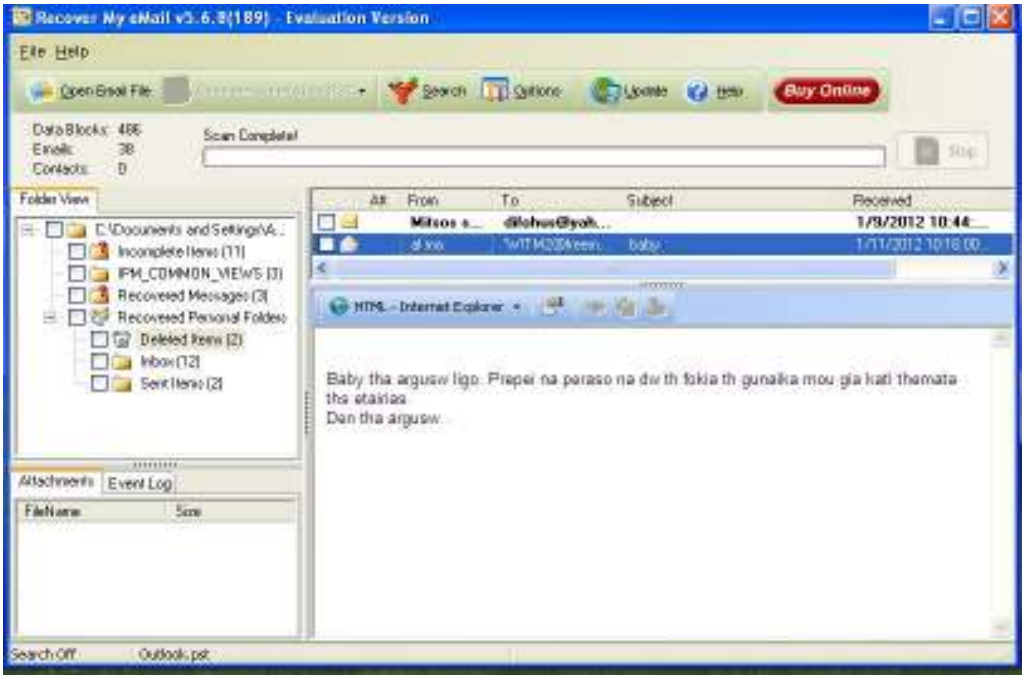
Μετά από μια μεθοδευμένη αναζήτηση διαπιστώνουμε ότι στα ανακτηθέντα αρχεία βρίσκουμε και άλλα πειστήρια που ενισχύουν την απάτη.



Εικόνα 65. Ανασύρουμε διαγραμμένες φωτογραφίες

Recover My Email

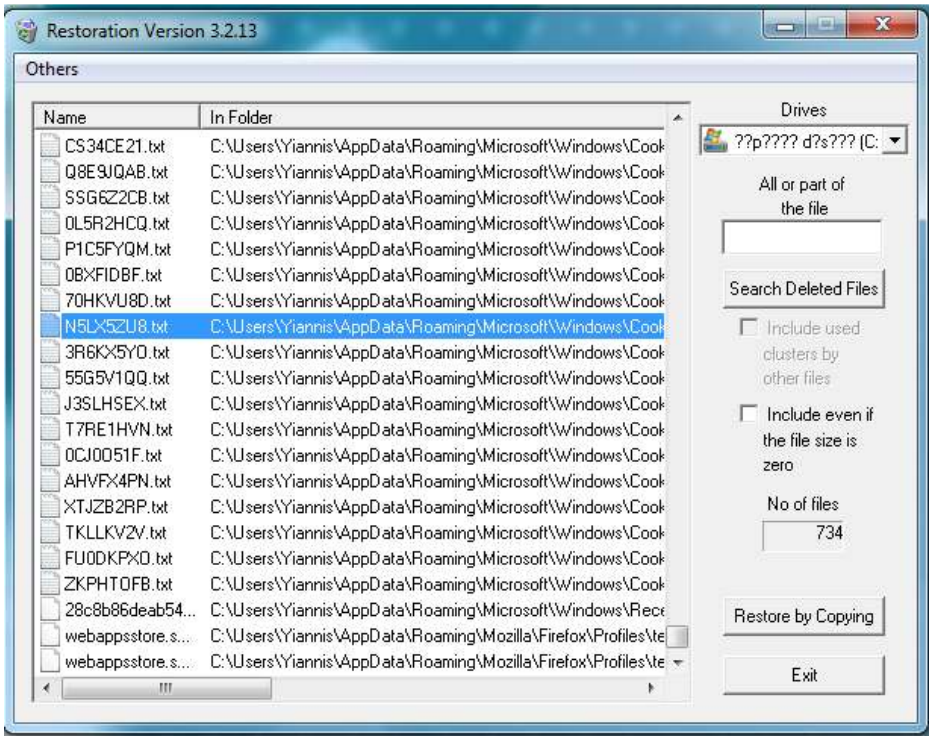
Με τη βοήθεια του **RecoverMyEmail** επανακτάμε διαγεγραμμένα mail. Και εδώ εντοπίζουμε ψηφιακές αποδείξεις που μας ενδιαφέρουν.



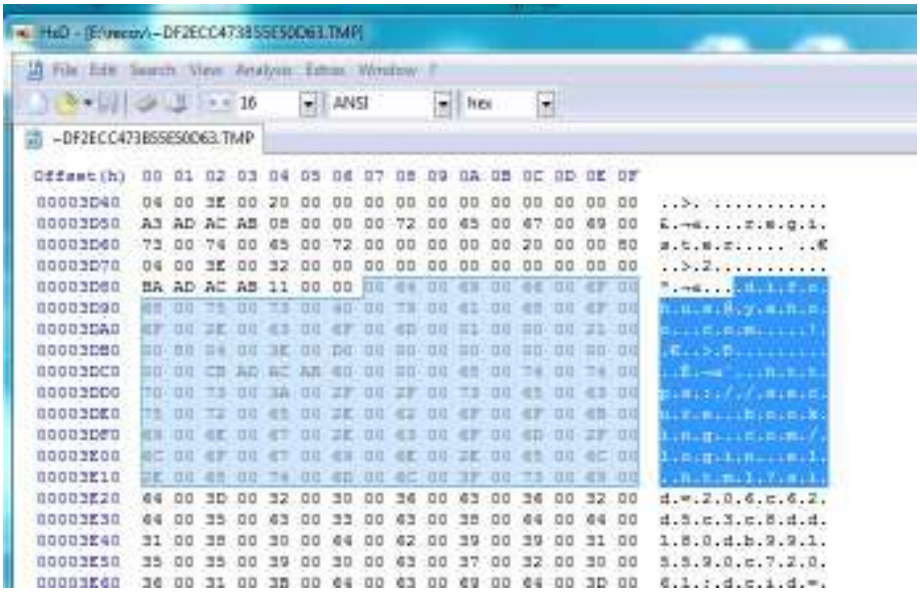
Εικόνα 66. Πρόσβαση στα e-mail του χρήστη

Restoration

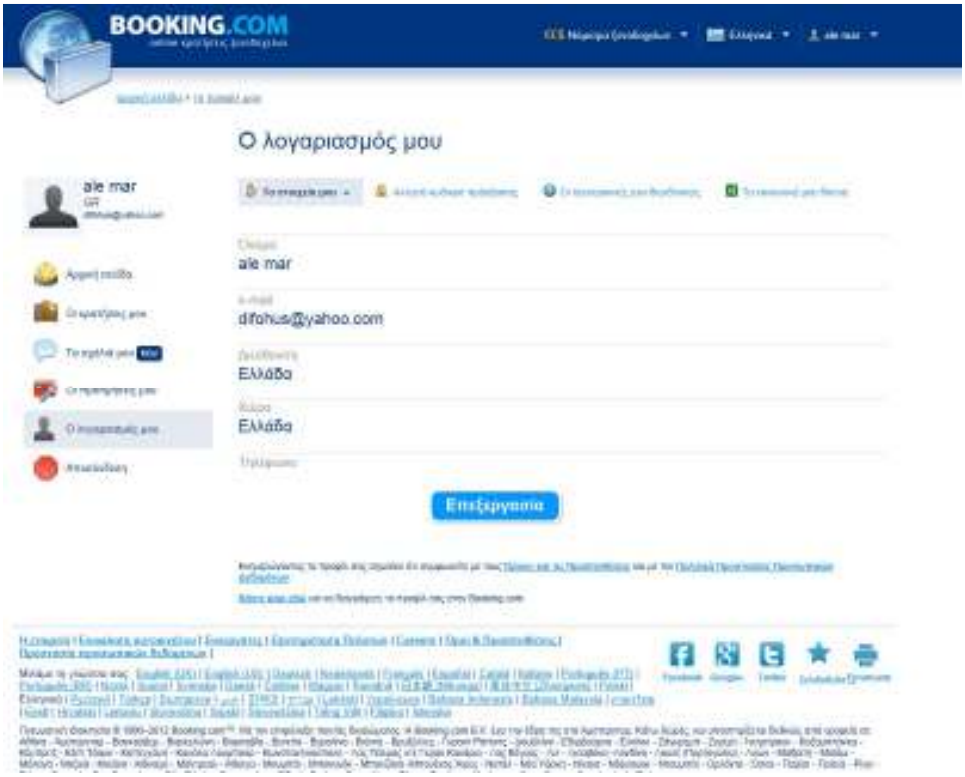
Με το **Restoration** επανακτούμε όλα τα cookies του browser (IE). Με αναζήτηση και τη βοήθεια ενός Hex Editor εντοπίζουμε ότι έχει πλοηγηθεί στο www.Booking.com σαν difohus@yahoo.com και κωδικό n3r0x1t1s. Επομένως εύκολα μπαίνουμε στην ιστοσελίδα και συγκεντρώνουμε και επιπλέον πληροφορίες.



Εικόνα 67. Ανάκτηση των cookies του browser



Εικόνα 68. Ανάγνωση με Hex Editor



Εικόνα 69. Πρόσβαση στο λογαριασμό του χρήστη στο booking.com

7.4 Κατοχή και Διακίνηση Παράνομου Ψηφιακού Υλικού (Παιδική Πορνογραφία)

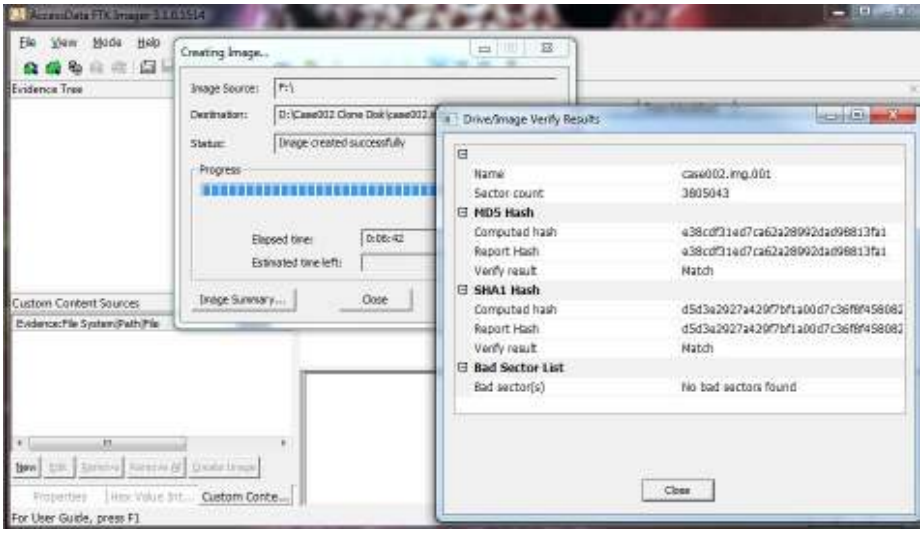
Η κα. Μαρία Παπαδοπούλου βρίσκεται στα κτήριο της Γ.Α.Δ.Α. Έχει αποφασίσει να κάνει μια σοβαρότατη καταγγελία. Βρισκόταν στο σπίτι του συναδέλφου της κ. Περικλή Άτιμου. Μόλις είχε πάρει προαγωγή και είχε κανονίσει μια μικρή γιορτή στο σπίτι του. Η κα. Παπαδοπούλου έφτασε πρώτη και περιμένοντας τους υπόλοιπους καλεσμένους, μπήκε στον προσωπικό υπολογιστή του κ. Άτιμου για να διαβάσει τα νέα στο Διαδίκτυο. Από περιέργεια άνοιξε ένα φάκελο στον υπολογιστή με φωτογραφίες. Ξαφνικά έμεινε εμβρόντητη γιατί ανάμεσα στις δεκάδες φωτογραφίες από τοπία, υπήρχε μια φωτογραφία σχετιζόμενη με παιδική πορνογραφία. Προφασίστηκε ότι δεν ένιωθε καλά και έφυγε αμέσως. Κατευθύνθηκε προς το κτήριο της Γ.ΑΔ.Α. και συγκεκριμένα στην υποδιεύθυνση της Δίωξης Ηλεκτρονικού Εγκλήματος. Έκανε επώνυμη καταγγελία και την υπόθεση αναλαμβάνει το τμήμα Προστασίας Ανηλίκων και στη συνέχεια ο Τομέας Εξέτασης Ψηφιακών Πειστηρίων.

Στο σπίτι του κ. Άτιμου φτάνει ο αστυνόμος κ. Τίμιος και ένα μέλος του τμήματος Εξέτασης Ψηφιακών Πειστηρίων, ο κ. Αποστολόπουλος. Ο αστυνόμος οδηγεί τον κ. Άτιμο στα γραφεία της υπηρεσίας και ο κ. Αποστολόπουλος ξεκινά την έρευνα.

Σφραγίζει το χώρο και κανένα μη εξουσιοδοτημένο άτιμο δεν μπορεί να έχει πρόσβαση σε αυτόν. Καταγράφει λεπτομερώς όλα τα στοιχεία και παίρνει φωτογραφίες. Στη συνέχεια προσπαθεί να αποκτήσει πρόσβαση στον υπολογιστή, ο οποίος είναι κλειδωμένος με password. Χρησιμοποιεί το πρόγραμμα **Kon boot** και αποκτά πρόσβαση στον υπολογιστή χωρίς την ανάγκη χρήσης password. Θα

μπορούσαμε να χρησιμοποιήσουμε και ένα live CD όπως το clonezilla, αλλά θεωρούμε ότι ο υπολογιστής είναι ανοιχτός και κλειδωμένος και δε θέλουμε να χάσουμε τα δεδομένα στην προσωρινή μνήμη.

Στη συνέχεια δημιουργεί ένα αντίγραφο του υπολογιστή. Πολύ σημαντικό βήμα, αφού η ανάλυση των στοιχείων δεν πρέπει να γίνει στο αρχικό φυσικό μέσο για να μην αλλοιωθούν τα δεδομένα. Χρησιμοποιεί το **FTK imager** της Access Data. Το συγκεκριμένο εργαλείο χρησιμοποιεί την μέθοδο hash/image/hash για την εξασφάλιση της ακεραιότητας των δεδομένων.



Εικόνα 70. FTK Imager

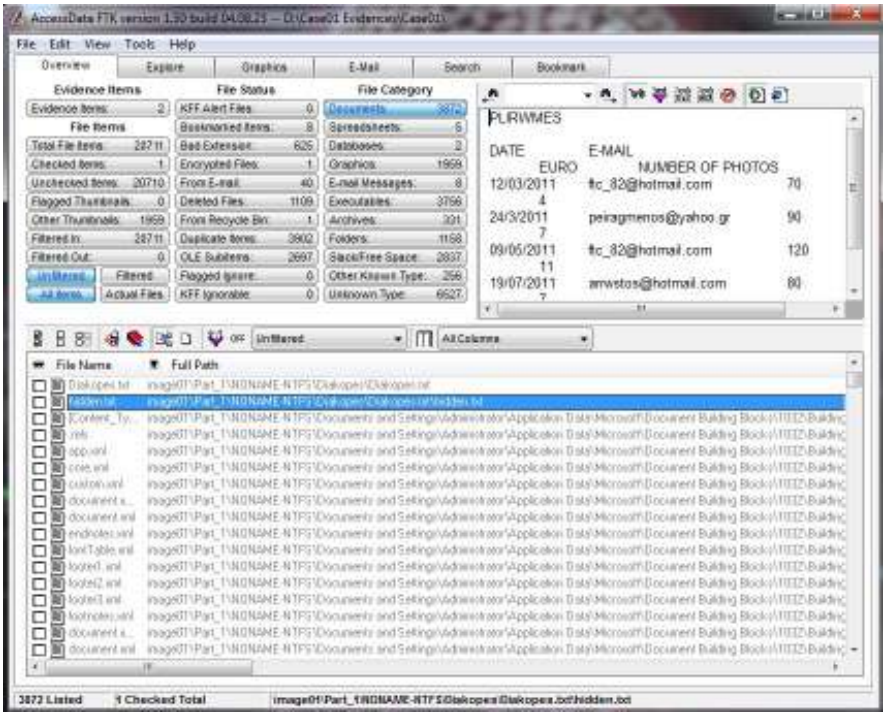
Το επόμενο βήμα είναι η ασφαλής μεταφορά του φυσικού μέσου και του αντιγράφου ασφαλείας στα εργαστήρια του τμήματος για ανάλυση. Μεταφέρονται σε ηλεκτροστατικές σακούλες σε προστατευμένο κουτί. Στο εργαστήριο δημιουργούμε ένα clone test pc χρησιμοποιώντας το **VMware vCenter Converter Standalone**. Έτσι αναπαριστούμε τον υπολογιστή του κ. Άτιμου σαν ένα virtual machine.

Φάση Ανάλυσης

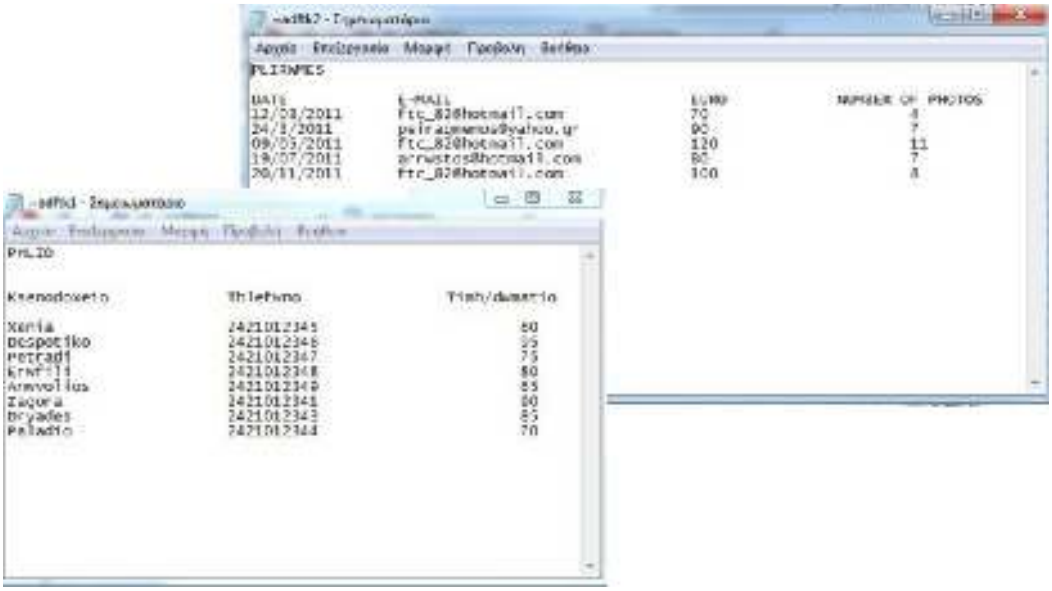
Χρησιμοποιούμε το εργαλείο **DiskDigger** για να επαναφέρουμε σβησμένα αρχεία. Ανακτούμε σβησμένες φωτογραφίες με περιεχόμενο παιδικής πορνογραφίας.

Εικόνα 71. Αποτελέσματα DiskDigger

Για την ανάλυση χρησιμοποιούμε το **FTK Analysis** της Access Data. Αρχικά ελέγχουμε τα Documents. Παρατηρούμε ότι υπάρχει ένα αρχείο diakopes.txt και μέσα σε αυτό είναι κρυμμένο ένα αρχείο hidden.txt. Το πρώτο περιέχει πληροφορίες για διακοπές και το κρυμμένο οικονομικές συναλλαγές.

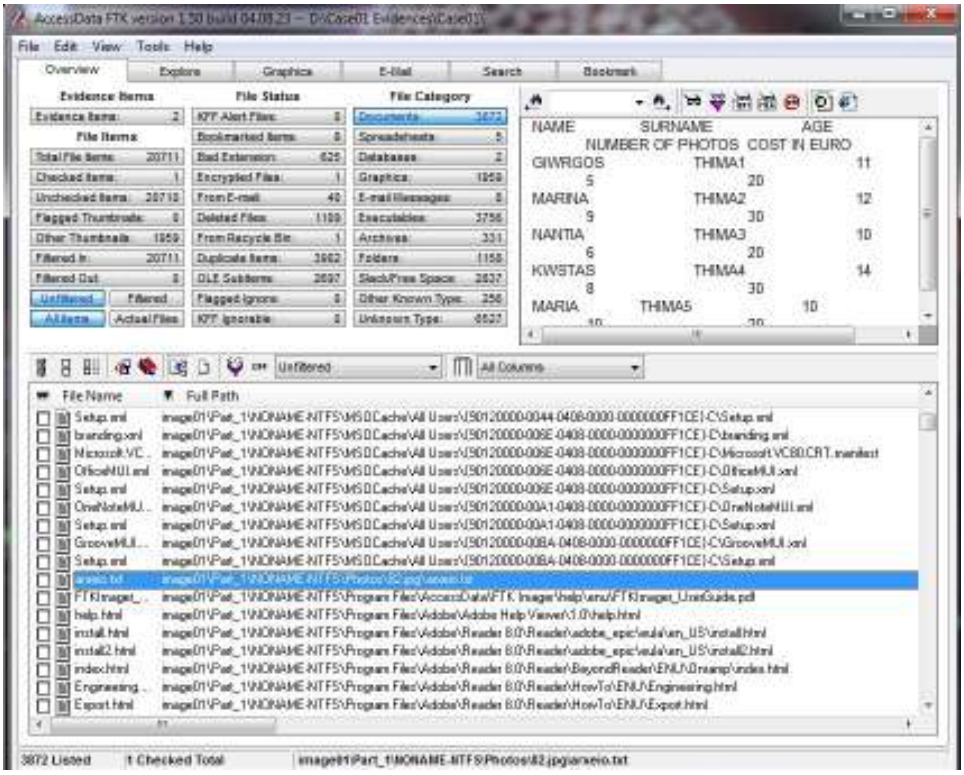


Εικόνα 72. Εντοπισμός κρυφού αρχείου .txt μέσα σε ένα άλλο .txt

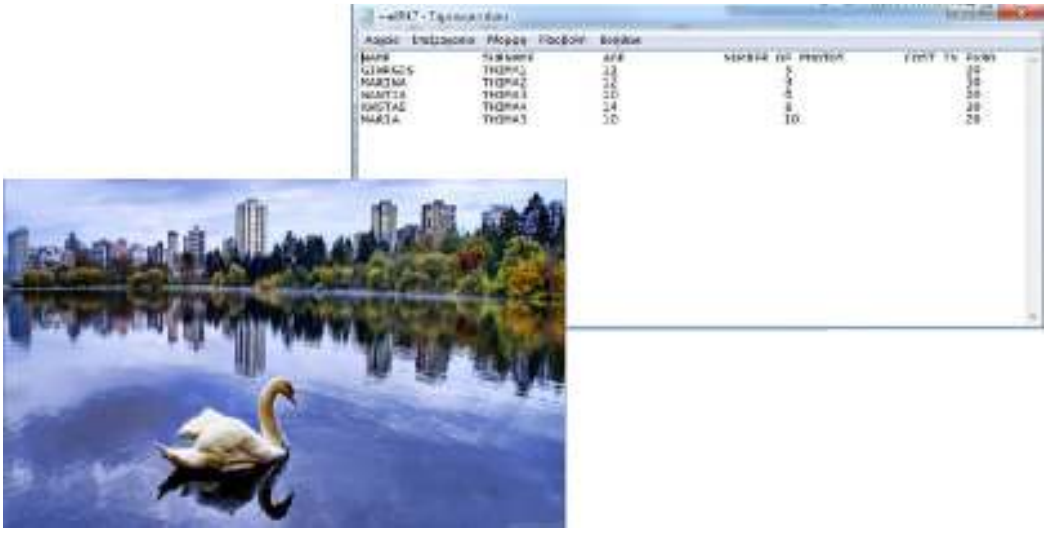


Εικόνα 73. Μέσα στο φανερό αρχείο diakopes.txt υπάρχει το hidden.txt

Το επόμενο εύρημα είναι ένα δεύτερο αρχείο txt κρυμμένο μέσα σε μια εικόνα.

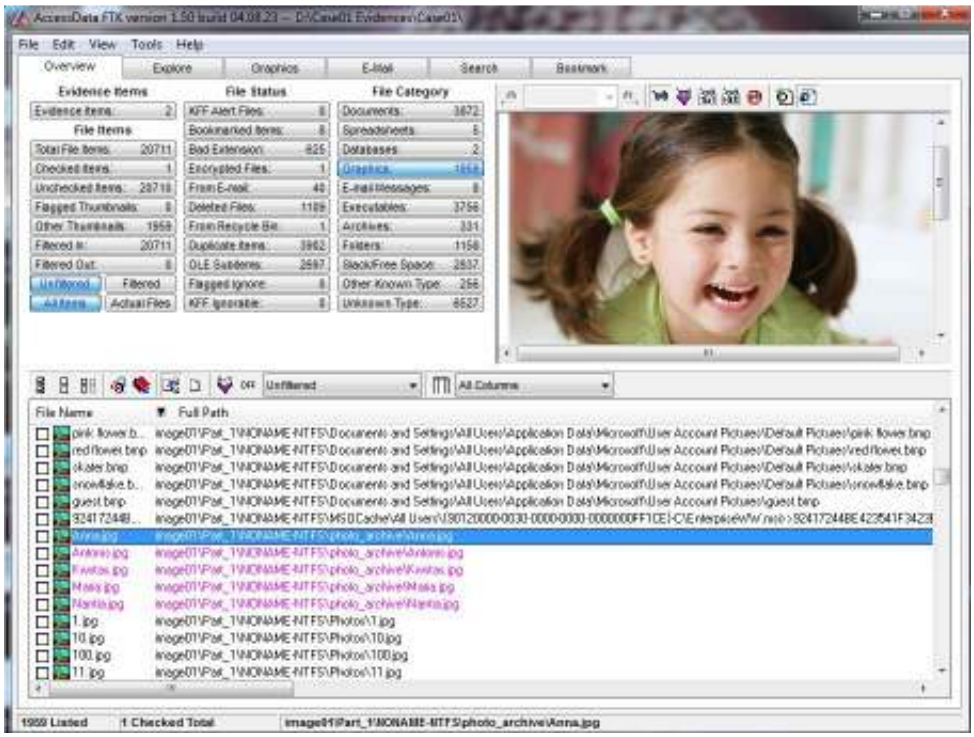


Εικόνα 74. Εντοπισμός κρυφού αρχείου .txt μέσα σε εικόνα



Εικόνα 75. Μέσα στην εικόνα 82.jpg υπάρχει το arxeio.txt

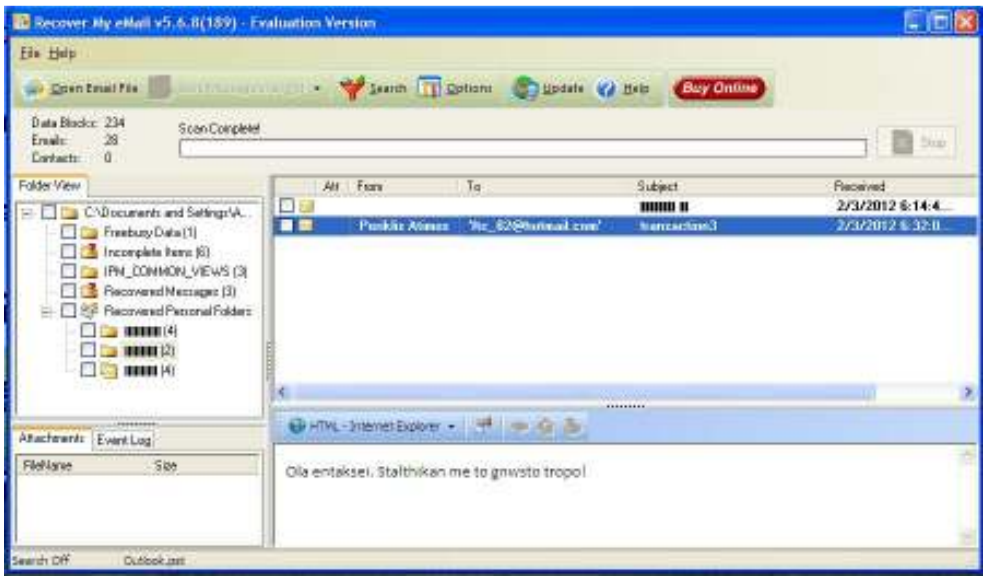
Στη συνέχεια ερευνούμε τα Graphics. Το πρόγραμμα έχει τη δυνατότητα να επαναφέρει κρυμμένους φακέλους και το περιεχόμενό τους. Βρήκε λοιπόν, ένα κρυφό φάκελο photo_archive με φωτογραφίες.



Εικόνα 76. Εντοπισμός κρυφού φακέλου και του περιεχομένου του

Τέλος, χρησιμοποιώντας το εργαλείο **Recover My eMail,** επαναφέρουμε τα e-mail του χρήστη, ακόμη και αν τα έχει σβήσει. Φαίνεται καθαρά, ότι υπάρχει οικονομική συναλλαγή.

Εικόνα 77. Επαναφορά σβησμένου εισερχόμενου μηνύματος



Εικόνα 78. Επαναφορά σβησμένου απεσταλμένου μηνύματος απάντησης

Μετά από τα ευρήματα της έρευνας παραδίδουμε την αναφορά της υπόθεσης, ένα αρχείο case01.xslx (επισυνάπτεται), το αρχικό αποθηκευτικό μέσο και το αντίγραφο ασφαλείας μαζί με το test Pc.

7.5 Καταστρατήγηση Ιδιωτικότητας Δεδομένων Θέσης

Ιδιωτικότητα θέσης

Στην προσπάθεια να ορίσουμε την ιδιωτικότητα θέσης, μπορούμε να πούμε ότι: είναι η δυνατότητα να εμποδίζουμε άλλα τρίτα μέλη να ενημερώνονται για την τρέχουσα ή προηγούμενη τοποθεσία στην οποία βρεθήκαμε.

Το επίπεδο ιδιωτικότητας θέσης του χρήστη καθορίζεται από πολλούς παράγοντες, αρκετοί από τους οποίους χρησιμοποιούνται σε σύστημα ελέγχου πρόσβασης (access control systems).

Οι βασικοί παράγοντες αναφέρονται παρακάτω:

- Ταυτότητα Αιτούντος: Θα πρέπει να σχετίζεται άμεσα και μοναδικά με κάποιο φυσικό πρόσωπο (explicit authentication) ή κάποια οντότητα (entity authentication).
- Ταυτότητα Αιτούμενου: Η πραγματική ταυτότητα του κατόχου των πληροφοριών θέσης ή εναλλακτικά ένα ψευδώνυμο που επιτρέπει την επικοινωνία της εφαρμογής και του χρήστη, προστατεύοντας όμως την ταυτότητα αυτού.
- Γεωγραφική Περιοχή: Η περιοχή μέσα στα όρια της οποίας επιτρέπεται η πρόσβαση σε πληροφορίες θέσης. Μπορεί να είναι απόλυτη π.χ. ο χρήστης Α μπορεί να εντοπίσει το χρήστη Β όταν αυτός βρίσκεται στο γραφείο του, είτε σχετική π.χ. ο χρήστης Α μπορεί να εντοπίσει το χρήστη Β όταν η μεταξύ τους απόσταση είναι 250 μέτρα.
- Χρονική Περίοδος: Διάστημα χρόνου στο οποίο επιτρέπεται η πρόσβαση σε πληροφορίες θέσης π.χ. ο εργοδότης μπορεί να έχει πρόσβαση στις πληροφορίες θέσης του εργαζόμενού του από τις 9π.μ μέχρι 5μ.μ.
- Συχνότητα Αιτήσεων: Αριθμός αιτήσεων για πρόσβαση σε πληροφορίες θέσης ανά μονάδα χρόνου. Μπορεί να φανεί ιδιαίτερα χρήσιμο μιας και δεν επιτρέπεται συνεχής πρόσβαση στις πληροφορίες θέσης όλων των χρηστών αλλά είναι ιδιαίτερα ευπαθής σε επιθέσεις τύπου άρνησης παροχής υπηρεσιών (Denial Of Service) αφού εάν οι συνεχείς αιτήσεις από τον επιτιθέμενο ξεπεράσουν τη μέγιστη επιτρεπτή συχνότητα τότε δεν θα μπορεί κανένας να έχει πρόσβαση στις πληροφορίες συμπεριλαμβανομένης και της εφαρμογής θέσης.
- Όριο Χρήσης Πληροφοριών: Πρόσβαση σε πληροφορίες μόνο από ορισμένες υπηρεσίες – εφαρμογές και κάτω από ορισμένες συνθήκες
- Καταγραφή Αιτήσεων: Καταγραφή όλων των προηγούμενων γεγονότων θέσης προκειμένου να είναι δυνατή η πρόβλεψη των μελλοντικών κινήσεων του χρήστη.
- Αμοιβαιότητα: Αμοιβαία ανταλλαγή πληροφοριών θέσης και ειδοποιήσεων μεταξύ του αιτούντος και του αιτούμενου.
- Προσδιορισμός χωρικής ακρίβειας: Το επίπεδο της ακρίβειας των πληροφοριών θέσης που στέλνει ο χρήστης. Το επίπεδο αυτό θα πρέπει να είναι το μικρότερο δυνατό, τέτοιο ώστε οι πληροφορίες που αποστέλλονται να είναι οι απολύτως απαραίτητες προκειμένου να λειτουργήσει σωστά η εφαρμογή, χωρίς καμία περιττή λεπτομέρεια που μπορεί να αποκαλύψει παραπάνω στοιχεία για την ταυτότητα του χρήστη.

Μέχρι πρόσφατα, η έννοια του location privacy ήταν άγνωστη: οι άνθρωποι συνήθως δεν είχαν πρόσβαση σε αξιόπιστες και επίκαιρες πληροφορίες σχετικά με την ακριβή θέση άλλων ατόμων, οπότε οι περισσότεροι άνθρωποι δεν είχαν να αντιμετωπίσουν επιπτώσεις στην ιδιωτικότητά τους σχετιζόμενες με την αποκάλυψη της θέσης τους, εκτός ίσως από ειδικές περιπτώσεις.

Με την εισαγωγή του pervasive computing, όμως, το μέγεθος του προβλήματος αλλάζει εντελώς. Πιθανόν να αδιαφορήσουμε αν κάποιος μάθει που βρεθήκαμε εχθές στις 12:30 το μεσημέρι, αλλά αν αυτός ο κάποιος μπορούσε να επιθεωρήσει το ιστορικό παρελθόν όλων των κινήσεών μας

καταγράφοντας την ακριβή μας θέση με ακρίβεια μικρότερη του ενός μέτρου, ενδεχομένως να αρχίζαμε να βλέπουμε τα πράγματα διαφορετικά.

Όταν συστήματα εντοπισμού θέσης (location systems) καταγράφουν χρήστες αυτόματα σε συνεχή βάση, παράγουν μια τεράστια ποσότητα δυνητικά ευαίσθητων πληροφοριών. Το απόρρητο των πληροφοριών τοποθεσίας (location information) είναι σχετικό με τον έλεγχο της πρόσβασης στις πληροφορίες αυτές. Δεν θέλουμε απαραιτήτως να απαγορεύσουμε οποιαδήποτε πρόσβαση - γιατί μερικές εφαρμογές μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να παρέχουν χρήσιμες υπηρεσίες - αλλά θέλουμε η όποια πρόσβαση να είναι ελεγχόμενη. Ορισμένοι στόχοι είναι αμοιβαία αποκλειόμενοι και δεν δύνανται να πληρούνται ταυτόχρονα: για παράδειγμα, το ενδεχόμενο να κρατήσουμε μυστική τη θέση μας και παράλληλα να θέλουμε οι συνάδελφοί μας να είναι σε θέση να μπορούν να μας εντοπίζουν.

Παρακολούθηση ενός κινητού τηλεφώνου (κατά συνέπεια και του χρήστη) με τη χρήση mobile forensics.

Στο σενάριο αυτό θα δείξουμε πως μπορεί κάποιος να βρει τη διαδρομή που έχει ακολουθήσει ένας χρήστης σε μια χρονική περίοδο. Το λειτουργικό σύστημα Android, όπως και το iOS διατηρούν στη μνήμη τους στοιχεία για τη σύνδεση του εκάστοτε κινητού με κάποιο ασύρματο δίκτυο ή με κάποιο BS (Base Station) τηλεπικοινωνιακού παρόχου. Στην περίπτωση του Android τα αρχεία αυτά είναι τα cache.wifi και cache.cell, τα οποία βρίσκονται στο φάκελο com.google.android.location της συσκευής.

Η συσκευή που χρησιμοποιήθηκε είναι η Sony Xperia X8, έχει εργοστασιακά έκδοση Android 2.1 και είναι rooted. Επιλέξαμε να κάνουμε το κινητό τηλέφωνο root για να αποφύγουμε τη διαδικασία απόκτησης δικαιωμάτων administrator σε αυτό με τεχνική privilege escalation.

Εικόνα 79. Συσκευή Sony Xperia x8

Δημιουργήσαμε έναν εικονικό υπολογιστή σε VMware με λειτουργικό Windows XP. Εγκαθιστούμε με τη σειρά:

- JDK (Java Development Kit)
- JRE (Java Runtime Environment)
- Android SDK

Όταν εγκατασταθεί το SDK, στο installation directory, εγκαθιστούμε το πρόσθετο που αντιστοιχεί στην έκδοση Android του κινητού. Αφού το κινητό έχει έκδοση Android 2.1 εγκαταστήσαμε τη 2.1 sdk. Σε περιβάλλον command prompt χρησιμοποιούμε το εργαλείο ADB. Συνδέουμε το κινητό σε μια θύρα usb με καλώδιο.

Βήματα για ανάκτηση των δυο αρχείων:

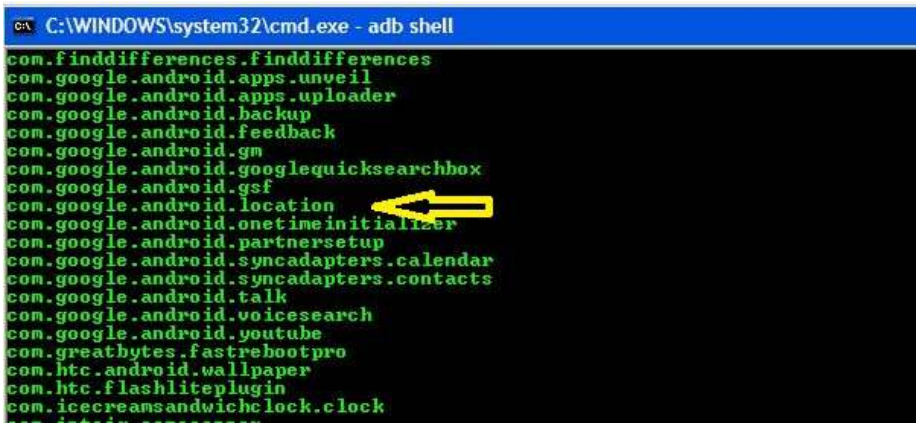
- **Βήμα 1:** Εντολή adb devices. Δείχνει το κινητό που είναι συνδεδεμένο με τον υπολογιστή.

Εικόνα 80. Εντολή adb devices

- **Βήμα 2:** Ενολή adb shell. Ανοίγει ένα shell στο κινητό. Στη συνέχεια οδηγούμαστε στο φάκελο data/data.

Εικόνα 81. Εντολή adb shell

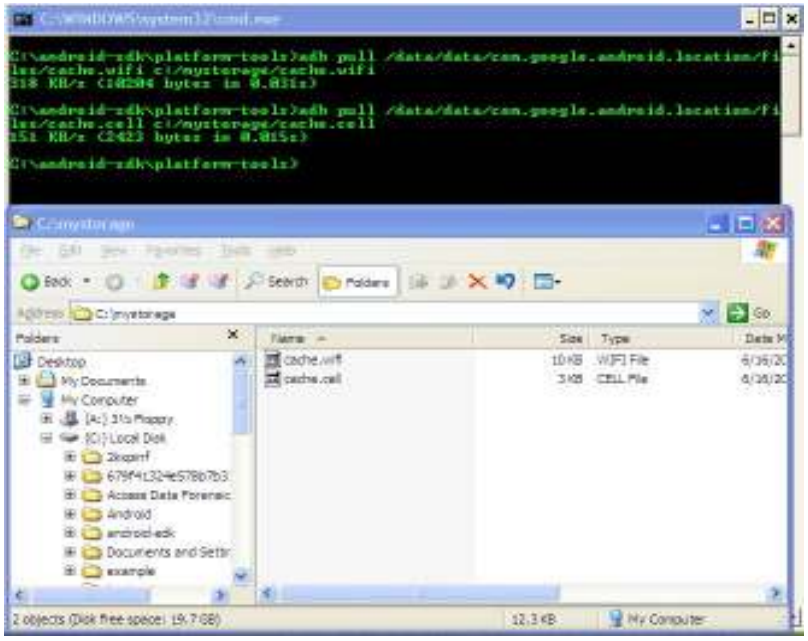
- **Βήμα 3:** Στο φάκελο data/data με την εντολή ls βλέπουμε τα περιεχόμενά του και εντοπίζουμε το φάκελο com.google.android.location. Μέσα στο φάκελο files εντοπίζουμε τα 2 αρχεία cache.wifi και cache.cell.



Εικόνα 82. Αναζήτηση των αρχείων cache.cell και cache.wifi

Εικόνα 83. Αναζήτηση των αρχείων cache.cell και cache.wifi

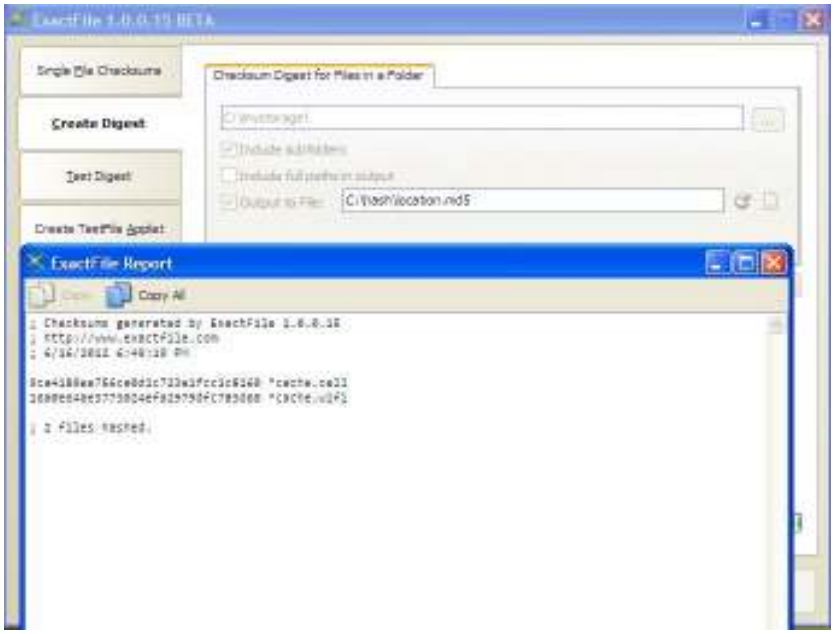
- **Βήμα 4: Εντολή adb pull για να αποθηκεύσουμε τα αρχεία στον υπολογιστή μας**



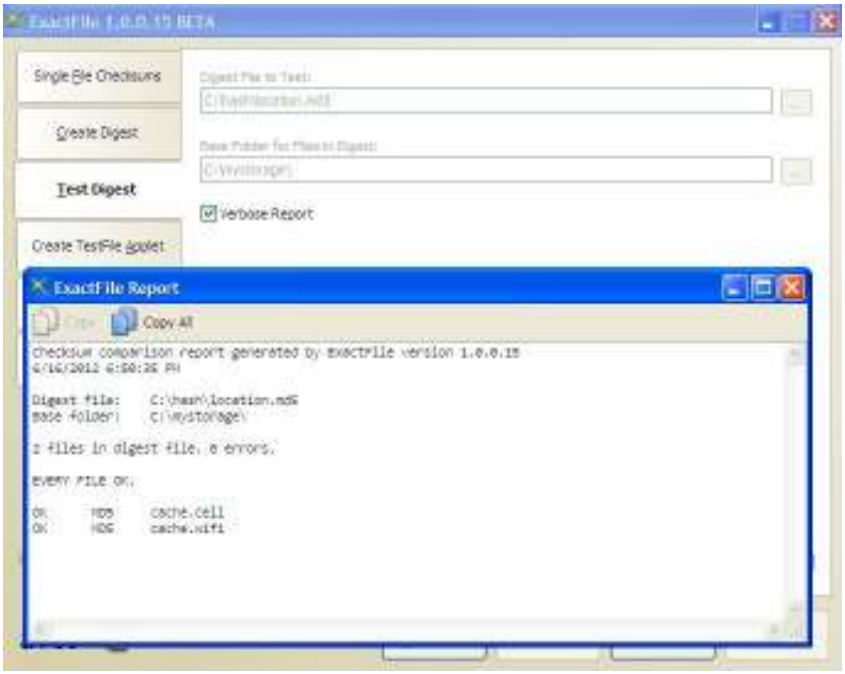
Εικόνα 84. Εντολή adb pull

Τα αρχεία που έχουμε πλέον στη διάθεσή μας θα πρέπει να τα επεξεργαστούμε κατάλληλα. Βασική όμως αρχή στα digital/mobile forensics είναι ότι δεν επεξεργαζόμαστε ποτέ τα ίδια τα αρχεία, αλλά αντίγραφά τους, έτσι ώστε να μην αλλοιωθεί η ακεραιότητα των δεδομένων κατά την επεξεργασία.

Χρησιμοποιώντας το πρόγραμμα **exactfile** *(http://www.exactfile.com/)* δημιουργούμε hash values για τα 2 αρχεία. Αυτό γίνεται για να εξασφαλίσουμε την ακεραιότητά τους και στη συνέχεια αντιγράφονται στο φάκελο location σε άλλο VM υπολογιστή ο οποίος τρέχει λειτουργικό ubuntu.



Εικόνα 85. Λειτουργία προγράμματος exactfile

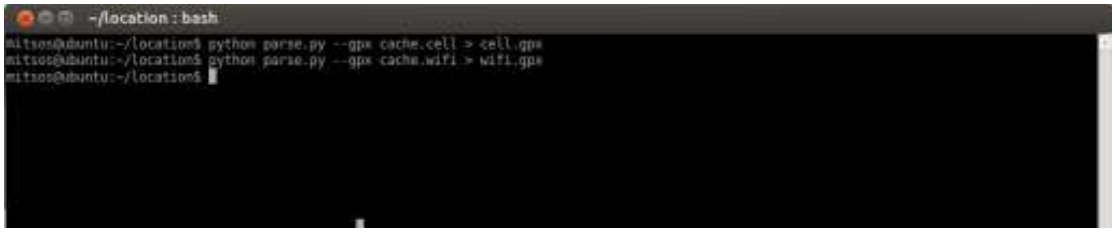


Εικόνα 86. Λειτουργία προγράμματος exactfile

Σε VM που έχει εγκατεστημένο λειτουργικό Ubuntu ανοίγουμε κονσόλα και μεταβαίνουμε στο φάκελο location. Από τη σελίδα *https://github.com/packetlss/android-locdump* κατεβάζουμε το script parse.py. Με τις ακόλουθες εντολές μετατρέπουμε τα 2 αρχεία σε αρχεία GPX (GPS eXchange format) cell.gpx και wifi.gpx.

python parse.py --gpx cache.wifi > wifi.gpx

python parse.py --gpx cache.cell > cell.gpx



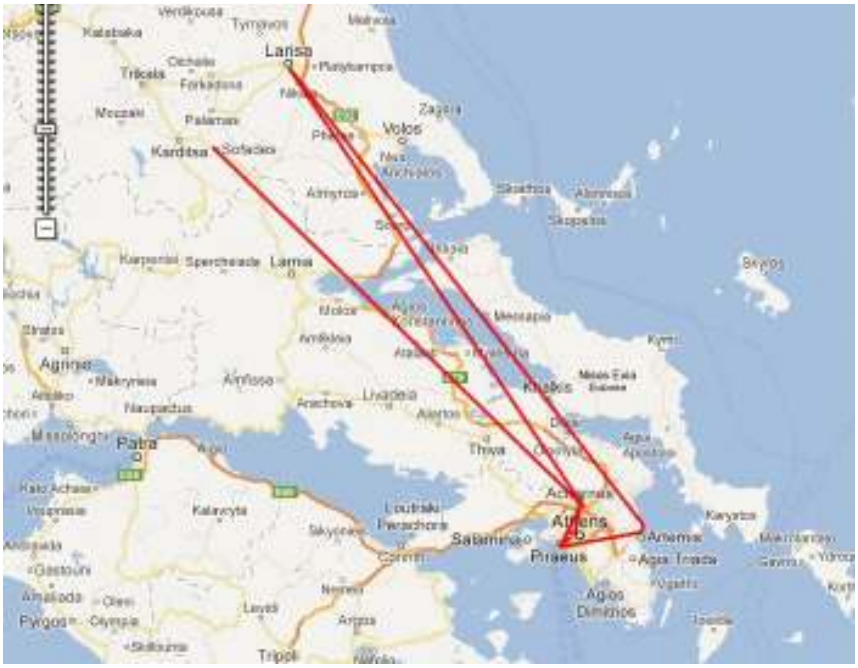
Εικόνα 87. Εντολές για μετατροπή των δυο αρχείων σε .gpx

Κατεβάζουμε το πρόγραμμα QuakeMap από τη σελίδα *http://www.earthquakemap.com/*. Χρησιμοποιώντας ως είσοδο τα αρχεία cell.gpx και wifi.gpx έχουμε την γραφική αναπαράσταση των σημείων που συνδέθηκε ο χρήστης είτε σε wi-fi είτε σε BS αντίστοιχα.

Εικόνα 88. Αναπαράσταση σημείων σύνδεσης από το cell.gpx

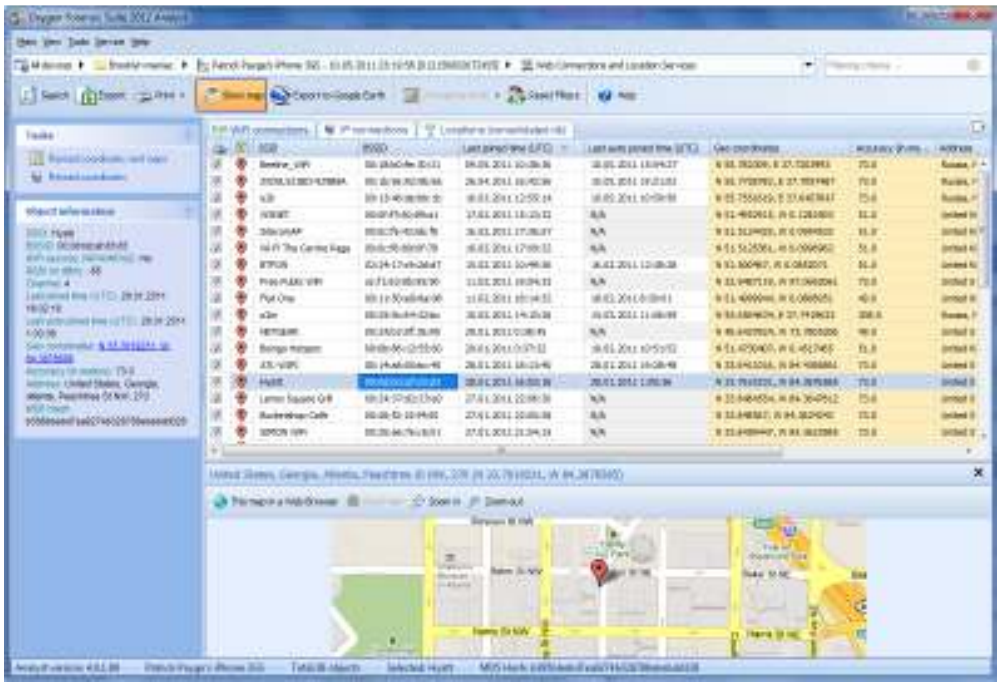
Εικόνα 89. Αναπαράσταση σημείων σύνδεσης από το wifi.gpx

Χρησιμοποιώντας ως είσοδο το αρχείο cell.gpx στη σελίδα *http://www.gpsvisualizer.com/map?output_home* φαίνεται καλύτερα η διαδρομή που ακολουθεί ο χρήστης. Αντίστοιχο αποτέλεσμα θα είχαμε και με τη χρήση του αρχείου wifi.gpx.



Εικόνα 90. Αναπαράσταση διαδρομής από τα σημεία σύνδεσης από το cell.gpx

Βέβαια όλη αυτή η διαδικασία θα μπορούσε να γίνει πολύ πιο απλά χρησιμοποιώντας ένα forensics εργαλείο, σαν το Oxyfen Forensic Suite 2012 *(http://www.oxygen-forensic.com/en/)*. Τέτοια εργαλεία όμως κοστίζουν από μερικές εκατοντάδες μέχρι μερικές χιλιάδες δολάρια.



Εικόνα 91. Oxygen Forensic suite 2012

Εντοπισμός θέσης από φωτογραφία

Στο παρελθόν, τις περισσότερες φορές σε μια φωτογραφία δεν υπήρχαν πολλές πληροφορίες. Πλέον όμως τα περισσότερα smart phones και οι ψηφιακές φωτογραφικές μηχανές τελευταίας γενιάς, έχουν ενσωματωμένο GPS σύστημα και προσθέτουν στοιχεία γεωγραφικού εντοπισμού στις φωτογραφίες (geo-tagging). Τα μεταδεδομένα (metadata) αυτά, όπως και άλλες πληροφορίες, εντοπίζονται σε στο τμήμα EXIF της φωτογραφίας. Στο συγκεκριμένο σενάριο θα δείξουμε πόσο εύκολο είναι να εκμαιεύσουμε πληροφορίες για την τοποθεσία της φωτογραφίας χρησιμοποιώντας μόνο μια web εφαρμογή.

Υποθέτουμε ότι ο χρήστης τράβηξε μια φωτογραφία με το Android smartphone Sony Xperia X8. Η διαδικασία που ακολουθούμε είναι πολύ απλή.

Εικόνα 92. Φωτογραφία στο κινητό

- Ακολουθώντας τα βήματα που περιγράψαμε προηγουμένως, ανακαλύπτουμε στην εσωτερική μνήμη ή στην sd card του κινητού τη φωτογραφία.
- Χρησιμοποιώντας την εντολή adb pull την αποθηκεύουμε στον υπολογιστή μας.
- Επισκεπτόμαστε τη σελίδα http://regex.info/exif.cgi.
- Επιλέγουμε browse,τη φωτογραφία που ανακτήσαμε από το κινητό και στη συνέχεια επιλέγουμε View Image From File.
- Τώρα μπορούμε να δούμε πολλές πληροφορίες καθώς και την τοποθεσία που λήφθηκε η φωτογραφία.

Exif Image Size	2,048 × 1,536
Make	Sony Ericsson
Camera Model Name	X8
Orientation	Horizontal (normal)
Software	JimdemDroid_8197
Modify Date	**2012:06:20** 17:48:12 5 hours, 54 minutes, 10 seconds ago
Y Cb Cr Positioning	Co-sited
Exposure Time	1/1000
ISO	40
Exif Version	0220
Date/Time Original	**2012:06:20** 17:48:12 5 hours, 54 minutes, 10 seconds ago
Create Date	**2012:06:20** 17:48:12 5 hours, 54 minutes, 10 seconds ago

Εικόνα 93. Λεπτομέρειες φωτογραφίας

Εικόνα 94. Λεπτομέρειες τοποθεσίας φωτογραφίας

8 Βιβλιογραφία

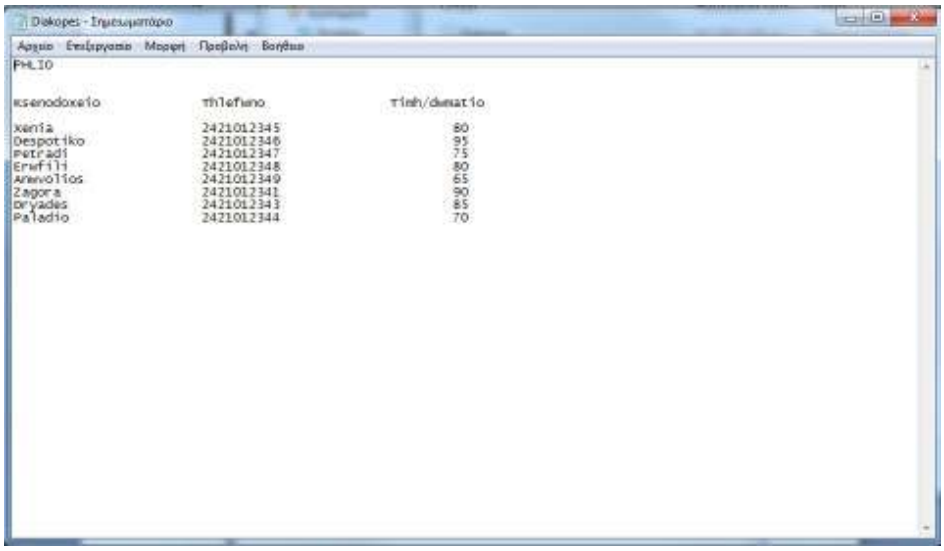
[1] http://www.e-crime.gr/computer_forensics.htm (Accessed on 18/05/2013)
[2] http://en.wikipedia.org/wiki/Mobile_device_forensics (Accessed on 18/05/2013)
[3] http://www.e-crime.gr/nomothesia.htm (Accessed on 23/05/2013)
[4] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang= (Accessed on 22/05/2013)
[5] http://www.dart.gov.gr (Accessed on 11/04/2012)
[6] http://www.adae.gr/ (Accessed on 23/05/2013)
[7] http://www.eett.gr/opencms/opencms/EETT/ (Accessed on 23/05/2013)
[8] http://www.csirt.org/ (Accessed on 25/05/2013)
[9] http://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt (Accessed on 25/05/2013)
[10] http://www.nis.gr/portal/page/portal/NIS/ (Accessed on 25/05/2013)
[11] http://www.cert.auth.gr/index.php/el/ (Accessed on 25/05/2013)
[12] http://www.accessdata.com/products/digital-forensics/ftk#.Uewoz23cPqc (Accessed on 25/06/2013)
[13] http://www.acronis.com/homecomputing/products/trueimage/ (Accessed on 25/06/2013)
[14] http://drivesnapshot.de/en/ (Accessed on 25/06/2013)
[15] http://www.farstone.com/software/totalrecovery-pro.php (Accessed on 25/06/2013)
[16] http://www.genie9.com/ (Accessed on 25/06/2013)
[17] http://www.forensicswiki.org/wiki/Dd (Accessed on 25/06/2013)
[18] http://www.partimage.org/Main_Page (Accessed on 20/06/2013)
[19] http://freecode.com/projects/lrs (Accessed on 20/06/2013)
[20] http://www.fogproject.org/ (Accessed on 20/06/2013)
[21] http://www.runtime.org/driveimage-xml.htm (Accessed on 20/06/2013)
[22] http://www.easeus.com/disk-copy/ (Accessed on 20/06/2013)
[23] http://clonezilla.org/
[24] http://code.google.com/p/lime-forensics/ (Accessed on 29/06/2013)
[25] http://www.guidancesoftware.com/encase-forensic.htm (Accessed on 29/06/2013)
[26] http://www.e-fense.com/h3-enterprise.php (Accessed on 29/06/2013)
[27] http://nhtcu.ru/0xFA_eng.html (Accessed on 29/06/2013)
[28] http://www.oxygen-forensic.com/en/ (Accessed on 29/06/2013)
[29] http://www.digital-detective.co.uk/netanalysis.asp (Accessed on 29/06/2013)
[30] http://www.magnetforensics.com/software/internet-evidence-finder/ (Accessed on 29/06/2013)
[31] http://www.backtrack-linux.org/ (Accessed on 11/04/2013)
[32] http://www.digital-forensic.org/ (Accessed on 03/07/2013)
[33] http://www.sleuthkit.org/ (Accessed on 03/07/2013)
[34] http://ptk.dflabs.com/download.html (Accessed on 03/07/2013)
[35] http://www.porcupine.org/forensics/tct.html (Accessed on 03/07/2013)
[36] http://computer-forensics.sans.org/community/downloads (Accessed on 03/07/2013)
[37] http://www.caine-live.net/ (Accessed on 03/07/2013)
[38] http://www.lnx4n6.be/ (Accessed on 29/06/2013)
[39] http://sumuri.com/ (Accessed on 29/06/2013)
[40] https://santoku-linux.com/ (Accessed on 29/06/2013)
[41] http://www.forevid.org/ (Accessed on 29/06/2013)

[42] Philip Craiger, Mark Pollitt, & Jeff Swauger. Digital Evidence and Digital Forensics. To appear in H. Bigdoli (Ed.), Handbook of Information Security. John Wiley &Sons, 2005.
[43] Casey, Eoghan. Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Cambridge: Cambridge University Press, 2000.
[44] Vacca, John R. Computer Forensics Computer Crime Scene Investigation. Massachusetts: Charles River Media, 2002.
[45] Megan Carney and Marc Rogers. The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction. International Journal of Digital Evidence (IJDE), 2(4), Spring 2004.
[46] Brian D. Carrier and Eugene H. Spafford. Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. In Proceedings of the 2005 Digital Forensic Research Workshop (DFRWS), 2005.
[47] Casey, Eoghan, and Cory Altheide. Handbook of Digital Forensics and Investigation. Burlington, MA: Elsevier Academic, 2010.
[48] Marshall, Angus M. Digital Forensics: Digital Evidence in Criminal Investigation. Chichester, UK: Wiley-Blackwell, 2008.
[49] Peterson, Gilbert, and Sujeet Shenoi. Advances in Digital Forensics VII. Berlin: Springer, 2011.
[50] Volonino, Linda, and Reynaldo Anzaldua. Computer Forensics for Dummies. Hoboken, NJ: Wiley, 2008.
[51] Dowling, Anthony John. Digital Forensics: A Demonstration of the Effectiveness of the Sleuth Kit and Autopsy Forensic Browser : A Thesis Submitted for the Degree of Master of Science (Information Science) at the University of Otago, Dunedin, New Zealand. 2006.
[52] Law Office Management in the 21st Century. Mechanicsburg, PA: Pennsylvania Bar Institute, 2006.
[53] Eoghan Casey," Digital evidence and computer crime forensic science computers and the internet" , 2011
[54] Giannakis Antoniou and Stefanos Gritzalis ,"RPINA- Network Forensics Protocol Embedding Privacy Enhancing Technologies" , 2006
[55] Γκρίτζαλης Στέφανος , “Enhancing Web Privacy & Anonymity in the Digital Era”, 2004
[56] Bajaj, R., Ranaweera, S.L., Agrawal, D.P., 2002. GPS: location- tracking technology. IEEE Computer, 92–94.
[57] Beresford, A.R., Stajano, F., 2003. Location privacy in pervasive computing. IEEE Pervasive Computing 2 (1), 46–55.
[58] G.F. Marias *, L. Kazatzopoulos, C. Delakouridis, P. Georgiadis. Applying privacy on the dissemination of location information. Telematics and Informatics 23 (2006) 211–225.
[59] C. Bettini, X. S. Wang, and S. Jajodia. Protecting privacy against location-based personal identifcation. In In 2nd VLDB Workshop SDM, pages 185{199, 2005.
[60] Kalle Lyytinen and Youngjin Yoo. Issues and challenges in ubiquitous computing. Communications of the ACM, 45(12):62.65, Dec. 2002. (Ref: p. 13.)

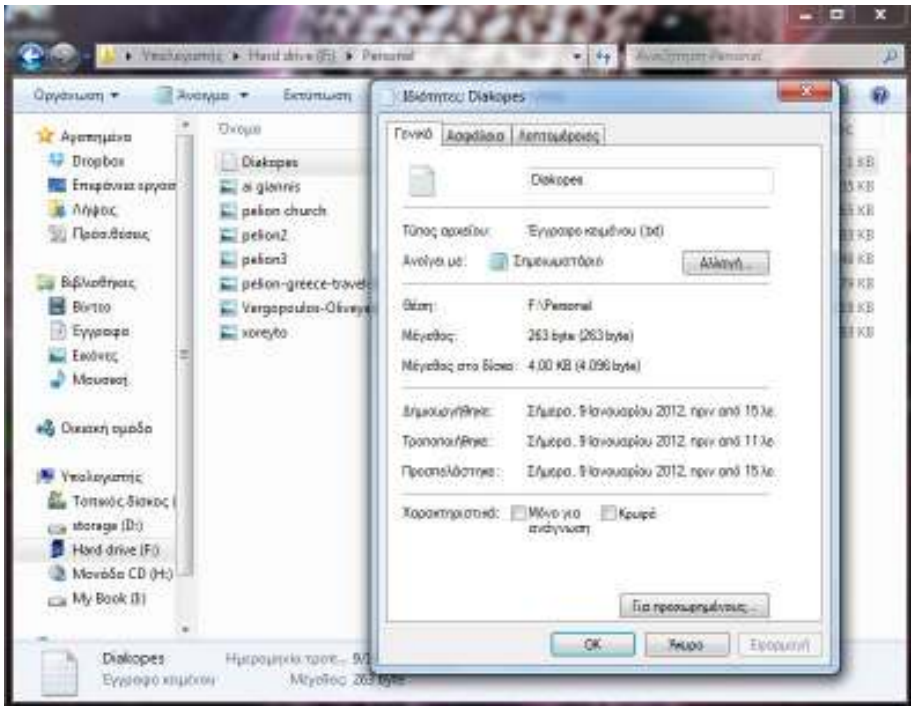
Παράρτημα Α

Ενέργειες κακόβουλου developer (Σενάριο 7.1)

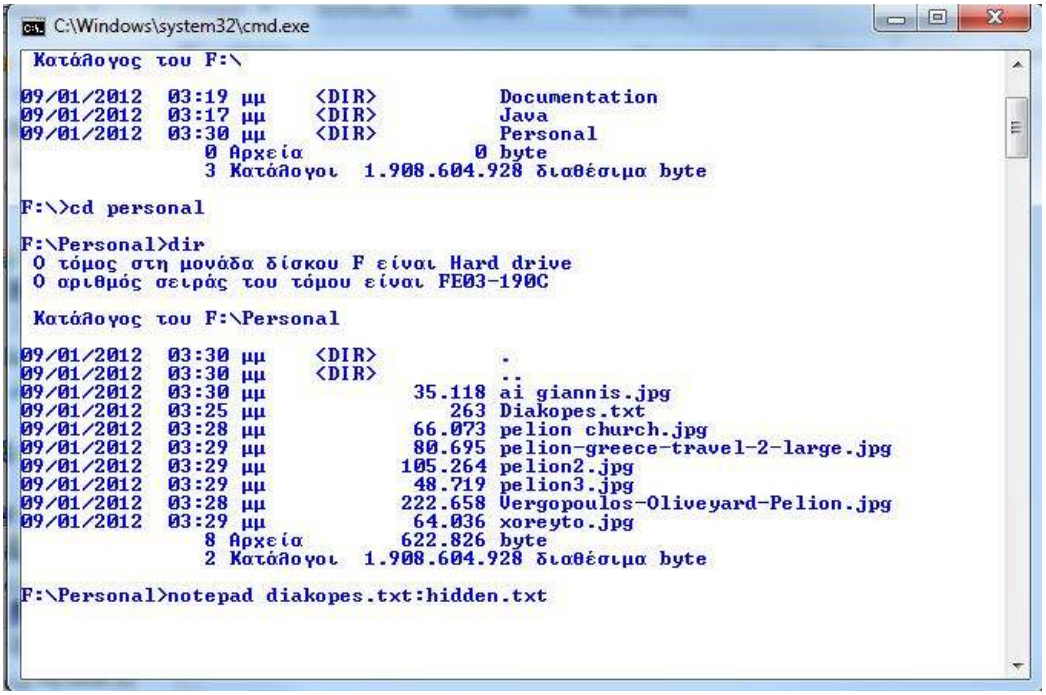
Θα πρέπει να θεωρήσουμε τον κακόβουλο χρήστη τουλάχιστον τόσο έξυπνο, όσο είμαστε εμείς. Έτσι λοιπόν δε θα χρησιμοποιούσε κάποιο πρόγραμμα στεγανογραφίας για να κρύψει την πληροφορία. Ειδικά αν χρειαζόταν και εγκατάσταση στον υπολογιστή που εργαζόταν, αμέσως θα υπήρχε μια καταγραφή στο log file των windows (τα log files της εταιρείας δεν αποθηκεύονται τοπικά). Τη δυνατότητα αυτή μας τη δίνουν και μερικές απλές εντολές σε command prompt.



Εικόνα 95. Το φανερό αρχείο diakopes.txt

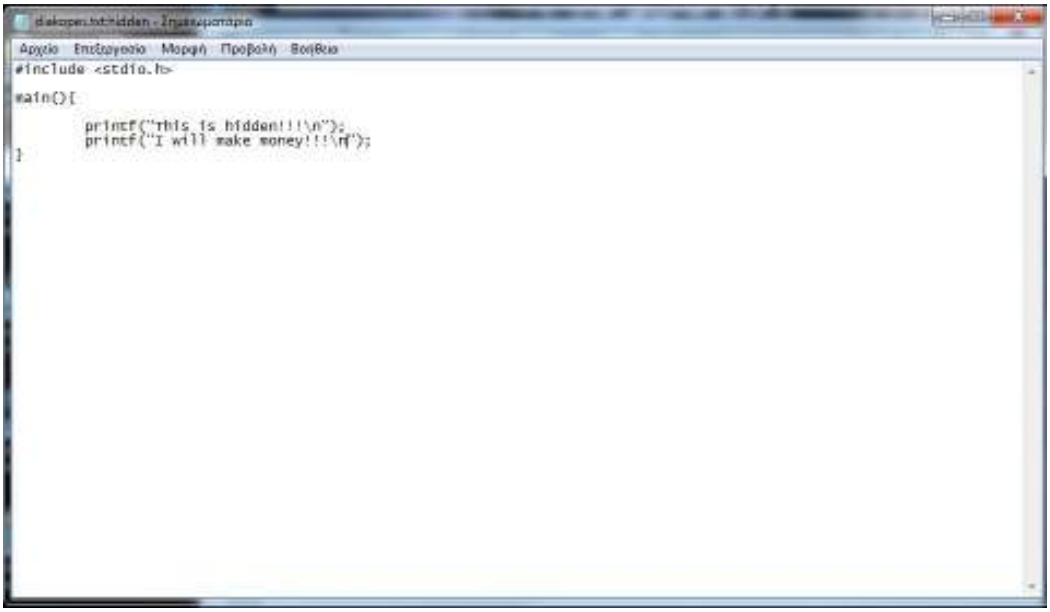


Εικόνα 96. Χαρακτηριστικά του φανερού αρχείου

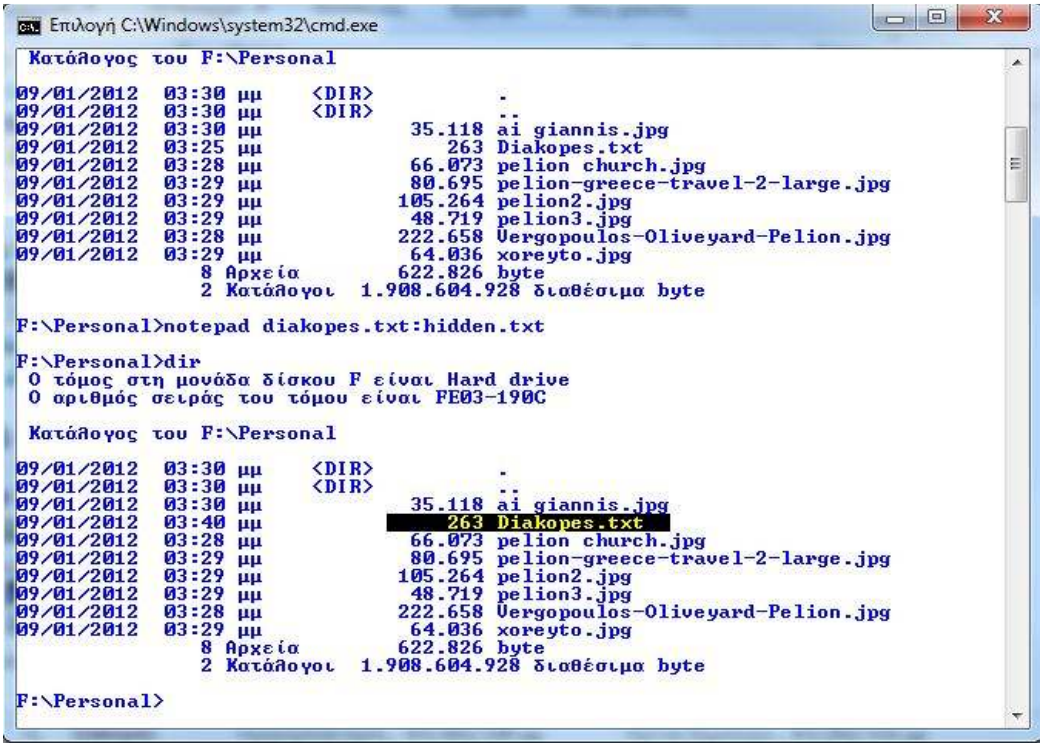


Εικόνα 97. Προσάρτηση του αρχείου hiiden.txt στο αρχείο diakopes.txt

Στο αρχείο μετέφερε κώδικα από το project στο οποίο εργαζόταν.

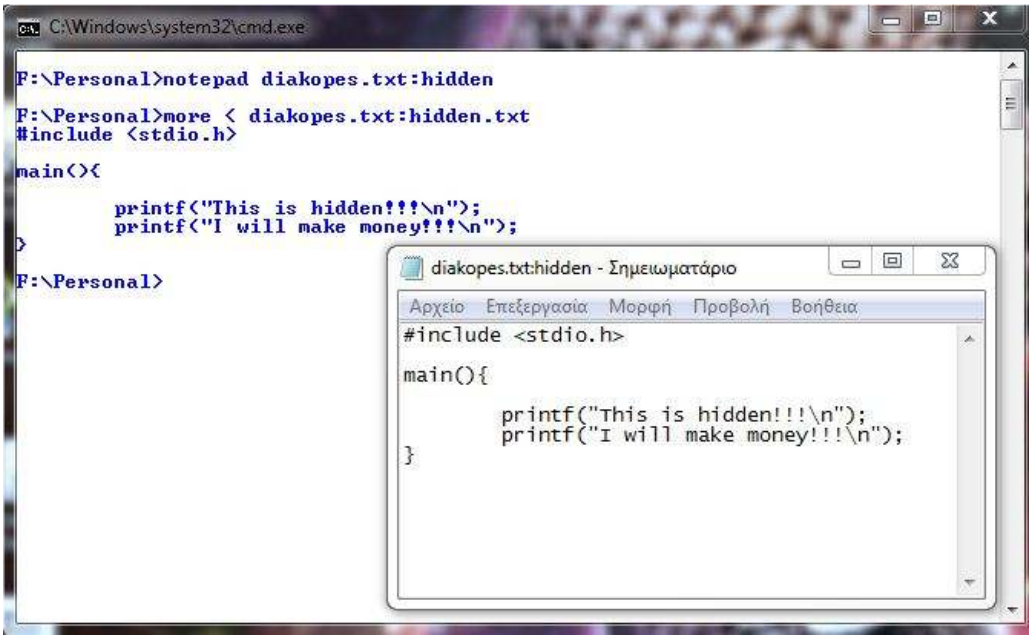


Εικόνα 98. Το αρχείο hidden.txt



Εικόνα 99. Το αρχείοdiakopes.txt παραμένει αμετάβλητο

Με την πρώτη εντολή ανοίγει το κρυφό αρχείο σε notepad και με τη δεύτερη μπορούμε να εμφανίσουμε τα περιεχόμενά του στο command prompt.



Εικόνα 100. Εμφάνιση περιεχομένων κρυφού αρχείου hidden.txt

Παράρτημα Β

Νομοθεσία για το Ηλεκτρονικό Έγκλημα [3]

Άρθρα Ποινικού Κώδικα

- Άρθρο 337 - Προσβολή της γενετήσιας αξιοπρέπειας.
- Άρθρο 348 - Διευκόλυνση ακολασίας άλλων.
- Άρθρο 348Α - Πορνογραφία ανηλίκων.
- Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους.
- Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας.
- Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.
- Άρθρο 370Γ - Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.
- Άρθρο 386Α - Απάτη με υπολογιστή.

Νόμοι

- Ν. 2472/1997 – «Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ενσωματωμένες τροποποιήσεις).
- Ν. 2867/2000 - «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις».
- Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων» Ν. 3115/2003 – «Αρχή Διασφάλισης του απορρήτου των επικοινωνιών».
- Ν. 3431/2006 – «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις».
- Ν. 3471/2006 - «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».
- Ν. 3917/2011 - «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

Προεδρικά Διατάγματα

- Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας».
- Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές».
- Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

Οδηγίες Ευρωπαϊκής Ένωσης

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Network Provision -ONP).
- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών.
- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.
- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.
- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).
- Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση).
- Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).
- Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).
- Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).
- Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Διεθνείς Συμβάσεις

- Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας.
- Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001.
- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948.
- Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ).

Αποφάσεις

- Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».
- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr».
- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής.