

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ψηφιακή Έρευνα και Computer Forensics

Νταλάκου Λαμπρινή

Μ3090008

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2011

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ψηφιακή Έρευνα

και Computer Forensics

Νταλάκου Λαμπρινή

Μ3090008

Επιβλέπουσα Καθηγήτρια: Μήτρου Λίλιαν

Εξωτερικός Κριτής: Τσούμας Βασίλειος

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2011

Περίληψη

Η ανάπτυξη των ψηφιακών συστημάτων και δικτύων έχει οδηγήσει σε μια νέα εποχή τη καθημερινότητα. Άτομα κάθε ηλικίας χρησιμοποιούν συνεχώς κάποιου είδους ψηφιακής συσκευής είτε για επαγγελματικούς λόγους ή για ψυχαγωγικούς. Τη σήμερον ημέρα, τα παιδιά μαθαίνουν να χειρίζονται υπολογιστικές συσκευές και να πλοηγούνται στο διαδίκτυο από μικρή ηλικία. Εντούτοις, με την εξάπλωση των ψηφιακών δυνατοτήτων δόθηκαν και νέες ευκαιρίες για την διάπραξη εγκλημάτων και άλλων παράνομων δραστηριοτήτων. Οι κίνδυνοι παραμονεύουν τόσο για τους απλούς χρήστες οι οποίοι πέφτουν συχνά θύματα λόγω της ελλιπής γνώσης για την προστασία τους από κακόβουλες ενέργειες, αλλά κυρίως για μεγάλες εταιρίες, τράπεζες, δημόσιους και ιδιωτικούς οργανισμούς όπου οι επιπτώσεις μιας εγκληματικής ενέργειας μπορεί να είναι καταστροφικές.

Για την αντιμετώπιση της νέας γενιάς εγκλημάτων και άλλου είδους παρανομιών με χρήση ψηφιακής τεχνολογίας, είναι απαραίτητη η ανάπτυξη ενός καινούριου τρόπου έρευνας που καλύπτει τις απαιτήσεις και ιδιαιτερότητες του ψηφιακού χώρου, καθώς και η μετατροπή της νομοθεσίας, ακόμα και με τη θέσπιση νέων νόμων, για να καλύπτει τις νέες συνθήκες διάπραξης παράνομων δραστηριοτήτων και κατ’ επέκταση τη καταπολέμησή τους. Στα πλαίσια αυτής της αντίδρασης προς τα νέα δεδομένα του εγκλήματος, αναπτύχθηκε μια νέα επιστήμη, αυτή των Computer Forensics, η οποία παρέχει νέες επιστημονικές μεθόδους για την απόκτηση, διατήρηση και καταγραφή ψηφιακών αποδεικτικών στοιχείων κατά τη διάρκεια μιας έρευνας σε υπολογιστικές συσκευές ή συστήματα, με τρόπο που θα διασφαλίζεται η ακεραιότητά τους και επομένως την αποδεικτική τους αξία έτσι ώστε να γίνονται αποδεκτές σε μια νομική διαδικασία.

Ο σκοπός της παρούσας εργασίας είναι να παρουσιάσει και να αναλύσει το τομέα των Computer Forensics και τα στάδια μιας ψηφιακής έρευνας όπου εφαρμόζεται. Συγκεκριμένα, περιγράφονται είδη δεδομένων που μπορεί να αποτελέσουν αποδεικτικά στοιχεία και οι πηγές τους, γνωστές τεχνικές που εφαρμόζονται σε διαδικασίες Computer Forensic, καθώς και οι δυσκολίες, λόγω της φύσης της έρευνας ή εξαιτίας ενεργειών του υπόπτου για την αποτροπή εντοπισμού αποδείξεων, που συναντώνται κατά τη διάρκεια της έρευνας. Επιπλέον, παρουσιάζονται γνωστοί μέθοδοι ψηφιακής έρευνας και εργαλεία που χρησιμοποιούνται ευρέως καθώς και κριτική αξιολόγησή τους. Τέλος, ορίζονται κάποια νομικά ζητήματα που αφορούν τη

διεξαγωγή και αποτελεσματικότητα μιας ψηφιακής έρευνας, αλλά και τη προστασία των ατόμων και της ιδιωτικής τους ζωής κατά τη διάρκεια της έρευνας.

Πιο αναλυτικά, στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στο ηλεκτρονικό έγκλημα και στην ανάγκη ύπαρξης των Computer Forensics. Ακολουθεί μια ιστορική αναδρομή των υπολογιστών και των δικτύων και της εξέλιξης του εγκλήματος, από την εκτέλεση μιας παράνομης πράξης με χρήση του υπολογιστή μέχρι την πλήρη διάπραξή της στο διαδίκτυο. Στη συνέχεια περιγράφεται η δημιουργία των πρώτων ειδικών ομάδων και εκπαιδευτικών προγραμμάτων για την απόκτηση ψηφιακών αποδείξεων και την καταπολέμηση του ηλεκτρονικού εγκλήματος, καθώς και η εξέλιξη της ψηφιακής έρευνας και των εργαλείων που χρησιμοποιούνται. Επιπλέον, ορίζονται οι βασικές έννοιες και οι απαραίτητες κατηγοριοποιήσεις και τονίζονται οι διαφορές της ψηφιακής με τη φυσική μορφή στην έρευνα και στα αποδεικτικά στοιχεία.

Το δεύτερο κεφάλαιο αφορά τη ψηφιακή έρευνα, δηλαδή των σύνολο των ενεργειών που χρησιμοποιούνται για τη συλλογή ψηφιακών δεδομένων από υπολογιστικές συσκευές ή συστήματα και αναλύονται τα κύρια σημεία και χαρακτηριστικά της έρευνας. Αρχικά γίνεται αναφορά στη προετοιμασία του ερευνητή πριν εμφανιστεί κάποιο περιστατικό και στην ετοιμότητα των οργανισμών έτσι ώστε να είναι αργότερα εύκολη η συλλογή στοιχείων. Όταν εντοπιστεί μια παράνομη δραστηριότητα οι αρχικές ενέργειες του ερευνητή είναι σημαντικές για τη διατήρηση της ακεραιότητας των δεδομένων. Ακολουθεί η αναζήτηση και συλλογή των δεδομένων, όπου περιγράφονται τρόποι συλλογής και σημεία που πρέπει να δοθεί προσοχή, όπως στη συλλογή ευμετάβλητων δεδομένων, δεδομένων από δίκτυα και φορητές συσκευές, και η δημιουργία εικονικών αντιγράφων, δηλαδή πιστών αντιγράφων των ψηφιακών αποθηκευτικών μέσων.

Το επόμενο βήμα είναι η ανάλυση των δεδομένων, όπου στη περίπτωση που είναι μεγάλο το μέγεθος εφαρμόζονται τεχνικές φιλτραρίσματος και μείωσης για τον περιορισμό τους. Στη συνέχεια ελέγχεται το είδος και η προέλευση των αρχείων, εντοπίζονται κρυπτογραφημένα ή στεγανογραφημένα αρχεία, ανακτούνται κρυφά και διαγραμμένα δεδομένα όπου είναι δυνατόν και καταγράφονται όλα τα στοιχεία που σχετίζονται με την υπόθεση. Τέλος, αν είναι εφικτό από τις αποδείξεις που συλλέχθηκαν, πραγματοποιείται η αναπαράσταση του συμβάντος για την καλύτερη κατανόησή του.

Στο τρίτο κεφάλαιο περιγράφονται κάποιες βασικές τεχνικές και διαδικασίες που εφαρμόζονται ευρέως στο τομέα των Computer Forensics. Από τις βασικότερες είναι η τεχνική του κατακερματισμού, η οποία εφαρμόζεται τόσο για την διαβεβαίωση της ακεραιότητας των αποθηκευτικών μέσων και των αντίγραφών τους, αλλά και για τον εντοπισμό ίδιων ή αρκετά παρόμοιων αρχείων. Ακολουθεί η διαδικασία της εικονικής αντιγραφής, η αποτελεσματικότητα της οποίας εξασφαλίζει ότι έχουν ληφθεί όλα τα δεδομένα του αποθηκευτικού μέσου χωρίς να έχει μεταβληθεί κανένα ούτε στο πρωτότυπο μέσο ούτε στο αντίγραφο, οπότε ο ερευνητής μπορεί να αναλύσει το αντίγραφο σίγουρος για την εγκυρότητά του και για την ασφάλεια των αρχικών δεδομένων.

Επόμενη τεχνική είναι η προστασία εγγραφής, η οποία συμβάλει στην εικονική αντιγραφή με το να παρεμποδίζει οποιαδήποτε μεταβολή ή εγγραφή δεδομένων κατά τη διάρκεια της αντιγραφής. Παρέχεται είτε από κάποιο λογισμικό πρόγραμμα, το οποίο μπορεί είναι διαφορετικό για κάθε λειτουργικό σύστημα, είτε από ειδική συσκευή η οποία είναι ανεξάρτητη του λειτουργικού καθώς εφαρμόζεται σε επίπεδο υλισμικού και εμποδίζει κάθε ηλεκτρικό σήμα. Επίσης, οι τεχνικές εξόρυξης δεδομένων συμβάλουν με καθοριστικό τρόπο στην έρευνα για τον εντοπισμό των σχετικότερων και σημαντικότερων δεδομένων. Εφαρμόζονται ιδιαίτερα σε περιπτώσεις οικονομικού εγκλήματος, στη τρομοκρατία και στη ταυτοποίηση στοιχείων σε μεγάλες βάσεις δεδομένων με εικόνες forensic, όπως πρόσωπα, γραφικοί χαρακτήρες και άλλα.

Το τέταρτο κεφάλαιο πραγματεύεται τις δυσκολίες και τα προβλήματα που συναντώνται σε μια ψηφιακή έρευνα και μπορούν να θέσουν σε κίνδυνο την αξιοπιστία των αποτελεσμάτων της. Ένα από τα σημαντικότερα προβλήματα είναι η εξακρίβωση της εγκυρότητας των χρονικών σημάνσεων των αρχείων. Οι τιμές των χρονικών σημάνσεων καθορίζονται κυρίως από το ρολόι του υπολογιστή το οποίο όμως εξαιτίας των τεχνικών του χαρακτηριστικών δεν θεωρείται πάντα αξιόπιστο. Επιπλέον, ο χρήστης έχει τη δυνατότητα να αλλοιώσει αυτές τις σημάνσεις προς όφελος του. Ωστόσο, στη συνέχεια παρουσιάζονται γνωστές τεχνικές για τον προσδιορισμό των πραγματικών χρόνων.

Επιπρόσθετα προβλήματα, που σχετίζονται με τη συλλογή δεδομένων, παρουσιάζονται κατά τη διάρκεια μιας έρευνας ψηφιακών αποδεικτικών στοιχείων. Κατά την αναζήτηση κάποια δεδομένα μπορεί να αγνοηθούν, άλλα να θεωρηθούν σημαντικά ενώ δεν είναι ή να έχουν παραποιηθεί για να αποπροσανατολίσουν τον ερευνητή. Επίσης, τίθενται νομικές δυσκολίες

στην αποδοχή των στοιχείων επειδή πρέπει να ακολουθούνται συγκεκριμένοι κανονισμοί σε κάθε ενέργεια του ερευνητή διαφορετικά μπορεί να απορριφτούν σε μια νομική διαδικασία. Ακόμα, έχουν αναπτυχθεί τεχνικές anti-forensics που έχουν σκοπό τη παρεμπόδιση της δουλείας του ερευνητή με τη καταστροφή, απόκρυψη ή μετατροπή των αποδείξεων, ή με την εκμετάλλευση αδυναμιών των εργαλείων που χρησιμοποιούνται ώστε να θεωρηθούν αναξιόπιστα. Αλλά, η έλλειψη επαρκής προτυποποίησης μεθόδων και εργαλείων και τυποποίησης των γνώσεων ενός ερευνητή forensics είναι που δημιουργεί το μεγαλύτερο πρόβλημα στην αναγνώριση των αποτελεσμάτων της έρευνας καθώς μπορεί να μην γίνουν ευρέως αποδεκτά.

Στο κεφάλαιο πέντε παρουσιάζονται εννιά από τα πιο διαδεδομένα μοντέλα ψηφιακής έρευνας με μια κριτική αξιολόγησή τους στο τέλος. Τα περισσότερα από αυτά εφαρμόζονται στη πλειοψηφία των περιπτώσεων και είναι με τέτοιο τρόπο διαμορφωμένα για την εύκολη επέκτασή τους για τη κάλυψη μελλοντικών αναγκών των ψηφιακών ερευνών, παραδείγματα είναι η μέθοδος του Casey και το αφηρημένο μοντέλο των Reith, Carr και Gunsh. Το Integrated Digital Investigation Model και η επέκτασή του από τους Baryamureeba και Tushabe επιτυγχάνουν το συνδυασμό της φυσικής με τη ψηφιακή έρευνα, ενώ το μοντέλο του Johnson στοχεύει στη γρήγορη αλλά αποτελεσματική επίλυση της υπόθεσης.

Επιπλέον, το μοντέλο Event Based Digital Forensic Investigation Framework εστιάζει στην ανάλυση των γεγονότων για τη δημιουργία υποθέσεων στις οποίες θα εστιάσει ο ερευνητής. Ένα πιο λεπτομερές μοντέλο είναι το ιεραρχικό μοντέλο των Beebe και Clark το οποίο αναλύει τις φάσεις και υποφάσεις μιας έρευνας καθώς και τις αρχές που πρέπει να εφαρμόζονται σε όλες τις διαδικασίες. Ωστόσο, λίγα είναι τα πιο εξειδικευμένα μοντέλα που προορίζονται για ειδικές περιπτώσεις. Σε αυτό το κεφάλαιο αναλύεται το Computer Forensics Field Triage Process, το οποίο περιγράφει μια σειρά βημάτων για ψηφιακή έρευνα στο χώρο του συμβάντος, και το μοντέλο του Ciarduain το οποίο αφορά την έρευνα εγκλημάτων στο κυβερνοχώρο.

Το έκτο κεφάλαιο αφορά τα εργαλεία forensics που χρησιμοποιεί ένας ερευνητής για την απόκτηση, ανάλυση και παρουσίαση δεδομένων. Αυτά τα εργαλεία είναι είτε κάποια συσκευή ή λογισμικά προγράμματα τα οποία διακρίνονται σε ανοιχτού ή κλειστού κώδικα. Ένα εργαλείο για να θεωρηθεί αξιόπιστο και να γίνουν αποδεκτά τα αποτελέσματά του θα πρέπει να πληροί κάποιες προδιαγραφές, για παράδειγμα στην Αμερική υπάρχει συγκεκριμένα η Ακρόαση

Daubert όπου ο δικαστής εξακριβώνει κατά πόσο πληρούνται. Στη συνέχεια περιγράφονται τα πιο διαδεδομένα εργαλεία, όπως το EnCase και το FTK τα οποία διαθέτουν πληθώρα λειτουργιών, και πως λειτουργικά τύπου Linux και η γλώσσα Python μπορούν να χρησιμοποιηθούν ως εργαλεία των Computer Forensics. Τέλος, παρατίθεται αξιολόγηση ορισμένων εργαλείων με βάση εκθέσεις του National Institute of Justice.

Αντίθετα, στο έβδομο κεφάλαιο γίνεται αναφορά στα εργαλεία anti-forensic, δηλαδή τα εργαλεία που χρησιμοποιούνται για την παρεμπόδιση του έργου του ερευνητή. Διακρίνονται στα εργαλεία κρυπτογράφησης και στεγανογράφησης, εργαλεία που αναπτύχθηκαν από τη Metasploit για να επισημάνουν αδυναμίες σε μεθόδους και εργαλεία forensic, και εργαλεία διαγραφής δεδομένων. Επειδή η τελευταία κατηγορία είναι από τις πιο διαδομένες, ωστόσο με αρκετά μειονεκτήματα τα οποία αναλύονται περισσότερο, παρέχεται και μια αξιολόγηση της αποτελεσματικότητάς τους.

Στο όγδοο κεφάλαιο γίνεται ανάλυση forensic των γνωστών λειτουργικών συστημάτων Windows, Linux και Mac OS. Ένας ερευνητής για να είναι πιο αποτελεσματικός πρέπει να έχει γνώσεις για τα ιδιαίτερα χαρακτηριστικά των λογισμικών που επεξεργάζεται για τον καλύτερο εντοπισμό αποδεικτικών στοιχείων. Δίνεται έμφαση στο κυριότερο μέρος ενός λειτουργικού, το σύστημα αρχείων και στο τρόπο που διαχειρίζεται τα αρχεία και ειδικότερα στη διαγραφή τους. Στα πλαίσια της εργασίας περιγράφονται τα συστήματα FAT και NTFS των Windows, τα Ext2 και Ext3 των Linux, και τα HFS και HFS+ των Mac OS. Επιπλέον αναφέρονται κάποιες άλλες πηγές δεδομένων που δημιουργούνται από τις δραστηριότητες των χρηστών και κατά την εκτέλεση εφαρμογών.

Το ένατο κεφάλαιο πραγματεύεται τα νομικά ζητήματα που προκύπτουν κατά τη διάρκεια της διεξαγωγής μιας ψηφιακής έρευνας και αναφέρεται το νομικό πλαίσιο και κανονισμοί που έχουν θεσπιστεί για την αντιμετώπισή τους. Ένα από τα βασικότερα ζητήματα είναι η προστασία της ιδιωτικής ζωής, καθώς οι τεχνικές των Computer Forensics που χρησιμοποιούνται μπορεί να παρέμβουν σε προσωπικές πληροφορίες ακόμα και ατόμων που δεν σχετίζονται με την υπόθεση. Επιπλέον, περιγράφεται το πρόβλημα καθορισμού δικαιοδοσίας, ειδικά σε διεθνής υποθέσεις όπου ο τόπος τέλεσης του εγκλήματος είναι δύσκολο να προσδιοριστεί. Στη συνέχεια, ορίζονται οι απαραίτητες προϋποθέσεις για τη πραγματοποίηση μιας νόμιμης έρευνας και κατάσχεσης και

η ανάγκη έκδοσης κατάλληλου εντάλματος. Επίσης, αναλύονται τα χαρακτηριστικά των ψηφιακών αποδεικτικών στοιχείων και η νομική ισχύς τους ανάλογα με το είδος της υπόθεσης.

Το τελευταίο κεφάλαιο συνοψίζει τα συμπεράσματα και τα προβλήματα που πρέπει να επιλυθούν στο τομέα των Computer Forensics και της ψηφιακής έρευνας. Νέες τεχνικές πρέπει να εφαρμοστούν για την αντιμετώπιση ενεργειών του χρήστη για την απόκρυψη πληροφοριών και την αποτελεσματικότερη ανάκτηση διαγραμμένων αρχείων. Η προτυποποίηση μεθόδων για τη διαχείριση ψηφιακών αποδείξεων θα συντελέσει στην έγκυρη και έγκαιρη διεξαγωγή έρευνας, ενώ η πιστοποίηση των ερευνητών συμβάλει στη διεθνή αναγνώριση των γνώσεών τους οι οποίες δεν πρέπει να περιορίζονται στη χρήση εργαλείων forensics, αλλά στον ευρύτερο τομέα της πληροφορικής. Τέλος, η ανάπτυξη ενός κοινού αποδεκτού νομοθετικού πλαισίου για την καταπολέμηση εγκληματικών ενεργειών και άλλων παράνομων δραστηριοτήτων κρίνεται απαραίτητη για την επίλυση διεθνών υποθέσεων.

Summary

The growth of digital systems and networks has led to a new era of everyday life. People of each age use all the time a digital device for professional use or entertainment. Today, children learn to use computers and access the internet by small age. Nevertheless, with the spread of digital possibilities, new chances were given for committing crimes and other illegal activities. Many dangers threaten common users, who fall frequently victims because of their lack of computer knowledge and so the lack of protective measures against malicious actions, but mainly large companies, banks, public and private services, in which the effects from a criminal action can be catastrophic.

To confront the new generation of crime and the other types of illegal activities with using digital technology, it is essential to develop a new way of research that covers the requirements and special characteristics of digital space, as well as the modification of the legislation, even with the establishment of new laws, in order to face the new conditions of committing illegal activities and to deal with it. To assist in this encounter with the new criminal facts, a new science was developed, the Computer Forensics, which provides new scientific methods for the acquisition, maintenance and documentation of digital evidences during the investigation into computer devices or systems, in a way that their integrity and probative value will be assured in order to be acceptable in any legal process.

The aim of this project is to present and analyze Computer Forensics and the stages of digital investigation that they are applied. In detail, types of data, that could be evidence, and their sources are being described, and also known techniques that are being applied in processes of Computer Forensics, as well as difficulties during the investigation, because of digital investigation's nature or the counter measures which the suspect applied to prevent discovery of criminal evidence. Moreover, well-known methods and tool for digital investigation are presented which are used widely and critical evaluation of them. Finally, legal issues are introduced about the conduction of a digital investigation and its effectiveness, and also concerns for the protection of people and their private life during the research.

More specific, in the first chapter it is introduced the electronic crime and the need for Computer Forensics. Then, it comes next a historical review of computers, networks and the development

of crime from the simple commit of illegal action using a computer up to the complete implementation of crimes in the internet. Furthermore, it is described the creation of first special units and educational programs for digital evidence acquisition and counter fight electronic crime, as well as the development of digital investigation and tools which are being used. Moreover, basic terminology and essential categorizations are being referred and it is highlighted the differences between digital and physical form in the investigation and evidence.

The second chapter is about the digital investigation, specifically all the action for collecting digital data from computer devices or systems. It is analyzed the main aspects and characteristics of the investigation. Firstly is the investigator's preparation before an incident occurs and the forensic readiness of the organization so as to be easier the collection of evidence after the incident. When an illegal activity is detected, the investigator's initial actions are important for the maintenance of data's integrity. After the first actions follows the search and collection of evidences. Basic ways of collection are described and challenges like the collection of volatile data, data from networks and mobile devices, and also the creation of image files from storage devices.

Next step of the investigation is the analysis of data. When there is a big amount of data, it is being applied infiltration and reduction techniques to decrease the data. Then, they are checked for their type and source, encrypted or stego files are being detected, deleted or damaged files are retrieved when it is possible and all the relevant findings are documented. Finally, a crime reconstruction is provided, if it is feasible from the evidences that have been collected, to gain a better understanding of the incidence.

In the third chapter basic techniques and processes are described which are applied widely in the field of Computer Forensics. The hashing technique is one of the most important, which is applied to assure the integrity of storage devices and their images, and also to detect same or similar enough files. Another technique is imaging, the effectiveness of which ensures that all the data have been taken from the storage devices without alterations neither in the original data the medium nor in the image copies; therefore the investigator can analyze the images and be certain for their validity and the safety of the initial data.

Next technique is write blocking, which contributes in imaging by blocking any change on the data during the process. Write blockers are either software, which is different for every operating system, or an independent hardware device that prevents any electric signal. Also, data mining techniques are uses in the investigation for detecting the most relative and important data. They are applied particularly in cases of economic crime, terrorism and to compare evidence with large scale forensic image databases, for example databases with fingerprints, faces, handwriting and others.

The fourth chapter deals with difficulties and problems facing the digital investigation and could endanger the reliability of its result. One of the most important problems is the verification of file's time stamps' validity. The values of timestamps are determined mainly by the computer's clock, which however is not considered always reliable because of its technical characteristics. Moreover, the user has the ability to change the timestamps according to his best interest. However, known techniques are presented which can determine close enough the real values of timestamps.

Additional problems are exposed during the investigation for digital evidences. At the search some data could be ignored, other could be presumed important while they are not or be counterfeited to confuse the investigator. Also, legal difficulties exist in the acceptance of evidences since legal regulations must be followed in every action taken otherwise they could be rejected in a legal process. Furthermore, anti-forensic techniques have been developed with intent the obstruction of investigator's work by destroying, hiding or altering the evidences, or by taking advantage the weaknesses of tools which are used so that they would be considered unreliable. Nevertheless, the lack of sufficient standardization of methods and tools and certification of investigator's knowledge and abilities is the most important problem of the reliability of the evidences because they could be not widely accepted.

In chapter five they are presented nine known models of digital investigation and a critical evaluation. Most of them are applied in the majority of cases and they are developed in a way to be easily adjustable to the future needs of digital investigation and Computer Forensics, like Casey's methodology and the abstract model of Reith, Carr and Gunsh. The Integrated Digital Investigation Model and its enhancement by Baryamureeba and Tushabe achieve the

combination of physical and digital investigation, while Johnson's model aims in the quick but effective resolution of the case.

Moreover, the Event Based Digital Forensic Investigation Framework focuses in the analysis of the facts to create possible assumptions about the case and focus on them. A more detailed model is the Hierarchical, Objectives-Based Framework for the Digital Investigations Process which analyzes the investigation's phases and sub phases as well as principles that could be applied in different ways to all phases. However, few models specialized in specific cases. For example, in this chapter are examined the Computer Forensics Field Triage Process, which describes a series of steps for digital investigation in the field of the incident, and the Extended Model of Cybercrime Investigation, which refers to the investigation of crimes in the cyberspace.

The sixth chapter refers to forensic tools which an investigator uses for the acquisition, analysis and presentation of the data. These tools are either a special device or a software program, which are distinguished in open or closed source. A tool in order to be reliable and its results be acceptable his results must fulfill quality requirements, for example in USA a forensic tool must meet the Daubert standard, a collection of rules regarding the admissibility of the investigation's results. Also, some widespread tools are described, like EnCase and FTK which execute a number of processes, and how Linux and the programming language Python can contribute as tools of Computer Forensics. Finally, there is an evaluation on some of the referred tools.

On the other hand, in the seventh chapter are referred the anti-forensic tools, which are used ot obstruct the work of an investigator. There are cryptography and steganography tools, some tools that were developed by Metasploit to stress weaknesses in forensic methods and tools, and tools that remove data by overwriting them. Due to the widely usage of data eraser tools, their effectiveness is analyzed and also the possibilities to detect evidence after their use.

In the eighth chapter there is forensic analysis of the operating systems Windows, Linux and Mac OS. An investigator in order to be more effective must have knowledge for the characteristics of the software that he examines for the better detection of evidence. On the operating systems more emphasis is given to their file systems and how they are managing the files especially the process of deletion. The file systems that are described are FAT and NTFS of

Windows, the Ext2 and Ext3 of Linux, and the HFS and HFS+ of Mac OS. Moreover there is reference to other sources of digital data from user's activities and the execution of applications.

The ninth chapter deals with legal issues during the conduction of digital investigation and are mentioned the legal structure and regulations that have been established for their resolution. One of the biggest issues is the protection of people's private life, since the techniques of Computer Forensics that are used could intervene in personal information even from people who are not related with the case. Moreover, is described the problem of allocating jurisdiction, especially in international crimes where the location of the crime committed is difficult to be determined. In addition, are described the essential conditions for a legal search and seizure as well as the need to obtain a warrant. Also, the characteristics of digital evidences are analyzed and their admissibility depending on the case type.

The last chapter summarizes the conclusions and the problems that should be solved in the field of Computer Forensics and digital investigation. New techniques should be applied for confronting the suspect's efforts to conceal information and for retrieving deleted files. The standardization of methods for processing digital evidence will contribute in a valid and convenient conduction of search, while the certification of investigators provides international recognition of their knowledge which should not be limited only in the use of specific forensic tools, but in the wider field of information technology. Finally, the development of a common acceptable legal structure for fighting electronic crimes and other illegal activities is estimated crucial for the resolution of international cases.

Ακρωνύμια

Ελληνικοί Όροι

Ακρωνύμιο	Σημασία
ΕΕ	Ευρωπαϊκή Ένωση
ΕΚ	Ευρωπαϊκό Κοινοβούλιο
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής

Αγγλικοί Όροι

Ακρωνύμιο	Σημασία
ADS	Alternate Data Streams
AES	Advanced Encryption Standard
CFFTPM	Computer Forensics Field Triage Process
DES	Data Encryption Standard
DSL	Digital Subscriber Line
EFS	Encrypting File System
ENFSI	European Network of Forensic Science Institutes
FAT	File Allocation Table
FBI	Federal Bureau of Investigation
FTK	Forensic Tool Kit
HFS	Hierarchical File System
IM	Instant Messaging
KB	Kilobyte
LCN	Logical Cluster Number
MAC	Modify – Access – Create timestamps

MD5	Message-Digest algorithm 5
MFS	Macintosh File System
MFT	Master File Table
MS-DOS	Micro-Soft-Disk Operating System
NIJ	National Institute of Justice
NTFS	New Technology File System
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
RAM	Random Access Memory
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identification Module
SOP	Standard Operating Procedure
SWGDE	Scientific Working Group on Digital Evidence
TIA	Total Information Awareness
UFS	Unix File System
UTC	Coordinated Universal Time
WWW	World Wide Web

Περιεχόμενα

Περίληψη 5

Summary 11

Ακρωνύμια 16

Περιεχόμενα 18

1 Εισαγωγή 23

1.1 Ιστορική Αναδρομή 24

1.1.1 Δημιουργία ομάδων αντιμετώπισης και ειδικού προσωπικού 26

1.1.2 Εξέλιξη ψηφιακής διερεύνησης 27

1.2 Βασικοί Ορισμοί και Κατηγορίες 28

1.2.1 Ορισμός Digital Forensics και υποκατηγορίες 29

1.2.2 Ψηφιακά Δεδομένα και Αποδεικτικά Στοιχεία 31

1.3 Διαφορές Ψηφιακής και Φυσικής Μορφής 35

2 Ψηφιακή έρευνα 38

2.1 Προετοιμασία 38

2.1.1 Ετοιμότητα Οργανισμών 39

2.2 Αρχικές ενέργειες 40

2.2.1 Καθορισμός Προτεραιοτήτων 41

2.2.2 Καταγραφή χώρου 41

2.2.3 Προφυλάξεις κατά τη μεταφορά 42

2.2.4 Στάδια Φύλαξης 42

2.3 Αναζήτηση και Συλλογή Δεδομένων 42

2.3.1 Μέθοδοι συλλογής δεδομένων 43

2.3.2 Αντιμετώπιση ενεργοποιημένου υπολογιστή 44

2.3.3 Συλλογή ευμετάβλητων δεδομένων 45
2.3.4 Δημιουργία εικονικών αντιγράφων 46
2.3.5 Συλλογή δεδομένων από δίκτυα 47
2.3.6 Αρχεία ήχου και εικόνας 47
2.3.7 Φορητές συσκευές 48
2.4 Ανάλυση Δεδομένων 49
2.4.1 Μέθοδοι φιλτραρίσματος και μείωσης δεδομένων 50
2.4.2 Είδος και προέλευση αρχείων 51
2.4.3 Ανάκτηση κρυφών ή διαγραμμένων αρχείων 51
2.4.4 Κρυπτογράφηση και στεγανογράφηση 52
2.5 Καταγραφή Ψηφιακών Αποδείξεων 53
2.6 Αναπαράσταση Συμβάντος 54
3 Ειδικές Τεχνικές 56
3.1 Κατακερματισμός (Hashing) 56
3.1.1 Βασικοί Αλγόριθμοι Κατακερματισμού 58
3.2 Εικονική Αντιγραφή (Imaging) 61
3.3 Προστασία Εγγραφής (Write Blocker) 64
3.4 Εξόρυξη Δεδομένων (Data Mining) 65
4 Προβλήματα και Δυσκολίες 69
4.1 Σημάνσεις χρόνου (Timestamps) 69
4.2 Ψηφιακές Αποδείξεις 72
4.3 Κρυπτογράφηση / Στεγανογράφηση 75
4.4 Τεχνικές Anti-Forensics 78
4.4.1 Καταστροφή αποδείξεων 78
4.4.2 Απόκρυψη αποδείξεων 79

4.4.3 Αποτροπή δημιουργίας δεδομένων 79
4.4.4 Δημιουργία πλαστών αποδείξεων 80
4.5 Ανάγκη για προτυποποίηση και πιστοποίηση 81
5 Μέθοδοι και Μοντέλα Ψηφιακής Έρευνας 84
5.1 Μέθοδος του Eoghan Casey 84
5.2 Μέθοδος του Thomas A. Johnson 88
5.3 Ένα αφηρημένο μοντέλο για Digital Forensics (An Abstract Digital Forensics Model) ... 90
5.4 Μια ενσωματωμένη Διαδικασία Ψηφιακής Έρευνας (An Integrated Digital Investigation Process) 92
5.5 Το ενισχυμένο μοντέλο της διαδικασίας ψηφιακής έρευνας (The Enhanced Digital Investigation Process Model) 94
5.6 Ένα επεκταμένο μοντέλο έρευνας κυβερνοεγκλήματος (An Extended Model of Cybercrime Investigation) 95
5.7 Ένα ιεραρχικό πλαίσιο για τη διαδικασία ψηφιακής έρευνας (A Hierarchical, Objectives-Based Framework for the Digital Investigations Process) 98
5.7.1 Πρώτη βαθμίδα φάσεων 98
5.7.2 Αρχές Ψηφιακής Έρευνας 99
5.7.3 Δεύτερη Βαθμίδα Φάσεων (Υπο-φάσεις) 99
5.8 Πλαίσιο ψηφιακής έρευνας βασισμένο σε γεγονότα (Event Based Digital Forensic Investigation Framework) 100
5.9 Computer Forensics Field Triage Process Model 101
5.10 Σύγκριση και συμπεράσματα 103
6 Εργαλεία Forensics 106
6.1 EnCase 109
6.2 Forensic ToolKit (FTK) 112
6.3 The Sleuth Kit 113

6.4 P2 Commander 114
6.5 Device Seizure 114
6.6 SafeBack 115
6.7 COFEE 116
6.8 OCFA 117
6.9 SMART 117
6.10 Τα Linux ως εργαλείο forensic 118
6.11 Γλώσσα Python 119
6.12 Αξιολόγηση Εργαλείων 119
7 Εργαλεία AntiForensic 121
7.1 Εργαλεία κρυπτογράφησης 121
7.2 Εργαλεία στεγανογράφησης 124
7.3 Εργαλεία από τη Metasploit 126
7.4 Εργαλεία διαγραφής δεδομένων 127
7.4.1 Μειονεκτήματα 131
7.4.2 Αξιολόγηση εργαλείων 132
8 Ανάλυση Forensic σε Λειτουργικά Συστήματα 135
8.1 Microsoft Windows 135
8.1.1 Σύστημα Αρχείων 136
8.1.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών 140
8.2 Linux 141
8.2.1 Σύστημα αρχείων 141
8.2.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών 143
8.3 Mac OS 144
8.3.1 Σύστημα Αρχείων 144

8.3.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών 146
9 Νομικά Ζητήματα 148
9.1 Προστασία Ιδιωτικότητας 148
9.1.1 Νομικό Πλαίσιο στις Η.Π.Α. 150
9.1.2 Νομικό Πλαίσιο στην Ε.Ε και Ελλάδα 150
9.2 Δικαιοδοσία 152
9.3 Νόμιμη Έρευνα και Κατάσχεση 154
9.4 Νομική Ισχύς Αποδείξεων 155
10 Επίλογος 158
Παράρτημα Α 161
Παράρτημα Β 163
Παράρτημα Γ 164
Παράρτημα Δ 165
Βιβλιογραφία 194

1 Εισαγωγή

Η σημερινή εποχή έχει κατακλυστεί από τις νέες ψηφιακές τεχνολογίες οι οποίες έχουν αλλάξει ριζικά την καθημερινή ζωή και έχουν προκαλέσει εξάρτηση από τα ψηφιακά συστήματα και δίκτυα. Συσκευές με υπολογιστικές ικανότητες έχουν γίνει απαραίτητες για τον μέσο άνθρωπο, ενώ η σύνδεση σε κάποιο δίκτυο αποτελεί συνήθεια αλλά και αναγκαιότητα για μερικούς. Επίσης, η πλειοψηφία των πληροφοριών που παράγονται κάθε μέρα είναι σε ψηφιακή μορφή και ελάχιστες είναι σε κάποια άλλη, για παράδειγμα έντυπη. Όλα αυτά έχουν ως αποτέλεσμα τη συνεχή μεταφορά πληροφοριών μέσω καλωδίων ή κυμάτων και την καταγραφή προσωπικών ή και ευαίσθητων δεδομένων των χρηστών κάθε στιγμή [19].

Όμως, η χρήση των ψηφιακών συσκευών και των δικτύων δεν γίνεται πάντα με ευσυνείδητο τρόπο. Η εξέλιξη της τεχνολογίας προκάλεσε και την εξέλιξη των παράνομων δραστηριοτήτων. Παραδοσιακά εγκλήματα, όπως η κλοπή ή η απάτη, μπορούν να γίνουν μέσω υπολογιστή, αλλά και νέα εγκλήματα έκαναν την εμφάνισή τους με την εκμετάλλευση των νέων ψηφιακών συνθηκών. Η κατάχρηση θέτει σε κίνδυνο απλούς χρήστες αλλά κυρίως επιχειρήσεις, οργανισμούς, το κράτος και τις κρίσιμες υποδομές του, προκαλώντας οικονομικό, κοινωνικό ή πολιτικό κόστος [2].

Η καθιέρωση του διαδικτύου προσφέρει πολλές ευκαιρίες για την εκτέλεση μη θεμιτών πράξεων. Η ανωνυμία που προσφέρεται και η ευελιξία δράσης ουσιαστικά οπουδήποτε παρέχουν ένα πέπλο προστασίας στους χρήστες. Ένα από τα πιο διαδεδομένα εγκλήματα στο κυβερνοχώρο είναι η παιδική πορνογραφία, κάθε χρόνο εξαρθρώνονται μεγάλα κυκλώματα παιδεραστίας που διακινούν υλικό μέσο του διαδικτύου. Επίσης, αρκετά συχνές είναι οι παράνομες προσβάσεις σε υπολογιστικά συστήματα, οι οποίες μπορούν να διαχωριστούν σε cracking και hacking. Η διαφορά τους είναι ότι στη πρώτη περίπτωση στόχος είναι το οικονομικό όφελος ενώ στη δεύτερη η περιέργεια και ευχαρίστηση.

Η λήψη κατάλληλων μέτρων ασφαλείας είναι κρίσιμη και αναγκαστική για τη προφύλαξη των χρηστών. Αλλά, στη περίπτωση που έχει πραγματοποιηθεί ένα συμβάν, εκτός από την αποκατάσταση του συστήματος, είναι σημαντικό και ο εντοπισμός των δραστών για να οδηγηθούν στη δικαιοσύνη. Η κάθε πράξη αφήνει πάντα ίχνη, σημασία έχει να μπορούν να

εντοπιστούν και να αναγνωριστούν ώστε να αποτελέσουν αποδεικτικά στοιχεία για τον δράστη και το έγκλημα που διέπραξε.

Ωστόσο, η συλλογή αποδείξεων για τα εγκλήματα που συνδέονται με ψηφιακές συσκευές δεν είναι εύκολη και αποτελούν νέα πρόκληση για την αστυνομία, τη δικαιοσύνη και τον ακαδημαϊκό τομέα λόγω των νέων χαρακτηριστικών που συνεχώς μεταβάλλονται εξαιτίας της γρήγορης εξέλιξής τους. Επομένως, ήταν επιτακτική η αντιμετώπιση τους όχι με τις γνωστές, παραδοσιακές μεθόδους, αλλά με μεθόδους που θα προστατεύουν την αξία και την ακεραιότητα των στοιχείων με βάση τις ιδιαιτερότητές τους. Ο σκοπός αυτός επιτυγχάνεται με το νέο επιστημονικό τομέα των Computer Forensics [2, 19].

Ο όρος Forensics χρησιμοποιείται για να προσδιορίσει μια έρευνα τα αποτελέσματα της οποίας μπορεί να παρουσιαστούν στο δικαστήριο. Αυτός είναι και ο σκοπός των Computer Forensics, η παρουσίαση ψηφιακών στοιχείων με τρόπο που γίνονται αποδεκτά σε μια νομική διαδικασία. Οι ψηφιακές αποδείξεις έχουν παρόμοιο ρόλο με τα δαχτυλικά αποτυπώματα και το DNA. Μπορούν να παρέχουν πληροφορίες για ένα έγκλημα, πότε έγινε, πού, πώς, από ποιον, γιατί, να συνδέσουν το θύτη με το θύμα ή να δώσουν κάποια καθοδήγηση στην έρευνα [2, 5].

Η χρήση των Computer Forensics είναι ιδιαίτερα σημαντική για δημόσιες και ιδιωτικές επιχειρήσεις και οργανισμούς για την προστασία ζωτικών αποδείξεων, για τη μείωση απωλειών και για τη προστασία δεδομένων από μελλοντικές επιθέσεις. Πολλές φορές, όταν παρουσιάζεται κάποιο συμβάν η πρώτη αντίδραση είναι η επίλυσή του, ωστόσο αυτή η αντιμετώπιση μπορεί να προκαλέσει την αλλοίωση δεδομένων και πιθανόν το μη εντοπισμό αδυναμιών στην ασφάλεια, συνεπώς, απαιτείται η διεξαγωγή κατάλληλης έρευνας από έμπειρο προσωπικό στα Computer Forensics [19]. Επιπλέον, η αξιοποίησή τους μπορεί να βοηθήσει στη διαλεύκανση πολλών περιπτώσεων εκτός από εγκλήματα, όπως αυτοκτονίες και εξαφανίσεις, καθώς και σε επιλύσεις διαφορών μεταξύ ατόμων ή επιχειρήσεων [2].

1.1 Ιστορική Αναδρομή

Όταν πρωτοεμφανίστηκαν οι υπολογιστές ήταν σε μέγεθος ενός δωματίου και πολύ λίγα άτομα γνώριζαν πως να τους χειριστούν καθώς απαιτούταν εξειδικευμένες γνώσεις. Δεν υπήρχαν

περιβάλλοντα φιλικά προς το χρήστη, και το κόστος απόκτησης υπολογιστή από ένα ιδιώτη ήταν απαγορευτικό. Όταν το κόστος και το μέγεθος των υπολογιστών μειώθηκε σημαντικά και αυξήθηκε η ευκολία χρήση τους, άρχισαν να εμφανίζονται τα περισσότερα ηλεκτρονικά εγκλήματα και πολλαπλασιάστηκαν με τη διάδοση των συνδέσεων μέσω Ethernet, ARPANet και στη συνέχεια με την επέκταση του Διαδικτύου. Αρχικά, η ασφάλεια των υπολογιστών αφορούσε μόνο το στρατιωτικό τομέα, αλλά όταν εμφανίστηκαν οι πρώτοι ιοί και "σκουλήκια" και διαδόθηκαν με ταχείς ρυθμούς, έγιναν εμφανείς οι κίνδυνοι που διέτρεχαν οι απλοί χρήστες [6].

Μέχρι τις αρχές του 1970, εγκλήματα σχετικά με υπολογιστές ήταν η απλή κλοπή τους ή καταστροφή τους και αργότερα εμφανίστηκαν οι παράνομες προσβάσεις σε υπολογιστές και οι απάτες. Μέσα στη δεκαετία του ’70 τα περισσότερα εγκλήματα με υπολογιστές αντιμετωπίζονταν με τους ήδη υπάρχοντες νόμους, ωστόσο η εφαρμογή κανόνων για τη προστασία υλικών αγαθών δεν ήταν κατάλληλη για την αντιμετώπιση εγκλημάτων στο ψηφιακό κόσμο. Επιπρόσθετα, ενώ οι περισσότερες αναλύσεις forensics, που σχετίζονται με DNA, αποτυπώματα, κτλ, γινόταν από ειδικά εκπαιδευμένο προσωπικό και σε ειδικό εργαστήριο, οι αναλύσεις σε υπολογιστές γινόταν από ανεκπαίδευτους αστυνομικούς ή άλλο προσωπικό χωρίς να λαμβάνουν απαραίτητα μέτρα προστασίας των αποδείξεων, και τις περισσότερες φορές σε ακατάλληλο χώρο χωρίς τον απαραίτητο εξοπλισμό [2].

Ο πρώτος νόμος που θεσπίστηκε για την αντιμετώπιση εγκλημάτων με χρήση υπολογιστή ήταν στη Φλόριντα του 1978, ύστερα από τη μεγάλη δημοσιότητα της απάτης στο Flagler Dog Track όπου οι υπάλληλοι χρησιμοποίησαν ένα υπολογιστή για να εκτυπώσουν ψεύτικα κερδοφόρα εισιτήρια. Παρόμοιοι νόμοι άρχισαν να θεσπίζονται και στις υπόλοιπες χώρες ιδιαίτερα μετά το ξέσπασμα δημοσιευμάτων για μη εξουσιοδοτημένες προσβάσεις τη δεκαετία του ’80, καθώς και να εμφανίζονται οι πρώτες επίσημες ορολογίες για αυτού του είδους παράνομες δραστηριότητες. Μετά το 1990, όταν ξεκίνησε η διάδοση του Διαδικτύου και του World Wide Web (WWW) με αποτέλεσμα την εξάπλωση των ηλεκτρονικών παράνομων δραστηριοτήτων, άρχισαν να οργανώνονται επιχειρήσεις για την αντιμετώπισή τους. Το 1992 έγινε η πρώτη μεγάλης έκτασης επιχείρηση για την αντιμετώπιση της παιδικής πορνογραφίας στο Διαδίκτυο, η επονομαζόμενη Operation Long Arm [2].

Περαιτέρω επιρροή στην εξέλιξη των ηλεκτρονικών εγκλημάτων είχε η πρόοδος στα ασύρματα δίκτυα, στις τεχνολογίες Web, όπως Java και ActiveX, στο e-banking, στη δυνατότητα απομακρυσμένης πρόσβασης σε υπολογιστές, στην ηλεκτρονική αλληλογραφία και άλλα. Επιπλέον, αν ο δράστης έχει γνώσεις για τα βασικά πρότυπα που ακολουθούνται σε διαδεδομένα λειτουργικά συστήματα και προγράμματα, μπορεί να ενεργήσει σε μεγάλο πλήθος ανυποψίαστων χρηστών. Με τις συνδέσεις DSL ο δράστης έχει απεριόριστο χρόνο να εφαρμόσει το σχέδιό του, ενώ παλιότερα με τις dial-up συνδέσεις είχε όσο χρόνο κρατούσε μια συνεδρία, και με τις μεγάλες ταχύτητες upload ο δράστης μπορεί να "ανεβάσει" αρχεία του θύματος γρηγορότερα σε σχέση με τις παλιές συνδέσεις. Ακόμα, οι ασύρματες συνδέσεις προσφέρουν εύκολο τρόπο πρόσβασης καθώς τα κύματα υπάρχουν στον αέρα και από σχετικά μακρινή απόσταση, χωρίς να γίνει αντιληπτός, επιτυγχάνεται σύνδεση με τον υπολογιστή του θύματος [6].

1.1.1 Δημιουργία ομάδων αντιμετώπισης και ειδικού προσωπικού

Η αύξηση των συγκεκριμένων εγκλημάτων οδήγησε στην ανάγκη για κατάλληλη εκπαίδευση και δημιουργία ειδικών ομάδων αντιμετώπισής τους, υπηρεσίες κτλ. Από το 1984 κάποιες υπηρεσίες είχαν ξεκινήσει την ανάπτυξη προγραμμάτων για την εξέταση αποδείξεων από υπολογιστές. Το FBI ίδρυσε την ομάδα Computer Analysis and Response Team (CART) η οποία ήταν μοναδική για τα τότε δεδομένα. Σκοπός της ήταν η αντιμετώπιση της αυξανόμενης απαίτησης έρευνας και δίωξης ηλεκτρονικών εγκλημάτων με δομημένο τρόπο. Αργότερα εμφανίστηκαν και άλλες υπηρεσίες που ασκούσαν παρόμοιες λειτουργίες με αυτή την ομάδα στην Αμερική και σε άλλες χώρες [63].

Το 1990 άρχισαν τα πρώτα εκπαιδευτικά προγράμματα και σχηματίστηκαν εξειδικευμένες ομάδες για την έρευνα εγκλημάτων που σχετίζονται με υπολογιστές. Σύντομα όμως παρατηρήθηκε ότι οι απαιτήσεις για επεξεργασία ψηφιακών δεδομένων ήταν πολύ μεγάλες και δεν μπορούσαν να καλυφθούν από τους πόρους που είχαν διατεθεί. Ήταν αναγκαίο όλο και περισσότερο προσωπικό να έχει μια βασική εκπαίδευση πάνω στα ψηφιακά δεδομένα, και πλέον να υπάρχει μια ιεραρχία όπου ξεκινάει με τα άτομα που έχουν βασικές ικανότητες στη συλλογή και εξέταση ψηφιακών δεδομένων, ακολουθεί η ύπαρξη ειδικά εξοπλισμένων εργαστηρίων για

δύσκολες υποθέσεις και τέλος να οργανωθούν εθνικά κέντρα για την αντιμετώπιση εξειδικευμένων υποθέσεων και παρουσίαση νέων εργαλείων.

Το 1996-97 ιδρύθηκε η μονάδα Computer Forensic στο Postal Inspection Service Laboratory το οποίο συνεργαζόταν στενά με το FBI για την ανάπτυξη μεθόδων ανάλυσης ψηφιακών αποδείξεων. Αργότερα, με τη μεταφορά από την αναλογική στη ψηφιακή μορφή άρχισαν να παρουσιάζονται ελλείψεις στον όρο Computer Forensics με αποτέλεσμα την υιοθέτηση ενός νέου όρου, το Digital Forensics. Παράλληλα σχηματίζεται η οργάνωση Scientific Working Group Digital Evidence (SWGDE) με σκοπό τη δημιουργία προτύπων για ψηφιακές αποδείξεις. Επιπλέον, τεχνικές ομάδες που ασχολούνταν με την επεξεργασία ψηφιακών αποδείξεων εξελίσσονται σε επιστημονικές ομάδες για το διαχωρισμό βασικών αρμοδιοτήτων [63, 71].

Τέτοιου είδους εκπαίδευση και εξειδίκευση δεν αφορά μόνο άτομα που είναι σε ομάδες αντιμετώπισης εγκλημάτων, αλλά και οργανισμούς ή εταιρίες που διαθέτουν εξελιγμένο πληροφοριακό σύστημα με μεγάλη πιθανότητα να δεχτούν εσωτερικές ή εξωτερικές επιθέσεις, επομένως απαιτείται η συλλογή ψηφιακών αποδείξεων για την αναγνώριση και αντιμετώπισή τους. Επιπλέον, απαιτείται η ύπαρξη εξειδικευμένων ατόμων στο τομέα της ασφάλειας και τουλάχιστον με βασικές γνώσεις σχετικά με Computer Forensics [2].

1.1.2 Εξέλιξη ψηφιακής διερεύνησης

Αρχικά, η έρευνα για ψηφιακές αποδείξεις γινόταν κατευθείαν στον υπολογιστή που είχε κατασχεθεί με κίνδυνο να αλλοιωθούν δεδομένα από το υπάρχον λειτουργικό σύστημα. Επιπλέον, γινόταν στα αρχεία που υπήρχαν, αγνοώντας τα διαγραμμένα, αν και υπήρχαν ήδη από τα μέσα του 1980 προγράμματα όπως το dd των UNIX που μπορούσαν να ανακτήσουν διαγραμμένα αρχεία από το σκληρό δίσκο. Στις αρχές του 1990 ξεκίνησαν να αναπτύσσονται εργαλεία όπως το SafeBack και το DIBS για να μπορέσουν οι ερευνητές να συλλέξουν όλα τα δεδομένα χωρίς να αλλάξουν σημαντικές λεπτομέρειες. Παρόμοια προγράμματα είχαν δημιουργηθεί από την US Internal Revenue Service (IRS) και από την Royal Canadian Mounted Police (RCMP) για την έρευνα και επεξεργασία δεδομένων από υπολογιστές. Αργότερα εμφανίστηκαν εργαλεία όπως το EnCase και το FTK για να καλύψουν πιο απαιτητικές ανάγκες

και να διευκολύνουν την έρευνα με χρήση αυτοματοποιημένων μεθόδων για αποτελεσματικότερη εξέταση [2].

Η χρήση των Linux ως πλατφόρμα για την εξέταση ψηφιακών αποδείξεων έχει διευρυνθεί τα τελευταία χρόνια και εργαλεία όπως το The Sleuthkit και το SMART αναπτύχθηκαν για τη παροχή ενός φιλικού περιβάλλοντος στον χρήστη κατά την έρευνα. Επιπλέον, υπάρχουν εργαλεία για την ανάκτηση διαγραμμένων δεδομένων που έχουν καλυφθεί από άλλα όμως το κόστος τους είναι αρκετά μεγάλο για να χρησιμοποιηθούν στις περισσότερες περιπτώσεις. Τα τελευταία χρόνια έχουν αναπτυχθεί εργαλεία ειδικά για έρευνα σε συγκεκριμένες συσκευές, όπως κινητά τηλέφωνα, PDAs, κτλ, όπου διαβάζουν τα δεδομένα κατευθείαν από τη συσκευή αλλά τα περισσότερα δεν έχουν πρόσβαση σε διαγραμμένα αρχεία ή αρχεία που προστατεύονται από κωδικό. Νέα εργαλεία έκαναν την εμφάνισή τους, όπως το ZERP και το TULP, για να αντιμετωπίσουν αυτές τις περιπτώσεις [2].

Τα εργαλεία που χρησιμοποιούνται για τη συλλογή ψηφιακών αποδείξεων δεν είναι πάντα αλάνθαστα, μπορεί να παρουσιάσουν προβλήματα ή σε κάποιες περιπτώσεις να μην εντοπίζουν στοιχεία. Γι’ αυτό το λόγο απαιτείται ο έλεγχός τους για να διασφαλιστεί η αξιοπιστία των αποτελεσμάτων τους. Με αυτό το σκοπό ιδρύθηκε η ομάδα Computer Forensic Tool Testing στο National Institute of Standards and Technology, για να διεξάγει ελέγχους σε συγκεκριμένα χαρακτηριστικά διαδεδομένων forensic εργαλείων [2, 3].

1.2 Βασικοί Ορισμοί και Κατηγορίες

Η θέσπιση ορολογίας είναι απαραίτητη σε κάθε επιστημονικό τομέα για τη χρήση των όρων με κοινά αποδεκτή σημασία και τον διαχωρισμό παρόμοιων εννοιών. Αρχικά ο όρος Computer Forensics θεωρούταν συνώνυμος με τον όρο Digital Forensics, ο οποίος αποτελούσε υποκατηγορία της επιστήμης Forensic, για την έρευνα και ανάκτηση υλικού από ψηφιακές συσκευές. Σήμερα όμως με τον όρο Digital Forensics καλύπτονται όλες οι συσκευές που είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα, ενώ ο όρος Computer Forensics αποτελεί μια υποκατηγορία [72].

1.2.1 Ορισμός Digital Forensics και υποκατηγορίες

Digital Forensics: είναι η χρήση των επιστημονικά παραγόμενων και αποδεδειγμένων μεθόδων με σκοπό τη συντήρηση, τη συλλογή, την επικύρωση, τον προσδιορισμό, την ανάλυση, την ερμηνεία, την τεκμηρίωση, και την παρουσίαση ψηφιακών στοιχείων που προήλθαν από ψηφιακές πηγές με σκοπό τη διευκόλυνση ή την προώθηση της αναδημιουργίας των γεγονότων που βρέθηκαν να είναι εγκληματικά ή να βοηθήσει στη πρόληψη μη εξουσιοδοτημένων ενεργειών που αποδείχτηκαν να είναι αποδιοργανωτικές σε οργανωμένες διαδικασίες [42].

Computer Forensics: είναι η επιστήμη της απόκτησης, διατήρησης και καταγραφής αποδείξεων από ψηφιακές ηλεκτρονικές αποθηκευτικές συσκευές, όπως υπολογιστές, PDAs, ψηφιακές κάμερες, κινητά τηλέφωνα και άλλες αποθηκευτικές συσκευές. Θα πρέπει να γίνουν με τέτοιο τρόπο σχεδιασμένο να διατηρήσουν την αποδεικτική αξία των αποδείξεων και να διασφαλίσουν την αποδεκτικότητα σε νομικές διαδικασίες [19].

Στα πλαίσια της εργασίας θα χρησιμοποιείται ο όρος "υπολογιστικά συστήματα" και "υπολογιστής" με μια ευρεία έννοια, οι οποίοι θα καλύπτουν επιτραπέζιους υπολογιστές, φορητούς υπολογιστές και γενικά οποιαδήποτε υπολογιστική συσκευή στην οποία περιέχονται ψηφιακά δεδομένα και μπορεί να εφαρμοστεί η επιστήμη των Computer Forensics.

Άλλες υποκατηγορίες των Digital Forensics είναι [72]:

- **Network Forensics / Internet Forensics / Cyberforensics:** περιλαμβάνει τεχνολογίες και μεθοδολογίες για τη συλλογή, διατήρηση και ανάλυση ψηφιακών δεδομένων από δίκτυα για έρευνα και την επιβολή νόμου [41].
- **Mobile Device Forensics:** αφορά τη συλλογή ψηφιακών δεδομένων από φορητές συσκευές.
- **Database Forensics:** σχετίζεται με την εξέταση βάσεων δεδομένων και των σχετικών μεταδεδομένων.

Οι υποθέσεις που απαιτούν τη χρήση των Computer Forensics μπορούν να χωριστούν σε δύο βασικές κατηγορίες, τις αστικές και τις εγκληματικές, όπου κάποια σημεία της έρευνάς τους είναι κοινά μεταξύ τους ενώ άλλα μπορεί να διαφέρουν αρκετά.

- **Αστικές υποθέσεις:** είναι δικαστικές διαδικασίες για την επίλυση διαφορών ανάμεσα σε δύο άτομα, επιχειρήσεις ή οργανισμούς.
- **Εγκληματικές υποθέσεις:** περιπτώσεις όπου ένα πρόσωπο κατηγορείται για τη διάπραξη ενός ή περισσότερων εγκλημάτων.

Στις αστικές υποθέσεις κάθε διάδικος προσκομίζει τις αποδείξεις που επικαλείται και είναι καταρχήν υπεύθυνος για την αξιοπιστία τους, η οποία ωστόσο ελέγχεται από το δικαστήριο. Αντίθετα στις εγκληματικές υποθέσεις η συλλογή και χρήση αποδείξεων συνδέεται καταρχήν με περισσότερες απαιτήσεις. Ανάλογα με τη φύση της έρευνας, η οποία διεξάγεται από τις αρμόδιες, δημόσιες αρχές, απαιτούνται συνήθως ανάλογα εντάλματα. Οι αστικές υποθέσεις είναι λιγότερο αυστηρές σε σχέση με τις εγκληματικές λόγω της φύσης τους. Παρόλα αυτά δεν πρέπει να αντιμετωπίζονται επιπόλαια και τα άτομα που έχουν αναλάβει την έρευνα πρέπει να διατηρούν τον επαγγελματισμό και την υπευθυνότητάς τους για να μην διακινδυνευτεί η υπόθεση [5].

Οι εγκληματικές υποθέσεις μπορούν να διαχωριστούν περαιτέρω σε [41]:

- **Ηλεκτρονικό έγκλημα** (electronic crime): ορίζεται ως μια παράνομη πράξη που πραγματοποιείται χρησιμοποιώντας έναν υπολογιστή ή ηλεκτρονικά μέσα.
- **Κυβερνοέγκλημα** (cyber crime): είναι ένα ηλεκτρονικό έγκλημα που πραγματοποιείται χρησιμοποιώντας το Διαδίκτυο, ή ένα έγκλημα του οποίου «η σκηνή του εγκλήματος» είναι το Διαδίκτυο.

Ο ρόλος όμως ενός υπολογιστή σε μία παράνομη δραστηριότητα μπορεί να είναι διαφορετικός, δηλαδή [2]:

- Ένας υπολογιστής μπορεί να είναι το *αντικείμενο* της παράνομης δραστηριότητας, όταν δηλαδή επηρεάζεται από την εγκληματική δράση, για παράδειγμα να κλαπεί ή να καταστραφεί.
- Ένας υπολογιστής μπορεί να είναι το *αντικείμενο μελέτης* της παράνομης πράξης, όταν είναι το περιβάλλον που εκτελέστηκε η παράνομη πράξη, για παράδειγμα όταν μολυνθεί από ιό ή να το υποβαθμίσει με κάποιο τρόπο προς όφελος του δράστη.
- Ένας υπολογιστής μπορεί να χρησιμοποιηθεί ως *εργαλείο* για τη διάπραξη ή σχεδιασμό του εγκλήματος, για παράδειγμα να χρησιμοποιηθεί για τη πλαστογράφηση εγγράφων ή να παραβιάσει άλλους υπολογιστές.

- Το *σύμβολο* του ίδιου του υπολογιστή μπορεί να χρησιμοποιηθεί για να εκφοβίσει ή να εξαπατήσει, για παράδειγμα ο δράστης να υποστηρίξει ότι έχει ένα πρόγραμμα που μπορεί να κερδίσει λεφτά και να επενδύσουν σε αυτό ανυποψίαστοι πελάτες.
- Ή μπορεί να αποτελέσει *πηγή* ψηφιακών αποδεικτικών στοιχείων για μια έρευνα.

Ο διαχωρισμός του υπολογιστικού συστήματος ως αντικείμενο ή αντικείμενο μελέτης σε μια παράνομη δραστηριότητα διευκολύνει στην κατανόηση των προθέσεων του δράστη. Ο συμβολικός χαρακτήρας του υπολογιστικού συστήματος εμφανίζεται συνήθως όταν το υπολογιστικό σύστημα είναι ο στόχος και απεικονίζει το πιθανό κίνητρο του δράστη. Αρκετές φορές το υπολογιστικό σύστημα δεν έχει χρησιμοποιηθεί με κάποιο τρόπο κατά τη διάπραξη αλλά αποτελεί πηγή αποδείξεων για ένα έγκλημα ότι όντως έγινε [2].

1.2.2 Ψηφιακά Δεδομένα και Αποδεικτικά Στοιχεία

Ο σκοπός των Computer Forensics είναι η έρευνα σε ψηφιακές αποθηκευτικές συσκευές, εντοπισμό και συλλογή δεδομένων που σχετίζονται με την υπόθεση, ανάλυσή τους και παρουσίαση των ψηφιακών αποδεικτικών στοιχείων που θα ανακαλυφθούν. Για την επίτευξη αυτού του στόχου είναι απαραίτητο να οριστούν και να κατηγοριοποιηθούν τα ψηφιακά δεδομένα και οι πηγές τους ώστε να διευκολυνθεί η διαδικασία της έρευνας, αλλά και οι ψηφιακές αποδείξεις καθώς αποτελούν το αποτέλεσμα της όλης διαδικασίας.

1.2.2.1 Χαρακτηριστικά και Κατηγορίες Ψηφιακών Δεδομένων

Το κύριο χαρακτηριστικό των ψηφιακών δεδομένων είναι ότι μεταβάλλονται εύκολα που μπορεί να οδηγήσει από μικρές αλλαγές μέχρι τη πλήρη διαγραφή τους. Λόγω της ευπάθειάς τους θα πρέπει να ανακτούνται και να χειρίζονται με ιδιαίτερη προσοχή. Τα ψηφιακά δεδομένα μπορούν να καταστραφούν, να φθαρούν ή να μετατραπούν με ποικίλους τρόπους όπως με ακατάλληλες διεργασίες ή εντολές, παγίδες, μαγνητικά πεδία, ακόμα και με την απλή εκκίνηση του υπολογιστή [19].

Τα δεδομένα που πρέπει να εξεταστούν κατά τη διάρκεια μιας ψηφιακής διερεύνησης διακρίνονται σε δύο βασικές κατηγορίες, στα ευμετάβλητα δεδομένα και στα μόνιμα δεδομένα [52].

Ευμετάβλητα δεδομένα (Volatile Data)

Ευμετάβλητα δεδομένα είναι αυτά τα οποία χάνονται όταν το υπολογιστικό σύστημα απενεργοποιηθεί. Είναι αποθηκευμένα στη μνήμη του συστήματος, δηλαδή σε καταγραφές (registries), κρυφή μνήμη (cache), στη μνήμη RAM και άλλους χώρους προσωρινής αποθήκευσης. Λόγω του ιδιαίτερου αυτού χαρακτηριστικού τους μπορούν εύκολα να μετατραπούν ή να χαθούν οπότε η συλλογή αυτών των δεδομένων απαιτείται να γίνει όσο το δυνατόν πιο γρήγορα [52].

Τα ευμετάβλητα δεδομένα περιέχουν πληροφορίες σχετικά με τις τρέχουσες ρυθμίσεις του συστήματος και την κατάσταση του υπολογιστή, όπως στοιχεία για το προφίλ του συστήματος, ημερομηνία και ώρα συστήματος, ιστορικό εντολών, εκτελούμενες διεργασίες και ανοιχτά αρχεία, χρήστες που είναι συνδεδεμένοι, προγράμματα και βιβλιοθήκες που χρησιμοποιούνται. Επιπλέον μπορούν να ανακτηθούν πληροφορίες για τη κατάσταση του δικτύου που μπορεί να είναι συνδεδεμένος ο υπολογιστής, όπως ανοιχτές συνδέσεις και υποδοχές, πληροφορίες σχετικά με το δρομολογητή (router) και τις ρυθμίσεις του, και άλλα [52].

Μόνιμα Δεδομένα (Persistent Data)

Μόνιμα λέγονται τα δεδομένα τα οποία παραμένουν αμετάβλητα, όταν απενεργοποιηθεί ο υπολογιστής. Είναι αποθηκευμένα σε σκληρούς δίσκους ή φορητά αποθηκευτικά μέσα συμπεριλαμβανομένου κινητά τηλέφωνα, μνήμες flash, PDAs. Τα μόνιμα δεδομένα είναι ιδιαίτερα σημαντικά καθώς είναι το πιο πιθανό να περιλαμβάνουν τις αποδείξεις που αναζητούνται κατά τη διεξαγωγή της έρευνας όπως αρχεία, ηλεκτρονική αλληλογραφία, διαγραμμένα αρχεία, κτλ [52].

Τύποι μόνιμων δεδομένων είναι [52, 19]:

- **Αρχεία συστήματος:** δεδομένα του λειτουργικού συστήματος του υπολογιστή που μπορούν να προσφέρουν πληροφορίες σχετικά με τις ενέργειες του χρήστη όπως ιστοσελίδες που επισκέφτηκε, cookies τα οποία μπορεί να περιλαμβάνουν μεταξύ άλλων και κωδικούς προστασίας.

- **Προσωρινά αρχεία:** αρχεία που έχουν δημιουργηθεί από προγράμματα ή το λειτουργικό σύστημα του υπολογιστή
- **Διαγραμμένα αρχεία:** αρχεία που υπάρχουν ακόμα ενώ έχουν διαγραφεί είτε κομμάτια τους που βρίσκονται σε νωθρό διάστημα (slack space) ή μη καταχωρημένο (unallocated space). Είναι δεδομένα που δεν έχουν επικαλυφθεί με καινούρια δεδομένα.
- **Εφεδρικά αντίγραφα:** αντίγραφα δεδομένων που δημιουργούνται από τους χρήστες ή οι εταιρίες για τη διασφάλιση των πληροφοριών τους, Συνήθως αποθηκεύονται σε φορητές συσκευές.
- **Μεταδεδομένα:** πληροφορίες σχετικά με τα αρχεία όπως ημερομηνία και ώρα δημιουργίας, χρήστης που το δημιούργησε, κτλ.
- **Δεδομένα επικοινωνίας:** δεδομένα που δημιουργούνται κατά τη διάρκεια μιας επικοινωνίας όπως με ποιον έχει επικοινωνήσει ο χρήστης, πότε έγινε, αρχεία που στάλθηκαν. Τα δεδομένα αυτά μπορεί να είναι αποθηκευμένα είτε στον υπολογιστή του χρήστη ή σε άλλες συσκευές του δικτύου όπως δρομολογητές ή συστήματα ανίχνευσης εισβολών.

1.2.2.2 Πηγές Ψηφιακών Δεδομένων

Η συνεχής εξέλιξη της τεχνολογίας και η αύξηση ηλεκτρονικών συσκευών που μπορούν να αποθηκεύσουν ή να μεταδώσουν δεδομένα προσφέρουν πολλές πιθανές τοποθεσίες που θα πρέπει να ελεγχθούν για ανεύρεση ψηφιακών αποδείξεων.

Οι πιο βασικοί τύποι πηγών δεδομένων είναι [64, 5]:

- **Υπολογιστικά συστήματα**, δηλαδή οι επιτραπέζιοι υπολογιστές, οι φορητοί, οι εξυπερετητές (servers)
- **Αποθηκευτικές συσκευές**, δηλαδή εσωτερικοί και εξωτερικοί σκληροί δίσκοι, DVDS, CDs, κάρτες μνήμης
- **Φορητές συσκευές**, δηλαδή κινητά και έξυπνα τηλέφωνα, PDAs, iPods
- **Περιφερειακές συσκευές**, δηλαδή πληκτρολόγιο, ποντίκι, κάμερα, συσκευές VoIP, εκτυπωτές
- **Συσκευές αποθήκευσης δικτύων**, όπως δρομολογητές, ασύρματα σημεία πρόσβασης

- Άλλες συσκευές όπως ψηφιακές φωτογραφικές μηχανές, συσκευές παρακολούθησης, καταγραφείς ήχου ή εικόνας, κονσόλες παιχνιδιών, GPS, ψηφιακοί τηλεφωνητές

Οι πηγές των ψηφιακών αποδείξεων μπορούν επίσης να διακριθούν και σε τρεις βασικές κατηγορίες [2]:

- **Ανοιχτά υπολογιστικά συστήματα:** οι παραδοσιακοί υπολογιστές με πληκτρολόγιο, ποντίκι, σκληρό δίσκο, οι φορητοί υπολογιστές και εξυπηρετητές (servers)
- **Συστήματα Επικοινωνίας:** παραδοσιακά τηλεφωνικά συστήματα, ασύρματα συστήματα τηλεπικοινωνίας
- **Ενσωματωμένα υπολογιστικά συστήματα:** κινητά τηλέφωνα, προσωπικοί ψηφιακοί βοηθοί (PDAs), έξυπνες κάρτες και άλλα συστήματα που έχουν ενσωματωμένα υπολογιστές μπορούν να περιέχουν ψηφιακές αποδείξεις.

1.2.2.3 Χαρακτηριστικά και Κατηγορίες Ψηφιακών Αποδεικτικών Στοιχείων

Ο σκοπός της ψηφιακής διερεύνησης είναι η ανακάλυψη ψηφιακών αποδεικτικών στοιχείων με τρόπο που θα παραμείνουν ακέραια και αξιόπιστα. Ψηφιακά αποδεικτικά στοιχεία ονομάζονται οι πληροφορίες με αποδεικτική αξία, οι οποίες είναι αποθηκευμένες ή διαβιβάζονται σε ψηφιακή μορφή [63]. Μπορεί να αποτελούν δεδομένα που συλλέχθηκαν αυτούσια από το υπολογιστικό σύστημα ή να είναι αποτέλεσμα αναλύσεων και άλλων ενεργειών του ερευνητή.

Κατά τη διάρκεια της έρευνας μπορούν να διακριθούν σε [63]:

- **Πρωτότυπα ψηφιακά αποδεικτικά στοιχεία** (Original Digital Evidence): Φυσικά στοιχεία και αντικείμενα με δεδομένα τα οποία συνδέονται με αυτά τα στοιχεία κατά την διάρκεια της απόκτησης ή της σύλληψης.
- **Αντίγραφα ψηφιακά αποδεικτικά στοιχεία** (Duplicate Digital Evidence): Μια ακριβής ψηφιακή αναπαραγωγή όλων των αντικειμένων με δεδομένα που περιέχονται στο αρχικό φυσικό στοιχείο.

Ένας από τους μεγαλύτερους κινδύνους των ψηφιακών αποδείξεων είναι η λανθασμένη μεταχείριση των δεδομένων, που συμβαίνει κυρίως στις περιπτώσεις όπου, όταν εμφανίζεται ένα πρόβλημα, η πρώτη κίνηση είναι να διορθωθεί χωρίς να ληφθεί υπόψη ότι μπορεί να πρόκειται

να κακόβουλη πράξη, με αποτέλεσμα να χαθούν δεδομένα που θα βοηθούσαν στην μετέπειτα έρευνα. Ακόμα κι αν έχουν διατηρηθεί κάποια δεδομένα, έχει εκτεθεί η αποδεικτική τους αξία [19].

1.3 Διαφορές Ψηφιακής και Φυσικής Μορφής

Η ψηφιακή αναπαράσταση των αντικειμένων έχει αντικαταστήσει ένα μεγάλο αριθμό φυσικών στοιχείων και συνεχώς αυξάνεται. Οποιαδήποτε πληροφορία σε έντυπη μορφή μπορεί πλέον να μετατραπεί σε ψηφιακή καθώς και διάφορες δραστηριότητες πραγματοποιούνται με ένα νέο ψηφιακό τρόπο. Από αυτήν την εξέλιξη δεν θα μπορούσε να μείνουν ανεπηρέαστα η διερεύνηση παράνομων δράσεων και τα αποδεικτικά στοιχεία που χρειάζονται για την καταδίκη των υπαιτίων.

Παρακάτω δίνονται κάποιοι βασικοί ορισμοί για να τονίσουν τη διαφορά της φυσικής μορφής με τη ψηφιακή [10]:

- **Φυσικές Αποδείξεις:** Τα φυσικά αντικείμενα που μπορούν να καθορίσουν ότι ένα έγκλημα έχει διαπραχτεί, μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του θύματός του, ή μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του δράστη του. Παραδείγματα φυσικών αποδείξεων είναι ο υπολογιστής, ο σκληρός δίσκος, ένα CD.
- **Ψηφιακές Αποδείξεις:** Τα ψηφιακά στοιχεία που μπορούν να καθορίσουν ότι ένα έγκλημα έχει διαπραχτεί, μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του θύματός του, ή μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του δράστη του. Τα στοιχεία στη μνήμη, στο σκληρό δίσκο, ή σε ένα τηλέφωνο κυττάρων είναι παραδείγματα των ψηφιακών στοιχείων.
- **Φυσική σκηνή του εγκλήματος:** Το φυσικό περιβάλλον όπου υπάρχουν φυσικές αποδείξεις ενός εγκλήματος ή ενός γεγονότος. Το περιβάλλον όπου το πρώτο έγκλημα εμφανίστηκε είναι η αρχική φυσική σκηνή του εγκλήματος και οι επόμενες σκηνές είναι δευτερεύουσες φυσικές σκηνές εγκλήματος.

- **Ψηφιακή σκηνή του εγκλήματος:** Το εικονικό περιβάλλον που δημιουργείται από το λογισμικό και το υλικό όπου τα ψηφιακά στοιχεία ενός εγκλήματος ή ενός γεγονότος υπάρχουν. Το περιβάλλον όπου το πρώτο έγκλημα εμφανίστηκε είναι η αρχική ψηφιακή σκηνή εγκλήματος και οι επόμενες σκηνές καλούνται δευτεροβάθμιες ψηφιακές σκηνές εγκλήματος.

Οι διαφορές των φυσικών με των ψηφιακών στοιχείων είναι αρκετά εμφανείς. Στη σημερινή εποχή τα ψηφιακά έγγραφα παράγονται με πολύ μεγαλύτερο ρυθμό σε σχέση με τα φυσικά. Καθημερινά δημιουργούνται εκατομμύρια αρχεία κειμένου, ήχου, εικόνας, αποστέλλεται ηλεκτρονική αλληλογραφία, επεκτείνονται βάσεις δεδομένων. Αυτά τα αρχεία δεδομένων μπορούν να αποθηκευτούν σε πολλά σημεία, αλλά ακόμα και ένα αρχείο μπορεί χωριστεί σε κομμάτια όπου το καθένα βρίσκεται σε διαφορετικές θέσεις ανάλογα με τη δομή του μέσου που είναι αποθηκευμένο. Ενώ αντίθετα ένα φυσικό έγγραφο βρίσκεται ολόκληρο σε μια τοποθεσία [19].

Η αντιγραφή και η μεταβολή των ψηφιακών αρχείων γίνεται πολύ πιο εύκολα, γρήγορα και οικονομικά σε αντίθεση με τα φυσικά. Επιπλέον, με την αντιγραφή δεν μειώνεται η ποιότητα των δεδομένων σε ψηφιακή μορφή, ενώ στα φυσικά δεδομένα, όπου είναι δυνατή η αντιγραφή, σταδιακά ελαττώνεται η ποιότητά τους. Ακόμα η μετατροπή των ψηφιακών αρχείων μπορεί σε αρκετές περιπτώσεις να γίνει με τέτοιο τρόπο που να μην αφήνει σημάδια αλλαγής, κάτι το οποίο δεν γίνεται εύκολα σε φυσικά αρχεία. Ένα επιπλέον χαρακτηριστικό των ψηφιακών αρχείων είναι ότι έχουν δεδομένα τα οποία μπορούν να αλλάξουν ανά πάσα στιγμή χωρίς ανθρώπινη παρέμβαση, όπως για παράδειγμα σελίδες στον Διαδίκτυο που ανανεώνουν το περιεχόμενό τους αυτόματα [19].

Στη περίπτωση της ψηφιακής διερεύνησης σε σχέση με τη φυσική παρατηρούνται πολλές διαφορές. Κατ' αρχάς δεν μπορούν να βρεθούν μάρτυρες καθώς η παράνομη πράξη εκτελείται μέσα σε υπολογιστές και δίκτυα. Οι αποδείξεις πλέον δεν είναι εμφανείς σε διάφορα σημεία στο τόπο του συμβάντος κυρίως γιατί δεν είναι πάντα εύκολο να οριστεί ποιος είναι ο τόπος του εγκλήματος, αλλά μπορούν να βρεθούν ύστερα από ανάλυση στον υπολογιστή του δράστη, κατά τη μεταφορά δεδομένων, ή στο πεδίο επιρροής τρίτων, όπως των παρόχων υπηρεσιών Διαδικτύου. Επιπλέον, ο μη εύκολος προσδιορισμός τόπου προκαλεί εμπόδια στην έκδοση

ενταλμάτων έρευνας και στη σωστή εξουσιοδότηση ατόμων για έρευνα με αποτέλεσμα να διακινδυνεύεται η ιδιωτικότητα πέρα του δράστη και του θύματος, αλλά και τρίτων ατόμων [38].

Μία βασική διαφορά των ψηφιακών αποδείξεων σε σχέση με τις φυσικές αποδείξεις είναι ότι δεν μπορεί να γίνει καμία ανάλυση στα πρωτότυπα αρχεία λόγω της μεγάλης πιθανότητας να μετατραπούν τα δεδομένα. Γι' αυτό το λόγο δημιουργούνται πιστά αντίγραφα για την εξασφάλιση της ακεραιότητάς τους. Επιπλέον, σε περίπτωση παρουσίασής τους σε δικαστήρια δεν χρησιμοποιούνται οι πρωτότυπες ψηφιακές αποδείξεις, αλλά αντίγραφά τους, εκτυπωμένα αρχεία ή η τελική αναφορά από την ανάλυση που έγινε. Αντίθετα, οι φυσικές αποδείξεις κατά ένα μεγάλο ποσοστό μπορούν να γίνουν περαιτέρω αναλύσεις στα πρωτότυπα χωρίς να διακινδυνευτεί η αποδεικτική τους αξία, και επίσης μπορούν να παρουσιαστούν απευθείας στο δικαστήριο [10].

2 Ψηφιακή έρευνα

Οι ορισμοί και κατηγοριοποιήσεις που γίνανε στο προηγούμενο κεφάλαιο είναι απαραίτητοι για τη διευκόλυνση της διεξαγωγής μιας ψηφιακής έρευνας. Για τις ανάγκες της συγκεκριμένης εργασίας ψηφιακή έρευνα ορίζεται η διαδικασία κατά την οποία εφαρμόζονται ειδικές τεχνικές σε υπολογιστικά συστήματα για τον εντοπισμό ψηφιακών δεδομένων που σχετίζονται με μία υπόθεση.

Η διερεύνηση ψηφιακών αποδείξεων είναι ιδιαίτερα χρονοβόρα και δαπανηρή, αλλά είναι σημαντική για την δίκαιη επίλυση ψηφιακών υποθέσεων. Για την ορθή εκτέλεση και αξιοποίηση των πορισμάτων της έρευνας πρέπει να πληρούνται ορισμένοι βασικοί όροι. Πρώτον, απαιτείται η διατήρηση της ακεραιότητας και αυθεντικότητας των δεδομένων με την εφαρμογή επιστημονικών μεθόδων για να αποφευχθεί τυχόν μεταβολή τους. Δεύτερον, η έρευνα πρέπει να διεξάγεται από άτομα κατάλληλα εκπαιδευμένα τα οποία θα καταγράφουν πλήρως κάθε ενέργεια και θα είναι υπεύθυνα για την τήρηση των ανάλογων νόμων και κανόνων. Τρίτον, είναι απαραίτητη η εξουσιοδότηση, κατά προτίμηση γραπτή, για τη πραγματοποίηση οποιασδήποτε έρευνας [28, 20]. Τέλος, τα στοιχεία που θα συλλεχθούν πρέπει να αξιόλογα, ουσιώδη και σχετικά με την υπόθεση που διερευνάται [6].

Έχουν παρουσιαστεί πολλών ειδών μέθοδοι ψηφιακής έρευνας, κάποιες από αυτές θα περιγραφθούν σε επόμενο κεφάλαιο. Παρ' όλες τις διαφορές στα βήματα που ακολουθούν, υπάρχουν κάποια βασικά κοινά στοιχεία και σημεία που πρέπει να δοθεί ιδιαίτερη προσοχή και αναλύονται στη συνέχεια.

2.1 Προετοιμασία

Πριν ξεκινήσει μια έρευνα για ψηφιακές αποδείξεις, το άτομο ή η ομάδα που θα την αναλάβει πρέπει να είναι κατάλληλα εκπαιδευμένο, ειδικευμένο στα Computer Forensics και εφοδιασμένο με τα απαραίτητα εργαλεία. Οι γνώσεις του δεν θα περιορίζονται μόνο στη χρήση των εργαλείων, αλλά θα διευρύνονται σε εις βάθος κατανόηση τόσο των εργαλείων όσο και της δομής των υπολογιστικών συστημάτων. Όλα τα μέσα που θα χρησιμοποιηθούν για αντιγραφή και μεταφορά δεδομένων θα πρέπει να είναι αποστειρωμένα, δηλαδή να έχει γίνει πλήρης

διαγραφή όλων των προηγούμενων αρχείων με ειδικά εργαλεία πριν χρησιμοποιηθούν ώστε να αποφευχθεί η εμφάνιση δεδομένων από παλιότερες υποθέσεις. Ιδανικότερα, θα πρέπει να είναι καινούρια, κατά προτίμηση αναλώσιμα, αλλά αυτό δεν είναι πάντοτε εφικτό. Επιπρόσθετα, οι εταιρίες πρέπει να ακολουθούν τα διεθνή πρότυπα και να διαθέτουν ένα καταστατικό Standard Operating Procedures στο οποίο θα περιγράφουν τη στρατηγική που θα ακολουθήσουν στη περίπτωση εμφάνισης κάποιου περιστατικού [20].

2.1.1 Ετοιμότητα Οργανισμών

Σημαντικοί οργανισμοί, εταιρίες και φορείς κρίσιμων υποδομών, όπου η εμφάνιση ενός σοβαρού περιστατικού που απαιτεί Computer Forensics είναι σημαντικά υψηλή, πέρα από τα ανάλογα μέτρα ασφαλείας που απαιτείται να λάβουν και το συνεχή έλεγχό τους, είναι αναγκαίο να είναι έτοιμοι στη περίπτωση που χρειαστεί να διεξαχθεί μία ψηφιακή διερεύνηση. Η λεγόμενη Δικανική Ετοιμότητα (Forensic Readiness) είναι η κατάσταση του οργανισμού όπου εφαρμόζονται ορισμένοι έλεγχοι προκειμένου να διευκολύνουν τις ψηφιακές διαδικασίες forensic και να διατηρούν στοιχεία κατά την αναμονή μη εξουσιοδοτημένων ενεργειών που έχουν ως στόχο την αποδιοργάνωση προγραμματισμένων διαδικασιών των οργανισμών [26].

Η ετοιμότητα αφορά τη συλλογή και διατήρηση ψηφιακών στοιχείων πριν την εμφάνιση κάποιου συμβάντος. Δεν περιορίζεται μόνο στον έλεγχο αρχείων καταγραφών, σκληρών δίσκων ή συστήματα ανίχνευσης εισβολών, αλλά επεκτείνεται και σε καταγραφές από κάμερες παρακολούθησης, συστήματα ελέγχου πρόσβασης και άλλα. Η εκτέλεση αυτών των μέτρων επιβάλλεται όταν ο οργανισμός συνεργάζεται στενά με τη κυβέρνηση ή υπάρχει σχετική νομική ρύθμιση, για παράδειγμα όταν διακινδυνεύονται προσωπικά δεδομένα πολιτών [54].

Η εξασφάλιση της ετοιμότητας είναι πολυδάπανη και απαιτεί προσωπικό κατάλληλα εκπαιδευμένο, συνεπώς εφαρμόζεται σε περιπτώσεις όπου μετά την ανάλυση επικινδυνότητας ο υπολειπόμενος κίνδυνος είναι αρκετά υψηλός. Το κόστος θα είναι μεγαλύτερο ιδιαίτερα εάν οι διοικητικές διαδικασίες ασφάλειας πληροφοριών είναι σε πρώιμο στάδιο. Τα οφέλη όμως από μία τέτοια διαδικασία είναι ανταποδοτικά επειδή αυξάνεται η αποτελεσματικότητα των διερευνήσεων ψηφιακών αποδείξεων και μειώνεται ο χρόνος και το κόστος της έρευνας. Όταν υπάρχουν τα κατάλληλα μέτρα ασφάλειας, η ετοιμότητα του οργανισμού μπορεί να

εξασφαλιστεί άμεσα καθώς αποτελεί περισσότερο μια διαδικαστική και εκπαιδευτική διαδικασία παρά τεχνολογική [26 , 54].

Κάποια βασικά βήματα για την αποτελεσματική εφαρμογή μέτρων ετοιμότητας είναι η ανάπτυξη σεναρίων που απαιτούνται ψηφιακές αποδείξεις, η αναγνώριση πηγών και όλων των πιθανών τύπων αποδείξεων, καθώς και ο προσδιορισμός των απαιτήσεων συλλογής δεδομένων. Στη συνέχεια ορίζονται μέτρα για την ασφαλή συλλογή, αποθήκευση και νομική διαχείριση των αποδεκτών πειστηρίων. Επόμενο βήμα είναι ο εντοπισμός μειζόνων περιστατικών και των αναγκαίων συνθηκών για τη διεξαγωγή πλήρους έρευνας. Η εκπαίδευση του προσωπικού και η κατανόηση του ρόλου καθενός είναι σημαντικά για την αξιόλογη συλλογή αποδείξεων και τη διευκόλυνση της έρευνας. Τέλος, μια νομική επισκόπηση όλων των μέτρων που θα ληφθούν διασφαλίζει την αξιοπιστία και αποδοχή των αποτελεσμάτων από τη συλλογή αποδείξεων [54].

2.2 Αρχικές ενέργειες

Οι αρχικές ενέργειες ενός ερευνητή κατά την είσοδο στο χώρο του συμβάντος είναι μια πρώτη αναγνώριση του υπολογιστικού συστήματος που υπάρχει για να χρησιμοποιηθεί το ανάλογο λογισμικό και υλικό. Πρέπει να ληφθούν όλες οι απαραίτητες προφυλάξεις για να αποφευχθεί οποιαδήποτε ‘‘μόλυνση’’ της περιοχής. Για να μειωθεί ο κίνδυνος απώλειας, μετατροπής ή φθοράς των ψηφιακών αποδείξεων, όλες οι περιοχές, εσωτερικά και εξωτερικά, πρέπει να προστατευθούν όσο το δυνατόν πιο γρήγορα με διαδικασίες που ακολουθούν τις κατάλληλες νομικές και τεχνικές οδηγίες. Επιπλέον πρέπει να αποτραπεί σε άλλους να χρησιμοποιήσουν τις συσκευές που θα βρεθούν ή να γίνει χρήση άλλων ηλεκτρομαγνητικών συσκευών [28].

Εάν υπάρχουν εκτυπωτές ενεργοποιημένοι πρέπει να επιτραπεί η ολοκλήρωση της εκτύπωσης που τυχόν πραγματοποιείται εκείνη τη στιγμή. Επιπλέον, πρέπει να εξακριβωθεί εάν ο υπολογιστής είναι ενεργοποιημένος, απενεργοποιημένος ή σε κατάσταση αναμονής το οποίο συνήθως φαίνεται αν οι φωτεινές ενδείξεις της κεντρικής μονάδας του υπολογιστή που αντιστοιχούν στο σκληρό δίσκο και στον επεξεργαστή είναι αναμμένα. Στη περίπτωση που είναι ενεργοποιημένος ο υπολογιστής πρέπει να γίνουν προσεχτικά οι επόμενες κινήσεις για να αποφευχθεί μεταβολή των δεδομένων [28].

2.2.1 Καθορισμός Προτεραιοτήτων

Γενικά, η διεξαγωγή μιας έρευνας απαιτείται να ολοκληρωθεί όσο πιο γρήγορα και αποτελεσματικά γίνεται για την άμεση εκμετάλλευση των δεδομένων ειδικά σε επείγουσες καταστάσεις αλλά και για τη μείωση της διατάραξης του χώρου. Όμως ο εντοπισμός ψηφιακών αποδείξεων, ειδικά σε περιπτώσεις που πρέπει να ερευνηθούν τεράστιες αποθήκες δεδομένων, ίσως και σε terabytes μέγεθος, είναι χρονοβόρος και ακριβός. Επιπλέον, η ανάκτηση δεδομένων από τους υπολογιστές με τρόπο που να διατηρηθεί η αξιοπιστία τους δεν είναι εύκολη καθώς μπορούν εύκολα να μετατραπούν κατά λάθος ή επίτηδες. Ο καθορισμός προτεραιοτήτων κατά τη διάρκεια μιας έρευνας ψηφιακών αποδείξεων συμβάλει στην επίτευξη των ιδιαίτερων στόχων κάθε υπόθεσης [20].

Για να εφαρμοστεί αποδοτικός καθορισμός προτεραιοτήτων στις διαδικασίες που πρέπει να γίνουν εξετάζονται οι προτεραιότητες και τα χρονικά περιθώρια, η φύση της υπόθεσης, χρονικοί παράγοντες και άλλα. Επιπλέον, λαμβάνουν προτεραιότητα αντικείμενα που περιέχουν ψηφιακά δεδομένα και χρειάζονται για άλλου είδους αναλύσεις, για παράδειγμα εύρεση δακτυλικών αποτυπωμάτων ή DNA, και αντικείμενα που είναι πιο πιθανόν να παρέχουν τις περισσότερες πληροφορίες ή αποτελούν τους καλύτερους στόχους για δεδομένα με αποδεικτική αξία [20].

2.2.2 Καταγραφή χώρου

Ο τόπος του συμβάντος πρέπει να φωτογραφηθεί, συμπεριλαμβανομένου του υπολογιστή, των συνδέσεων, εικόνων από οθόνες και άλλα, έτσι ώστε να είναι διαθέσιμα στοιχεία του χώρου. Το πρώτο άτομο που θα εισέλθει στη τοποθεσία ενός ηλεκτρονικού εγκλήματος έχει την υποχρέωση να διατηρήσει όσο το δυνατόν περισσότερες αποδείξεις για τη μετέπειτα εξέτασή τους. Αυτό σημαίνει ότι πρέπει να αναγνωρίσει και να καταγράψει στοιχεία που μπορούν να βρεθούν σε όλων των ειδών συσκευές (υπολογιστές, PDAs, κινητά τηλέφωνα, RAM, εκτυπωτές), άλλα μέσα (συστήματα, έξυπνες κάρτες, κτλ) ακόμα και σε έντυπα αντίγραφα που υπάρχουν στον χώρο [20].

2.2.3 Προφυλάξεις κατά τη μεταφορά

Είναι ζωτικής σημασίας όλα τα αντικείμενα που θα κατασχεθούν κατά την αρχική έρευνα να διατηρηθούν ασφαλείς. Κατά τη διάρκεια της κατάσχεσης και μεταφοράς των αντικειμένων που περιέχουν αποδείξεις πρέπει να ληφθούν μέτρα για τη προστασία από εξωτερικούς παράγοντες όπως ηλεκτρικούς κινδύνους, μαγνητικά ή στατικά πεδία και ακραίες θερμοκρασίες. Οι συσκευασίες που περιέχουν τα φυσικά στοιχεία πρέπει να συνοδεύονται από ετικέτες που θα αναφέρουν ένα μοναδικό αναγνωριστικό, το όνομα του υπεύθυνου ατόμου ή και οργανισμού για τη συλλογή και πακετάρισμα του υλικού, μία περιγραφή του αντικειμένου π.χ. φορητός υπολογιστής, τη τοποθεσία της κατάσχεσης, και τέλος ημερομηνία και ώρα συλλογής του συγκεκριμένου αντικειμένου [20, 28].

2.2.4 Στάδια Φύλαξης

Τα στάδια φύλαξης (chain of custody) αναφέρονται στη καταγραφή της κίνησης των αποδεικτικών στοιχείων, από την αρχική τους πηγή μέχρι την παρουσίασή τους σε μια νομική διαδικασία. Καταγράφονται τα άτομα που είχαν στη κατοχή τους τα στοιχεία, η τοποθεσία και το χρονικό διάστημα κράτησης, και το λόγο κατοχής τους. Επιπλέον περιέχονται πληροφορίες σχετικά με τη διαδικασία μεταφοράς στον επόμενο υπεύθυνο. Ο σκοπός τους είναι να αποδεικνύουν ότι δεν έχει προστεθεί ή μετατραπεί κάποια πληροφορία, έχουν δημιουργηθεί πιστά αντίγραφα και όλες οι συσκευές που περιέχουν δεδομένα είναι κατάλληλα ασφαλισμένα, επομένως έχει διασφαλιστεί η εγκυρότητα των δεδομένων [20, 6].

2.3 Αναζήτηση και Συλλογή Δεδομένων

Το στάδιο της αναζήτησης και συλλογής δεδομένων αποτελεί ένα από τα πιο κρίσιμα σημεία σε μια ψηφιακή έρευνα. Η χρήση μεθόδων από κατάλληλο προσωπικό που θα προστατεύσουν την ακεραιότητα των δεδομένων διασφαλίζει την αξία των αποδείξεων που θα παρουσιαστούν, αντίθετα λάθος κινήσεις θα προκαλέσουν αλλαγές και πιθανή απώλεια δεδομένων. Πέρα από τις πηγές ψηφιακών δεδομένων που περιγράφτηκαν στο προηγούμενο κεφάλαιο, πληροφορίες,

όπως κωδικοί πρόσβασης των χρηστών, μπορούν να αναζητηθούν σε έντυπα ή άλλα μέσα που υπάρχουν στον ευρύτερο χώρο.

2.3.1 Μέθοδοι συλλογής δεδομένων

Η συλλογή ψηφιακών δεδομένων από το τόπο του συμβάντος μπορεί να γίνει με τρεις βασικούς τρόπους, με τη κατάσχεση του υλισμικού (hardware) που πιθανόν περιέχει χρήσιμες πληροφορίες, με τη συλλογή όλων των ψηφιακών δεδομένων από το υλισμικό χωρίς να πραγματοποιηθεί κατάσχεσή του, και τη συλλογή μόνο των δεδομένων που θεωρείται ότι χρειάζονται [2].

Η κατάσχεση του υλισμικού ενδείκνυται σε περιπτώσεις που το ίδιο αποτελεί φυσική απόδειξη ή περιέχει μεγάλο πλήθος ψηφιακών αποδείξεων. Τα πλεονεκτήματα αυτής της μεθόδου είναι ότι η κατάσχεση μπορεί να γίνει από άτομα με απλές βασικές γνώσεις στη προστασία ψηφιακών δεδομένων και η ανάλυση τους πραγματοποιείται αργότερα σε ένα ελεγχόμενο περιβάλλον όπου έχουν πρόσβαση τα απολύτως απαραίτητα και εξειδικευμένα άτομα [2].

Με αυτόν τον τρόπο δεν διαφεύγουν δεδομένα και κάποιο λογισμικό με ιδιαίτερες απαιτήσεις που ίσως να έχει ο δράστης μπορεί να ελεγχθεί απευθείας στον υπολογιστή του [4]. Οι κίνδυνοι της κατάσχεσης είναι η πιθανότητα φθοράς του υλισμικού κατά τη μεταφορά προκαλώντας απώλεια δεδομένων. Επιπλέον μπορεί να διαταράξει τον εργασιακό χώρο και γενικά τη ζωή ατόμων περισσότερο από ότι θα κρινόταν αναγκαίο [2].

Με το δεύτερο τρόπο γίνεται συλλογή μόνο των ψηφιακών δεδομένων και όχι του υλισμικού, ειδικά σε περιπτώσεις που είναι αδύνατη η κατάσχεσή του, επομένως αποφεύγονται τα μειονεκτήματα του προηγούμενου τρόπου. Τα προβλήματα σε αυτή τη περίπτωση είναι η αναγκαία παρουσία ειδικού προσωπικού στο χώρο με τον ανάλογο εξοπλισμό. Επίσης, είναι χρονοβόρα και μπορεί να συλλεχθούν δεδομένα που είναι σε προστατευμένες περιοχές ή να μην έχουν πρόσβαση σε κρυπτογραφημένα δεδομένα που ίσως περιέχουν πληροφορίες [2].

Ο τρίτος τρόπος είναι η συλλογή μόνο των δεδομένων που θεωρείται ότι χρειάζονται, έτσι ο ερευνητής εξοικονομεί χρόνο, προσπάθεια, πόρους και προκαλεί όσο το δυνατόν λιγότερη αναστάτωση στο χώρο. Είναι κατάλληλος ιδιαίτερα σε περιπτώσεις που το μέγεθος των

δεδομένων είναι πολύ μεγάλο (terabytes). Παρόλα αυτά είναι αναγκαία η λεπτομερής καταγραφή κάθε ενέργειας και μειονεκτεί στο ότι μπορεί να παραβλεφθούν πληροφορίες σημαντικές για την έρευνα ή να χαθούν δεδομένα που δεν συλλέχθηκαν σωστά [2, 4].

2.3.2 Αντιμετώπιση ενεργοποιημένου υπολογιστή

Όταν ο υπολογιστής είναι απενεργοποιημένος η διαδικασία που ακολουθείται για τη συλλογή δεδομένων αποτελείται από κοινά αποδεκτά βήματα. Η αντιμετώπιση όμως στην περίπτωση που είναι ενεργοποιημένος έχει διχάσει τους ειδικούς των Computer Forensics. Είναι γενικά αποδεκτό ότι ο υπολογιστής πρέπει να παραμείνει ενεργοποιημένος αλλά είναι προτιμότερο να αποσυνδεθεί από το μόντεμ ή οποιαδήποτε σύνδεση επικοινωνίας. Εάν πρόκειται για ενσύρματη σύνδεση είναι εύκολα να εντοπιστεί από τα καλώδια, αλλά όταν είναι ασύρματη πρέπει να εντοπιστούν μόντεμ ή άλλα μέσα σύνδεσης στον ευρύτερο χώρο [20, 28].

Κάποιες φορές ο υπολογιστής βρίσκεται σε κατάσταση αναμονής και είναι ενεργοποιημένη η προφύλαξη οθόνης. Με τον έλεγχο των φωτεινών λυχνιών στη κεντρική μονάδα ή αν είναι ζεστή και ακούγεται κάποιος θόρυβος μπορεί να εξακριβωθεί και μετά με ένα απλό κούνημα του ποντικιού απενεργοποιείται η προφύλαξη οθόνης και γίνεται καταγραφή των πληροφοριών που εμφανίστηκαν. Δεν πρέπει να γίνει χρήση του πληκτρολογίου ή πάτημα πλήκτρων του ποντικιού γιατί μπορεί να προκαλέσει αλλαγές στο σύστημα. Στη συνέχεια πρέπει να διασωθούν τα ευμετάβλητα δεδομένα και προσωρινά αρχεία τα οποία χάνονται με την διακοπή παροχής ρεύματος [20, 28].

Ιδιαίτερη σημασία πρέπει να δοθεί στην ημερομηνία και ώρα του υπολογιστικού συστήματος που ερευνάται επειδή μπορεί να μην συμβαδίζει με τη τοπική ή με τη διεθνώς αποδεκτή ώρα UTC όταν πρόκειται για διεθνή υπόθεση. Η εμφάνιση διαφορετικής ώρας μπορεί να οφείλεται σε τεχνικό πρόβλημα ή να είναι επιτήδεια ενέργεια του δράστη με στόχο την εμφάνιση διαφορετικής ημερομηνίας και ώρας στα αρχεία του συστήματος και εκμετάλλευση αυτού του γεγονότος προς υπεράσπισή του [6].

Ποικίλες λύσεις έχουν προταθεί για τον τρόπο που πρέπει να απενεργοποιηθεί ο υπολογιστής. Η πιο διαδεδομένη είναι η αποσύνδεση της τροφοδοσίας, κατά προτίμηση από τη θύρα του

υπολογιστή για να αποτραπεί η εγγραφή νέων δεδομένων, αλλά υπάρχει ο κίνδυνος διαγραφής δεδομένων του συστήματος. Ο άλλος τρόπος είναι η κανονική απενεργοποίηση και εφαρμόζεται συνήθως σε εξυπηρετητές. Αν και προκαλεί τη μεταβολή κάποιων δεδομένων, κάποια άλλα ίσως σημαντικότερα αποθηκεύονται. Όμως πρέπει να δοθεί προσοχή στην επόμενη εκκίνηση καθώς υπάρχει κίνδυνος να ενεργοποιηθούν παγίδες που τοποθέτησε ο δράστης με σκοπό τη διαγραφή ενοχοποιητικών στοιχείων [20, 28, 6].

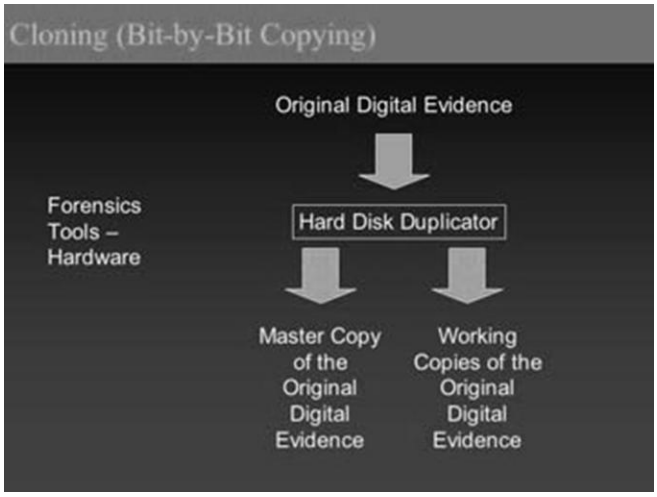
2.3.3 Συλλογή ευμετάβλητων δεδομένων

Πριν την απενεργοποίηση ενός υπολογιστικού συστήματος προηγείται η συλλογή των ευμετάβλητων δεδομένων τα οποία χάνονται μετά τη διακοπή παροχής ηλεκτρικού ρεύματος. Ωστόσο, η συλλογή τους είναι αρκετά δύσκολη και μπορεί να προκαλέσει αλλαγές στο σύστημα, επομένως πολλοί πρώτοι αποκριτές στο χώρο του συμβάντος εσφαλμένα παραβλέπουν αυτό το βήμα της έρευνας παρόλο που παρέχει σημαντικές πληροφορίες για την πρόσφατη κατάσταση του συστήματος [52].

Οι πληροφορίες των ευμετάβλητων δεδομένων μπορούν να διακριθούν σε πληροφορίες συστήματος, σχετικά δηλαδή με το υπολογιστικό σύστημα, τον χρήστη, τα προγράμματα που εκτελούνται και αρχεία που είναι ανοιχτά, και σε πληροφορίες δικτύου που αφορούν συνδέσεις, ανοιχτές θύρες (ports) και υποδοχές (sockets), στοιχεία δρομολογητών και άλλα [6, 52].

Η απόκτηση αυτών των δεδομένων μπορεί να πραγματοποιηθεί από λίγα διαθέσιμα εργαλεία, ο καλύτερος τρόπος όμως είναι η χρήση κατάλληλων εντολών Unix ή των αντίστοιχων των Windows, για παράδειγμα τις εντολές netstat και nbstat για την εμφάνιση ενεργών συνδέσεων. Οι εντολές όμως δεν πρέπει να εκτελούνται απευθείας από το σύστημα του υπόπτου, αλλά από κάποιο κατάλληλη CD, για να μειωθεί στο ελάχιστο οποιαδήποτε παρέμβαση αλλά και επειδή η χρήση των εντολών μπορεί να ενεργοποιήσει κακόβουλο λογισμικό του χρήστη με σκοπό τη διαγραφή δεδομένων [6, 52].

2.3.4 Δημιουργία εικονικών αντιγράφων



Εικόνα 1: Δημιουργία εικονικών αντιγράφων ψηφιακών δεδομένων.

Η ανάλυση των δεδομένων δεν γίνεται ποτέ στα αρχικά δεδομένα, εκτός από ελάχιστες περιπτώσεις, αλλά σε ειδικά αντίγραφα που δημιουργούνται είτε αμέσως στο χώρο του συμβάντος ή στο εργαστήριο εάν έχει γίνει κατάσχεση του υλισμικού, για την αποτροπή τυχόν αλλαγών στα αυθεντικά στοιχεία. Η δημιουργία ενός ακριβούς αντιγράφου γίνεται με ειδικές διαδικασίες και σε αποστειρωμένες συσκευές αποθήκευσης, δηλαδή συσκευές που έχουν διαγραφεί τα προηγούμενα δεδομένα με εξειδικευμένες τεχνικές, χωρίς να αφήσουν ίχνη [20, 28].

Για τη διατήρηση της ακεραιότητας των δεδομένων εφαρμόζονται μέθοδοι προστασίας εγγραφής και έλεγχοι ιών κατά τη διαδικασία αντιγραφής των πρωτότυπων δεδομένων σε άλλες συσκευές για την μετέπειτα ανάλυσή τους. Ο σκοπός τους είναι η αποφυγή εγγραφής νέων δεδομένων ή διαγραφής των υπαρχουσών, εγγυώντας ότι οι αποδείξεις που θα συλλεχθούν δεν έχουν μετατραπεί με κάποιο τρόπο όσο διαρκούσε η έρευνα [20]. Ωστόσο, τα δεδομένα μπορεί να έχουν αλλαχτεί πριν τη δημιουργία των εικονικών αντιγράφων και την εφαρμογή μεθόδων προστασίας εγγραφής. Μόνο το άτομο που συλλέγει τα δεδομένα μπορεί να εγγυηθεί ότι είναι αμετάβλητα, γι’ αυτό το λόγο πρέπει να θεωρείται αξιόπιστο [33].

Επιπλέον, για να διασφαλιστεί η ακεραιότητα των δεδομένων υπολογίζεται μία αριθμητική τιμή με βάση συναρτήσεις κατακερματισμού (hashing) (όπως οι συναρτήσεις MD5, SHA) ή αθροίσματα ελέγχου [20, 28]. Η τιμή αυτή ονομάζεται τιμή κατακερματισμού, ή τιμή hash για συντομία, και είναι μοναδική για κάθε ξεχωριστό σύνολο δεδομένων. Σε πολύ σπάνιες περιπτώσεις μπορεί η τιμή hash του πρωτότυπου αρχείου με αυτή του αντιγράφου να μην ταιριάζουν, το οποίο μπορεί να οφείλεται στη λανθασμένη αντιγραφή των δεδομένων λόγω φυσικών ζημιών στην συσκευή που είναι αποθηκευμένα τα πρωτότυπα αρχεία, ή στη συσκευή προστασίας εγγραφής ή στα καλώδια που χρησιμοποιούνται για τη σύνδεση [5].

2.3.5 Συλλογή δεδομένων από δίκτυα

Σήμερα σχεδόν κάθε υπολογιστικό σύστημα συνδέεται με κάποιο δίκτυο, είτε είναι κάποιο τοπικό ή το διαδίκτυο, του οποίου τα δεδομένα από εφαρμογές ή δικτυακά προγράμματα μπορεί να περιέχουν πληροφορίες για την υπόθεση που ερευνάται και πρέπει να συλλεχθούν. Λαμβάνοντας υπόψη το μοντέλο OSI Seven Layer διασφαλίζεται ότι κανένα πεδίο δεν θα παραβλεφθεί και θα εντοπιστούν διαφορετικών ειδών πληροφορίες [20].

Κάποιες φορές, πέρα από τη συλλογή δεδομένων από τον υπολογιστή του δράστη ή και του θύματος, είναι απαραίτητη η συλλογή από άλλες πηγές, για παράδειγμα από εξυπηρετητές ή δρομολογητές, ή και από τα αρχεία που διατηρούν οι πάροχοι σύνδεσης στο διαδίκτυο. Μπορεί να περιέχουν σημαντικές πληροφορίες σχετικά με το είδος των δεδομένων που στάλθηκαν και ελήφθη, τη χρονική στιγμή που πραγματοποιήθηκε η μεταφορά και τη διάρκειά της, αναγνωριστικά στοιχεία του αποστολέα και του παραλήπτη, καθώς και ποια διαδρομή ακολουθήθηκε [38].

Λόγω του μεγάλου αριθμού ειδών δικτύων και συνδέσεων που έχουν αναπτυχθεί για τη μεταφορά δεδομένων και των ακόμα περισσότερων ειδικών χαρακτηριστικών του καθενός κρίθηκε απαραίτητο η δημιουργία ενός ξεχωριστού κλάδου forensics, το Network Forensic. Η εφαρμογή του είναι αποκλειστικά για έρευνα και ανάλυση δεδομένων σε δίκτυα.

2.3.6 Αρχεία ήχου και εικόνας

Σε περιπτώσεις που η διαδικασία της συλλογής έχει στόχο αρχεία ήχου και εικόνας θα πρέπει να αναγνωριστεί ο τύπος του αρχείου, να εντοπιστούν όλες οι συνηθισμένες τοποθεσίες που είναι αποθηκευμένα ψηφιακά δεδομένα (σκληροί δίσκου, CD, DVD κτλ), συσκευές αναπαραγωγής μουσικής (πχ mp3 player) και φωτογραφικές μηχανές, στη συνέχεια να γίνει καταγραφή των αντικειμένων καθώς και των ατόμων που είχαν πρόσβαση σε αυτά. Θα πρέπει να ληφθεί υπόψη ότι όταν γίνεται ψηφιοποίηση αναλογικού ήχου ή εικόνας είναι πιθανό να χαθούν κάποιες πληροφορίες, για παράδειγμα κάποια κομμάτια του αρχείου μπορεί να χαθούν ή να μειωθεί η ποιότητά του [20].

Ακόμα, θα πρέπει να σημειωθούν ειδικές καταστάσεις, όπως μια ταινία που έχει εγκατασταθεί ανάποδα με σκοπό την εξαπάτηση και διανομή συγκεκριμένων παράνομων ειδών εικόνας (πχ παιδική πορνογραφία), όπως και οποιαδήποτε πληροφορία σχετικά με τη κάμερα ή τους καταγραφείς, τις παραμέτρους εγγραφής, δηλαδή χρόνο εγγραφής και ταχύτητα, καθώς και την ώρα του συστήματος για να συγκριθεί με τη πραγματική [20].

2.3.7 Φορητές συσκευές

Για τη κατάσχεση φορητών συσκευών, όπως κινητά τηλέφωνα, PDAs, smart cards, πρέπει να ληφθούν μέτρα που θα αποτρέπουν τη πρόσβαση ιδιαίτερα από τον ιδιοκτήτη και να καταγραφεί οποιασδήποτε πληροφορία σχετικά με τη συσκευή (μοντέλο, μάρκα, κατασκευαστής, κτλ). Τα στοιχεία που εμφανίζονται πρέπει να σημειωθούν ή φωτογραφηθεί η οθόνη για να μην παραλειφθούν πληροφορίες. Επιπλέον, είναι απαραίτητες μονάδες επαναφόρτισης ή μπαταρίες για τις συσκευές για να αποφευχθεί η απώλεια δεδομένων στη περίπτωση που αποφορτιστεί η μπαταρία [20, 28].

Μαζί με τη συσκευή κατάσχεται και οτιδήποτε μπορεί να σχετίζεται μαζί αυτή, όπως μπαταρίες, καλώδια, οδηγίες χρήσεως, CD με λογισμικό, κάρτες SIM, σημειώσεις που μπορεί να περιέχουν κωδικούς PIN ή άλλους προσωπικούς αριθμούς. Θα πρέπει να ληφθούν υπόψη τυχόν ασύρματες συνδέσεις της συσκευής με κάποια άλλη, καθώς οποιοσδήποτε υπολογιστική συσκευή στη περιοχή μπορεί να έχει συγχρονιστεί με τη συγκεκριμένη. Επίσης, κατάλληλα μέτρα προστασίας απαιτούνται όταν η συσκευή χρειάζεται και για άλλου είδους εξετάσεις όπως εύρεση DNA ή αποτυπωμάτων [20].

Ειδικά για την έρευνα σε φορητές ψηφιακές συσκευές ασχολείται ο κλάδος των Mobile Forensics. Περιλαμβάνει μεθόδους και τεχνικές για τη συλλογή και ανάλυση δεδομένων πολλών φορητών συσκευών. Εξελίσσεται συνεχώς λόγω της ραγδαίας ανάπτυξης νέων ειδών συσκευών και την προσθήκη λειτουργιών που τις μετατρέπουν σε μικρές αλλά δυνατές υπολογιστικές συσκευές.

2.4 Ανάλυση Δεδομένων

Σε κάποιες καταστάσεις η διαδικασία της ανάλυσης δεδομένων απαιτείται να γίνει στο χώρο του συμβάντος και συνήθως κάτω από αυστηρούς χρονικούς περιορισμούς, για παράδειγμα όταν ένα άλλο έγκλημα μπορεί να διαπραχτεί σύντομα από το δράστη ή μπορεί να διαφύγει. Σε αυτές τις περιπτώσεις πρέπει να υπάρχει ένας μάρτυρας κατά τη διάρκεια της έρευνας ο οποίος θεωρείται κατάλληλος να δώσει κατάθεση σε δίκη αν χρειαστεί για την αξιοπιστία των ευρημάτων [28]. Σε κανονικές συνθήκες όμως η εξέταση πρέπει να γίνεται αναλυτικά σε ελεγχόμενο περιβάλλον [2].

Όταν γίνεται η ανάλυση των δεδομένων για την εύρεση αποδείξεων πρέπει να τηρηθούν κάποιες βασικές αρχές για να προστατευθεί η ακεραιότητα και αυθεντικότητά τους [20]:

- Να μην γίνει καμία αλλαγή στα δεδομένα.
- Μόνο ικανά και εξουσιοδοτημένα άτομα να έχουν πρόσβαση στις ψηφιακές αποδείξεις.
- Να γίνεται αναλυτική καταγραφή κάθε ενέργειας σχετικά με τη πρόσβαση, ανάκτηση, αποθήκευση και μεταφορά των ψηφιακών αποδείξεων.
- Να είναι εμφανές ποιος είναι υπεύθυνος για τα δεδομένα.

Κατά τη διάρκεια της ανάλυσης των δεδομένων προτεραιότητα έχει να ληφθούν όλα τα απαραίτητα μέτρα για αποφυγή τυχόν μόλυνσής τους και να εφαρμόζονται συστηματικές και επιστημονικές μέθοδοι. Η έρευνα πρέπει να διατηρεί το σκοπό για τον οποίο ξεκίνησε, στη περίπτωση που βρεθούν αποδείξεις για άλλες παράνομες ενέργειες, θα πρέπει να καταγραφούν και να συνεχιστεί η έρευνα παρά να ξεκινήσει μία άλλη χωρίς την απαραίτητη εξουσιοδότηση επειδή αργότερα μπορεί να αμφισβητηθεί η αξιοπιστία των ευρημάτων [33].

Ο χειρισμός των δεδομένων γίνεται στα αντίγραφα που δημιουργήθηκαν για τη προστασία των αρχικών δεδομένων. Κατά την εξέταση θα πρέπει να εντοπιστούν και ανακτηθούν αρχεία που είχαν καταστραφεί ή διαγραφεί, να γίνει ένα χρονοδιάγραμμα γεγονότων και να εξακριβωθεί η σχέση μεταξύ των δεδομένων αν υπάρχει [20, 28]. Εξαιτίας του μειωμένου κόστους αποθήκευσης και την ευκολία δημιουργίας και απόκτησης αρχείων, ο ερευνητής μπορεί να έρθει αντιμέτωπος με ένα μεγάλο πλήθος δεδομένων όπου κάποια από αυτά μπορεί να μην είναι από την αρχή εμφανή, αναγκάζοντας έτσι τη χρήση ειδικών μεθόδων για τον εντοπισμό αποδείξεων [2].

Ο ιδιοκτήτης των ψηφιακών δεδομένων μπορεί να έχει χρησιμοποιήσει κωδικό πρόσβασης για να περιορίσει τη διαθεσιμότητα των αρχείων σε άλλους με αποτέλεσμα να περιορίζει και τη διαδικασία ανάκτησης δεδομένων. Στη καλύτερη περίπτωση μπορεί να δώσει ο ίδιος στον ερευνητή το κωδικό αλλά συνήθως δεν συμβαίνει συνεπάγοντας την εφαρμογή άλλων μέτρων για την απόκτησή του όπως λεξικά με συνηθισμένες λέξεις κλειδιά, καταγραφέα πληκτρολογίου, εύρεση στη κρυφή μνήμη στη περίπτωση που έχει αποθηκευτεί ο κωδικός στο σύστημα για να το θυμάται και να συνδέεται ο χρήστης πιο γρήγορα, και άλλα [5].

2.4.1 Μέθοδοι φιλτραρίσματος και μείωσης δεδομένων

Ο σκοπός εφαρμογής μεθόδων φιλτραρίσματος και μείωσης των δεδομένων είναι ο αποκλεισμός αρχείων που δεν σχετίζονται με την έρευνα, για παράδειγμα αρχεία του συστήματος, και να γίνει εστίαση σε αρχεία που έχει δημιουργήσει ο χρήστης και πιθανόν να περιέχουν χρήσιμες πληροφορίες. Επιπλέον, γίνεται διαχωρισμός περιττών αρχείων που εμφανίζονται δύο ή περισσότερες φορές σε διαφορετικές τοποθεσίες, όπως σε πολλαπλά αντίγραφα ασφαλείας. Με τη χρήση διαφορετικών εργαλείων εξακριβώνονται αντιφάσεις που εμφανίζονται στα ψηφιακά δεδομένα, δηλαδή αρχεία που μπορεί να αγνοήθηκαν, λάθη κατά τον υπολογισμό τιμών hash και άλλα [2].

Τεχνικές που προέρχονται από τον τομέα την εξόρυξης δεδομένων μπορούν να εφαρμοστούν για την εύρεση αποδείξεων. Η σύγκριση των hash τιμών που παράχθηκαν από τα δεδομένα με ήδη γνωστές τιμές που αντιστοιχούν σε συγκεκριμένα είδη αρχείων είναι ένας τρόπος. Ένας πιο αυτοματοποιημένος είναι η χρήση ενός εξειδικευμένου honeypot, δηλαδή μια διαδικασία προσέλκυσης επιλεγμένων αρχείων, όπου ο στόχος του είναι να βρίσκει αρχεία τα οποία ταιριάζουν λόγω της διαφοροποίησής τους από τα άλλα αρχεία ενός συνόλου [53]. Λιγότερο μεθοδικοί τρόποι αναζήτησης είναι με χρήση λέξεων ή φράσεων ή τύπους αρχείων. Τα μειονέκτημα αυτού τους είδους αναζήτησης είναι η πιθανή παράλειψη σημαντικών στοιχείων και το αποτέλεσμα αυτής της διαδικασίας να εξακολουθεί να είναι πολύ μεγάλο για να το αναλύσει ο ερευνητής [2].

2.4.2 Είδος και προέλευση αρχείων

Στα αρχεία που θα ελεγχτούν και μπορεί να περιέχουν αποδείξεις πρέπει να εξακριβωθεί η ταυτότητά τους και η προέλευσή τους. Η αναγνώρισή τους γίνεται με τη κατηγοριοποίηση των ψηφιακών στοιχείων σύμφωνα με κοινά χαρακτηριστικά μιας κατηγορίας. Γίνεται σύγκριση με γνωστά αρχεία για τον εντοπισμό παρόμοιας δομής και έτσι μπορούν να αναγνωριστούν κρυμμένα ή αλλαγμένα αρχεία καθώς και διαγραμμένα όπου έχουν εντοπιστεί μόνο κάποια κομμάτια τους. Επιπλέον, η κεφαλίδα, το υποσέλιδο και άλλα χαρακτηριστικά του αρχείου υποδηλώνουν με ποιο λογισμικό δημιουργήθηκε ή από ποια ψηφιακή συσκευή προήλθε. Πρέπει να δοθεί προσοχή όταν παρόμοια αρχεία προέρχονται από διαφορετικά υπολογιστικά συστήματα καθώς τα χαρακτηριστικά κατηγορίας διαφοροποιούνται και είναι δυσκολότερο να εντοπιστούν οι ομοιότητες [2].

Για τον προσδιορισμό της προέλευσης των δεδομένων γίνεται σύγκριση των στοιχείων για να εξακριβωθεί αν προέρχονται από την ίδια πηγή ή διαφορετική. Ο εντοπισμός της πηγής δεν σημαίνει αναγκαστικά ότι εκεί δημιουργήθηκε το αρχείο, αλλά μπορεί να είχε μετατραπεί ή κατατμηθεί, πάντως είναι σχεδόν σίγουρο ότι για κάποιο χρονικό διάστημα βρισκόταν στη συγκεκριμένη συσκευή [2]. Όμως, ο ιδιοκτήτης της συσκευής που είναι η πηγή κάποιων δεδομένων δεν είναι αυτόματα και ο δράστης, ιδιαίτερα αν μπορούν να αποκτήσουν πρόσβαση και άλλα άτομα. Η χρήση κωδικών λέξεων πρόσβασης δεν θεωρείται πλέον αποτελεσματική αυθεντικοποίηση χρηστών παρά μόνο βιομετρικά χαρακτηριστικά όπως δαχτυλικά αποτυπώματα ή η καταγραφή καθαρής εικόνας από κάμερα του υπόπτου όταν δρούσε [5].

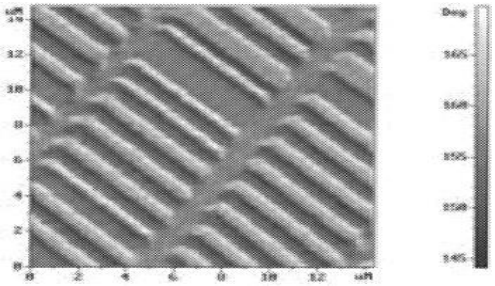
2.4.3 Ανάκτηση κρυφών ή διαγραμμένων αρχείων

Η ανάκτηση διαγραμμένων αρχείων και ο εντοπισμός άλλων που δεν είναι στα πιο εμφανή σημεία ενός αποθηκευτικού μέσου είναι δύσκολο αλλά όχι αδύνατο. Εξαρτάται από το είδος των δεδομένων και τη κατάστασή τους, το λειτουργικό σύστημα, το είδος και τις ρυθμίσεις του λογισμικού και υλισμικού. Δεδομένα μπορούν να βρεθούν σε μη καταχωρημένες περιοχές (unallocated area), σε περιοχές ανταλλαγής (swap area) ή σε νωθρά διαστήματα (slack spaces), δηλαδή περιοχές μεταξύ του λογικού τέλους του αρχείου και του τέλους της αποθηκευτικής μονάδας (cluster) για το συγκεκριμένο αρχείο. Ένας έμπειρος χρήστης μπορεί να έχει

τοποθετήσει ενοχοποιητικά στοιχεία σε αυτές τις περιοχές για να αποτρέψει το γρήγορο εντοπισμό τους [5, 2, 33, 6].

Η ενέργεια διαγραφής ενός αρχείου από το χρήστη δεν ισοδυναμεί με τη διαγραφή του από το σύστημα, το μόνο που συμβαίνει είναι η μηδένιση της αντίστοιχης εγγραφής στον πίνακα καταχώρησης αρχείων. Με την επικάλυψη του από ένα νέο αρχείο μπορεί να χαθεί ένα σημαντικό κομμάτι αλλά τις περισσότερες φορές παραμένουν κάποια τμήματά του στο δίσκο. Εάν έχει καλυφτεί η κεφαλίδα του αρχείου γίνεται πιο δύσκολη η ανάκτησή του αλλά όχι αδύνατη καθώς μπορεί να συγκριθεί το υπολειπόμενο κομμάτι με γνωστά αρχεία για να εντοπιστούν ομοιότητες. Η διαδικασία αυτή είναι πιθανότερο να επιτύχει όταν πρόκειται για αρχεία κειμένου παρά σε εικόνας ή ήχου καθώς η κεφαλίδα τους περιέχει πολλές πληροφορίες για τη δομή τους όπως διαστάσεις, ανάλυση και άλλα χαρακτηριστικά [5, 2].

Παρά την επικάλυψη παλαιότερων αρχείων από καινούρια εμφανίζονται συχνά δεδομένα σκιές (shadow data) τα οποία υπάρχουν εξαιτίας της κάθετης και οριζόντιας ευθυγράμμισης των μηχανικών κεφαλών που γράφουν στο δίσκο η οποία δεν είναι ακριβώς ίδια κάθε φορά που εκτελείται μια διαδικασία εγγραφής με αποτέλεσμα να παραμένουν ίχνη από τα προηγούμενα αρχεία [6].



Εικόνα 2: Μαγνητικό σχέδιο σε ένα σκληρό δίσκο.

2.4.4 Κρυπτογράφηση και στεγανογράφηση

Η εύρεση κρυπτογραφημένων αρχείων υποδεικνύει πιθανές αποδείξεις που συγκαλύπτει ο δράστης. Η απόκτηση τους απαιτεί εύρεση του κλειδιού κρυπτογράφησης ή τα δεδομένα σε αποκρυπτογραφημένη μορφή, στη δεύτερη όμως περίπτωση μπορεί να αμφισβητηθούν οι αποδείξεις σε μια νομική διαδικασία καθώς δεν εξασφαλίζει σίγουρα ότι είναι τα κρυπτογραφημένα δεδομένα αυτούσια. Το κλειδί αποκρυπτογράφησης μπορεί να ζητηθεί από τον δημιουργό του αρχείου, όμως αν με αυτό το τρόπο συμβάλει στην ενοχοποίησή του μάλλον θα αρνηθεί με αποτέλεσμα οι μόνες λύσεις να είναι η δοκιμή πιθανών κλειδιών και η χρήση εργαλείων αποκρυπτογράφησης [2].

Τα στεγανογραφημένα δεδομένα είναι αρχεία ενσωματωμένα σε κάποια άλλα και απαιτείται η χρήση ειδικών διαδικασιών στεγανάλυσης για τον εντοπισμό τους. Τα bits του αρχείου που τοποθετείται είναι διασκορπισμένα σε περιοχές του άλλου αρχείου που δεν είναι εμφανείς οι αλλαγές που προκαλούνται λόγω της προσθήκης. Συνήθως χρησιμοποιούνται αρχεία εικόνας και ήχου για την απόκρυψη πληροφοριών. Η εύρεση λογισμικού δημιουργίας αυτού του είδους αρχεία υποδεικνύει την πιθανή ύπαρξή τους και τη λήψη μέτρων για τον εντοπισμό τους [6].

2.5 Καταγραφή Ψηφιακών Αποδείξεων

Από τη στιγμή που θα γίνει είσοδος στο τόπο του συμβάντος μέχρι την ολοκλήρωση της έρευνας, πρέπει να καταγράφονται όλες οι ενέργειες του προσωπικού που έχει αναλάβει την έρευνα. Αρχικά γίνεται καταγραφή του χώρου με ψηφιακή φωτογραφική μηχανή ή βιντεοκάμερα για να είναι πιο λεπτομερής αποφεύγοντας με αυτό το τρόπο ανθρώπινα λάθη και μεροληψίες που μπορεί να εμφανίζονταν με τη χειρόγραφη. Οι ψηφιακές εικόνες και βίντεο πρέπει να αποθηκευτούν το συντομότερο δυνατόν και προτείνεται ο υπολογισμός hash τιμών για να διασφαλιστεί ότι δεν έχουν μετατραπεί με κανένα τρόπο [6, 5].

Κάθε κατάσχεση καταγράφεται από το άτομο που τη πραγματοποίησε και συμπεριλαμβάνει το όνομά του, περιγραφή, αρχική τοποθεσία και κατάσταση του αντικειμένου, ημερομηνία και ώρα, και ένα μοναδικό αναγνωριστικό αριθμό για να ξεχωρίζει από οποιοδήποτε άλλο αντικείμενο. Στη συνέχεια, σε όλη τη διάρκεια της έρευνας γίνεται καταγραφή των σταδίων φύλαξης των αποδείξεων και περιλαμβάνει στοιχεία του υπεύθυνου για τις αποδείξεις, το χρονικό διάστημα και το λόγο που ήταν στην κατοχή του [6, 5].

Επίσης, με την καταγραφή ενός συστήματος πανομοιότυποι υπολογιστές με πανομοιότυπες ρυθμίσεις μπορούν να διαχωριστούν καθώς και τα αντίγραφα με τα πρωτότυπα δεδομένα. Όταν οι αποδείξεις αντιγράφονται σε άλλα μέσα θα πρέπει να δοθούν ετικέτες οι οποίες θα περιλαμβάνουν τη τωρινή ημερομηνία και ώρα καθώς και την ημερομηνία και ώρα του υπολογιστικού συστήματος, το όνομα του ατόμου που δημιούργησε τα εικονικά αντίγραφα, το λειτουργικό σύστημα, τα προγράμματα ή εντολές που χρησιμοποιήθηκαν για την αντιγραφή του αρχείου και πληροφορίες που πιστεύεται ότι περιέχονται στα αρχεία [20].

Τέλος, κάθε διαδικασία που εφαρμόστηκε κατά την ανάλυση των δεδομένων καταγράφεται λεπτομερώς αναφέροντας τα άτομα που ήταν παρόντα και ποιες ήταν οι ενέργειές τους, τα αποτελέσματα από κάθε διαδικασία και τις πιθανές αποδείξεις, ημερομηνία και ώρα. Στις ψηφιακές αποδείξεις μπορεί να προστεθεί μια κρυπτογραφική ψηφιακή υπογραφή εφόσον δεν προκαλεί καμία μετατροπή στα δεδομένα για τη διασφάλιση της ακεραιότητας τους [6].

Η τελική αναφορά του ερευνητή περιέχει όλα τα ευρήματα και τα συμπεράσματα με ατράνταχτα επιχειρήματα που στηρίζουν τις αποδείξεις και τη καθιστούν αξιόπιστη σε μια νομική διαδικασία. Επιπλέον, περιγράφει τα εργαλεία και τις διαδικασίες που χρησιμοποιήθηκαν για την εξέταση και ανάλυση των δεδομένων. Για να θεωρηθεί επαρκής η καταγραφή που έγινε θα πρέπει να είναι αρκετά λεπτομερής έτσι ώστε ένας ανεξάρτητος ειδικός των Computer Forensics, να μπορέσει να εκτιμήσει τις ενέργειες που έγιναν και τα ευρήματα [2, 20].

2.6 Αναπαράσταση Συμβάντος

Η αναπαράσταση του συμβάντος, είτε σχετίζεται με μια αστική υπόθεση ή με μια εγκληματική ενέργεια, είναι μια διαδικασία αποκόμισης πλήρους κατανόησης του συμβάντος με βάση τις διαθέσιμες αποδείξεις. Δίνει μια πλήρη εικόνα για το τι έγινε, ποιος το προκάλεσε, πότε, που, πως και γιατί. Υπάρχουν τρεις τύποι αναπαράστασης: η χρονική, η συσχετιστική και η λειτουργική [2, 3].

Η χρονική ανάλυση προσδιορίζει το χρόνο και τη σειρά των γεγονότων και γίνεται μια γενική επισκόπηση του συμβάντος. Υποδεικνύει πότε τα αρχεία δημιουργήθηκαν, μετατράπηκαν και χρησιμοποιήθηκαν. Με αυτόν τον τρόπο αναγνωρίζονται πρότυπα και κενά, τα οποία μπορεί να οδηγήσουν σε άλλες πηγές δεδομένων. Συνήθως χρησιμοποιούνται οι ημερομηνίες και ώρες που καταγράφονται στα αρχεία με προσοχή καθώς μπορεί να μην ανταποκρίνονται στη πραγματικότητα [2, 3].

Όταν δεν είναι διαθέσιμες οι άμεσες χρονικές πληροφορίες, εφαρμόζεται η τεχνική της ψηφιακής στρωματογραφίας, η οποία ελέγχει τη θέση των αρχείων και μπορεί να προσδιορίσει περίπου το χρόνο δημιουργίας. Για παράδειγμα, όταν ένα αρχείο έχει επικαλυφθεί από κάποιο άλλο τότε σίγουρα δημιουργήθηκε νωρίτερα [2, 3].

Ο δεύτερος τύπος αναπαράστασης είναι η συσχετιστική η οποία αναγνωρίζει σχέσεις μεταξύ υπόπτων, θυμάτων και τοποθεσιών. Προσδίδει γεωγραφικές τοποθεσίες στα άτομα και υπολογιστές καθώς και στην επικοινωνία ή συναλλαγές που είχαν μεταξύ τους. Υπάρχουν ειδικά εργαλεία ανάλυσης σχέσεων ειδικά για τέτοιες περιπτώσεις όπως το Watson από την Xanalys και το NetMap [2, 3].

Τέλος, η λειτουργική ανάλυση εξακριβώνει πως ένα συγκεκριμένο σύστημα ή εφαρμογή λειτουργεί και πως είχε ρυθμιστεί κατά τη διάρκεια του συμβάντος. Επομένως, μπορεί καθοριστεί αν ήταν δυνατόν να εκτελεστεί η παράνομη πράξη και αν οι αποδείξεις είναι αυθεντικές ή τοποθετήθηκαν εν αγνοία του υπόπτου. Επιπλέον, γίνεται καλύτερη κατανόηση των αποδείξεων και του εγκλήματος και μπορούν να προσδιοριστούν οι προθέσεις και τα κίνητρα του δράστη ή αν τελικά ήταν ατύχημα [2, 3].

3 Ειδικές Τεχνικές

Σε αυτό το κεφάλαιο θα περιγραφούν κάποιες βασικές τεχνικές και διαδικασίες που χρησιμοποιούνται ευρέως στον τομέα των Computer Forensics. Η λειτουργία του κατακερματισμού έχει εφαρμογή τόσο στην προστασία ακεραιότητας δεδομένων όσο και στην αναζήτηση αποδείξεων, ενώ η εικονική αντιγραφή και προστασία εγγραφής εγγυώνται τη μη μεταβλητότητα των αρχικών αποδείξεων. Τέλος, περιγράφεται πως τεχνικές από τον τομέα της εξόρυξης δεδομένων μπορούν να συμβάλουν σε μια ψηφιακή έρευνα.

3.1 Κατακερματισμός (Hashing)

Η διαδικασία του κατακερματισμού (hashing) περιλαμβάνει τη χρήση ενός μαθηματικού αλγορίθμου σε κάποια δεδομένα για τον υπολογισμό μιας αντιπροσωπευτικής αριθμητικής τιμής. Παράγει μια μοναδική τιμή, αποτελούμενη από αριθμούς και γράμματα, για να προσδιορίσει το συνδυασμό bytes που αποτελούν ένα συγκεκριμένο αρχείο ή ομάδα αρχείων ή ολόκληρο το δίσκο. Η τιμή που υπολογίζεται ονομάζεται κατακερματισμένη αξία (hash value) ή αλλιώς συμπυκνωμένη απεικόνιση (condensed representation) ή αφομοιωμένο μήνυμα (message digest), στη συνέχεια του κειμένου θα αναφέρεται ως τιμή hash. Ο μαθηματικός αλγόριθμος που χρησιμοποιείται είναι μονόδρομος, δηλαδή μπορεί να υπολογιστεί μια τιμή από τα δεδομένα, αλλά από τη συγκεκριμένη τιμή δεν μπορούν να υπολογιστούν τα δεδομένα με κάποιο τρόπο [5, 56].

Η ικανότητα παραγωγής μιας μοναδικής τιμής είναι που κάνει αυτήν την τεχνική ενδιαφέρουσα για τα Computer Forensics. Μια από τις χρησιμότητές της είναι η εξακρίβωση της ακεραιότητας των ψηφιακών δεδομένων. Από τα αρχικά δεδομένα υπολογίζεται η hash τιμή τους και στη συνέχεια δημιουργείται το πιστό αντίγραφό τους, εάν η τιμή hash του αντίγραφου είναι ίδια με αυτή του πρωτότυπου συμπεραίνεται ότι το αντίγραφο περιέχει ακριβώς τα ίδια δεδομένα με το αρχικό και δεν έχει αλλαχτεί κανένα bit [19].

Οι τιμές hash εκτός από ένα σύνολο δεδομένων σε κάποιο δίσκο μπορούν να υπολογιστούν και για κάθε αρχείο ή πρόγραμμα χωριστά. Ορισμένα εργαλεία ανάλυσης μπορούν από ένα εικονικό αντίγραφο να ξεχωρίσουν τα αρχεία και να υπολογίσουν μοναδικές τιμές για το καθένα. Στη

συνέχεια οι τιμές που θα παραχθούν συγκρίνονται με σύνολα hash τιμών από γνωστά αρχεία. Με αυτήν τη δυνατότητα ο ερευνητής μπορεί να ξεδιαλύνει από το σύνολο των δεδομένων αυτά που σίγουρα δεν χρειάζονται, όπως αρχεία του συστήματος, και να επικεντρωθεί σε αρχεία που πιθανόν περιέχουν αποδεικτικά στοιχεία [56].

Η σύγκριση των τιμών hash με γνωστές τιμές βοηθάει στον εντοπισμό συγκεκριμένων αρχείων και προγραμμάτων, για παράδειγμα κακόβουλο λογισμικό ή προγράμματα στεγανογράφησης. Επιπλέον, αν η τιμή από κάποιο άγνωστο αρχείο είναι ίδια με κάποιου γνωστού αρχείου τότε και τα αρχεία είναι ακριβώς ίδια, καθώς οι hash τιμές είναι σαν δαχτυλικά αποτυπώματα των αρχείων [56]. Το Child Victim Identification Program το οποίο είναι μέρος του Innocent Images National Initiative του FBI[1], είναι μια εφαρμογή αυτής της λειτουργίας για την αντιμετώπιση της παιδικής πορνογραφίας [33].

Ωστόσο, οι πιο επιδέξιοι δράστες που γνωρίζουν αυτή τη τεχνική κάνουν μικρές αλλαγές στα ενοχοποιητικά αρχεία για να έχουν διαφορετική τιμή hash και όταν γίνεται η σύγκριση με τη βάση οι τιμές να μην ταιριάζουν. Υπάρχουν όμως τεχνικές που μπορούν να αντιμετωπίσουν αυτό το πρόβλημα, ο ασαφής κατακερματισμός (fuzzy hashing) και ο τμηματικός κατακερματισμός (segmentation hashing). Οι συγκεκριμένες τεχνικές συγκρίνουν μέρος του αρχείου, όχι ολόκληρο, για ομοιότητες με τα σύνολα γνωστών τιμών hash. Η πρώτη τεχνική επιλέγει κομμάτια από το αρχείο και υπολογίζει τις hash τιμές τους με βάση πιθανές ομοιότητες, ενώ η δεύτερη τεμαχίζει το αρχείο σε ίσου μεγέθους κομμάτια και στη συνέχεια συγκρίνει κάθε κομμάτι με κομμάτια γνωστών αρχείων [3]. Με αυτές τις τεχνικές μπορούν να εντοπιστούν και παλαιότερες εκδόσεις ενός αρχείου ή προγράμματος [31].

Μια ακόμη χρησιμότητα του κατακερματισμού είναι στη εύρεση κωδικών πρόσβασης του χρήστη. Στο σύστημα δεν αποθηκεύονται συνήθως οι κωδικοί αλλά οι hash τιμές τους για να αποτραπεί η είσοδος σε πιθανούς εισβολείς με εφαρμογή αντίστροφης μηχανικής (reverse engineering). Αλλά, με χρήση ωμής βίας (brute force), δηλαδή τη συνεχή χρησιμοποίηση λέξεων μέχρι να βρεθεί η σωστή ή να εξαντληθούν οι πόροι, ή τη χρήση λεξικών με συνήθεις κωδικούς, που μπορεί να βασιστούν σε προτιμήσεις του χρήστη ανάλογα με ιστοσελίδες που επισκέφτηκε

[1] http://foia.fbi.gov/cvip.htm

άλλα δεδομένα, υπολογίζονται οι τιμές hash και γίνεται συγκριτική ανάλυση μέχρι να βρεθεί κάποιο ταίριασμα [3, 6, 5].

Έχουν διατυπωθεί προβληματισμοί με το κατά πόσο η διαδικασία κατακερματισμού παρεμβαίνει στην ιδιωτική ζωή του ιδιοκτήτη των δεδομένων. Εντούτοις, η διαδικασία αυτή προστατεύει την ιδιωτικότητα του ατόμου επειδή από τις hash τιμές δεν υπολογίζονται τα αρχεία από τα οποία προήλθαν και δεν μπορεί να αποκαλύψει κανένα ουσιαστικό στοιχείο σχετικά με είδος και τις πληροφορίες του αρχείου. Αποτελεί μια λειτουργική αναγκαιότητα με την ελάχιστη δυνατή παρέμβαση σε προσωπικά δεδομένα [56].

3.1.1 Βασικοί Αλγόριθμοι Κατακερματισμού

Σε αυτό το σημείο περιγράφονται κάποιοι βασικοί αλγόριθμοι κατακερματισμού που εφαρμόζονται ευρύτατα σε διαδικασίες των Computer Forensics.

3.1.1.1 Cryptographic Hashes

Οι κρυπτογραφικοί αλγόριθμοι κατακερματισμού είναι ντετερμινιστικές διαδικασίες που δέχονται για είσοδο ένα αυθαίρετο μέγεθος δεδομένων και επιστρέφουν μια σταθερή συμβολοσειρά. Είναι οι παραδοσιακοί αλγόριθμοι που χρησιμοποιούνται για την επικύρωση του αποθηκευτικού μέσου των δεδομένων, τον εντοπισμό ακριβών αντιγραμμένων αρχείων και αρχεία που έχουν ενδιαφέρον ή αποφυγή αρχείων που σίγουρα δεν περιέχουν αποδείξεις. Η αλλαγή ενός μόνο bit διαμορφώνει τελείως διαφορετικά τη hash τιμή. Οι πιο γνωστοί αλγόριθμοι που χρησιμοποιούνται ευρέως είναι ο MD5 και ο SHA-1 [31, 72].

MD5 (Message-Digest algorithm 5): χρήση αφομοιωμένου μηνύματος μεγέθους 128 bits. Θεωρητικά είναι υπολογιστικά ανέφικτο η παραγωγή ίδιων τιμών MD5 από δύο διαφορετικά μηνύματα. Παρόλο που έχουν εμφανιστεί περιπτώσεις σύγκρουσης, δηλαδή από δυο διαφορετικά μηνύματα να υπολογιστεί ίδια τιμή κατακερματισμού, αυτό συμβαίνει μόνο κάτω από πολύ ειδικές συνθήκες και είναι σχεδόν αδύνατον να εμφανιστεί στη καθημερινή ζωή. Σχεδιάστηκε από τον Ron Rivest [5, 72, 45].

SHA-1 (Secure Hash Algorithm): είναι ένας αλγόριθμος συμπυκνωμένης απεικόνιση ενός μηνύματος ή αρχείου. Η απεικόνιση είναι καθορισμένου μεγέθους και χρησιμοποιείται σαν δαχτυλικό αποτύπωμα. Σχεδιάστηκε από τη National Security Agency [5, 72].

3.1.1.2 Rolling Hashes

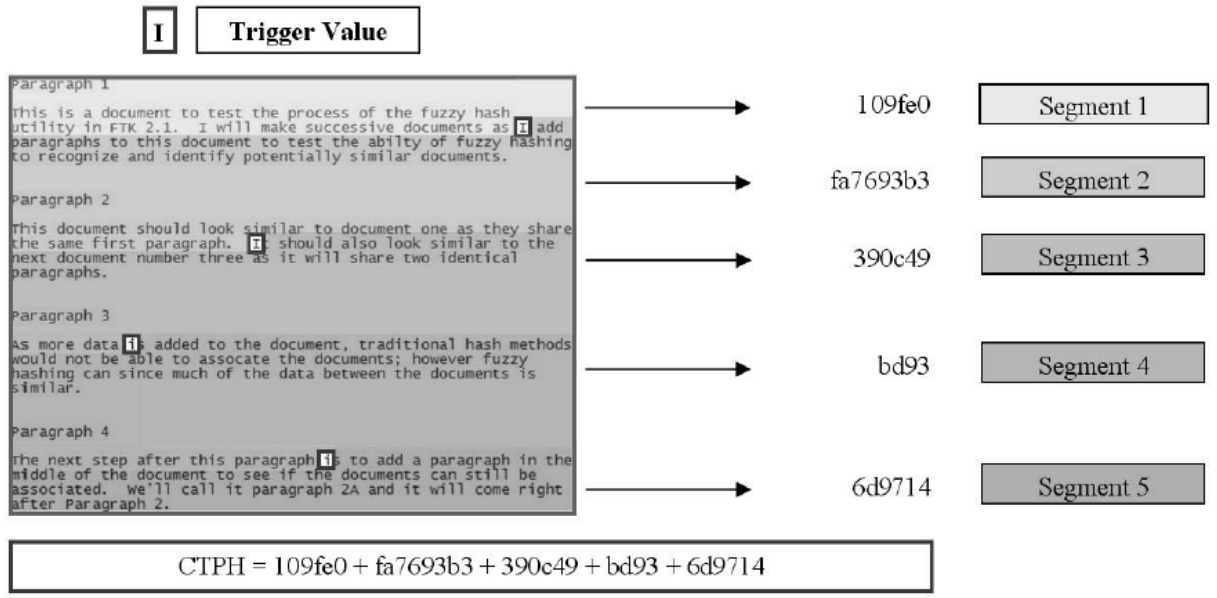
Ένας αλγόριθμος κυλιόμενου κατακερματισμού (rolling hash) προσδιορίζει τα όρια των τμημάτων με τη χρήση μιας τιμής ώθησης (trigger value), ή ενός σημείου αναστοιχειοθέτησης (reset point), που παράγεται από την rolling hash μηχανή για τον καθορισμό της θέσης δημιουργίας των τμημάτων. Μόλις τοποθετηθούν, τα δεδομένα πριν και μετά από κάθε σημείο αναστοιχειοθέτησης επεξεργάζονται για τη δημιουργία σειράς από παραδοσιακές συμβολοσειρές κατακερματισμού [31].

3.1.1.3 CTP Hashes

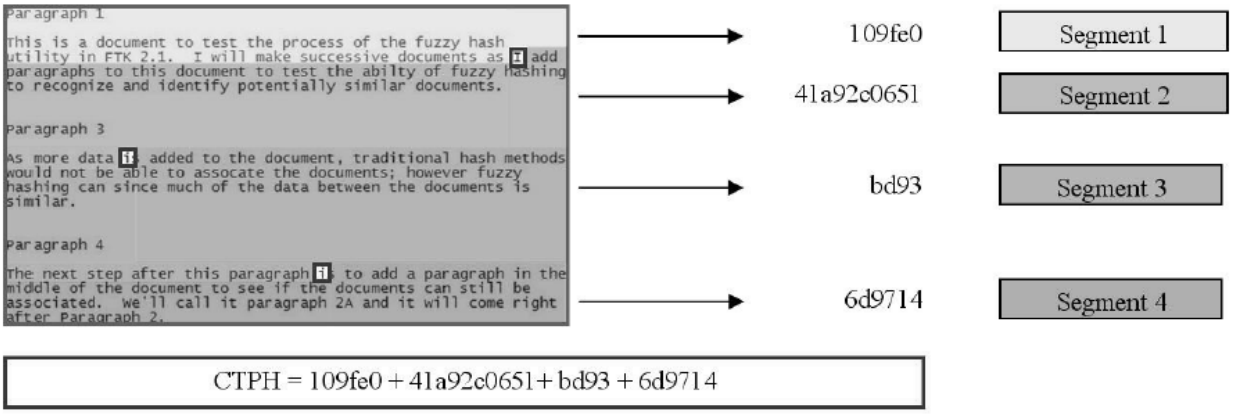
Οι Context Triggered Piecewise Hash βασίζονται σε τμήματα των παραδοσιακών hashes. Γίνονται συγκρίσεις μεταξύ αρχείων με παρόμοιες συμβολοσειρές δεδομένων που δεν είναι ακριβή αντίγραφα [31].

3.1.1.4 Fuzzy Hashing

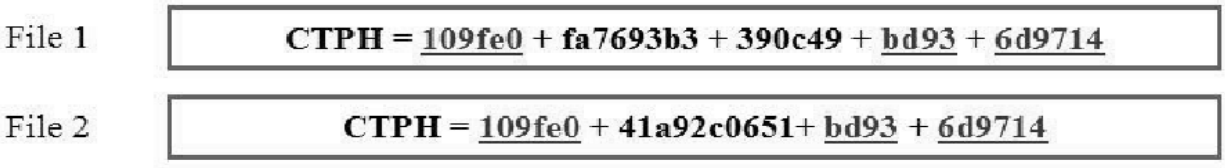
Ο ασαφής κατακερματισμός ανακαλύπτει πιθανά ενοχοποιητικά στοιχεία, που δεν μπορούν να εντοπιστούν με τις παραδοσιακές μεθόδους κατακερματισμού, συνδυάζοντας τους τρεις προαναφερθείς αλγορίθμους. Χρησιμοποιείται για παρόμοια αρχεία που δεν είναι ακριβώς ίδια, τα ονομαζόμενα ομόλογα αρχεία (homologous files). Ο CTP hash εκμεταλλεύεται τους αλγόριθμους rolling hash, που ορίζει τα τμήματα, και τον cryptographic, που υπολογίζει αξίες κατακερματισμού για κάθε κομμάτι ξεχωριστά, ώστε να δημιουργήσει μια τμηματοποιημένη hash για τον έλεγχο του αρχείο για ταιριαστές δυαδικές συμβολοσειρές [31].



Εικόνα 3: Context Trigged Piecewise Hash - Αρχικό αρχείο



Εικόνα 4: Context Trigged Piecewise Hash - Αλλαγμένο αρχείο



Εικόνα 5: Context Trigged Piecewise Hash – Σύγκριση τιμών

Στο παραπάνω παράδειγμα είναι εμφανείς οι ομοιότητες που εντοπίζονται μεταξύ των δύο αρχείων παρά τις αλλαγές, κάτι το οποίο θα ήταν αδύνατον με τη χρήση παραδοσιακών μεθόδων κατακερματισμού. Ωστόσο, ο fuzzy hash δεν είναι με όλα τα αρχεία τόσο αποτελεσματικός καθώς εξαρτάται από το μέγεθος της αλλαγής του αρχείου. Μετατροπές εκτός από το περιεχόμενο αλλά και στο μορφότυπο του αρχείου μπορούν να επηρεάσουν σημαντικά την απόδοσή του. Επιπρόσθετα, η δημιουργία των συνόλων fuzzy hash είναι χρονοβόρα και εφαρμόζεται αναγκαστικά σε αρχεία μεγαλύτερα από 100 bytes [31].

Σε περιπτώσεις που αναζητείται ένα συγκεκριμένο γνωστό αρχείο αλλά δεν μπορεί να εντοπιστεί στο ενεργό σύστημα αρχείων του υπόπτου, τότε εφαρμόζεται η fuzzy hash σε αυτό το αρχείο και στη συνέχεια ελέγχεται αν υπήρχε κάποια στιγμή το αρχείο στο σύστημα του υπόπτου. Επιπλέον, μπορεί να χρησιμοποιηθεί για αναγνώριση αρχείων που η κεφαλίδα τους έχει χαθεί όμως η επιτυχία του εξαρτάται από το είδος του μορφοτύπου του αρχείου [31].

3.2 Εικονική Αντιγραφή (Imaging)

Εικονική αντιγραφή είναι η διαδικασία παραγωγής ακριβών αντιγράφων των αρχικών δεδομένων. Είναι από τις σημαντικότερες τεχνικές που εφαρμόζονται στα Computer Forensics επειδή προστατεύεται η ακεραιότητα των αρχικών δεδομένων ενώ ο οποιοσδήποτε έλεγχος και επεξεργασία γίνεται στα αντιγραμμένα δεδομένα χωρίς την ύπαρξη συνεπειών από τη πιθανή μετατροπή των δεδομένων [6].

Ενώ και η απλή αντιγραφή περιέχει σχεδόν όλα τα δεδομένα, εκτός από κάποια μεταδεδομένα, η βασική διαφορά είναι ότι δεν απεικονίζεται η ακριβής θέση που είχε το αρχείο στον αρχικό δίσκο, το οποίο γίνεται με την εικονική αντιγραφή. Συγκεκριμένα, η δημιουργία ενός αντιγράφου bitstream, όπου κάθε φυσικός τομέας του αρχικού δίσκου αντιγράφεται με ειδικό τρόπο, εμφανίζει τα δεδομένα στην ίδια ακριβώς θέση [6].

Η αρχική χρήση της απεικόνισης δίσκων δεν ήταν για τα forensics, αλλά για τη μελέτη ιών στους υπολογιστές. Η απλή αντιγραφή των αρχείων του ιού δεν ήταν πάντα αποτελεσματική καθώς κάποιοι έπρεπε να βρίσκονται σε συγκεκριμένα σημεία του δίσκου για να ενεργήσουν. Με αυτό τον τρόπο μπορούσε να εκτελεστεί ο κώδικας του ιού χωρίς να κινδυνεύουν τα αρχικά

δεδομένα. Αργότερα αξιοποιήθηκε και στη διαδικασία της ψηφιακής έρευνας για τη προστασία των δεδομένων που συλλέγονταν [6].

Άλλες εφαρμογές του είναι στη δημιουργία ακριβών αντιγράφων ασφαλείας γρήγορα και εύκολα ειδικά για περιπτώσεις που μπορεί να εμφανιστεί ανάγκη για άμεση αντικατάσταση του αρχικού δίσκου, ή για την επιτάχυνση διαδικασιών σε μεγάλα υπολογιστικά συστήματα που έχουν τις ίδιες ρυθμίσεις. Για αυτές τις λειτουργίες το πιο διαδεδομένο εργαλείο είναι το Norton Ghost, τα αντίγραφα όμως που δημιουργεί δεν είναι bit-by-bit, έχουν τις ίδιες ρυθμίσεις και δεδομένα αλλά δεν είναι ακριβή [6].

Με βάση τις προαναφερθείσες εφαρμογές, οι μέθοδοι εικονικής αντιγραφής μπορούν να διακριθούν σε δυο κύριες κατηγορίες [5]:

- **Εικονική Αντιγραφή Μονάδας (Drive):** συλλογή όλων των δεδομένων της μονάδας συνήθως με τη δημιουργία μιας εικόνας ειδώλου (mirror image) η οποία μπορεί να είναι ακριβές αντίγραφο ή όχι. Συνήθως χρησιμοποιούνται για τη δημιουργία αντιγράφων ασφαλείας (backup).
- **Εικονική Αντιγραφή Κατά Τομέα ή bitstream**: αποτελεί μια πιο εξειδικευμένη μέθοδο η οποία ξεκινάει από την αρχή του δίσκου και αντιγράφει κάθε διφύο (bit) μέχρι το τέλος χωρίς τη διαγραφή ή μετατροπή του περιεχομένου. Χρησιμοποιείται για τη δημιουργία εικονικών αντίγραφων στα Computer Forensics.

Η εικονική αντιγραφή μπορεί να πραγματοποιηθεί με διάφορους τρόπους ανάλογα με τις συνθήκες της εκάστοτε υπόθεσης. Ένας τρόπος είναι η απομάκρυνση του δίσκου του υπόπτου και τη σύνδεσή του σε άλλο υπολογιστή κατά προτίμηση στο εργαστήριο forensics για τη δημιουργία του αντίγραφου. Όταν δεν είναι δυνατή η απομάκρυνση των μονάδων από το χώρο του συμβάντος μπορεί να γίνει σύνδεση ενός άλλου δίσκου στον υπολογιστή του υπόπτου. Εναλλακτικά, χρησιμοποιούνται ειδικές αυτόνομες συσκευές απεικόνισης όπως το RAID, ή μέσω δικτυακής σύνδεσης για παράδειγμα Ethernet, USB, modem, για τη μεταφορά των περιεχομένων του δίσκου σε άλλο υπολογιστή [6].

Οι ενέργειες που πρέπει να εκτελεί ένα εργαλείο εικονικής αντιγραφής δίσκων είναι η δημιουργία ενός αντίγραφου του αρχικού δίσκου ή τομέα ενώ παράλληλα δεν θα προκαλεί καμία μετατροπή, το οποίο επαληθεύεται με τη σύγκριση τιμών hash που υπολογίζονται πριν και

μετά την αντιγραφή. Επιπλέον, η εταιρεία DIBS ανέπτυξε το πρωτόκολλο Digital Integrity Verification and Authentication (DIVA) για να διασφαλίσει ότι τα αυθεντικά και τα αντιγραμμένα δεδομένα δεν έχουν μεταβληθεί [39, 57].

Το αντίγραφο μπορεί να αποθηκευτεί είτε σε έναν άλλο δίσκο ή να συμπιεστεί σε ένα εικονικό αρχείο (image file). Στη πρώτη περίπτωση όμως πρέπει να έχουν εφαρμοστεί ειδικές διαδικασίες καθαρισμού για να διαγραφούν πλήρως παλιότερα δεδομένα τα οποία θα μπορούσαν να επηρεάσουν την έρευνα. Σημαντική ενέργεια είναι και η καταγραφή λαθών εισόδου και εξόδου που παρουσιάζονται συνήθως κατά τη διάρκεια αντιγραφής ελαττωματικών δίσκων, καθώς και πληροφορίες σχετικά με την υπόθεση (ημερομηνία, ώρα, τοποθεσία) και τον υπεύθυνο της διαδικασίας αντιγραφής [39, 57, 4].

Επιπρόσθετες ικανότητες των εργαλείων δημιουργίας εικονικών αντιγράφων μπορούν να θεωρηθούν ο υπολογισμός τιμών hash εκτός από όλο το δίσκο αλλά και για κάποιο τμήμα χωριστά καθώς και η δυνατότητα σύγκρισης δίσκων ίδιου ή διαφορετικού μεγέθους. Ακόμα, να έχουν τη δυνατότητα να προσομοιώνουν ελαττωματικούς δίσκους με χρήση κατάλληλου λογισμικού ή άλλων συσκευών εάν απαιτείται. Όταν ο δίσκος προορισμού είναι μικρότερος από τον αρχικό πρέπει να παράγεται κατάλληλη προειδοποίηση, αλλά και αν είναι ο δίσκος μεγαλύτερος πρέπει να αναλύεται ο τρόπος αντιμετώπισης του πλεονάζοντα χώρου από το εργαλείο. Τέλος, αν ο αρχικός δίσκος είχε δυνατότητα εκκίνησης είναι επιθυμητό να έχει προστεθεί και στο αντίγραφο [39].

Για να αντιγραφεί γρήγορα και επιτυχώς ένα μεγάλο σύνολο δεδομένων αναπτύχθηκε το SmartSector Imaging το οποίο σαρώνει όλο το δίσκο και δημιουργεί εικονικά αντίγραφα μόνο των τομέων που εντοπίζονται δεδομένα. Μία άλλη μέθοδος είναι η εικονική αντιγραφή κατά αρχείο (File-by-file Imaging) η οποία διαβάζει κάθε κομμάτι αρχείου αλλά είναι πιο χρονοβόρα. Επιπλέον, προτείνεται η χρήση διαφορετικών εργαλείων για να εγγυηθούν την ακρίβεια των δεδομένων και να παρέχονται μέθοδοι συμπίεσης για τη μείωση του απαιτούμενου χώρου αποθήκευσης όλων των αποδεικτικών αρχείων [57].

Τα εργαλεία δημιουργίας εικόνων των δεδομένων (data imaging) διαφοροποιούνται ανάλογα με το σκοπό εφαρμογής τους συνεπώς τα παραγόμενα αποτελέσματα δεν είναι πάντα κατάλληλα για οποιονδήποτε σκοπό. Ένας ερευνητής στο τομέα των forensics δεν πρέπει να βασίζεται για

παράδειγμα σε εκδόσεις Ghost για τη δημιουργία αντιγραφών γιατί δεν παράγουν επακριβή αντίγραφα, εκτός αν δεν έχει καμία άλλη επιλογή εκείνη τη στιγμή [6].

Κατάλληλα εργαλεία που χρησιμοποιούνται στη ψηφιακή έρευνα είναι το SafeBack, το Encase και το ProDiscover. Κάποια αυτόνομα εργαλεία όπως το DIBS Portable Evidence Recovery Unit (PERU) και το Rapid Action Imaging Device (RAID) εξαλείφουν την ανάγκη ύπαρξης δεύτερου υπολογιστή, δημιουργούν τα αντίγραφα σε καθαρούς σκληρούς δίσκους ή οπτικά μέσα χωρίς την απομάκρυνση του αρχικού δίσκου από τον υπολογιστή του υπόπτου [6].

Επιπλέον έρευνες γίνονται για την κατανόηση των περιορισμών στο λογισμικό και υλισμικό της εικονικής αντιγραφής από το United States National Institute of Standards and Technology (NIST), καθώς και για τη καθιέρωση προτύπων στη συγκεκριμένη διαδικασία. Ένα πρόβλημα που έχει παρατηρηθεί σε κάποια εργαλεία είναι ότι σε ελάχιστες περιπτώσεις μπορεί να αποτύχουν να αποτυπώσουν το τελευταίο τομέα του δίσκου παρόλο που όλα τα άλλα στοιχεία είναι ακριβή. Ωστόσο μπορεί να αποδειχθεί ότι δεν υπάρχουν στοιχεία σε αυτό το τομέα επειδή πολλά λειτουργικά συστήματα το χρησιμοποιούν για να αποθηκεύσουν επιπλέον αντίγραφα κάποιων δεδομένων [4].

Τέλος, μπορεί να μην είναι δυνατή ή επιθυμητή η δημιουργία bitstream αντιγράφων οπότε εφαρμόζονται άλλοι μέθοδοι για τη συλλογή δεδομένων και ανάλυση του συμβάντος. Κάποια λογισμικά μπορούν να δημιουργήσουν ένα στιγμιότυπο της κατάστασης του υπολογιστή, όπως το Coroner’s Toolkit, και να παρέχουν πληροφορίες σχετικά με εργασίες που εκτελούνται, τη κατάσταση του δικτύου, διαγραμμένα αρχεία, πληροφορίες χρηστών και άλλα. Όταν απλά χρειάζεται η παρουσίαση ενός αρχείου και όχι άλλα δεδομένα τότε δεν χρειάζεται να αντιγραφεί όλος ο δίσκος, αρκεί μόνο η απόκτηση ενός αντιγράφου του συγκεκριμένου αρχείου [6].

3.3 Προστασία Εγγραφής (Write Blocker)

Ένα από τα σημαντικότερα μέτρα που πρέπει να λαμβάνονται κατά τη συλλογή δεδομένων είναι η προστασία εγγραφής. Ένας ερευνητής των Computer Forensics πρέπει οπωσδήποτε να διαθέτει εργαλεία που παρέχουν προστασίας από την εγγραφή νέων δεδομένων ή μεταβολή των υπαρχουσών. Χρησιμοποιείται για να αποτρέψει το λειτουργικό σύστημα να προκαλέσει



Εικόνα 6: Σύνδεση του iPhone στο φορητό υπολογιστή μέσω ενός USB write blocker.

οποιαδήποτε αλλαγή σε αποθηκευτικές συσκευές του υπόπτου, με σκοπό τη διατήρηση της ακεραιότητας των αποδεικτικών στοιχείων. Τα περισσότερα λογισμικά εργαλεία forensics έχουν ενσωματωμένη λειτουργία προστασίας εγγραφής, εντούτοις υπάρχουν και ειδικές συσκευές προστασίας για τη κάλυψη περισσότερων καταστάσεων και ιδιαίτερων αποθηκευτικών μέσων [5].

Η προστασία εγγραφής που εφαρμόζεται από κάποιο συγκεκριμένο λογισμικό εκτελείται μόνο στο λειτουργικό σύστημα που του αναλογεί και όχι σε διαφορετικά. Αντίθετα, μια συσκευή προστασίας είναι ανεξάρτητη από το λειτουργικό σύστημα επειδή εφαρμόζεται σε επίπεδο υλισμικού και αναχαιτίζει κάθε ηλεκτρονικό σήμα προς το αποθηκευτικό μέσο. Από τα πιο διαδεδομένα εργαλεία είναι το Digital Intelligence το οποίο αναγνωρίζει όλα τα πρότυπα μορφότυπα αποθηκευτικών συσκευών, ειδικά λογισμικά της Paraben τα οποία είναι κατάλληλα και για ασύρματες συσκευές αφού μπορούν να τις απομονώσουν και να φιλτράρουν οποιαδήποτε επικοινωνία, και το Wiebetech το οποίο παρέχει προστασία σε ένα ευρύ σύνολο συσκευών και συστημάτων [5].

3.4 Εξόρυξη Δεδομένων (Data Mining)

Η εξόρυξη δεδομένων είναι μια διαδικασία ανακάλυψης προτύπων και σχέσεων σε ένα σύνολο δεδομένων. Οι κύριοι στόχοι αυτής της διαδικασίας είναι η πρόβλεψη συμπεριφοράς κάποιων μεταβλητών που βασίζονται σε κάποιες άλλες, η περιγραφή προτύπων και η αναπαράσταση δεδομένων με όσο το δυνατόν πιο απλό και αξιοποιήσιμο τρόπο.

Για την επίτευξη αυτών των στόχων οι μέθοδοι εξόρυξης δεδομένων χρησιμοποιούν κάποιες βασικές διεργασίες, για παράδειγμα [1]:

- **Κατηγοριοποίηση (classification):** με βάση τα χαρακτηριστικά ενός αντικειμένου το αντιστοιχεί σε ένα προκαθορισμένο σύνολο.
- **Συσταδοποίηση (clustering):** καταμερίζει ένα ετερογενές σύνολο σε περισσότερα με βάση την ομοιότητα που παρουσιάζουν μεταξύ τους τα μέλη των συνόλων.
- **Κανόνες συσχέτισης (association rules):** ανακαλύπτουν σχέσεις μεταξύ των αντικειμένων ενός συνόλου.
- **Πρότυπα ακολουθιών (sequential patterns):** εξόρυξη προτύπων που εμφανίζονται πιο συχνά και είναι σχετικά με χρόνο ή άλλες ακολουθίες.
- **Απεικόνιση και μείωση διαστάσεων:** χρήση τεχνικών, όπως παράλληλες συντεταγμένες, για την απεικόνιση της κατανομής δεδομένων υψηλών διαστάσεων και για τη μείωση των διαστάσεων του χώρου.

Τα τελευταία χρόνια έχει διαδοθεί αρκετά η χρήση μεθόδων εξόρυξης δεδομένων στο τομέα των Computer Forensics, κυρίως για τον εντοπισμό των σημαντικότερων και πιο σχετικών αποδείξεων. Τεχνικές που εφαρμόζονται είναι η μαζική συλλογή δεδομένων, η στατιστική ανάλυση και η επαγωγική μάθηση, τα οποία απαιτούν μεγάλο σύνολο δεδομένων για να εξαχθούν πληροφορίες και να εντοπιστούν πρότυπα. Με την αξιοποίηση μεθόδων εξόρυξης εντοπίζονται συσχετίσεις ανάμεσα σε δεδομένα από διαφορετικές πηγές που φαινομενικά δεν υπήρχαν [41].

Η εξόρυξη δεδομένων έχει διαδοθεί ευρέως στην εξιχνίαση οικονομικών υποθέσεων όπου εξειδικεύεται η δικανική λογιστική (forensic accounting) και λόγω του μεγάλου αριθμού ψηφιακών αρχείων εφαρμόζονται τεχνικές Computer Forensics. Ο συγκεκριμένος κλάδος forensics έχει στόχο τον εντοπισμό ενεργειών που υποδεικνύουν ξέπλυμα χρήματος ή άλλες απάτες σε μια εταιρία ή οργανισμό. Οι μέθοδοι εξόρυξης βοηθάνε στην εύρεση σχέσεων ανάμεσα σε αριθμητικά και μη δεδομένα, καθώς και στην αναζήτηση για εξαιρέσεις, ασυνήθιστα στοιχεία, πρότυπα ή ύποπτες συναλλαγές [8, 49].

Ανάμεσα σε τεχνικές που έχουν προταθεί για την αντιμετώπιση του συγκεκριμένου είδους εγκλημάτων είναι και η Hybrid Evidence Correlation (HEC) η οποία εξετάζει ασυνήθιστα και ύποπτα πρότυπα με σκοπό τον αυτόματο εντοπισμό οικονομικής απάτης [8]. Η αποτελεσματικότητα αυτών των τεχνικών απαιτεί, εκτός από μεγάλο μέγεθος δεδομένων, κατάλληλη επιλογή μεταβλητών. Ακόμα, πρότυπα που είχαν αναγνωριστεί παλιότερα τώρα

μπορεί να μην ισχύουν, αλλά και νέοι τύποι απάτης να μην έχουν αναγνωριστεί ακόμα συνεπώς να μην εντοπίζονται. Επομένως, η χρήση τους πρέπει να συνοδεύεται από ειδικευμένο προσωπικό για τον εντοπισμό λαθών και την καλύτερη αναζήτηση [49].

Μία άλλη εφαρμογή είναι η αυτόματη σύνδεση ανόμοιων πληροφοριών για την αντιμετώπιση της τρομοκρατίας. Εργαλεία όπως το Total Information Awareness (TIA) χρησιμοποιούν μεθόδους εξόρυξης δεδομένων για τον εντοπισμό τρομοκρατών μέσω του συνεχώς αυξανόμενου συνόλου των δημόσια διαθέσιμων δεδομένων. Αλλά έχει ως έμμεση επίπτωση τον έλεγχο προσωπικών πληροφοριών πολλών μη ύποπτων ατόμων και πιθανή χρησιμοποίησή τους για μη θεμιτούς σκοπούς [41].

Η διεύρυνση των τρόπων επικοινωνίας μέσω του διαδικτύου είχε ως αποτέλεσμα την ανάπτυξη εφαρμογών άμεσων μηνυμάτων (Instant Messaging - IM). Αρχικά προοριζόταν για προσωπικές επικοινωνίες αλλά αργότερα επεκτάθηκε σε οργανισμούς για την παροχή εύκολης εσωτερικής επικοινωνίας. Με τη μεγαλύτερη διάδοση τα άμεσα μηνύματα έγινα πιο επιρρεπείς σε επιθέσεις τύπου man-in-the-middle attack, ή στη παράνομη πρόσβαση στον υπολογιστή του χρήστη, οπότε δεν είναι πάντα γνωστό ποια πρόσωπα όντως επικοινωνούν [7].

Γι’ αυτόν το λόγο αναπτύχθηκαν τεχνικές που χρησιμοποιούν κατηγοριοποίηση της εξόρυξης δεδομένων για την αναγνώριση των μελών που επικοινωνούν μέσω γλωσσικών προτύπων και χαρακτηριστικών. Δημιουργείται αρχικά ένα σύνολο χαρακτηριστικών από ένα μεγάλο αριθμό μηνυμάτων ενός χρήστη IM και στη συνέχεια κατηγοριοποιούνται με βάση ομοιότητες με γνωστές συμπεριφορές συγκεκριμένων ατόμων για την αναγνώρισή του [7].

Επιπλέον, σε μεγάλες βάσεις δεδομένων που περιέχουν forensic εικόνες, όπως δαχτυλικά αποτυπώματα, αποτυπώματα παπουτσιών, γραφικούς χαρακτήρες, πρόσωπα και άλλα, μπορεί να εφαρμοστεί η εξόρυξη δεδομένων για την αναζήτηση ταιριάσματος με βάση το σχήμα, χρώμα και άλλα χαρακτηριστικά. Η μέθοδος αυτή έχει σκοπό την μείωση των συσχετίσεων και έπειτα την εξακρίβωσή τους από κάποιον ειδικό, ο οποίος μπορεί να εντοπίσει καλύτερα από μια αυτοματοποιημένη μηχανική διαδικασία τις ομοιότητες, αλλά δεν είναι εφικτό να ελέγξει από την αρχή μεγάλες ποσότητες δεδομένων [62].

Τεχνικές που εφαρμόζουν μεθόδους εξόρυξης δεδομένων έχουν αναπτυχθεί και για τη βελτίωση της διαδικασίας αναζήτησης αποδείξεων με τον αυτόματο προσδιορισμό στόχων που πιθανόν

διαθέτουν χρήσιμα δεδομένα, αλλά και για τον εντοπισμό αρχείων και καταλόγων που δημιουργήθηκαν ή μεταβλήθηκαν κατά τη διάρκεια ενός συμβάντος. Ωστόσο, παρουσιάζουν υψηλό ποσοστό λανθασμένων θετικών αποτελεσμάτων (false positives) κυρίως λόγω της δυσκολίας προσδιορισμού των χαρακτηριστικών που θα μπορούσαν να έχουν τα αποδεικτικά στοιχεία. Περισσότερες έρευνες απαιτούνται σε αυτό το τομέα καθώς η αποτελεσματικότητά τους δεν είναι ίδια σε κάθε σύστημα και σε όλες τις συνθήκες [11].

4 Προβλήματα και Δυσκολίες

Στο τομέα των Computer Forensics εμφανίζονται κάποια βασικά προβλήματα, τα οποία μπορεί να θέσουν σε κίνδυνο την αξιοπιστία των αποτελεσμάτων. Παρακάτω αναλύονται κάποιες από αυτές τις δυσκολίες και προτεινόμενοι τρόποι αντιμετώπισής τους. Ιδιαίτερη έμφαση δίνεται στις σημάνσεις χρόνου επειδή αποτελεί ένα από τα πιο δισεπίλυτα ζητήματα και στη συνέχεια αναλύονται άλλα προβλήματα που εμφανίζονται κατά τη διάρκεια της ψηφιακής έρευνας, όπως κρυπτογραφημένα αρχεία, χρήση εργαλείων antiforensic και άλλα.

Στις περισσότερες δύσκολες περιπτώσεις που αναλύονται έχουν βρεθεί τρόποι και εργαλεία για την αντιμετώπισή τους. Ωστόσο, έρευνες συνεχώς διεξάγονται για την αντιμετώπιση νέων προκλήσεων αλλά και για τη βελτίωση των τωρινών μεθόδων στοχεύοντας στην αύξηση της αποδοτικότητας και των θετικών αποτελεσμάτων. Τέλος, από τα μεγαλύτερα προβλήματα του τομέα είναι η έλλειψη επαρκής προτυποποίησης μεθόδων και πιστοποίησης ατόμων προκαλώντας δυσκολίες στην αντιμετώπιση διεθνών υποθέσεων.

4.1 Σημάνσεις χρόνου (Timestamps)

Ο σωστός προσδιορισμός ημερομηνίας και ώρας ενός γεγονότος παίζει καθοριστικό ρόλο στη διαλεύκανση μιας υπόθεσης. Οι σωστοί χρόνοι των ψηφιακών γεγονότων μπορούν να συνδυαστούν με φυσικά γεγονότα και να κατοχυρώσουν μια σχέση αιτίας και αποτελέσματος σε μια έρευνα forensics. Μπορούν να δώσουν άλλοθι στον ύποπτο ή να το καταρρίψουν, καθώς και να συμβάλουν στη δημιουργία ενός χρονοδιαγράμματος που θα βοηθήσει στην αναπαράσταση και κατανόηση του συμβάντος [9, 24].

Πολλοί λόγοι όμως μπορούν να συντελέσουν στην εμφάνιση λανθασμένης ώρας ή και ημερομηνίας στο σύστημα, δηλαδή να μην συμβαδίζει με τη πραγματική ώρα που είναι σύμφωνη με το Coordinated Universal Time (UTC). Οι δυσκολίες εξακρίβωσης της χρονικής στιγμής που έγινε μια ενέργεια, καθώς και αν μια προσωρινή συμπεριφορά του υπολογιστή ήταν συνεπής καθ’ όλη τη διάρκεια της λειτουργίας του, αποτελούν από τις πιο συχνές προκλήσεις σε μια ψηφιακή διερεύνηση [4, 9].

Κάθε ψηφιακό αρχείο χαρακτηρίζεται από τρεις βασικούς χρόνους, το χρόνο δημιουργίας τους (Create timestamp), το χρόνο πρόσβασης (Access timestamp), και το χρόνο μετατροπής (Modify timestamp), οι οποίοι αποτελούν τα μεταδεδομένα MAC του αρχείου. Ο χρόνος δημιουργίας προσδιορίζει πότε δημιούργησε ο χρήστης το αρχείο, ο χρόνος πρόσβασης δείχνει τη τελευταία φορά που είχε κάποιος πρόσβαση στο συγκεκριμένο αρχείο, ενώ ο χρόνος μετατροπής δείχνει πότε έγινε η τελευταία μετατροπή [5].

Οι χρόνοι αυτοί συνήθως ορίζονται με βάση το ρολόι του λειτουργικού συστήματος το οποίο είναι σύμφωνο με το Real Time Clock, δηλαδή το ρολόι του υπολογιστή. Εξαιτίας της μη σταθερότητας των υλικών του ρολογιού, ανά τακτά διαστήματα είναι απαραίτητος ο συγχρονισμός με την κατάλληλη ζώνη ώρας της περιοχής ή απευθείας με το UTC. Επιπλέον, για το συγχρονισμό των υπολογιστών και άλλων δικτυακών συσκευών αναπτύχθηκε το Network Time Protocol (NTP), ο στόχος του οποίου είναι να διατηρεί με ακρίβεια millisecond το χρόνο σύμφωνα με το UTC [5, 9].

Άλλες αιτίες που μπορούν να επηρεάσουν την ακρίβεια των αναγραφόμενων χρόνων είναι η μετατόπιση ή λοξότητα του ρολογιού, καθώς και περιβαλλοντολογικοί παράγοντες όπως η θερμοκρασία, τάση, θόρυβος, ή λάθη στο λογισμικό του ρολογιού και πιθανές παρερμηνείες, χωρίς να γίνεται πάντα αισθητή η αλλαγή. Επιπλέον, η τοποθεσία παίζει ουσιαστικό ρόλο στη ρύθμισή του λόγω του συγχρονισμού με τη τοπική ώρα. Ο πιο απρόβλεπτος όμως παράγοντας είναι ο ανθρώπινος επειδή μπορεί να αλλοιώσει την ώρα με λανθασμένες ρυθμίσεις κατά λάθος ή κατά βούληση με σκοπό συνήθως την κάλυψη αποδεικτικών στοιχείων [9].

Η μετατροπή της ημερομηνίας και ώρας κατά τη δημιουργία ενός αρχείου είναι από τις πιο συνηθισμένες επιτήδειες ενέργειες και εμφανίζονται κυρίως σε περιπτώσεις οικονομικού εγκλήματος. Αλλά κάθε ενέργεια αλλαγής ώρας αφήνει ίχνη τα οποία με κατάλληλη έρευνα μπορούν να εντοπιστούν [60]. Για παράδειγμα, σημάνσεις χρόνου μπορούν να βρεθούν σε HTTP δεδομένα, κεφαλίδες από ηλεκτρονική αλληλογραφία και άλλα δεδομένα που αποθηκεύτηκαν από κάποια δικτυακή επικοινωνία και μπορούν να συμβάλουν στην εξακρίβωση της πραγματικής ώρας ενός γεγονότος [24].

Μια επιπρόσθετη αιτία εμφάνισης λανθασμένων χρόνων είναι η δυσκολία συσχέτισης χρονικών σημάνσεων από διαφορετικά ρολόγια υπολογιστών που δεν είναι συγχρονισμένα. Η πιο

συνηθισμένη τακτική αντιμετώπισης αυτού του προβλήματος είναι η καταγραφή των χρόνων στα αρχικά στάδια της έρευνας και σύγκρισή τους με ένα αξιόπιστο διακομιστή ώρας [9]. Ωστόσο, υπάρχει το ενδεχόμενο προηγούμενης μετατροπής και στη συνέχεια επαναφοράς του στη πραγματική ώρα. Σε αυτές τις περιπτώσεις έχουν προταθεί διάφορες τεχνικές από ερευνητές για τον εντοπισμό τέτοιων αλλαγών οι οποίες αναλύονται παρακάτω.

Για τον εντοπισμό αλλαγών στους χρόνους, οι Schatz et. al. προσπάθησαν να αναπτύξουν μια αυτόματη διαδικασία αναγνώρισης της χρονικής συμπεριφοράς του συστήματος συσχετίζοντας έμπιστες σημάνσεις χρόνου σε ψηφιακές αποδείξεις με έμπιστες πηγές ώρας. Χρησιμοποιήθηκαν εγγραφές του ιστορικού και της κρυφής μνήμης του περιηγητή ιστού (browser) ως πηγή χρόνων πρόσβασης και επεξεργασίας, λόγω της παρουσίας του συγκεκριμένου είδους λογισμικού σχεδόν σε κάθε σύστημα [9].

Μια παρόμοια μέθοδος είναι αυτή του Weil, η οποία εφαρμόζει μια δυναμική ανάλυση της χρονικής συμπεριφοράς του συστήματος συσχετίζοντας σημάνσεις χρόνου με τους χρόνους πρόσβασης και μετατροπής των αρχείων στο ευρετήριο κρυφής μνήμης του Διαδικτύου. Ο σκοπός της είναι η προσαρμογή των εμφανιζόμενων MAC χρόνων στη πραγματική ώρα και η αποκόμιση της πραγματικής ώρας του συστήματος [59].

Οι Gladyshev και Patel εφάρμοσαν μια τεχνική όπου χρησιμοποιούν επιβεβαιωμένες πηγές ώρας για να προσδιορίσουν τα χρονικά όρια γεγονότων που δεν είναι γνωστό πότε ακριβώς έγιναν. Πιο αναλυτικά, γνωρίζοντας ένα προγενέστερο και ένα μεταγενέστερο γεγονός πότε ακριβώς έγιναν μπορεί να προσδιοριστεί περίπου πότε έγινε κάποιο ενδιάμεσο γεγονός [50].

Μια εναλλακτική προσέγγιση που προέρχεται από τον Willassen είναι η χρήση υποθέσεων και στη συνέχεια ελέγχεται κατά πόσο μπορεί να είναι συνεπής με τις σημάνσεις χρόνου που έχουν εντοπιστεί στις αποδείξεις μέσω της κατασκευής ενός μοντέλου ενεργειών που επηρεάζουν τους συγκεκριμένους χρόνους στο σύστημα που διερευνάται. Αναλυτικότερα, δημιουργείται μια λίστα με τις πιθανές σειρές σημάνσεων χρόνων και εντοπίζονται οι σειρές εκείνες που είναι εφικτές καθώς και η σειρά ενεργειών που μπορεί να τις προκαλέσει [61].

Για το συγχρονισμό ρολογιών από διαφορετικά συστήματα, ο Stevens ανέπτυξε ένα μοντέλο όπου γίνεται συσχέτιση σημάνσεων χρόνου από πολλαπλά χρονοδιαγράμματα. Συγκεκριμένα,

ορίζεται ένα βασικό ρολόι που ακολουθεί το UTC και τα ρολόγια από τα άλλα υπολογιστικά συστήματα ορίζονται αναλόγως [9]. Μια παρόμοια λειτουργία σχεδίασε και ο Buchholz με μετατροπή των χρόνων σε μια κοινή ώρα αναφοράς [15].

Πέρα από τεχνικές, αναπτύχθηκαν και πολλά εργαλεία για την εύρεση των σημάνσεων χρόνων και την ανάλυση χρονοδιαγραμμάτων. Για παράδειγμα το Sleuthkit και το Helix παράγουν χρονοδιαγράμματα αλλά είναι περιορισμένα σε συγκεκριμένες μορφές αρχείων εισόδου και εξόδου. Άλλα εργαλεία που περιέχουν παρόμοιες δυνατότητες είναι το EnCase και το EasyTimeline, αλλά πιο εξελιγμένο θεωρείτε το Zeitline το οποίο δέχεται πολλών ειδών αρχείων και παρέχει ικανοποιητική οπτικοποίηση των αποτελεσμάτων. Εργαλεία που βρίσκονται ακόμα σε φάση ανάπτυξης είναι το Ex-Tip, το οποίο σχεδιάστηκε με Perl [18], το TimeStampLogic στόχος του οποίου είναι ο εντοπισμός αρχείων με αλλαγμένες σημάνσεις χρόνων [60], καθώς και το CyberForensic Timelab το οποίο κατατάσσει τα αρχεία με βάση τις χρονικές μεταβλητές και σχεδιάζει ένα χρονοδιάγραμμα [34].

Εκτός από τα αρχεία του υπόπτου, ανάγκη για σωστές σημάνσεις χρόνων υπάρχει και για τα στοιχεία που θα παρουσιαστούν στο τέλος μια έρευνας. Για την εξασφάλιση της χρονικής ακεραιότητας και την αδιαμφισβήτητη σύνδεση των αποδεικτικών στοιχείων με τους αντίστοιχους χρόνους πρέπει να υπάρχει ιχνηλασιμότητα σε νόμιμες πηγές ώρας, ο χρόνος διανομής να μην είναι επιρρεπής σε επιθέσεις και αλλαγές και να εφαρμοστούν μέτρα ασφάλειας στις ψηφιακές σημάνσεις χρόνου [30].

4.2 Ψηφιακές Αποδείξεις

Η διαδικασία της αναζήτησης, συλλογής και ανάλυσης ψηφιακών δεδομένων κρύβει αρκετές δυσκολίες και προκλήσεις για τον ερευνητή. Μια λάθος ενέργεια μπορεί να προκαλέσει από μικρές αλλαγές μέχρι τη καταστροφή των δεδομένων. Επιπλέον, είναι δύσκολο να οριστεί ποιες πρακτικές είναι οι καταλληλότερες σε μια έρευνα έτσι ώστε να θεωρούνται τα αποτελέσματα αποδεκτά από όλους, γι’ αυτό το λόγο έχει οριστεί ένα σύνολο καλών πρακτικών που μπορούν να εφαρμοστούν [4].

Η συλλογή πάρα πολλών αποδείξεων δημιουργεί αρκετά προβλήματα στην αναζήτηση αποδείξεων, οπότε πρέπει να περιοριστούν, ενώ αν είναι πολύ λίγες μπορεί να σημαίνει ότι παραλήφθηκαν άλλες αποδείξεις. Μεγαλύτερη πιθανότητα υπάρχει να έχουν αγνοηθεί δεδομένα από τις καταγραφές του δικτύου που σχετίζονται με δικτυακά σημεία, παραδείγματος χάρη δεδομένα κατά τη μεταφορά, ή διαγραμμένα αρχεία, αντίγραφα ασφαλείας και άλλα [4].

Κατά τη διάρκεια αναζήτησης αποδείξεων πρέπει να αξιολογηθούν τα δεδομένα έτσι ώστε να μην θεωρηθούν λανθασμένα σημαντικά στοιχεία ενώ δεν είναι ή αντίστροφα στοιχεία που είναι σημαντικά να μην ληφθούν υπόψη [4]. Για την μείωση μεγάλων ποσοτήτων δεδομένων και αποφυγή παράβλεψης πιθανών αποδεικτικών στοιχείων χρησιμοποιούνται διάφορες τεχνικές κατακερματισμού, εξόρυξης δεδομένων και άλλες [32].

Επιπλέον, κάποιες πληροφορίες μπορεί να μην αναζητούνται είτε επειδή αγνοείται η ύπαρξή τους και η σχέση που μπορεί να έχουν με την υπόθεση, είτε είναι άγνωστη η τοποθεσία τους ή μπορεί να απαγορεύεται η πρόσβαση σε αυτές. Σε κάποιες περιπτώσεις η αναζήτησή τους ίσως να μην είναι επιθυμητή για διάφορους λόγους, όπως η ύπαρξη χρονικών περιορισμών ή οι ελάχιστοι πόροι να μην επιτρέπουν την αναζήτηση όλων των ειδών πληροφοριών σε ολόκληρο το υπολογιστικό σύστημα [4].

Ωστόσο, σημαντικές πληροφορίες, ειδικά σε καταγραφές εξυπηρετητών, που είναι για ένα ορισμένο χρονικό διάστημα αποθηκευμένα, πρέπει να εντοπίζονται γρήγορα πριν τη διαγραφή τους. Σε αυτή τη φάση παρουσιάζονται προβλήματα κατά την καταγραφή των σταδίων φύλαξης επειδή συμμετέχει μεγάλος αριθμός ατόμων στη μεταφορά των δεδομένων. Άλλες αποδείξεις που δεν αποθηκεύονται μόνιμα, όπως στη μνήμη RAM, πρέπει να συλλεχθούν απευθείας στο χώρο του συμβάντος με ειδικές διαδικασίες και από εκπαιδευμένο προσωπικό [4].

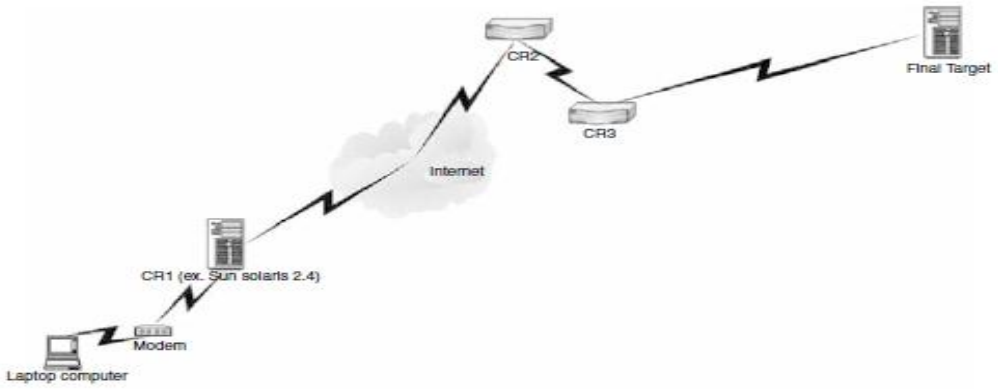
Ένα άλλο πρόβλημα κατά την έρευνα είναι η εμφάνιση μη αληθινών αποδείξεων. Εάν δεν υπάρχουν σοβαρές ενδείξεις ή καταγγελία είναι δύσκολο να ξεχωρίσουν τα στοιχεία που τοποθετήθηκαν από τις πραγματικές αποδείξεις. Αλλά και ο ύποπτος μπορεί να ισχυριστεί ότι πραγματικές αποδείξεις είναι πλαστές και τοποθετήθηκαν εν αγνοία του για να αποφύγει τη δίωξη. Αυτές οι περιπτώσεις αντιμετωπίζονται με τον εντοπισμό της προέλευσης των συγκεκριμένων στοιχείων καθώς και με τον έλεγχο για ιούς ή άλλα κακόβουλα λογισμικά που μπορεί να προκάλεσαν τη δημιουργία τους [4].

Επιπρόσθετα, πρέπει να ελεγχθεί κατά πόσο ένα πρόγραμμα δημιούργησε ή μετέτρεψε ένα αρχείο, το οποίο αποτελεί αποδεικτικό στοιχείο. Πρέπει να εξασφαλιστεί ότι το χρονικό διάστημα που έγινε η επεξεργασία το πρόγραμμα ήταν ενεργό και έχει τη δυνατότητα δημιουργίας και μετατροπής του συγκεκριμένου είδους αρχείου, το δικαίωμα να το κάνει αλλά και να καθοριστεί η προέλευση της εντολής που προκάλεσε τη συγκεκριμένη λειτουργία, αν ήταν από τον χρήστη ή από κάποιο άλλο πρόγραμμα [4]. Για την εξακρίβωση των παραπάνω στοιχείων είναι απαραίτητο ο ερευνητής να γνωρίζει τον τρόπο λειτουργίας των προγραμμάτων και να κατανοεί διαφορές σε μορφότυπα αρχείων [32].

Συχνά, κυρίως σε αστικές υποθέσεις, παρατηρούνται μετατροπές σε ψηφιακά αρχεία, κυρίως εικόνας και ήχου, με σκοπό τη δημιουργία παραπλανητικών εντυπώσεων. Οι αλλαγές αυτές στην πλειοψηφία τους μπορούν εύκολα να εντοπιστούν, για παράδειγμα σε μια εικόνα ελέγχονται το φώς, οι σκιές, εμφανίσεις ακατάλληλης κλιμάκωσης γωνίας και αποστάσεων, και άλλα χαρακτηριστικά που υποδεικνύουν πιθανές μεταβολές, άρα και πλαστά στοιχεία [4].

Όσο αφορά την αναζήτηση αποδείξεων στο διαδίκτυο, έχουν βρεθεί τρόποι απόκρυψής τους, για παράδειγμα με χρήση κρυφών καναλιών για την αποφυγή ανάλυσης κυκλοφορίας. Ακόμα, έχει αναπτυχθεί το εργαλείο NCovert το οποίο χρησιμοποιεί τεχνικές εξαπάτησης (spoofing) για να κρύψει τη πηγή επικοινωνίας και τα δεδομένα που μεταφέρονται στο δίκτυο [4].

Επίσης, έχει ανακαλυφθεί ένας εναλλακτικός τρόπος δρομολόγησης, ο Onion Routing, όπου δεν είναι εφικτή η ανάλυσης κυκλοφορίας πακέτων εξαιτίας της χρήσης κρυπτογραφικών μεθόδων στη δικτύωση με αποτέλεσμα να εμφανίζονται ως ανώνυμα πακέτα. Πιο αναλυτικά, μια ομάδα onion routers είναι κατανεμημένη στο δίκτυο με σκοπό τη κρυπτογράφηση των συνδέσεων υποδοχής (socket connections) και τη λειτουργία τους ως πληρεξούσιοι (proxy). Τα βασικά πλεονεκτήματά της είναι η αμφίδρομη επικοινωνία σε πραγματικό χρόνο, ανεξάρτητη από εφαρμογές και δεν υπάρχει κάποιο κεντρικό στοιχείο το οποίο θα μπορούσε να αποτελέσει αδυναμία της συγκεκριμένης τεχνικής [25].



Εικόνα 7: Παράδειγμα Onion Routing

Δυσκολίες προκαλούνται και από εξωτερικούς παράγοντες, όπως το νομοθετικό σύστημα, όπου η μη εφαρμογή νόμιμων μεθόδων και τεχνικών οδηγεί στην μη αποδοχή των αποδείξεων. Η κάθε λεπτομέρεια μετράει και οποιαδήποτε μη νομικά αποδεκτή κίνηση μπορεί να προκαλέσει την απόρριψη των αποδεικτικών στοιχείων και τελικά την αθώωση του υπόπτου. Ένα τέτοιο παράδειγμα είναι η καταγραφή δεδομένων η οποία συνήθως πρέπει να είναι γνωστή σε όλους όσους συμμετέχουν στην επικοινωνία διαφορετικά δεν γίνεται αποδεκτή σε ένα δικαστήριο ανεξάρτητα από τις πληροφορίες που μπορεί να αποκαλύπτονται. Τέλος, τα συμπεράσματα στα οποία καταλήγει ο ερευνητής πρέπει να στηρίζονται σε αξιόπιστα στοιχεία και όχι σε αυθαίρετες υποθέσεις [4].

Όλες οι δυσκολίες και προκλήσεις που εντοπίζονται κατά τη διάρκεια μιας έρευνας μπορούν να αντιμετωπιστούν επιτυχώς και να διασφαλιστεί η ακεραιότητα και αξιοπιστία των αποτελεσμάτων της. Αν και είναι εύκολη η καταστροφή ή μετατροπή δεδομένων κατά λάθος ή επίτηδες, η χρήση των εικονικών αντιγράφων προστατεύει τα αυθεντικά δεδομένα. Αλλά και η ευκολία αντιγραφής και αποθήκευσης σε πολλά μέσα διευκολύνουν τον εντοπισμό δεδομένων σε πολλαπλά σημεία. Συμπερασματικά, η εφαρμογή επιστημονικών μεθόδων και εργαλείων ανταπεξέρχεται επιτυχώς στις περισσότερες δύσκολες συνθήκες έρευνας ψηφιακών αποδείξεων.

4.3 Κρυπτογράφηση / Στεγανογράφηση

Η χρήση κρυπτογράφησης και στεγανογράφησης είχε ως αρχικό σκοπό τη προστασία δεδομένων από τρίτα άτομα. Στόχος τους είναι η αποκάλυψη των δεδομένων σε συγκεκριμένα

άτομα και η προστασία της ακεραιότητάς τους [6]. Ωστόσο πολλοί εκμεταλλεύονται αυτές τις τεχνικές για την απόκρυψη πληροφοριών και πιθανών αποδεικτικών στοιχείων από μία έρευνα. Παρόλα αυτά υπάρχουν τρόποι για να ξεπεραστεί αυτό το εμπόδιο σε ένα ικανοποιητικό αριθμό περιπτώσεων.

Η κρυπτογράφηση είναι μια διαδικασία που μετατρέπει ένα απλό ψηφιακό αντικείμενο σε μη αναγνωρίσιμη μορφή με τη χρήση μιας μαθηματικής μεθόδου. Εφαρμόζεται συνήθως σε ψηφιακές υπογραφές, πιστοποιητικά και στη προστασία δικτυακών συναλλαγών. Η αποτελεσματικότητά της εξαρτάται από το μέγεθος του κλειδιού και στη δυσκολία εύρεσής του. Δύο είναι οι βασικές κατηγορίες κρυπτογράφησης, η συμμετρική και η ασύμμετρη [2, 6].

Η συμμετρική κρυπτογράφηση χρησιμοποιεί ένα κλειδί . Το κλειδί αυτό πρέπει να είναι γνωστό στον αποστολέα και στον παραλήπτη για να μπορέσει ο παραλήπτης να αποκρυπτογραφήσει το μήνυμα. Αυτό αποτελεί είναι το κυριότερο μειονέκτημα αυτής της κατηγορίας κρυπτογράφησης γιατί με κάποιο ασφαλή τρόπο πρέπει να γίνει η ανταλλαγή του κλειδιού χωρίς να μαθευτεί από άλλους. Στη περίπτωση όμως που απλά ο ύποπτος θέλει να αποκρύψει δεδομένα κατά την έρευνα δεν εμφανίζεται αυτό το πρόβλημα, παρά μόνο αν επικοινωνήσει με κρυπτογραφημένα μηνύματα με κάποιο συνεργό. Ο Data Encryption Standard (DES), ο triple-DES και ο Advanced Encryption Standard (AES) αποτελούν παραδείγματα συμμετρικής κρυπτογράφησης.

Στην ασύμμετρη κρυπτογράφηση γίνεται χρήση ενός ζευγαριού κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Το ιδιωτικό κλειδί δεν γίνεται γνωστό σε κανένα, ενώ το δημόσιο είναι διαθέσιμο σε όλους. Λόγω των μαθηματικών συναρτήσεων που χρησιμοποιούνται ο υπολογισμός των ιδιωτικών κλειδιών από το κρυπτογραφημένο μήνυμα είναι δύσκολος και χρονοβόρος. Η ασύμμετρη κρυπτογράφηση εξαλείφει το μειονέκτημα της συμμετρικής αφού δεν απαιτείται κάποια επαφή του αποστολέα με τον παραλήπτη για την ανταλλαγή του κλειδιού. Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για τη κρυπτογράφηση και ο παραλήπτης με το ιδιωτικό του κλειδί μπορεί να το αποκρυπτογραφήσει [6]. Από τα πιο γνωστά συστήματα ασύμμετρης κρυπτογράφησης είναι ο RSA των Ronald Rivest, Adi Shamir και Len Adleman από τους οποίους πήρε το όνομα.

Το μειονέκτημα της συμμετρικής κρυπτογράφησης είναι ότι απαιτεί αρκετό χρόνο να ολοκληρωθεί ιδιαίτερα αν είναι μεγάλο το μήνυμα. Γι’ αυτό το λόγο συχνά χρησιμοποιείται ένας

συνδυασμός της συμμετρικής με ασύμμετρη κρυπτογραφία. Το μήνυμα κρυπτογραφείται με συμμετρικό κλειδί το οποίο έχει σταλθεί στον παραλήπτη με χρήση ασύμμετρης κρυπτογράφησης για την ασφαλή μεταφορά του [2].

Όσο αφορά τη στεγανογράφηση, ο σκοπός της δεν είναι μόνο η απόκρυψη του περιεχομένου όπως στη κρυπτογράφηση, αλλά την απόκρυψη ύπαρξης ολόκληρου του αρχείου. Σε κάποια είδη αρχείων, συνήθως ήχου ή εικόνας, υπάρχουν λιγότερο σημαντικά bits, τα οποία μπορούν να χρησιμοποιηθούν για την αποθήκευση ενός αρχείου κρυπτογραφημένου ή απλού. Καμία αλλαγή δεν είναι εμφανής στο αρχικό αρχείο και η απόκτηση του μηνύματος απαιτεί ειδικά εργαλεία ανάκτησης και πιθανών αποκρυπτογράφησης [6].

Επιπρόσθετα, μπορεί να χρησιμοποιηθεί ένα κλειδί stego όχι μόνο για τη κρυπτογράφηση του μηνύματος, αλλά για την τυχαία κατανομή των bits στο αρχείο που κρύβεται [36]. Μία εναλλακτική μέθοδος στεγανογράφησης είναι η χρησιμοποίηση κρυφών υδατογραφημάτων τα οποία χρησιμοποιούνται τις περισσότερες φορές για την ενσωμάτωση ενός εμπορικού σήματος ή άλλου συμβόλου στο αρχείο [6].

Οι μέθοδοι στεγανογράφησης μπορούν να χωριστούν σε δύο βασικές κατηγορίες, τεχνική και γλωσσολογική. Η πρώτη χρησιμοποιεί επιστημονικές μεθόδους για την απόκρυψη του μηνύματος, ενώ η δεύτερη αποκρύπτει το μήνυμα με μη εμφανείς τρόπους και διακρίνεται σε semagrams και ανοιχτούς κώδικες, οι οποίοι αντίστοιχα μπορούν να διακριθούν σε semagram κειμένου ή οπτικό και σε jargon κώδικα ή covered ciphers [36].

Ο εντοπισμός της στεγανογράφησης και η απόκτηση του κρυφού μηνύματος από ένα τρίτο άτομο ονομάζεται στεγανάλυση. Σε αντίθεση με τη κρυπτογράφηση όπου δεν γίνεται προσπάθεια κάλυψης των κρυπτογραφημένων δεδομένων, η στεγανογράφηση δεν διαπιστώνεται από την αρχή. Η ανίχνευση εργαλείων στεγανογράφησης είναι ένα πρώτο βήμα εντοπισμού, καθώς και η χρήση στατιστικής ανάλυσης για εύρεση παραμορφώσεων σε αρχεία [36].

Ακόμα κι αν εντοπιστούν κρυπτογραφημένα ή στεγανογραφημένα αρχεία, χρειάζεται το κατάλληλο κλειδί για την απόκτηση του κρυφών δεδομένων. Μια αρχική προσπάθεια εύρεσης μπορεί να γίνει με απευθείας ερώτηση του υπόπτου ή με τη χρήση social engineering. Όταν αποτυγχάνουν, γίνεται αναζήτηση του κλειδιού με χρήση λεξικών με πιθανές λέξεις κλειδιά,

ειδικά λογισμικά, ή εύρεση κωδικών σε άλλους λογαριασμούς που ίσως βοηθήσουν στην ανακάλυψη του κλειδιού [32].

4.4 Τεχνικές Anti-Forensics

Ο όρος anti-forensic στο τομέα των computer forensics είναι αρκετά νέος και δεν έχει θεσπιστεί ένας γενικά αποδεκτός ορισμός. Αναφέρεται σε μεθόδους και εργαλεία που έχουν ως στόχο την αποτροπή εφαρμογής της επιστήμης των computer forensics από κατάλληλα εξουσιοδοτημένο προσωπικό για την ψηφιακή διερεύνηση μιας παράνομης πράξης. Η χρήση μέτρων anti-forensic έχει ως αποτέλεσμα να εμποδίζεται η αναγνώριση, συλλογή και ανάλυση αποδεικτικών στοιχείων καθώς και να διακινδυνεύεται η ακεραιότητά τους [29, 16].

Οι μέθοδοι που χρησιμοποιούνται μπορούν να διαχωριστούν σε κατηγορίες ανάλογα με τη βασική λειτουργία που εκτελούν, για παράδειγμα να προκαλέσουν τη καταστροφή ή την απόκρυψη δεδομένων. Άλλοι μέθοδοι αποτρέπουν τη δημιουργία δεδομένων για να μην υπάρχουν στοιχεία που μπορούν να εντοπιστούν, ή εκμεταλλεύονται αδυναμίες των εργαλείων που χρησιμοποιεί ένας ερευνητής ώστε να θεωρηθούν αναξιόπιστα σε μια νομική διαδικασία. Επιπλέον, χρησιμοποιούνται τεχνικές για την κάλυψη ιχνών όπως τον αποστολέα ή παραλήπτη ενός ηλεκτρονικού μηνύματος [29, 16, 37].

Κάποιες τεχνικές μπορεί να εφαρμοστούν με σκοπό όχι την απόκρυψη αποδείξεων αλλά την καθυστέρηση του εντοπισμού τους από τον ερευνητή έτσι ώστε να χάσουν την αξία τους εάν είναι χρονικά ευαίσθητα [37]. Κάθε κατηγορία αποτελείται από διακριτές ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα και χρησιμότητα των αποδείξεων σε μια διαδικασία forensic. Στη συνέχεια αναλύονται οι κυριότερες κατηγορίες μεθόδων anti-forensic.

4.4.1 Καταστροφή αποδείξεων

Η καταστροφή των αποδείξεων μπορεί να επιτευχθεί με χρήση μαγνητικών τεχνικών όπως η απομαγνήτιση του αποθηκευτικού μέσου ή με τη χρήση βίας για τη καταστροφή της συσκευής. Τεχνικές που δεν απαιτούν τη φυσική καταστροφή του δίσκου είναι η διαγραφή του με

κατάλληλα λογισμικά εργαλεία, η εγγραφή άλλων δεδομένων, ή η σημαντική αλλαγή στη σύνθεσή τους. Με αυτό τον τρόπο προκαλείται ζημία στην ακεραιότητα των δεδομένων και αφαιρούνται ίχνη τους. Αλλά, η διαδικασία καταστροφής μπορεί να αφήσει άλλου είδους αποδεικτικών στοιχείων, όπως ίχνη από το εργαλείο που διέγραψε τα δεδομένα [29, 16].

4.4.2 Απόκρυψη αποδείξεων

Με την απόκρυψη στοιχείων απομακρύνονται δεδομένα από μέρη που είναι εύκολο να εντοπιστούν από έναν ερευνητή. Δεν καταστρέφονται ή μετατρέπονται με κάποιο τρόπο οπότε ο χρήστης μπορεί να διατηρήσει τη πρόσβασή του σε αυτά, αλλά τοποθετούνται σε σημεία που είναι λιγότερο πιθανό να εξεταστούν, για παράδειγμα εξαιτίας περιορισμών των εργαλείων που χρησιμοποιούνται. Τέτοια μέρη για την απόκρυψη αρχείων και μεταδεδομένων είναι μη καταχωρημένες ή κρυμμένες περιοχές του αποθηκευτικού δίσκου, προστατευμένες περιοχές του συστήματος, ακόμα και το κύκλωμα του BIOS (Basic Input/ Output System) [37, 29].

Επιπλέον, μπορεί να γίνει εκμετάλλευση του ανθρώπινου παράγοντα και των αντιληπτικών του ικανοτήτων, για παράδειγμα ένα ύποπτο αρχείο μπορεί να μην γίνει αντιληπτό από τον ερευνητή με την αλλαγή του ονόματος του αρχείου ή με τη χρήση κρυφών χαρακτήρων, όπως 0xFF, ή με τη δημιουργία πολύ μεγάλων μονοπατιών αρχείου (file path). Επίσης, η κρυπτογράφηση και στεγανογράφηση, που αναλύθηκαν προηγουμένως, αποτελούν μεθόδους anti-forensics για την απόκρυψη δεδομένων. Τέλος, τα αρχεία μπορούν να αποθηκευτούν σε συσκευές άλλων ατόμων, σε εξυπηρετητές που δεν προστατεύονται επαρκώς ή σε άλλους διαθέσιμους χώρους στο διαδίκτυο [37, 29, 16].

4.4.3 Αποτροπή δημιουργίας δεδομένων

Με αυτό τον τρόπο αποτρέπεται η δημιουργία στοιχείων από συγκεκριμένες εφαρμογές. Επομένως δεν χρειάζεται η καταστροφή ή απόκρυψή τους καθώς ποτέ δεν εμφανίστηκαν στο σύστημα. Μπορεί να επιτευχθεί με χρήση Root Kits ή με τη τροποποίηση του συστήματος ώστε που να μην είναι δυνατόν να παραχθούν σχετικά και αξιόπιστα δεδομένα. Παρότι περιορίζεται η δημιουργία δεδομένων, επηρεάζεται όμως και η λειτουργία του συστήματος το οποίο μπορεί να

περιορίσει τις δυνατότητες του χρήστη. Επίσης, η ίδια η διαδικασία εξάλειψης πηγών δεδομένων μπορεί να αφήσει ίχνη, καθώς και η έλλειψη δεδομένων, που σε συνηθισμένες συνθήκες θα έπρεπε να υπήρχαν, αποτελεί απόδειξη μη θεμιτής δράσης [29, 16].

4.4.4 Δημιουργία πλαστών αποδείξεων

Η δημιουργία πλαστών αποδείξεων έχει σκοπό τον αποπροσανατολισμό του ερευνητή και τη δημιουργία δεδομένων που φαίνονται να είναι κάτι άλλο. Ένα παράδειγμα αυτής της μεθόδου αποτελεί η δημιουργία αποδείξεων που στην πραγματικότητα αποτελούν ένα είδος επίθεσης ενάντια στο εργαλείο που χρησιμοποιήθηκε για τον εντοπισμό τους. Σε αυτή τη περίπτωση μπορεί να έχουν χρησιμοποιηθεί υπαρκτές αποδείξεις ή να έχουν δημιουργηθεί ψεύτικες για να αλλοιώσουν την εγκυρότητα των πραγματικών αποδείξεων [29].

Αυτές οι τεχνικές αντικρούουν επιτυχώς τις μεθόδους forensic επειδή εκμεταλλεύονται αδυναμίες τόσο των εργαλείων όσο και των ίδιων των ερευνητών. Για την αντιμετώπισή τους απαιτείται η συνεχής εκπαίδευση και ενημέρωση των ειδικών forensics για να ανταπεξέλθουν σε αυτές τις προκλήσεις. Επίσης, πρέπει να αποφεύγεται η χρήση ενός μόνο εργαλείου, αλλά να χρησιμοποιούνται διαφορετικά εργαλεία που εκτελούν την ίδια λειτουργία για να γίνεται διασταύρωση των αποτελεσμάτων και να καλύπτονται τυχόν αδυναμίες τους [29].

Ακόμα, τα εργαλεία forensics πρέπει να ενημερώνονται διαρκώς με βάση τις τεχνολογικές εξελίξεις για να είναι έτοιμα να αντιμετωπίσουν νέες προκλήσεις αλλά επιπλέον είναι αναγκαίο να αναπτυχθούν αμυντικοί μηχανισμοί για να αντιμετωπίζουν πιθανές επιθέσεις. Ακόμα, η χρήση στατιστικών στοιχείων μπορεί να διευκολύνει και να επιταχύνει μια έρευνα καθώς μπορούν να εντοπίσουν μη συνηθισμένες καταστάσεις σε ένα σύστημα, όπως αρχεία εικόνας που είναι αποθηκευμένα σε ένα φάκελο με αρχεία αποκλειστικά για το λειτουργικό σύστημα επειδή ο χρήστης θεωρούσε ότι ο ερευνητής δεν θα ελέγξει το συγκεκριμένο σημείο[29].

4.5 Ανάγκη για προτυποποίηση και πιστοποίηση

Παρόλη την εξέλιξη της ψηφιακής διερεύνησης και των εργαλείων που χρησιμοποιούνται, καθώς και την αλλαγή του τρόπου αντιμετώπισης των συγκεκριμένων εγκλημάτων από νομική πλευρά, υπάρχουν ακόμα σημαντικά κενά. Με το πέρασμα των χρόνων και την εμπειρία που αποκτήθηκε από περιπτώσεις όπου η λανθασμένη χρήση των ψηφιακών δεδομένων είχε αρνητικές συνέπειες, έγινε εμφανής η ανάγκη για προτυποποίηση και πιστοποίηση [44, 2].

Ο όρος προτυποποίηση αναφέρεται στη δημιουργία κανόνων και προτύπων για την κοινή αντιμετώπιση καταστάσεων τα οποία θα καλύπτουν κάποιες απαραίτητες προϋποθέσεις ποιότητας, συμβατότητας, διαλειτουργικότητας, ασφάλειας και άλλα, και θα είναι γενικά αποδεκτά από την επιστημονική κοινότητα. Η πιστοποίηση είναι η επικύρωση συγκεκριμένων χαρακτηριστικών, όπως γνώσεων και ικανοτήτων, από επίσημους αναγνωρισμένους φορείς [72].

Η μη ύπαρξη γενικών προτύπων προκαλεί την εμφάνιση αδυναμιών και ελλείψεων στην τεκμηρίωση της συλλογής, ανάλυσης και διατήρησης των ψηφιακών αποδείξεων με αποτέλεσμα οι δικαστές να έχουν αμφιβολίες και να οδηγούνται σε λάθος αποφάσεις. Ο λόγος που δεν έχουν αμφισβητηθεί πλήρως οι ψηφιακές αποδείξεις είναι επειδή οι υποθέσεις που δικάζονται δεν στηρίζονται μόνο σε αυτές αλλά και σε φυσικές αποδείξεις. Στο μέλλον όμως με τη μεγαλύτερη διάδοση των ψηφιακών τεχνολογιών κάτι τέτοιο μπορεί να μην είναι εφικτό [2].

Η χρήση βασικών προτύπων κρίνεται αναγκαία κατά τη διάρκεια της έρευνας, κατάσχεσης και ανάλυσης των ψηφιακών δεδομένων για να εξασφαλίσει την αξιοπιστία και εγκυρότητα των αποδείξεων που θα παρουσιαστούν αργότερα [44]. Η μη τήρηση βασικών κανόνων σε οποιαδήποτε φάση μπορεί να προκαλέσει αμφισβήτηση των δεδομένων σε κάποια δικαστήρια και να μην θεμελιωθεί το πόρισμα του ερευνητή με πιθανή συνέπεια την αθώωση του δράστη αν δεν υπάρχουν άλλα στοιχεία ή ίσως και την τιμωρία κάποιου αθώου [2].

Ένα άλλο ζήτημα που τίθεται αφορά τα χαρακτηριστικά που πρέπει να έχει κάποιος ειδικός ώστε να μπορεί να καταθέτει επίσημα την άποψή του ως εμπειρογνώμονας. Σε κάποιες περιπτώσεις μπορεί να θεωρηθεί κάποιος που απλά γνωρίζει πώς να χρησιμοποιεί κάποια εργαλεία για Computer Forensics, σε άλλες όμως απαιτείται βαθύτερη γνώση της λειτουργίας αυτών των εργαλείων και των στοιχείων ενός υπολογιστή, όπως το σύστημα αρχείων. Γι’ αυτόν

το λόγο είναι σημαντικό η πιστοποίηση ατόμων με βάση κάποια βασικά χαρακτηριστικά που θα τεκμηριώνουν τις γνώσεις του κατόχου της πιστοποίησης και θα τον καθιστούν κατάλληλο για τέτοιου είδους έρευνες [44].

Εντούτοις, η δημιουργία προτύπων δεν μπορεί να επιτευχθεί εύκολα. Λόγω της διαρκούς εξέλιξης της τεχνολογίας, τα πρότυπα πρέπει να προσαρμόζονται εύκολα και γρήγορα στα νέα δεδομένα. Επιπλέον, κάθε φάση της έρευνας πρέπει να αναλυθεί διεξοδικά για τον προσδιορισμό των καταλληλότερων μεθόδων και τεχνικών, ενώ τα πιστοποιητικά που χορηγούνται ίσως χρειαστεί να είναι εξειδικευμένα σε συγκεκριμένες φάσεις της έρευνας αφού δεν συμμετέχουν πάντα τα ίδια άτομα σε όλες τις φάσεις [44]. Επίσης, επειδή το ηλεκτρονικό έγκλημα δεν γνωρίζει γεωγραφικά σύνορα, είναι σημαντική η επίτευξη παγκόσμιας προτυποποίησης και πιστοποίησης στο τομέα των Computer Forensics για αποτελεσματικότερη διεξαγωγή έρευνας σε διεθνή πλαίσια και δίκαιη νομική δίωξη των δραστών [63].

Τα πρώτα βήματα που έχουν γίνει για την επίτευξη αυτού του σκοπού ήταν η ίδρυση του International Organization of Computer Evidence, ήδη στα μέσα του 1990 με σκοπό τη διασφάλιση αρμονίας στις μεθόδους και τεχνικές που χρησιμοποιούνται στα διάφορα έθνη και να εγγυηθεί τη δυνατότητα χρήσης ψηφιακών αποδείξεων που συλλέχτηκαν σε μία χώρα σε δικαστήρια κάποιας άλλης. Το 1998 ιδρύθηκε η Scientific Working Group on Digital Evidence (SWGDE) και το 2001 οργανώθηκε για πρώτη φορά το Digital Forensics Research Work Shop, στο οποίο συμμετείχαν άτομα από τον ακαδημαϊκό τομέα, το στρατιωτικό και τον ιδιωτικό και οδήγησε στη δημιουργία του International Journal of Digital Evidence, ενός επιστημονικού περιοδικού αφιερωμένο αποκλειστικά στις ψηφιακές αποδείξεις. Αργότερα, το 2004 η αγγλική υπηρεσία UK Forensic Science Service σχεδίασε την ανάπτυξη μητρώου με εξειδικευμένα άτομα και αρκετούς ευρωπαϊκούς οργανισμούς συμπεριλαμβανομένου το European Network of Forensic Science Institutes (ENFSI) για την έκδοση οδηγιών για τη διεξαγωγή ψηφιακών ερευνών [2].

Κάποια βασικά πρότυπα που έχουν προταθεί από την SWGDE για υπηρεσίες που εφαρμόζουν Computer Forensics είναι [63]:

Πρότυπο 1: Όλες οι υπηρεσίες που κατάσχουν και/ή εξετάζουν ψηφιακές αποδείξεις πρέπει να διατηρούν ένα καταστατικό Standard Operating Procedure (SOP), στο οποίο καταγράφονται

όλες οι οδηγίες ελέγχου ποιότητας, οι οποίες θα υποστηρίζονται από κατάλληλες εγγραφές των υποθέσεων και θα χρησιμοποιούνται ευρέως αποδεκτές διαδικασίες, εξοπλισμό και υλικά. Όλα τα στοιχεία της πολιτικής και των διαδικασιών της υπηρεσίας που αφορούν ψηφιακές αποδείξεις πρέπει να αναφέρονται καθαρά στο καταστατικό SOP.

Πρότυπο 2: Η διοίκηση της υπηρεσίας θα πρέπει να αναθεωρεί το SOP σε ετήσια βάση για να διασφαλίσει τη συνεχή καταλληλότητα και αποτελεσματικότητα του.

Πρότυπο 3: Οι διαδικασίες που χρησιμοποιούνται πρέπει να είναι γενικά αποδεκτές σε αυτό το τομέα ή να υποστηρίζονται από δεδομένα που συλλέχτηκαν και καταγράφηκαν με επιστημονικό τρόπο.

Πρότυπο 4: Η υπηρεσία πρέπει να διατηρεί έντυπα αντίγραφα των κατάλληλων τεχνικών διαδικασιών.

Πρότυπο 5: Η υπηρεσία πρέπει να χρησιμοποιεί υλισμικό και λογισμικό το οποίο είναι κατάλληλο και αποτελεσματικό σε διαδικασίες συλλογής και ανάλυσης.

Πρότυπο 6: Όλες οι δραστηριότητες που σχετίζονται με τη συλλογή, αποθήκευση, εξέταση ή μεταφορά ψηφιακών αποδείξεων πρέπει να καταγραφούν και να είναι διαθέσιμες για επιθεώρηση και κατάθεση.

Πρότυπο 7: Οποιαδήποτε ενέργεια μπορεί να προκαλέσει αλλαγή, φθορά ή καταστροφή με οποιοδήποτε τρόπο των πρωτότυπων αποδείξεων πρέπει να διεξαχθεί από εξειδικευμένο άτομο.

Με τη χρήση γενικά αποδεκτών προτύπων και πιστοποιήσεων δίνονται οι βάσεις για να κριθεί μια έρευνα και να εξακριβωθούν τα προσόντα κάποιου που δηλώνει ότι είναι ειδικός σε αυτό το τομέα. Είναι απαραίτητη η συμφωνία σε πρότυπα τεχνικών και εκπαίδευσης και την απαίτηση από τους ερευνητές να κατέχουν τις κατάλληλες πιστοποιήσεις για τη διεθνή αναγνώρισή τους [2].

5 Μέθοδοι και Μοντέλα Ψηφιακής Έρευνας

Ο τομέας των Computer Forensics είναι σχετικά καινούριος, τα μοντέλα και μέθοδοι έρευνας ψηφιακών αποδείξεων ξεκίνησαν ουσιαστικά να αναπτύσσονται από το 2000, αν και τα πρώτα βήματα είχαν γίνει από τα μέσα της δεκαετίας του ’90. Παρακάτω περιγράφονται κάποια από τα πιο αναγνωρισμένα και διαδεδομένα μοντέλα ψηφιακής έρευνας καθώς και ένα ιδιαίτερο μοντέλο για την απευθείας έρευνα στο τόπο του συμβάντος.

5.1 Μέθοδος του Eoghan Casey

Στο βιβλίο του Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet [2], περιγράφεται μια ολοκληρωμένη διαδικασία έρευνας που διασφαλίζει τη κατάλληλη διαχείριση των αποδείξεων και μειώνει τη πιθανότητα εμφάνισης λαθών.



Εικόνα 8: Κατηγορίες του μοντέλου της ερευνητικής διαδικασίας

Στην παραπάνω εικόνα εμφανίζονται τα βήματα από τα οποία αποτελείται η συγκεκριμένη διαδικασία. Είναι κατάλληλη για εγκληματικές, αστικές ή στρατιωτικές υποθέσεις και τα αποτελέσματά της παρουσιάζονται στον κατήγορο ή διευθυντικό στέλεχος αναλόγως για να

κρίνει την αξιοπιστία των αποδείξεων. Στόχος της είναι η ευρεία επιστημονική αποδοχή και παροχή αξιοπιστίας, εφαρμογής της ανεξαρτήτων συνθηκών, και παρουσίαση μιας λογικής σύνδεσης μεταξύ υπόπτου και θύματος μέσω των αποδείξεων.

Σε κάποιες περιπτώσεις που εφαρμόζεται η συγκεκριμένη μέθοδος μπορεί να εμφανιστεί η ανάγκη επιστροφής σε κάποιο από τα προηγούμενα βήματα το οποίο δεν πρέπει να αποφευχθεί και να αντιμετωπίζεται με δυσχέρεια, διαφορετικά το αποτέλεσμα της έρευνας δεν θα είναι ολοκληρωμένο. Στη συνέχεια δίνεται μια περιγραφή για κάθε βήμα της μεθόδου.

1. Κατηγορία ή Ειδοποίηση Συμβάντος (Accusation or Incident Alert)

Μια κατηγορία ή ειδοποίηση για ένα συμβάν που παρατηρήθηκε αποτελεί την αφετηρία για να ξεκινήσει μια έρευνα. Μπορεί να είναι ένα σήμα από το σύστημα ανίχνευσης εισβολών, ή ασυνήθιστες καταγραφές του εξυπηρετητή ή κάποιου προγράμματος. Ακόμα και η καταγγελία ενός πολίτη μπορεί να οδηγήσει στην έρευνα ψηφιακών στοιχείων. Ωστόσο, σε κάθε περίπτωση πρέπει να γίνεται ένας έλεγχος για την αξιοπιστία των δεδομένων που θα προκαλέσουν την έναρξη της έρευνας γιατί μπορεί να είναι μια λάθος ειδοποίηση ή παρανόηση του γεγονότος από το άτομο που το κατήγγειλε. Εάν τελικά χρειαστεί να γίνει αρχική έρευνα στο τόπο του συμβάντος θα πρέπει να ληφθούν όλα τα νόμιμα μέτρα για να μην υπονομευθεί η υπόθεση.

2. Αποτίμηση της αξίας (Assessment of Worth)

Αυτό το βήμα είναι σημαντικό όταν εκκρεμούν αρκετές υποθέσεις και οι πόροι για την έρευνα είναι περιορισμένοι. Η απόφαση για το αν θα διεξαχθεί μια ολοκληρωμένη έρευνα επηρεάζεται από παράγοντες όπως πιθανές σημαντικές απώλειες, απειλή για σωματική βλάβη και άλλα. Το αποτέλεσμα αυτού του βήματος μπορεί να είναι η ανάληψη της έρευνας για την εύρεση αποδείξεων ή να μη γίνει καμία περαιτέρω ενέργεια επειδή τα πρώτα στοιχεία δεν υποδεικνύουν την ύπαρξη παράνομου περιστατικού.

3. Πρωτόκολλα Τοποθεσίας Συμβάντος / Εγκλήματος (Incident/Crime Scene Protocols)

Σε αυτή τη φάση έχει εξουσιοδοτηθεί μια πλήρης έρευνα για τη διερεύνηση της υπόθεσης. Όλα τα απαραίτητα και αρμόδια πρωτόκολλα, τεχνικές και μέθοδοι πρέπει να εφαρμοστούν για την αποφυγή λαθών και παραλείψεων. Ο υπεύθυνος της έρευνας υποχρεούται να προστατέψει το χώρο του συμβάντος για να διασφαλίσει την αξιοπιστία των στοιχείων.

4. Αναγνώριση ή Κατάσχεση (Identification or Seizure)

Ο σκοπός αυτού του βήματος είναι η δικαιολογημένη κατάσχεση φυσικών και ψηφιακών αποδείξεων. Πλήρης καταγραφή απαιτείται για οτιδήποτε συλλεχθεί καθώς και των σταδίων φύλαξης για να πιστοποιούν την αυθεντικότητά τους. Λόγω της φύσης των ψηφιακών δεδομένων και των πολλών μορφών τους, όπως αρχεία καταγραφών, βιομετρικά δεδομένα, μεταδεδομένα και άλλα, η αναγνώριση και συλλογή τους αποτελεί πρόκληση για τον ερευνητή ειδικά για αποδείξεις που βρίσκονται στο διαδίκτυο ή σε μεγάλους εξυπηρετητές.

5. Διατήρηση (Preservation)

Κατάλληλες ενέργειες πρέπει να ληφθούν για τη διατήρηση της ακεραιότητας των πιθανών αποδείξεων, φυσικών και ψηφιακών, ειδικά για δεδομένα που βρίσκονται σε πτητικές μνήμες και είναι περισσότερο ευμετάβλητα. Οι μέθοδοι που θα εφαρμοστούν και τα εργαλεία που θα χρησιμοποιηθούν παίζουν καθοριστικό ρόλο, η ακρίβεια και η αξιοπιστία τους δεν πρέπει να μπορούν να αμφισβητηθούν.

6. Ανάκτηση (Recovery)

Η φάση της ανάκτησης αναφέρεται στη συλλογή δεδομένων που έχουν διαγραφεί, αποκρύπτονται ή είναι καμουφλαρισμένα ή βρίσκονται σε περιοχές που δεν είναι από την αρχή εμφανείς. Επιπλέον, όπου είναι δυνατόν και αναγκαίο πραγματοποιείται αναδημιουργία αρχείων από κομμάτια τους που έχουν εντοπιστεί. Οι ενέργειες αυτές θα πρέπει να γίνονται σε πιστά αντίγραφα των αρχικών δεδομένων εκτός αν δεν είναι εφικτό για παράδειγμα εάν βρίσκονται σε ενσωματωμένα συστήματα.

7. Συγκέντρωση (Harvesting)

Η συγκέντρωση αφορά τη συλλογή δεδομένων που είναι πιο πιθανό να σχετίζονται με το συμβάν που ερευνάται. Τα αποτελέσματα από τις διεργασίες που εκτελούνται στηρίζουν ή καταρρίπτουν μια υπόθεση της ερευνητικής ομάδας. Η συλλογή δεν γίνεται με βάση το περιεχόμενο ή κάποια έννοια των αρχείων, αλλά κατηγοριοποιούνται ανάλογα με το τύπο και τα χαρακτηριστικά τους για μετέπειτα ανάλυση.

8. Μείωση (Reduction)

Όταν τα δεδομένα είναι πάρα πολλά εφαρμόζονται διαδικασίες μείωσης για να ολοκληρωθεί πιο γρήγορα η έρευνα. Ποια δεδομένα θα παραμείνουν εξαρτάται από εξωτερικούς παράγοντες όπως διαδικασίες hashing, από τον τύπο και άλλα χαρακτηριστικά τους. Ο στόχος αυτής της διαδικασίας είναι να υπάρξει στο τέλος ένα σύνολο που περιέχει δεδομένα με τη πιθανότερη μεγαλύτερη αξία. Τα κριτήρια που θα χρησιμοποιηθούν για τη μείωση είναι πολύ σημαντικά και υπάρχει πιθανότητα να αμφισβητηθούν από δικαστές, ενόρκους ή άλλα εξουσιοδοτημένα άτομα.

9. Οργάνωση και Έρευνα (Organization and Search)

Η οργάνωση των δεδομένων, η τοποθέτηση ετικετών για εύκολη αναγνώριση και ομαδοποίησή τους σε σημαντικά σύνολα διευκολύνουν τον ερευνητή να εντοπίσει και να αναγνωρίσει στοιχεία κατά τη διάρκεια της ανάλυσης και στη συνέχεια να τα παρουσιάσει με σωστά τεκμηριωμένο τρόπο στη τελική αναφορά. Η δημιουργία ενός ευρετηρίου βοηθάει στη γρήγορη αναζήτηση σχετικών ή μη δεδομένων και στην επανάληψη διαδικασιών ανάλυσης εφόσον χρειαστεί.

10. Ανάλυση (Analysis)

Μετά τη προεπεξεργασία των δεδομένων παραμένει ένα υποσύνολο των αρχικών το οποίο αναλύεται διεξοδικά. Σε αυτό το σημείο εξετάζονται τα εσωτερικά χαρακτηριστικά των αρχείων για το σχηματισμό συνδέσεων και τον εντοπισμό προέλευσης των δεδομένων. Η διαδικασία της ανάλυσης περιλαμβάνει τέσσερεις βασικές υποκατηγορίες:

- **Αξιολόγηση:** προσδιορισμός παραγόντων όπως κίνητρα, ευκαιρίες, μέσω των ψηφιακών στοιχείων.
- **Πειραματισμός:** καινούριες ή μη θεμιτές τεχνικές μπορεί να χρειαστεί να εφαρμοστούν σε μια έρευνα, οι οποίες πρέπει να τεκμηριωθούν αυστηρά για να γίνουν αποδεκτές, διαφορετικά απορρίπτονται.
- **Συσχέτιση:** οι ψηφιακές αποδείξεις δεν είναι συνήθως αρκετές για να περιγράψουν όλη την υπόθεση, γι’ αυτό το λόγο γίνεται συσχέτιση με άλλες αποδείξεις για να δοθεί μια πλήρης εικόνα του συμβάντος.
- **Επικύρωση:** Το τελικό αποτέλεσμα της διαδικασίας που θα αποτελέσει την έμπειρη γνωμάτευση του ερευνητή.

11. Αναφορά (Reporting)

Η τελική αναφορά περιέχει όλα τα στοιχεία και λεπτομερής περιγραφή των διαδικασιών που ακολουθήθηκαν σε όλες τις φάσεις της έρευνας με στόχο την παρουσίαση έγκυρων αποδείξεων και συμπερασμάτων.

12. Πειθώς και Μαρτυρία (Persuasion and Testimony)

Σε μερικές περιπτώσεις είναι απαραίτητο η παρουσίαση των αποτελεσμάτων της έρευνας σε μη εξειδικευμένα άτομα. Οι τεχνικές και μέθοδοι που εφαρμόστηκαν θα πρέπει να εξηγηθούν με κατανοητό τρόπο χωρίς όμως να παραληφθούν σημαντικές λεπτομέρειες.

5.2 Μέθοδος του Thomas A. Johnson

Ο Thomas A. Johnson μέσω του βιβλίου του Forensic Computer Crime Investigation [4] και σε συνεργασία με τον Ross E. Mayfield προτείνουν μια απλή εμπειρική στρατηγική έρευνας η οποία βασίζεται σε λιγότερα βήματα και την όσο το δυνατόν λιγότερη προσπάθεια που απαιτείται για την επιτυχή επίλυση μιας υπόθεσης. Η συγκεκριμένη μέθοδος μπορεί να εφαρμοστεί σε εγκληματικές και αστικές ή εταιρικές έρευνες.

Η στρατηγική έρευνας ηλεκτρονικών εγκλημάτων είναι:

1. Καθορισμός ύπαρξης πιθανής αιτίας για τη διάπραξη του συγκεκριμένου εγκλήματος.
2. Καθορισμός αρχής που θα έχει την αρμοδιότητα στην έρευνα της υπόθεσης.
3. Συλλογή πληροφοριών σχετικά με την υπόθεση.
4. Καθορισμός των κρίσιμων παραγόντων επιτυχίας για να κλείσει η υπόθεση.
5. Συλλογή σημαντικών στοιχείων για την υπόθεση.
6. Προετοιμασία πειστηρίων, συμπερασμάτων και αναφορών για τους κατήγορους.
7. Παροχή κατάθεσης εμπειρογνώμονα εάν απαιτείται.

Ο συγγραφέας αντιλαμβάνεται την έρευνα ως ένα σύστημα, δηλαδή μια διαδικασία που δέχεται κάποια δεδομένα ως είσοδο, τα επεξεργάζεται και τα αποτελέσματα αποτελούν την έξοδο. Σε μια έρευνα ηλεκτρονικού εγκλήματος η είσοδος μπορεί να είναι μια υπόθεση εσωτερικής

έρευνας στην αστυνομία, καταγγελίες στην αστυνομία από πολίτες ή επιχειρήσεις, παραπομπή υποθέσεων από άλλες υπηρεσίες ή και περιπτώσεις που προέκυψαν από προληπτική έρευνα ή προειδοποιήσεις. Ακολουθεί η ανάλυση των βημάτων αυτής της μεθόδου.

1. Καθορισμός ύπαρξης πιθανής αιτίας

Στο πρώτο στάδιο ελέγχεται κατά πόσο υπάρχει λογική αιτία να θεωρηθεί ότι έχει διαπραχτεί κάποια παράνομη ενέργεια. Συνήθως είναι εμφανές από την υπόθεση αν έχει γίνει κάποιο έγκλημα αλλά αν δεν έχει αναγνωριστεί συγκεκριμένη παραβίαση τότε δεν πραγματοποιείται έρευνα.

2. Καθορισμός αρμόδιας αρχής

Εφόσον εγκριθεί η ανάγκη για έρευνα, ακολουθεί ο καθορισμός αρχής που θα είναι αρμόδια για την έρευνα της υπόθεσης. Ωστόσο, δεν είναι πάντα εύκολο ειδικά σε διεθνείς περιπτώσεις ή υποθέσεις όπου συνεργάζονται πολλές υπηρεσίες. Συνήθως, ένας κατήγορος μπορεί να ορίσει τις αρμοδιότητες που θα αναλάβει κάθε αρχή όπου υπάρχει αμφιβολία.

3. Συλλογή πληροφοριών

Σε αυτό το στάδιο συλλέγονται επαρκής πληροφορίες σχετικά τις συνθήκες του περιστατικού για τον εντοπισμό κρίσιμων παραγόντων επιτυχίας της έρευνας. Το είδος των πληροφοριών εξαρτάται από τη κατηγορία της παράνομης πράξης. Βασικά εργαλεία που προτείνει ο συγγραφέας είναι μια χρονολογική καταγραφή της υπόθεσης και ένας μεγάλος πίνακας.

Η χρονολογική καταγραφή είναι μια λίστα των ενεργειών με βάση ημερομηνία και ώρα, ενέργεια και το αποτέλεσμά της, η οποία μπορεί να βοηθήσει στην ανακάλυψη στοιχείων και την εύκολη επανεστίαση στην υπόθεση. Αποτελεί πηγή ευρημάτων και γεγονότων, συνοψίζει τις αναφορές έρευνας, αναλύει τις αποδείξεις και μπορεί να χρησιμοποιηθεί ως σημείο αναφοράς σε μια κατάθεση.

Ένας μεγάλος πίνακας στο τοίχο είναι χρήσιμος για τη συλλογή πληροφοριών ειδικά σε περιπτώσεις όπου υπάρχουν πολλοί ερευνητές και δουλεύουν σε διαφορετικά στοιχεία της ίδιας υπόθεσης. Διευκολύνει στον εντοπισμό σχέσεων μεταξύ στοιχείων και την εξαγωγή συμπεράσματος ή επόμενων βημάτων για την επίλυση της υπόθεσης.

4. Καθορισμός κρίσιμων παραγόντων επιτυχίας

Κρίσιμοι παράγοντες επιτυχίας ορίζονται σε αυτή τη περίπτωση ως ο ελάχιστος αριθμός ενεργειών που πρέπει να γίνουν σωστά για την επιτυχή επίλυση της υπόθεσης. Η επιτυχία μπορεί να οριστεί διαφορετικά αναλόγως με την υπόθεση, για παράδειγμα μπορεί να είναι η αδιαμφισβήτητη παρουσίαση των αποδείξεων σε ένα δικαστή ή ενόρκους, ή η στήριξη μιας κατηγορίας για τη καταδίκη του υπόπτου.

5. Συλλογή κρίσιμων αποδείξεων

Η φάση της συλλογής αποδείξεων αποτελεί την πιο απαιτητική και χρονοβόρα. Τα προηγούμενα στάδια διευκολύνουν στην επιλογή του είδους των αρχείων που αναζητούνται και τις τοποθεσίες που πιθανόν να είναι αποθηκευμένες. Οι πληροφορίες που θα συλλεχθούν είναι απαραίτητες για ένα ένταλμα έρευνας και την κλήτευση αρχείων. Είναι εξαιρετικά σημαντικό η απόκτηση καταγραφών του υπολογιστή όσο το δυνατόν γρηγορότερα ειδικά όσες αφορούν δικτυακή σύνδεση επειδή δεν διατηρούνται για μεγάλο χρονικό διάστημα.

6. Πειστήρια, αναφορές και ευρήματα

Με βάση τη παρομοίωση της έρευνας ως σύστημα με εισόδους, διεργασίες και εξόδους, μπορεί να θεωρηθεί ότι οι έξοδοι είναι οι αποδείξεις σε μορφή πειστηρίων, αναφορών και ευρημάτων. Η παρουσίασή τους πρέπει να γίνει με απλούς όρους για την εύκολη κατανόηση και κάθε γεγονός ή συμπέρασμα πρέπει να τεκμηριώνεται κατάλληλα.

7. Κατάθεση εμπειρογνώμονα

Συνήθως, εάν ο ερευνητής έχει κάνει καλή δουλεία και οι αποδείξεις είναι αξιόπιστες δεν χρειάζεται να καταθέσει για την υπόθεση. Σε περιπτώσεις όμως που κριθεί αναγκαίο, πρέπει να αποδείξει ότι διαθέτει τις απαραίτητες γνώσεις που τον κάνουν ειδικό στην έρευνα ψηφιακών αποδείξεων και να υπερασπιστεί τα συμπεράσματά του εναντίον μιας αντίθετης άποψης από την πλευρά της υπεράσπισης του κατηγορουμένου.

5.3 Ένα αφηρημένο μοντέλο για Digital Forensics (An Abstract Digital Forensics Model)

Ένα μοντέλο το οποίο δεν εξαρτάται από καμία τεχνολογία ή ηλεκτρονικό έγκλημα είναι το αφηρημένο μοντέλο των Reith, Carr και Gunsh. Παρέχει ένα συνεπές και σταθερό πλαίσιο για

την ανάπτυξη τεχνικών digital forensics, με τρόπο που να μπορούν να προσαρμοστούν στις μελλοντικές ψηφιακές τεχνολογίες, αλλά έχει και τη δυνατότητα ενσωμάτωσης μη ψηφιακών τεχνολογιών [42].

Τα κύρια στάδια αυτού του μοντέλου είναι:

1. Αναγνώριση (Identification): γίνεται αναγνώριση του συμβάντος και προσδιορίζεται ο τύπος του.
2. Προετοιμασία (Preparation): αφορά την προετοιμασία εργαλείων, τεχνικών, ενταλμάτων έρευνας και τον προσδιορισμό αρμοδιοτήτων.
3. Προσέγγιση Στρατηγικής (Approach Strategy): δυναμική διαμόρφωση μιας προσέγγισης βασισμένη σε πιθανές συνέπειες. Στόχος είναι η μεγιστοποίηση της συλλογής δεδομένων με παράλληλη ελαχιστοποίηση των επιπτώσεων στο θύμα.
4. Διατήρηση (Preservation): απομόνωση, ασφάλιση και διατήρηση της κατάστασης των φυσικών και ψηφιακών αποδείξεων, καθώς και απαγόρευση χρήσης των συγκεκριμένων συσκευών ή άλλων ηλεκτρομαγνητικών συσκευών σε κοντινή απόσταση.
5. Συλλογή (Collection): καταγραφή της φυσικής σκηνής και αντιγραφή των ψηφιακών αποδείξεων χρησιμοποιώντας πρότυπες και αποδεκτές διαδικασίες.
6. Εξέταση (Examination): συστηματική αναζήτηση σε βάθος για την εύρεση αποδείξεων που σχετίζονται με το συμβάν. Σε αυτή τη φάση γίνεται εστίαση στην αναγνώριση και τον εντοπισμό πιθανών αποδείξεων ακόμα και σε μη εύκολα προσιτές περιοχές. Επιπλέον, συντάσσεται λεπτομερής καταγραφή και τεκμηρίωση για τη διαδικασία της ανάλυσης.
7. Ανάλυση (Analysis): καθορισμός της σημασίας των στοιχείων, ανακατασκευή κομματιών δεδομένων και εξαγωγή συμπερασμάτων βασισμένα στις αποδείξεις που βρέθηκαν.
8. Παρουσίαση (Presentation): παροχή σύνοψης και επεξήγησης των συμπερασμάτων.
9. Επιστροφή αποδείξεων (Returning evidence): διασφαλίζεται ότι τα φυσικά και ψηφιακά στοιχεία επιστρέφονται στον νόμιμο ιδιοκτήτη ενώ προηγουμένως έχει καθοριστεί πως και ποιες εγκληματικές αποδείξεις πρέπει να διαγραφούν.

Τα παραπάνω στάδια δεν είναι διαφορετικά από αυτά που εφαρμόζονται στη συλλογή φυσικών αποδείξεων, όμως σε αυτή τη περίπτωση εφαρμόζονται με πιο αφηρημένη έννοια για να

συμπεριλαμβάνουν περιστατικά με ψηφιακές αποδείξεις αλλά και για προσαρμόζεται εύκολα σε μελλοντικές καταστάσεις. Ωστόσο, ένα από τα βασικά μειονεκτήματά του είναι ότι μπορεί να θεωρηθεί πολύ γενικό για να ακολουθηθεί στη πράξη.

5.4 Μια ενσωματωμένη Διαδικασία Ψηφιακής Έρευνας (An Integrated Digital Investigation Process)

Οι Carrier και Spafford σχεδίασαν μια μέθοδο η οποία θεωρεί ότι ο υπολογιστής αποτελεί την ψηφιακή σκηνή του εγκλήματος. Χρησιμοποιούν ειδικές τεχνικές για την εύρεση αποδείξεων οι οποίες στηρίζονται στο γεγονός ότι ο δράστης αφήνει ίχνη κατά την εκτέλεση κάποιου λογισμικού, για παράδειγμα προσωρινά αρχεία, κομμάτια από διαγραμμένα αρχεία και άλλα. Το μοντέλο αυτό αποτελείται από 17 φάσεις οι οποίες μπορούν να χωριστούν σε πέντε ομάδες, στις [10]:

1. Φάσεις ετοιμότητας (Readiness Phases)
2. Φάσεις ανάπτυξης (Deployment Phases)
3. Φάσεις έρευνας στη φυσική σκηνή του εγκλήματος (Physical Crime Scene Investigation Phases)
4. Φάσεις έρευνας στην ψηφιακή σκηνή του εγκλήματος (Digital Crime Scene Investigation Phases)
5. Φάση επανεξέτασης (Review Phase)

Η έρευνα στο φυσικό και ψηφιακό περιβάλλον γίνονται σχεδόν παράλληλα έτσι ώστε τα αποτελέσματα της ψηφιακής έρευνας να βοηθήσουν τη φυσική έρευνα και να επιλυθεί η υπόθεση.

1. Φάσεις Ετοιμότητας

Ο σκοπός των φάσεων ετοιμότητας είναι να διασφαλίσουν τη δυνατότητα σε επιχειρήσεις και οργανισμούς να συμβάλουν σε μια έρευνα με τη κατάλληλη συλλογή και διατήρηση αποδείξεων. Αποτελείται από τις φάσεις ετοιμότητας πράξεων και υποδομής (Operations Readiness Phase, Infrastructure Readiness Phase) όπου στη πρώτη παρέχεται εκπαίδευση και

εξοπλισμός στο προσωπικό, ενώ στη δεύτερη φάση διασφαλίζεται η ύπαρξη των αναγκαίων δεδομένων σε περίπτωση που διεξαχθεί μια έρευνα.

2. Φάσεις Ανάπτυξης

Οι φάσεις ανάπτυξης παρέχουν ένα μηχανισμό εντοπισμού και επιβεβαίωσης περιστατικών. Στη φάση Εντοπισμού και Ειδοποίησης (Detection and Notification Phase) εντοπίζεται το συμβάν και ειδοποιούνται τα κατάλληλα άτομα. Στη φάση της Επιβεβαίωσης και Εξουσιοδότησης (Confirming and Authorization Phase) αν πρόκειται για έγκλημα απαιτείται ένταλμα έρευνας ή άλλες νομικές διαδικασίες να εκτελεστούν αρχικά, ενώ σε μια εταιρία ακολουθούνται οδηγίες με βάση τη πολιτική της.

3. Φάσεις έρευνας στη φυσική σκηνή του εγκλήματος

Σκοπός των συγκεκριμένων φάσεων είναι η συλλογή και ανάλυση των φυσικών αποδείξεων και αναπαράσταση των ενεργειών που έγιναν κατά τη διάρκεια του περιστατικού. Η φάση της διατήρησης (Preservation Phase) περιλαμβάνει την ασφάλιση του χώρου, προσδιορισμό του συμβάντος και των φαινομενικών επιπτώσεων, και τον εντοπισμό υπόπτων και μαρτύρων. Στη φάση επισκόπησης (Survey Phase) παρατηρείται η σκηνή του εγκλήματος, αναγνωρίζονται οι εμφανείς αποδείξεις και αναπτύσσεται μια αρχική θεωρεία σχετικά με το συμβάν. Στη φάση τεκμηρίωσης (Documentation Phase) φωτογραφίζεται ή βιντεοσκοπείται ο χώρος για την απαθανάτιση όσο το δυνατόν περισσότερων πληροφοριών και σημαντικών λεπτομερειών από το χώρο.

Στη φάση έρευνας και συλλογής (Search and Collection Phase) πραγματοποιείται μια εις βάθος έρευνα και συλλογή επιπρόσθετων αποδείξεων και προσανατολισμός σε συγκεκριμένα στοιχεία. Η φάση της αναπαράστασης (Reconstruction Phase) περιλαμβάνει την οργάνωση των αποτελεσμάτων της ανάλυσης των φυσικών και ψηφιακών αποδείξεων, και το συνδυασμός τους που μπορεί να συσχετίσει ένα άτομο με τα ψηφιακά γεγονότα. Τέλος, στη φάση παρουσίασης (Presentation Phase) παρουσιάζονται οι αποδείξεις και οι θεωρίες που αναπτύχθηκαν από την αναπαράσταση.

4. Φάσεις έρευνας στην ψηφιακή σκηνή του εγκλήματος

Οι φάσεις έρευνας σε ψηφιακό επίπεδο ξεκινάνε όταν συλλέγονται συσκευές που περιέχουν ψηφιακά δεδομένα ή ανακτούνται από το δίκτυο μέσω καταγραφής της κίνησης. Κάθε ψηφιακή συσκευή θεωρείται διαφορετική σκηνή του εγκλήματος και τα αποτελέσματα στέλνονται στη φάση της αναπαράστασης της φυσικής σκηνής του εγκλήματος ώστε να αναγνωριστούν οι συνδέσεις μεταξύ των συσκευών. Επίσης, με αυτόν τον τρόπο γίνεται ανάλυση διαφορετικών τύπων συσκευών σε διαφορετικές τοποθεσίες. Οι φάσεις στην ψηφιακή έρευνα είναι ίδιες με αυτές της φυσικής μόνο που πλέον αναφέρονται σε ψηφιακές αποδείξεις και τοποθεσίες.

5. Φάση επανεξέτασης

Η τελευταία φάση είναι η φάση επανεξέτασης στην οποία ελέγχονται όλες οι διαδικασίες της έρευνας για να τη βελτίωση όπου κρίνεται αναγκαίο και τη διαβεβαίωση ότι τα αποτελέσματα της ψηφιακής έρευνας συμφωνούν με της φυσικής. Από αυτή τη φάση μπορεί να προκύψουν νέες διαδικασίες ή τρόποι εκπαίδευσης εάν εντοπίστηκε κάτι που για πρώτη φορά αντιμετωπίστηκε.

5.5 Το ενισχυμένο μοντέλο της διαδικασίας ψηφιακής έρευνας (The Enhanced Digital Investigation Process Model)

Σε αυτό το μοντέλο οι Baryamureeba και Tushabe βασίζονται και ενισχύουν στο Integrated Digital Investigation Model των Carrier και Spafford. Το μοντέλο αποτελείται από πέντε κύριες ομάδες φάσεων [58]:

1. Φάσεις ετοιμότητας (Readiness Phases): αποτελούν τις ίδιες φάσεις του μοντέλου Integrated Digital Investigation Model που αναλύθηκε προηγουμένως.
2. Φάσεις ανάπτυξης (Deployment Phases): παρέχουν ένα μηχανισμό για την ανίχνευση και επιβεβαίωση συμβάντων. Αποτελείται από τις φάσεις:
    i. Εντοπισμού και Ειδοποίησης (Detection and Notification Phase)
    ii. Έρευνας στη φυσική σκηνή του εγκλήματος (Physical Crime Scene Investigation)
    iii. Έρευνας στη ψηφιακή σκηνή του εγκλήματος (Digital Crime Scene Investigation)

iv. Επιβεβαίωσης (Confirmation Phase): επιβεβαίωση του συμβάντος και λήψη αρμοδιοτήτων και κατάλληλων ενταλμάτων έρευνας
v. Υποβολής (Submission Phase): παρουσίαση των φυσικών και ψηφιακών αποδείξεων σε νομικές οντότητες ή στη διοίκηση της εταιρίας

3. Φάσεις ιχνηλασιμότητας (Traceback Phases): σε αυτές τις φάσεις εντοπίζεται η τοποθεσία από την οποία έδρασε ο αυτουργός και αναγνωρίζονται οι συσκευές που χρησιμοποιήθηκαν για την εκτέλεση του συμβάντος. Αποτελείται από την έρευνα του ψηφιακού χώρου του εγκλήματος και τη φάση εξουσιοδότησης όπου νόμιμες οντότητες παρέχουν επιπλέον αρμοδιότητες για την συνέχιση της έρευνας και την πρόσβαση σε περισσότερες πληροφορίες.
4. Δυναμικές φάσεις (Dynamite Phases): σε αυτό το σημείο ερευνάται η κύρια σκηνή του εγκλήματος με σκοπό τη συλλογή και ανάλυση αντικειμένων για την απόκτηση περισσότερων αποδείξεων. Οι φάσεις αυτές είναι:
   i. Έρευνα στη φυσική σκηνή του εγκλήματος (Physical Crime Scene Investigation Phase)
   ii. Έρευνα στη ψηφιακή σκηνή του εγκλήματος (Digital Crime Scene Investigation Phase)
   iii. Φάση Αναπαράστασης (Reconstruction Phase)
   iv. Φάση Επικοινωνίας (Communication Phase): περιλαμβάνει τη παρουσίαση των τελικών ερμηνειών και συμπερασμάτων με βάση τις φυσικές και ψηφιακές αποδείξεις.
5. Φάση επανεξέτασης (Review Phase): όλη η έρευνα επανεξετάζεται και αναγνωρίζονται τομείς που προσφέρουν περιθώρια βελτίωσης.

5.6 Ένα επεκταμένο μοντέλο έρευνας κυβερνοεγκλήματος (An Extended Model of Cybercrime Investigation)

Ο Ciarduain χρησιμοποιεί τα προϋπάρχοντα μοντέλα τα οποία τα συνδυάζει, γενικεύει και επεκτείνει με τη προσθήκη νέων ενεργειών. Καλύπτει όλες τις ροές πληροφορίας και παρουσιάζει την έρευνα από όλες τις σκοπιές και χωρίς να δίνει έμφαση μόνο στην επεξεργασία

των δεδομένων. Το αποτέλεσμα ήταν η δημιουργία ενός επεκταμένου μοντέλου επικεντρωμένο στην έρευνα κυβερνοεγκλημάτων (Extended Model of Cybercrime Investigation) [17] και αποτελείται από 13 βήματα.

1. Επίγνωση (Awareness)

Το πρώτο βήμα είναι η επίγνωση της ανάγκης για έρευνα. Μπορεί να καθοριστεί είτε από εξωτερικούς παράγοντες όπως μια καταγγελία, ένας έλεγχος, ή από εσωτερικούς για παράδειγμα μια ειδοποίηση από το σύστημα ανίχνευσης εισβολών.

2. Εξουσιοδότηση (Authorization)

Στη συνέχεια είναι απαραίτητη η κατάλληλη εξουσιοδότηση για τη διεξαγωγή της έρευνας. Σε περίπτωση μιας εσωτερικής έρευνας σε εταιρία συνήθως είναι αρκετή η άδεια από τη διοίκηση. Σε άλλες περιπτώσεις απαιτείται από κάποιον νομικά αρμόδιο η έκδοση εντάλματος έρευνας ή δικαστική απόφαση.

3. Σχεδιασμός (Planning)

Ο σχεδιασμός της έρευνας επηρεάζεται από εξωτερικούς παράγοντες, δηλαδή κανονισμούς και νομοθεσία, ή από πληροφορίες που συλλέχτηκαν από άλλες πηγές. Εσωτερικοί παράγοντες που πρέπει να ληφθούν υπόψη είναι για παράδειγμα η πολιτική της εταιρίας ή πληροφορίες από προηγούμενες έρευνας.

4. Ειδοποίηση (Notification)

Αυτό το βήμα περιλαμβάνει την ενημέρωση του υποκειμένου της έρευνας ή άλλων ενδιαφερόμενων ότι πραγματοποιείται η έρευνα. Σε ειδικές υποθέσεις μπορεί να μην υπάρξει ειδοποίηση όταν για παράδειγμα χρειάζεται το στοιχείο της έκπληξης έτσι ώστε να αποτραπεί πιθανή καταστροφή των αποδείξεων από τον ύποπτο.

5. Αναζήτηση και Αναγνώριση Αποδείξεων (Search and Identification of Evidence)

Σε αυτή τη φάση πραγματοποιείται ο εντοπισμός αποδεικτικών στοιχείων και η εξακρίβωση στοιχείων που χρειάζονται για την επόμενη φάση. Στην απλούστερη περίπτωση μπορεί να είναι ο υπολογιστής του υπόπτου, αλλά σε πιο περίπλοκες μπορεί να χρειαστεί ο εντοπισμός περισσότερων υπολογιστικών συσκευών πιθανόν και σε άλλες χώρες.

6. Συλλογή (Collection)

Η ερευνητική ομάδα συλλέγει τις πιθανές αποδείξεις με τρόπο που μπορούν να διατηρηθούν και να αναλυθούν αργότερα. Κάποιοι από τους τρόπους συλλογής είναι η δημιουργία εικονικού αντίγραφου των σκληρών δίσκων ή η κατάσχεση ολόκληρου του υπολογιστή.

7. Μεταφορά (Transport)

Μετά τη συλλογή, οι αποδείξεις πρέπει να μεταφερθούν σε μια κατάλληλη τοποθεσία για την μετέπειτα εξέτασή τους. Συνήθως περιλαμβάνει την μεταφορά των φυσικών στοιχείων σε ασφαλές μέρος αλλά μπορεί να γίνεται και μεταφορά των ψηφιακών αποδείξεων μέσω δικτύων. Κατά τη διάρκεια της μεταφοράς τα στοιχεία πρέπει να παραμείνουν έγκυρα και να μην επηρεαστεί με οποιοδήποτε τρόπο η ακεραιότητά τους.

8. Αποθήκευση (Storage)

Τις περισσότερες φορές η εξέταση δεν γίνεται αμέσως, γι' αυτό το λόγο οι αποδείξεις πρέπει να αποθηκευτούν προσωρινά σε ασφαλείς περιοχές όπου θα προστατεύεται η ακεραιότητά τους με τη λήψη κατάλληλων μέτρων.

9. Εξέταση (Examination)

Η εξέταση των αποδείξεων απαιτεί τη χρήση πολλών τεχνικών για την εύρεση και την ανάλυση σημαντικών δεδομένων. Χρησιμοποιούνται αυτοματοποιημένες τεχνικές εάν το μέγεθος των δεδομένων είναι πολύ μεγάλο και ίσως χρειαστεί επιδιόρθωση κατεστραμμένων δεδομένων.

10. Υπόθεση (Hypothesis)

Οι ερευνητές δημιουργούν μια υπόθεση για το τι ακριβώς συνέβη με βάση τα αποτελέσματα από την εξέταση των αποδεικτικών στοιχείων. Σε αστυνομικές έρευνες η υπόθεση πρέπει να είναι λεπτομερής και κατάλληλα τεκμηριωμένη για να γίνει αποδεκτή σε ένα δικαστήριο. Σε εσωτερικές έρευνες μιας εταιρίας δεν είναι απαραίτητο να είναι τόσο αυστηρή, αρκεί να είναι κατανοητά τα γεγονότα στα οποία βασίζεται.

11. Παρουσίαση (Presentation)

Η υπόθεση του προηγούμενου βήματος πρέπει να παρουσιαστεί σε άλλα άτομα όπως ενόρκους ή στη διοίκηση της εταιρίας για να ληφθούν ανάλογες αποφάσεις.

12. Απόδειξη / Υπεράσπιση (Proof / Defense)

Η υπόθεση που αναπτύχθηκε από τους ερευνητές μπορεί να αμφισβητηθεί και δεχτεί κριτική. Η εγκυρότητά της εξασφαλίζεται με ατράνταχτες αποδείξεις, διαφορετικά θα πρέπει οι ερευνητές να επιστρέψουν σε προηγούμενα βήματα για να συλλέξουν και εξετάσουν περισσότερα στοιχεία για τη θεμελίωση μιας καλύτερης υπόθεσης.

13. Διάδοση (Dissemination)

Στη τελευταία φάση πραγματοποιείται η διάδοση των πληροφοριών από την διεξαγωγή της έρευνας. Κάποιες ίσως πρέπει να είναι διαθέσιμες μόνο στην ερευνητική ομάδα ενώ άλλες μπορούν να διαδοθούν ευρέως.

5.7 Ένα ιεραρχικό πλαίσιο για τη διαδικασία ψηφιακής έρευνας (A Hierarchical, Objectives-Based Framework for the Digital Investigations Process)

Οι Beebe και Clark παρουσιάζουν ένα ιεραρχικό πλαίσιο πολλών βαθμίδων για τη καθοδήγηση μιας ψηφιακής έρευνας, το Hierarchical, Objectives-Based Framework for the Digital Investigations [47]. Περιλαμβάνει στάδια βασισμένα σε στόχους (objectives-based phases) τα οποία είναι εφαρμόσιμα σε πολλαπλά αφαιρετικά επίπεδα και σε όποια επιπλέον επίπεδα μπορούν να προστεθούν μελλοντικά αν χρειαστεί. Ακόμα, στο συγκεκριμένο πλαίσιο περιλαμβάνονται και κάποιες αρχές που μπορούν να εφαρμοστούν αναλόγως τη φάση του πλαισίου.

5.7.1 Πρώτη βαθμίδα φάσεων

Οι φάσεις στη πρώτη βαθμίδα είναι διακριτές και καλά ορισμένες, ξεκινάνε λόγω κάποιου γεγονότος και καταλήγουν σε κάποιο αποτέλεσμα. Είναι στοιχισμένες σε συνάρτηση με το χρόνου. Οι φάσεις αυτές είναι:

1. Φάση προετοιμασίας (Preparation Phase): περιλαμβάνει τις ενέργειες που λαμβάνουν οι εταιρίες για να μεγιστοποιήσουν τη διαθεσιμότητα ψηφιακών αποδείξεων και να υποστηρίξουν την έρευνα.

2. Φάση απόκρισης στο συμβάν (Incident Response Phase): αποτελείται από τον εντοπισμό και την αρχική απόκριση σε ένα συμβάν που πιθανόν να υποδηλώνει παράνομη δραστηριότητα. Σκοπός αυτής της φάσης είναι ο εντοπισμός, η αξιολόγηση, η εκτίμηση και ο καθορισμός μιας στρατηγικής για την αντιμετώπιση του περιστατικού.
3. Φάση συλλογής δεδομένων (Data Collection Phase): η συλλογή δεδομένων γίνεται με βάση τη στρατηγική που ορίστηκε και το σχέδιο έρευνας.
4. Φάση ανάλυσης δεδομένων (Data Analysis Phase): αποτελεί τη πιο περίπλοκη και χρονοβόρα φάση όλης της έρευνας. Ο στόχος της ανάλυσης είναι να επιβεβαιώσει ή να απορρίψει της ισχυρισμούς της ύποπτης δραστηριότητας, και να γίνει αναπαράσταση του συμβάντος.
5. Φάση παρουσίασης ευρημάτων (Presentation of Findings Phase): σκοπός αυτής της φάσης είναι η παρουσίαση των αποτελεσμάτων σε διαφορετικά πρόσωπα, όπως στη διοίκηση μιας εταιρίας, στο τεχνικό ή νομικό προσωπικό ή σε άτομα επιβολής νόμου.
6. Φάση κλεισίματος υπόθεσης (Incident Closure Phase): εστιάζει στη περάτωση της έρευνας και διατήρηση νέων γνώσεων που μπορεί να παράχθηκαν από τη συγκεκριμένη έρευνα.

5.7.2 Αρχές Ψηφιακής Έρευνας

Σε όλες τις φάσεις της ερευνητικής διαδικασίας εφαρμόζονται κάποιες αρχές. Αντιπροσωπεύουν τους πρωταρχικούς στόχους που μπορεί να επιτυγχάνονται με διαφορετικές ενέργειες σε κάθε φάση. Παραδείγματα τέτοιων αρχών είναι η διατήρηση των αποδείξεων, η τεκμηρίωση, η κατάλληλη εξουσιοδότηση έρευνας, ο καθορισμός προτεραιοτήτων και η ανατροφοδότηση για τη βελτίωση της διαδικασίας έρευνας.

5.7.3 Δεύτερη Βαθμίδα Φάσεων (Υπο-φάσεις)

Εξαιτίας της πολυπλοκότητας της ψηφιακής έρευνας, είναι αναγκαίος ο ορισμός κι άλλων βαθμίδων, σχηματίζοντας έτσι ένα ιεραρχικό πλαίσιο με υπό-φάσεις βασισμένες σε συγκεκριμένους στόχους και ιεραρχικές εργασίες (objectives-based sub-phases). Πρέπει να

περιλαμβάνονται όλοι οι πιθανοί τύποι παράνομων δραστηριοτήτων και ψηφιακών αποδείξεων. Οι υπό-φάσεις παραμένουν συνεπείς σε κάθε κατάσταση αλλά οι ανάλογες εργασίες που επιλέγονται ποικίλουν ανάλογα με τις μοναδικές ανάγκες κάθε έρευνας ξεχωριστά.

5.8 Πλαίσιο ψηφιακής έρευνας βασισμένο σε γεγονότα (Event Based Digital Forensic Investigation Framework)

Ένα μετέπειτα μοντέλο που ανέπτυξαν οι δημιουργοί του Integrated Digital Investigation Process, Carrier και Spafford, είναι το Event Based Digital Forensic Investigation Framework [12] το οποίο εστιάζει στην αναπαράσταση των γεγονότων χρησιμοποιώντας τις αποδείξεις ώστε να αναπτυχθούν κάποιες υποθέσεις και να δοκιμαστούν. Αποτελείται από τις φάσεις:

1. Φάσεις Ετοιμότητας:
    i. Φάση ετοιμότητας λειτουργιών
    ii. Φάση ετοιμότητας υποδομών
2. Φάσεις Ανάπτυξης:
    i. Φάση εντοπισμού και ειδοποίησης
    ii. Φάση επιβεβαίωσης και εξουσιοδότησης
3. Φάσεις έρευνας φυσικής σκηνής του εγκλήματος
4. Φάσεις έρευνας ψηφιακής σκηνής του εγκλήματος
    i. Διατήρηση ψηφιακής σκηνής και τεκμηρίωση
    ii. Αναζήτηση ψηφιακών αποδείξεων και τεκμηρίωση
    iii. Αναπαράσταση ψηφιακών γεγονότων και τεκμηρίωση
5. Φάση παρουσίασης

Το μοντέλο δεν αναλύεται περαιτέρω καθώς τα βήματα από τα οποία αποτελείται είναι παρόμοια με το αρχικό μοντέλο που οι Carrier και Spafford είχαν αναπτύξει αλλά σε πιο απλοποιημένη μορφή για να αποτελέσει ένα πιο γενικευμένο πλαίσιο της διαδικασίας ψηφιακής έρευνας.

5.9 Computer Forensics Field Triage Process Model

Το μοντέλο Computer Forensics Field Triage Process (CFFTPM) των Rogers, Goldman, Mislan, Wedge και Debrota [40] προτείνει μια προσέγγιση έρευνας απευθείας στο χώρο που έγινε το περιστατικό παρέχοντας ένα πλαίσιο για γρήγορη αναγνώριση, ανάλυση και ερμηνεία των αποδείξεων χωρίς να απαιτείται η μεταφορά του συστήματος ή άλλων αντικειμένων στο εργαστήριο για μια πιο αναλυτική εξέταση. Το συγκεκριμένο μοντέλο έχει χρησιμοποιηθεί επιτυχώς σε πραγματικές υποθέσεις, είναι ευρέως αναγνωρίσιμο και τα αποτελέσματά του γίνονται αποδεκτά στα δικαστήρια.

Το CFFTPM ορίζεται από τις διαδικασίες έρευνας που διεξάγονται τις αρχικές ώρες μιας έρευνας, οι οποίες παρέχουν πληροφορίες από τη συνέντευξη του υπόπτου και από τη φάση εκτέλεσης της αναζήτησης. Λόγω της ανάγκης απόκτησης πληροφοριών σε ένα σχετικά σύντομο χρονικό διάστημα, το μοντέλο περιλαμβάνει μια επιτόπου ανάλυση του υπολογιστικού συστήματος. Το μοντέλο εστιάζει στην άμεση εύρεση χρήσιμων πληροφοριών, στην αναγνώριση θυμάτων που βρίσκονται σε άμεσο κίνδυνο, στην καθοδήγηση της τρέχουσας έρευνας, στην αναγνώριση πιθανών διώξεων και στην ακριβή εκτίμηση κινδύνου που θέτει ο δράστης την κοινωνία.

Τα στάδια του CFFTPM προήλθαν από το μοντέλο Integrated Digital Investigation Process, των Carrier και Spafford, και από το Digital Crime Scene Analysis του Rogers. Περιλαμβάνει τις εξής φάσεις:

1. Σχεδιασμός (Planning)

Στο πρώτο στάδιο γίνεται ένας κατάλληλος αρχικός σχεδιασμός όπου ιδανικά ο ερευνητής έχει συνυπολογίσει ποικίλες πιθανότητες σχετικά με τη σκηνή του εγκλήματος, τον ύποπτο και τις ψηφιακές αποδείξεις. Με αυτό τον τρόπο προσδιορίζεται τι είναι γνωστό και τι όχι ώστε να καθοριστεί στη συνέχεια τι πρέπει να αναζητηθεί. Οι πληροφορίες που είναι επιθυμητό να συλλεχθούν είναι σχετικά με τις ικανότητες του υπόπτου και συγκεκριμένες ενέργειές του, με τον εντοπισμό φυσικής και ψηφιακής τοποθεσίας που έδρασε, με στοιχεία όπως ηλεκτρονική διεύθυνση, ψευδώνυμα, κωδικούς και άλλες χρήσιμα στοιχεία. Επιπλέον, τα χρονικά στιγμιότυπα από πληροφορίες που συλλέχθηκαν προηγουμένως παρέχουν ένα χρονικό πεδίο για την έρευνα που θα πραγματοποιηθεί στον ενσύρματο και ασύρματο εξοπλισμό στον τόπο του

συμβάντος. Αφού συλλεχθούν οι παραπάνω πληροφορίες, ο ερευνητής ορίζει επακριβώς τους στόχους της έρευνας και το αναγκαίο προσωπικό.

2. Διαλογή (Triage)

Μετά την ολοκλήρωση του σχεδιασμού ξεκινάει η διαλογή, η οποία για το συγκεκριμένο μοντέλο ορίζεται ως η διαδικασία κατά την οποία ταξινομούνται τα αντικείμενα ανάλογα με τη σημαντικότητά τους ή άλλου είδους προτεραιότητα. Για παράδειγμα, τα στοιχεία, τα σύνολα δεδομένων ή συσκευές που πιθανόν περιέχουν αποδείξεις πιο σημαντικές ή ευαίσθητες εξετάζονται πρώτα. Οι ψηφιακές αποθηκευτικές συσκευές αναγνωρίζονται και ταξινομούνται με βάση τη σχετικότητα των στοιχείων με την έρευνα και αν μπορούν να ανακτηθούν σε σύντομο χρονικό διάστημα ή υπάρχει κίνδυνος να διαγραφούν σύντομα.

3. Προφίλ χρήσης και χρηστών (Usage/User Profile)

Μόλις έχει αναγνωριστεί και ταξινομηθεί ένα σύστημα ή αποθηκευτικό μέσο ξεκινάει η εξέταση και η ανάλυσή του κατά την οποία γίνεται αναζήτηση ενός συνδέσμου μεταξύ των αποδείξεων και του υπόπτου που υποδηλώνει ότι το συγκεκριμένο άτομο είναι υπεύθυνο για το συμβάν. Μια πλήρης γνώση του προφίλ του χρήστη και τον αντικειμένων που χρησιμοποιήθηκαν μπορεί να συμβάλει στο γρήγορο εντοπισμό της σύνδεσης ή να διευκρινιστεί αν είναι δυνατόν να γίνει σε εύλογο χρονικό διάστημα. Το προφίλ του χρήστη αποτελείται από μια συλλογή αρχείων, φακέλων και άλλα στοιχεία τα οποία είναι αποκλειστικά συσχετισμένα με ένα μοναδικό λογαριασμό χρήστη.

4. Χρονολόγηση / Χρονοδιάγραμμα (Chronology / Timeline)

Ο προσδιορισμός του χρονολογικού πεδίου της υπόθεσης μπορεί να καθοριστεί από τους χρόνους MAC (Modification, Access, Created) του αρχείου, που δείχνουν πότε δημιουργήθηκε το αρχείο, πότε μετατράπηκε τελευταία φορά και πότε ήταν η τελευταία φορά που είχε κάποιος πρόσβαση σε αυτό. Αρχικά ορίζονται κάποιοι χρονικοί περίοδοι κανονικής χρήσης από τον ύποπτο και άλλους γνωστούς χρήστες αν υπάρχουν. Στη συνέχεια αναγνωρίζονται και αναλύονται τα προγράμματα και αρχεία που χρησιμοποιήθηκαν τη χρονική περίοδο του συμβάντος, και τέλος εντοπίζονται οι τελευταίες αποθηκευμένες πληροφορίες.

5. Διαδικτυακή Δραστηριότητα (Internet Activity)

Σχεδόν σε κάθε περίπτωση θα χρειαστεί να γίνει εξέταση διαδικτυακής δραστηριότητας, για παράδειγμα σε άμεσα μηνύματα, ηλεκτρονική αλληλογραφία και περιήγηση στον ιστό. Ο τρόπος της εξέτασης εξαρτάται από τις συνθήκες και χρονικούς περιορισμούς, τα προγράμματα που χρησιμοποιήθηκαν, το είδος δραστηριότητας που εξετάζεται καθώς και αν ο υπολογιστής ανήκει στον δράστη ή στο θύμα.. Μια αποτελεσματική πρακτική είναι η αξιολόγηση των ενεργειών που εκτέλεσε ο δράστης στο διαδίκτυο και κατά πόσο σχετίζονται με την υπόθεση.

6. Συγκεκριμένες αποδείξεις για την υπόθεση (Case Specific Evidence)

Το είδος των αποδείξεων που πρέπει να εντοπιστούν και ανακτηθούν είναι διαφορετικό ανάλογα με την υπόθεση που ερευνάται. Για παράδειγμα σε μια υπόθεση παιδικής πορνογραφίας γίνεται αναζήτηση αρχείων εικόνας στο σκληρό δίσκο ή συγκεκριμένες ιστοσελίδες. Ενώ σε οικονομικά εγκλήματα ελέγχονται αρχεία κειμένου που μπορεί να περιέχουν οικονομικά στοιχεία ή αρχεία συγκεκριμένων οικονομικών εφαρμογών αν είναι εγκατεστημένα, όπως το MS Money.

Το συγκεκριμένο μοντέλο δεν είναι κατάλληλο για όλες τις περιπτώσεις. Καταρχάς πρέπει να υπάρχει η κατάλληλη εξουσιοδότηση για την απευθείας έρευνα στο χώρο και να υπολογιστεί κατά πόσο μπορεί να επηρεάσει την ακεραιότητα των πρωτότυπων αποδείξεων. Επιπλέον, εξαρτάται από τον τύπο του συστήματος και αν πρέπει να παραμείνει ενεργοποιημένο ή όχι, αν υπάρχουν χρονικοί περιορισμοί και αν υπάρχει ο κατάλληλος εξοπλισμός για τη διεξαγωγή τέτοιου είδους έρευνας.

5.10 Σύγκριση και συμπεράσματα

Παραπάνω περιγράφηκαν και αναλύθηκαν κάποια μοντέλα έρευνας ψηφιακών αποδείξεων. Τα περισσότερα από αυτά στηρίζονται σε αρχές και διαδικασίες παραδοσιακών μοντέλων έρευνας φυσικών αποδείξεων, επειδή έχουν εφαρμοστεί και αξιολογηθεί αμέτρητες φορές. Οι εμπειρίες και οι γνώσεις που αποκτήθηκαν μέσα από λάθη και επιτυχίες μεθόδων της παραδοσιακής φυσικής έρευνας έχουν βοηθήσει στην γρήγορη και αποτελεσματική αντιμετώπιση παρόμοιων προβλημάτων και προκλήσεων που συναντώνται στην ψηφιακή έρευνα.

Η έρευνα αποδεικτικών στοιχείων, είτε φυσικών είτε ψηφιακών, μπορεί να απλοποιηθεί σε συγκεκριμένα βήματα. Αρχικά, αναγνωρίζονται τα στοιχεία που μπορεί να αποτελούν αποδείξεις, συλλέγονται από το τόπο του συμβάντος και διατηρούνται σε ασφαλές περιβάλλον. Στη συνέχεια εξετάζονται και αναλύονται τα ευρήματα σε κατάλληλα διαμορφωμένο χώρο για τη προστασία τους και τέλος παρουσιάζονται με μια τελική αναφορά που υποδεικνύει την αξία των αποδείξεων και ότι έχουν ληφθεί όλα τα μέτρα για να μη τεθεί σε κίνδυνο η ακεραιότητά τους.

Ως αφετηρία τα παραπάνω βήματα, αναπτύσσονται συνεχώς γενικές μέθοδοι για την αντιμετώπιση ερευνών φυσικών ή και ψηφιακών αποδείξεων. Επίσης, ένα μοντέλο μπορεί να είναι πιο λεπτομερές και να απευθύνεται σε ειδικές καταστάσεις και συνθήκες που μπορεί να πραγματοποιηθεί μια έρευνα.

Ειδικά για τα μοντέλα που περιγράφηκαν παραπάνω, παρατηρείται ότι κάθε ένα δίνει έμφαση σε διαφορετικά σημεία μιας έρευνας προσπαθώντας όμως τα περισσότερα να διατηρήσουν όσο γίνεται ένα γενικό χαρακτήρα ώστε να είναι εφικτή η εφαρμογή τους σε μεγάλο αριθμό ερευνών. Λίγα είναι τα μοντέλα τα οποία εξειδικεύονται αποκλειστικά σε συγκεκριμένου είδους έρευνες. Χαρακτηριστικά παραδείγματα είναι το Computer Forensics Field Triage Process (υποκεφάλαιο 5.9), το οποίο περιγράφει μια σειρά βημάτων για ψηφιακή έρευνα στο χώρο του συμβάντος, και το μοντέλο του Ciarduain (υποκεφάλαιο 5.6) το οποίο αφορά εγκλήματα στο κυβερνοχώρο.

Υπάρχουν μοντέλα που παρέχουν ένα ευέλικτο πλαίσιο έρευνας για την προσαρμογή τους σε κάθε κατάσταση και την δυνατότητα επέκτασή τους σε νέες τεχνολογίες και δεδομένα όπως το αφηρημένο μοντέλο των Reith, Carr και Gunsh (υποκεφάλαιο 5.3). Το συγκεκριμένο μοντέλο δίνει έμφαση περισσότερο στην ευελιξία του παρά στην παροχή αναλυτικών βημάτων που θα διευκόλυναν έναν ερευνητή. Ενώ άλλα μοντέλα στοχεύουν στη γρήγορη επίλυση της υπόθεσης, σαν το μοντέλου του Johnson (υποκεφάλαιο 5.2), το οποίο είναι επιθυμητό όταν υπάρχουν αυστηροί χρονικοί περιορισμοί, όμως υπάρχει κίνδυνος να παραλειφθούν λιγότερο ορατά στοιχεία.

Αρκετά είναι και τα μοντέλα που συνδυάζουν τη φυσική με τη ψηφιακή έρευνα, για παράδειγμα το Integrated Digital Investigation Model (υποκεφάλαιο 5.4) εμφανίζει τη ψηφιακή έρευνα ως μια ενσωμάτωση στην φυσική έρευνα που σκοπό έχει να την ενισχύσει. Αυτό το μοντέλο καθώς

και επεκτάσεις του (υποκεφάλαιο 5.5) είναι αρκετά λεπτομερές αλλά δεν μπορεί να εφαρμοστεί σε καθαρά ψηφιακές έρευνες. Ένα μετέπειτα μοντέλο, το Event Based Digital Forensic Investigation Framework (υποκεφάλαιο 5.8), εστιάζει στην ανάλυση των γεγονότων για τη δημιουργία υποθέσεων. Ενώ το ιεραρχικό μοντέλο των Beebe και Clark (υποκεφάλαιο 5.7) περιγράφει με μεγαλύτερη λεπτομέρεια τις φάσεις ψηφιακής έρευνας οι οποίες μπορούν να διαχωριστούν σε υποφάσεις για περαιτέρω ανάλυση.

Από τα παραπάνω είναι εμφανές ότι η ύπαρξη ενός γενικευμένου μοντέλου για όλες τις έρευνες δεν είναι αποτελεσματικό. Κάθε παράνομη δραστηριότητα έχει τα δικά της ξεχωριστά χαρακτηριστικά και οι συνθήκες κάτω από τις οποίες μπορεί να πραγματοποιηθεί ποικίλουν κάθε φορά ανάλογα με τον δράστη, τον τόπο του συμβάντος και άλλα. Παρόλα αυτά έχουν αναπτυχθεί γενικευμένα μοντέλα για τη κάλυψη όσο το δυνατών περισσότερων περιπτώσεων. Ωστόσο τα περισσότερα είναι αρκετά αφηρημένα. Είναι αναγκαία η ύπαρξη πιο ειδικών μοντέλων έρευνας που θα παρέχουν όσο γίνεται πιο λεπτομερή περιγραφή της διαδικασίας που θα ακολουθηθεί σε ένα υποσύνολο καταστάσεων.

Με αυτό τον τρόπο θα υπάρχουν κοινοί αποδεκτοί τρόποι που θα καλύπτουν συνολικά σχεδόν όλα τα είδη ερευνών χωρίς να υποκύπτουν στη γενίκευση των διαδικασιών έρευνας. Ωστόσο πρέπει να δοθεί προσοχή στη περιγραφή των συνθηκών που θα πρέπει να επικρατούν για να μπορεί να εφαρμοστεί κάποιο εξειδικευμένο μοντέλο ώστε να μην δημιουργεί συγχύσεις στους ερευνητές ως προς ποιο μοντέλο πρέπει να επιλεχθεί σε μια συγκεκριμένη υπόθεση.

6 Εργαλεία Forensics

Τα εργαλεία χρησιμοποιούνται για την εφαρμογή τεχνικών που αποτελούν μέρος μιας μεθόδου, όπου μέθοδος είναι ένας συστηματικός τρόπος εκτέλεσης μιας εργασίας χρησιμοποιώντας ένα σύνολο τεχνικών για την απόκτηση πληροφοριών ή αγαθών [72]. Οπότε, η αποτελεσματικότητα και η αξιοπιστία ενός εργαλείου για την εκτέλεση ενός έργου εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των τεχνικών και της μεθόδου για την οποία χρησιμοποιούνται.

Σε μια ψηφιακή διερεύνηση, ο ερευνητής θα χρειαστεί κάποια εργαλεία για την ανάκτηση και ανάλυση των ψηφιακών δεδομένων με σκοπό τον εντοπισμό αποδεικτικών στοιχείων. Αρχικά προορίζονταν μόνο για συγκεκριμένες υπηρεσίες της κυβέρνησης και του στρατού όπου απαιτούταν για την διερεύνηση παράνομων δραστηριοτήτων. Με τη διάδοση όμως των υπολογιστικών συστημάτων στον επιχειρησιακό τομέα και στο ευρύ κοινό, συνεπάγοντας την εξάπλωση του ηλεκτρονικού εγκλήματος, τα εργαλεία έγιναν απαραίτητα τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα.

Τα εργαλεία digital forensics μπορεί να είναι είτε κάποια συσκευή που εκτελεί μια συγκεκριμένη διαδικασία, όπως προστασία εγγραφής, ή μπορεί να είναι κάποιο λογισμικό το οποίο είτε είναι εξειδικευμένο σε μια συγκεκριμένη ή μικρό αριθμό λειτουργιών, είτε καλύπτει ένα ευρύ φάσμα διαδικασιών που είναι απαραίτητες σε έναν ερευνητή. Τα λογισμικά εργαλεία μπορούν να χωριστούν σε δύο βασικές κατηγορίες λογισμικού, ανοιχτού κώδικα και κλειστού, το καθένα με τα δικά του πλεονεκτήματα και μειονεκτήματα.

Τα λογισμικά κλειστού κώδικα δημιουργούνται από ένα άτομο ή εταιρία και κατέχει τα πλήρη δικαιώματα διάθεσης και εκμετάλλευσης για εμπορικούς σκοπούς. Συνήθως συνοδεύονται από οδηγίες χρήσης και τεχνική υποστήριξη για την αντιμετώπιση τυχόν προβλημάτων. Πολλές εταιρίες δίνουν περισσότερη βαρύτητα στις υπηρεσίες εξυπηρέτησης και συχνά εμφανίζουν στην αγορά ένα όχι καλά δοκιμασμένο λογισμικό με αποτέλεσμα να γίνονται συνεχώς νέες ενημερώσεις (updates) για την διόρθωση προβλημάτων που έχουν εντοπίσει οι χρήστες. Επιπλέον, το κόστος είναι συνήθως μεγάλο και με τη μη δημοσίευση του κώδικα είναι αδύνατη η δοκιμή από άλλα εξειδικευμένα άτομα που δεν θα είναι προκατειλημμένα για τη λειτουργία του λογισμικού [14].

Αντίθετα, τα εργαλεία που βασίζονται σε ανοιχτό κώδικα είναι διαθέσιμα για δοκιμές και βελτιώσεις από τον καθένα και συνήθως είναι δωρεάν. Ο χρήστης μπορεί να τα προσαρμόσει με βάση τις δικές του ανάγκες και να τα βελτιώσει όπου κρίνει ότι χρειάζεται. Ακόμα, με την ελεύθερη διάδοσή τους τα εργαλεία μπορούν να εξεταστούν από οποιονδήποτε ειδικό ενδιαφέρεται με διάφορους τρόπους με αποτέλεσμα να εντοπίζονται περισσότερα λάθη και να διορθώνονται. Το μειονέκτημά τους είναι ότι δεν παρέχονται οδηγίες χρήσης ή αυτές που δίνονται δεν είναι πλήρης, και επιπλέον δεν διαθέτεται συγκεκριμένη τεχνική υποστήριξη αλλά αναζητείται μέσω επικοινωνίας με τους δημιουργούς και χρήστες [14].

Ανεξαρτήτως του είδους του εργαλείου, συσκευή ή λογισμικό, τα αποτελέσματα από τη χρήση των εργαλείων για να γίνουν αποδεκτά σε μια νομική διαδικασία πρέπει να είναι αξιόπιστα και σχετικά με την υπόθεση. Μια έρευνα forensics μπορεί να διακριθεί σε τρεις βασικές φάσεις όπου είναι απαραίτητη η χρήση εργαλείων [14]:

- **Φάση Απόκτησης:** Αντιγραφή δεδομένων από τις αποθηκευτικές συσκευές του υπόπτου σε ασφαλείς συσκευές με όσο το δυνατόν λιγότερες μετατροπές. Γίνεται χρήση εργαλείων για τη δημιουργία εικονικών αντιγραφών των δεδομένων σε εντοπίσιμες και μη περιοχές.
- **Φάση Ανάλυσης:** Εντοπισμός δεδομένων που υποστηρίζουν ή διαψεύδουν μια υπόθεση ή στοιχεία που υποδεικνύουν ότι έγιναν μετατροπές με σκοπό την μη αναγνώριση των δεδομένων. Τα εργαλεία ανάλυσης καταγράφουν περιεχόμενο φακέλων και ονόματα των αρχείων, ανακτούν διαγραμμένα αρχεία και παρουσιάζουν τα δεδομένα σε πιο χρήσιμη μορφή.
- **Φάση Παρουσίασης:** Σε αυτή τη φάση παρουσιάζονται τα αποτελέσματα της έρευνας με βάση το νομικό πλαίσιο ή τη πολιτική της εταιρίας. Για να γίνουν αποδεκτά τα στοιχεία πρέπει να τηρούνται κάποιες προϋποθέσεις.

Στην Αμερική η αξιοπιστία των αποτελεσμάτων ενός εργαλείου digital forensic εξακριβώνεται από μια προδικαστική «Ακρόαση Daubert». Σκοπός της είναι να εξακριβώσει ο δικαστής αν οι μεθοδολογίες και τεχνικές που υλοποιούν τα εργαλεία για την αναγνώριση του αποδεικτικού στοιχείου είναι έγκυρες και αξιόπιστες. Υπάρχουν τέσσερις γενικές κατηγορίες που χρησιμοποιούνται ως κατευθυντήριες γραμμές [14]:

- **Δοκιμασία:** Η διαδικασία πρέπει να έχει δοκιμαστεί για να διασφαλιστεί ότι παρέχει ακριβή αποτελέσματα. Δύο είναι τα βασικά είδη δοκιμασιών, Λανθασμένα Αρνητικά και Λανθασμένα Θετικά. Στη πρώτη περίπτωση διασφαλίζεται ότι παρέχονται όλα τα διαθέσιμα δεδομένα ενώ στη δεύτερη ότι δεν παρουσιάζονται νέα δεδομένα. Τα λογισμικά ανοιχτού κώδικα μπορούν να δοκιμαστούν από τον οποιοδήποτε και να δημοσιεύσει τυχόν σφάλματα που εντοπίστηκαν. Αντίθετα, στου κλειστού κώδικα ο έλεγχος γίνεται από τα άτομα που το δημιούργησαν ή δουλεύουν στην ίδια εταιρία με άμεση συνέπεια να είναι επηρεασμένα από τον τρόπο που ανατήχθηκε ο κώδικας και να τους διαφύγουν λάθη.
- **Ποσοστό σφαλμάτων:** Ελέγχεται αν υπάρχει κάποιο γνωστό ποσοστό σφαλμάτων. Εάν οι σχεδιαστές γνωρίζουν ακριβώς τις προδιαγραφές του συστήματος που χρησιμοποιείται, για παράδειγμα ενός συστήματος αρχείων (NTFS/FAT), το εργαλείο θεωρητικά δεν θα παρουσιάσει σφάλματα. Αλλά πολλά συστήματα δεν δημοσιεύουν το κώδικα ούτε αναλυτικές προδιαγραφές, με αποτέλεσμα αν μην είναι πλήρως κατανοητά από τους σχεδιαστές των εργαλείων και να υπάρχει πιθανότητα εμφάνισης σφαλμάτων. Δύο κατηγορίες σφαλμάτων εμφανίζονται στα εργαλεία forensics, Σφάλματα Εφαρμογής, που προκαλούνται από λάθη στον κώδικα ή στη προδιαγραφή, και Σφάλματα Αφαίρεσης τα οποία εμφανίζονται όταν οι αποφάσεις δεν είναι 100% σωστές όπως κατά τη χρήση τεχνικών μείωσης δεδομένων.
- **Δημοσίευση:** Πρέπει η διαδικασία που ελέγχεται να έχει δημοσιευθεί και αξιολογηθεί. Συνήθως δημοσιεύονται στο International Journal of Digital Evidence και σε άλλα τεχνολογικά περιοδικά. Ωστόσο, τα λογισμικά ανοιχτού κώδικα δεν παρέχουν διαδικαστικές λεπτομέρειες δημόσια εκτός από τον πηγαίο κώδικα, και τα μη ελεύθερα λογισμικά διαθέτουν μόνο τις βασικές προδιαγραφές του εργαλείου δημοσίως.
- **Αποδοχή:** Η αποδοχή ενός εργαλείου γίνεται μέσω της αξιολόγησης των δημοσιευμένων διαδικασιών από τη σχετική πανεπιστημιακή κοινότητα. Οι δημιουργοί των εργαλείων κλειστού κώδικα υποστηρίζουν ότι ο αριθμός των χρηστών τους υποδεικνύει την αποδοχή του, αλλά είναι διαφορετική η αποδοχή ενός εργαλείου που μπορεί να στηρίζεται στο καλύτερο περιβάλλον εργασίας και τη τεχνική υποστήριξη, από την αποδοχή μιας διαδικασίας που πραγματοποιεί.

Από τα παραπάνω είναι εμφανές ότι εργαλεία που στηρίζονται σε λογισμικό ανοιχτού κώδικα καλύπτουν περισσότερο τις προδιαγραφές που απαιτούνται για να θεωρηθούν αξιόπιστα σε μια νομική διαδικασία παρά τα κάποια ελαττώματά τους. Μια ενδιάμεση λύση για του κλειστού κώδικα εργαλεία είναι η δημοσίευση του κώδικα που αφορά συγκεκριμένες διαδικασίες επεξεργασίας δεδομένων για αξιολόγηση, και όχι μέρος του κώδικα που αφορά την παρουσίαση των αποτελεσμάτων.

Στη συνέχεια περιγράφονται εργαλεία που χρησιμοποιούνται για τη διεξαγωγή μιας ψηφιακής διερεύνησης. Σε κάποια από αυτά συμπεριλαμβάνεται αξιολόγηση πρόσφατων εκδόσεών τους σύμφωνα με εκθέσεις του National Institute of Justice (NIJ). Λόγω της συνεχής βελτίωσης των εργαλείων ενδέχεται κάποια προβλήματα που προέκυψαν κατά τις δοκιμασίες να μην ισχύουν πλέον.

6.1 EnCase



Εικόνα 9: Εργαλείο EnCase

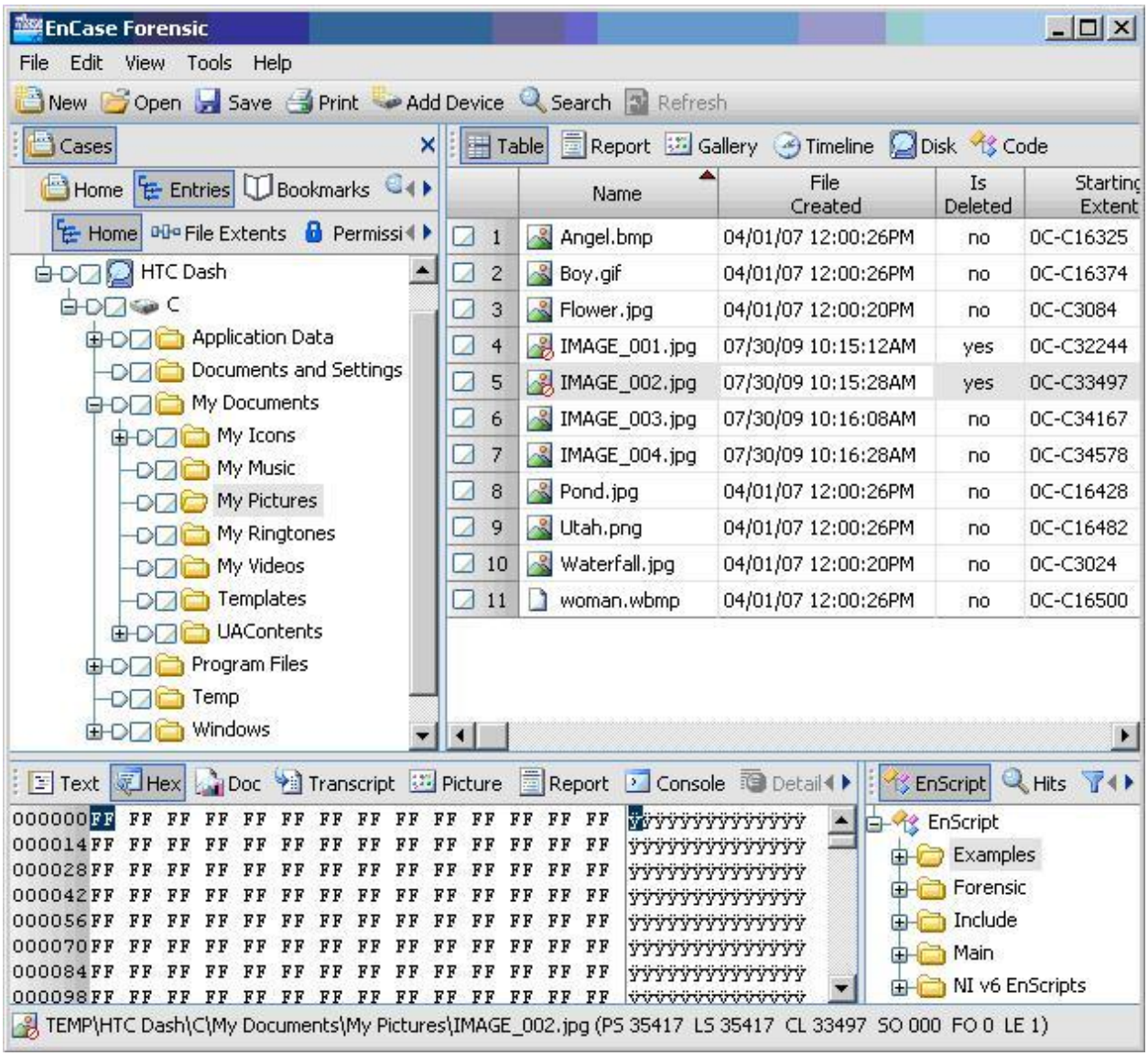
Το EnCase της Guidance Software, είναι από τα πιο δημοφιλή εργαλεία στο τομέα των Computer Forensics, θεωρείται ως πρότυπο για τη συλλογή ψηφιακών δεδομένων και είναι αναγνωρίσιμο από δικαστήρια σε όλο τον κόσμο. Περιλαμβάνει όλες τις βασικές λειτουργίες που θα χρειαστεί ένας ερευνητής όπως ανάκτηση δεδομένων, αναζήτηση, καταγραφή και τρέχει σε λειτουργικό των Windows [76].

Μπορεί να δημιουργήσει ακριβή αντίγραφα των αρχικών δίσκων τα οποία συνοδεύονται από τιμές hash.Η εξέταση των αρχείων γίνεται με εργαλεία όπως document viewer και hex editor και παράγει μια αναφορά με τις αποδείξεις που σημειώθηκε ότι εντοπίστηκαν. Μια πρόσθετη λειτουργία είναι το EnScript όπου δίνεται η δυνατότητα στον χρήστη με γνώσεις προγραμματισμού να αναπτύξει διαδικασίες για την επεξεργασία των αποδείξεων με βάση τις δικές του ανάγκες [76].

Το NIJ δημοσίευσε το Σεπτέμβριο του 2009 μια έκθεση αξιολόγησης για το EnCase 6.5 δοκιμάζοντας τις δυνατότητές του στην ανάκτηση ψηφιακών δεδομένων. Το EnCase κατάφερε επιτυχώς να συλλέξει ορατούς και κρυφούς τομείς των δοκιμαστικών αποθηκευτικών μέσων με ακρίβεια χωρίς προβλήματα, με εξαίρεση τέσσερεις ειδικές περιπτώσεις όπου απέτυχε να ανακτήσει κάποιους τομείς δεδομένων ή εμφανίστηκαν διαφορές σε μεταδεδομένα του εικονικού αντιγράφου [23].

Το EnCase κυκλοφορεί σε διάφορες εξειδικευμένες εκδόσεις, όπως [76]:

- EnCase eDiscovery: Προσφέρει μια γρήγορη πρώτη ανάλυση δεδομένων για τη λήψη άμεσων αποφάσεων και οργάνωση στρατηγικών ειδικά σε κρίσιμες καταστάσεις.
- EnCase Enterprise: Προορίζεται για τον εντοπισμό παραβιάσεων της πολιτικής της εταιρίας.
- EnCase Forensic Edition: Είναι μία δυνατή πλατφόρμα έρευνας η οποία συλλέγει ψηφιακά δεδομένα, αναλύει και καταγράφει τα αποτελέσματα τα οποία στη συνέχεια διατηρεί σε μορφή που γίνεται αποδεκτή σε ένα δικαστήριο.
- EnCase Lab Edition: Βελτιώνει την επικοινωνία μεταξύ του προσωπικού που εμπλέκεται σε μια έρευνα και βοηθάει στην αποτελεσματικότητά της για παράδειγμα με τη παροχή οδηγιών από τους αστυνομικούς στους ειδικούς ερευνητές σε πραγματικό χρόνο.
- EnCase Portable: Μια φορητή έκδοση σε USB συσκευή για την άμεση αναζήτηση και συλλογή δεδομένων από οποιονδήποτε και στη συνέχεια μεταβιβάζεται σε εξειδικευμένο προσωπικό για την περαιτέρω ανάλυση.
- EnCase Field Intelligence Model: Εξειδικευμένο για διεξαγωγή έρευνας μέσω δικτύου με χρήση ενός φορητού υπολογιστή ή μεταφέρσιμου σταθμού εργασίας.



Εικόνα 10: EnCase GUI

Εξαιτίας όμως της μεγάλης διάδοσής του έχουν εμφανιστεί εργαλεία που προσπαθούν να εμποδίσουν την αποτελεσματική λειτουργία του EnCase. Το Metaspoilt Project έχει αναπτύξει ένα σύνολο εργαλείων που μπορούν να αποκρύψουν δεδομένα αλλά και να προκαλέσουν μεταβολές στο σύστημα αρχείων. Αντίγραφα του EnCase που έχουν διαδοθεί παράνομα (πχ μέσω peer-to-peer συνδέσεων) με αποτέλεσμα την ανάλυσή του και τον εντοπισμό ευπαθειών [72].

6.2 Forensic ToolKit (FTK)

Το εργαλείο Forensic ToolKit της Access Data είναι ένα ακόμα από τα πιο διαδεδομένα λογισμικά computer forensics για περιβάλλον Windows. Ανάμεσα στις δυνατότητές του είναι η αποκρυπτογράφηση δεδομένων, ο εντοπισμός στεγανογραφημένων αρχείων και η εύρεση κωδικών πρόσβασης με χρήση λεξικών. Πιο συγκεκριμένα, το FTK3 είναι ένα γρήγορο και σταθερό λογισμικό με εύχρηστη διεπαφή, ανάλυση ηλεκτρονικής αλληλογραφίας και εξατομικεύσιμες παρουσιάσεις δεδομένων [75].



Εικόνα 11: FTK

Ένα από τα βασικά πλεονεκτήματά του είναι ότι δεν χάνεται εύκολα η διαδικασία που εκτελείται εξαιτίας κολλήματος λόγω του διαχωρισμού των βασικών μερών του εργαλείου. Για παράδειγμα αν τη γραφική διεπαφή κολλήσει οι διαδικασίες ανάλυσης θα συνεχίσουν να εκτελούνται κανονικά.

Το National Institute of Justice δοκίμασε και αξιολόγησε συγκεκριμένα το FTK Imager 2.5.3.14 και παρουσίασε την έκθεση αξιολόγησης τον Ιούνιο του 2008. Με εξαίρεση τρεις περιπτώσεις, το συγκεκριμένο εργαλείο κατάφερε να καλύψει όλες τις απαιτήσεις μιας διαδικασίας συλλογής δεδομένων από εμφανείς και κρυφούς τομείς του αποθηκευτικού μέσου. Στις άλλες δύο περιπτώσεις δεν κατάφερε να εντοπίσει τομείς κρυμμένους σε προστατευόμενη περιοχή του ιδιοκτήτη (host protected area - HPA) και από συσκευές επικάλυψης δομής (device configuration overlay - DCO). Ενώ στη τρίτη περίπτωση απέτυχε να παρουσιάσει καταστραμμένα δεδομένα στο εικονικό αντίγραφο [46].

Άλλα εργαλεία της Access Data για χρήση forensic είναι [75]:

- MPE+ (Mobile Phone Examiner Plus): Είναι μια συσκευή tablet για την άμεση διεξαγωγή έρευνας σε κινητά τηλέφωνα και μπορεί να συνδεθεί απευθείας με το FTK.

- AD Lab (AccessData Lab): Διευκολύνει τη συνεργασία εξειδικευμένου προσωπικού στα forensics μεταξύ τους καθώς και με άτομα άλλης ειδικότητας, πχ δικηγόροι. Απευθύνεται κυρίως σε μεγάλα εργαστήρια που έρχεται αντιμέτωπο με μεγάλο μέγεθος δεδομένων και απαιτείται κατανεμημένη εργασία.
- AD Enterprise (AccessData Enterprise): Λογισμικό για την ψηφιακή διερεύνηση μέσω δικτύου. Βασίζεται και περιέχει λειτουργίες του FTK και αναλύει αποτελεσματικά ευμετάβλητα και μη δεδομένα.
- SilentRunner Mobile: Ελέγχει, καταγράφει, αναλύει και παρουσιάζει τη δικτυακή κίνηση για τον έλεγχο ενεργειών ενός υπόπτου κατά τη διάρκεια μιας έρευνας.
- Decryption: Η Access Data έχει δημιουργήσει διάφορα λογισμικά για τη διαδικασία της αποκρυπτογράφησης, όπως το Password Recovery Toolkit το οποίο ανακτά κωδικούς πρόσβασης από γνωστές εφαρμογές, και το Distributed Network Attack που ανακτά κωδικούς μέσω ωμής βίας (brute force) με τη χρήση πολλών υπολογιστών.
- Triage – Live response: Χρησιμοποιείται από ερευνητές και ειδικούς στην ασφάλεια για τη συλλογή δεδομένων που χάνονται μετά την απενεργοποίηση του υπολογιστικού συστήματος.

6.3 The Sleuth Kit

Το Sleuth Kit είναι ένα εργαλείο ανάλυσης με βιβλιοθήκη C και συλλογή εντολών αρχείων και συστήματος. Τα εργαλεία του συστήματος αρχείου επιτρέπουν την εξέταση του ύποπτου υπολογιστικού συστήματος χωρίς να εισβάλει. Επειδή δεν βασίζεται στο λειτουργικό σύστημα εμφανίζονται διαγραμμένα και κρυμμένα αρχεία. Κατάλληλο για λειτουργικά Windows και UNIX [78].

Το Autopsy Forensic Browser αποτελεί τη γραφική διεπαφή των εργαλείων του Sleuth Kit για τη διευκόλυνση της διεξαγωγής έρευνας. Περιλαμβάνει αυτοματοποιημένες λειτουργίες όπως διαχείριση περίπτωσης, ακεραιότητα εικόνας, αναζήτηση με λέξης κλειδιά [78].

6.4 P2 Commander



Εικόνα 12: P2 Commander

Η Paraben παρουσίασε το P2 Commander, ένα εργαλείο forensic σχεδιασμένο για αποτελεσματική εξέταση πολλών δεδομένων. Χρησιμοποιεί προηγμένη αρχιτεκτονική για τη δημιουργία διαδικασιών που επικεντρώνονται σε ηλεκτρονική αλληλογραφία, καταγραφές ομιλίας, ανάλυση αρχείων διαδικτύου και άλλα που μπορούν να αυξήσουν το μέγεθος των δεδομένων που υφίστανται επεξεργασία και αξιοποιώντας πόρους μέσω multi-threading και προγραμματισμό εργασιών [77].

6.5 Device Seizure

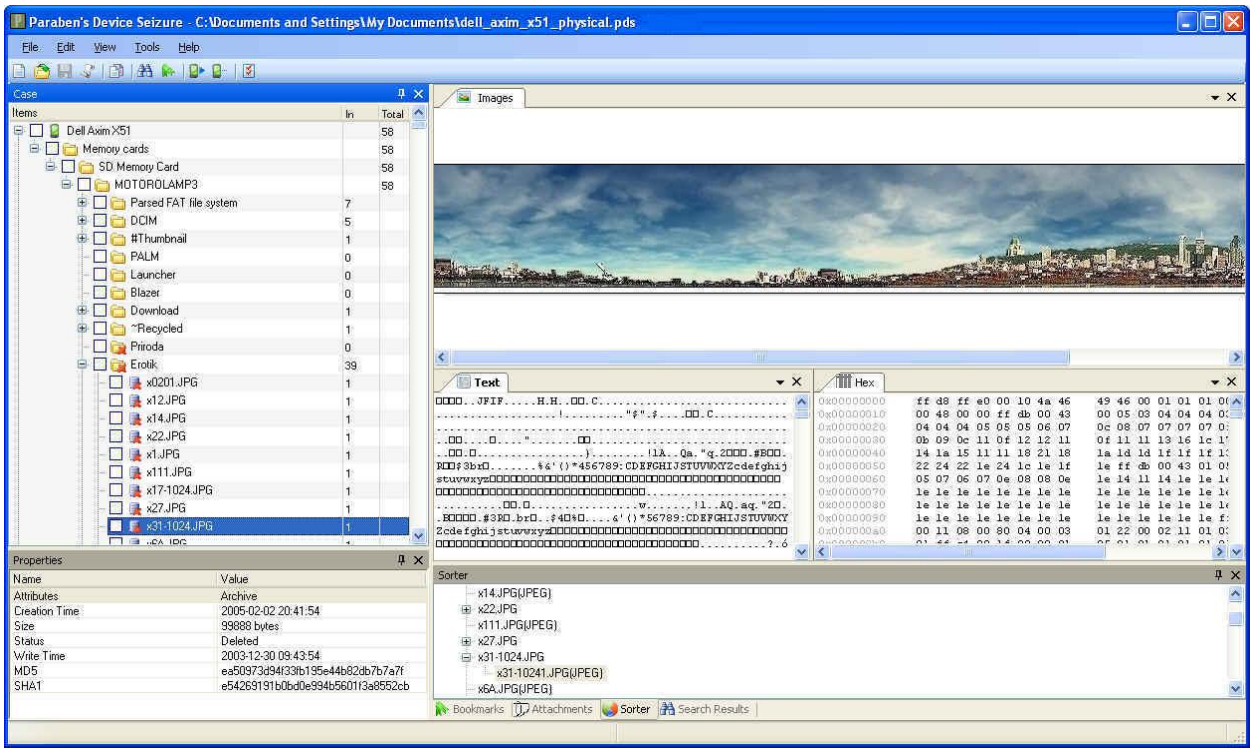
Το Device Seizure είναι ένα ακόμα εργαλείο της Paraben. Είναι ένα προηγμένο εργαλείο forensics για την απόκτηση και ανάλυση δεδομένων από κινητά τηλέφωνα, PDAs και GPS. Περιλαμβάνει το απαραίτητο λογισμικό και υλισμικό για mobile forensics. Σε αντίθεση με άλλα παρόμοια εργαλεία, ανακτά διαγραμμένα αρχεία και αρχεία του χρήστη όπως γραπτά μηνύματα και εικόνες [77].

Με βάση έκθεση αξιολόγησης του National Institute of Justice το Νοέμβριο του 2010, συγκεκριμένα για το Device Seizure 3.1, αντεπεξήλθε επιτυχώς στις δοκιμασίες συλλογής όλων των δεδομένων με ακρίβεια. Ωστόσο, υπήρχαν κάποιες μεμονωμένες περιπτώσεις όπου δεν κατάφερε να συνδεθεί επιτυχώς με συγκεκριμένα μοντέλα ή να συλλέξει και να παρουσιάσει κάποια δεδομένα της συσκευής [22].

Άλλες εκδόσεις του είναι:

- Deployable Device Seizure (DDS): Σχεδιασμένη κατάλληλη για εφαρμογή στο τόπο συμβάντος. Με μία εντολή ανακτά βασικές πληροφορίες του κινητού όπως πρόσφατες τηλεφωνικές κλήσεις, τηλεφωνικό κατάλογο, γραπτά μηνύματα κτλ.

- SIM Card Seizure: Ανακτά διαγραμμένα μηνύματα και αναλύει τα δεδομένα από κάρτες SIM. Περιλαμβάνει το λογισμικό και μια συσκευή ανάγνωσης των συγκεκριμένων καρτών.



Εικόνα 13: Device Seizure

6.6 SafeBack



Εικόνα 14: SafeBack

Το SafeBack είναι ένα εργαλείο για τη δημιουργία εικονικών αντιγράφων αρχείων, σκληρών δίσκων ή τμήματά τους. Χρησιμοποιεί μαθηματικούς αλγόριθμους κατακερματισμού για την αυθεντικοποίηση των δεδομένων οι οποίοι είναι αποδεκτοί από το National Institute Of Standards and Technology. Τα αντιγραμμένα αρχεία που δημιουργεί μπορούν να αποθηκευτούν σε οποιοδήποτε αποθηκευτικό μέσο και περιλαμβάνει όλα τα δεδομένα του πρωτότυπου μέσου

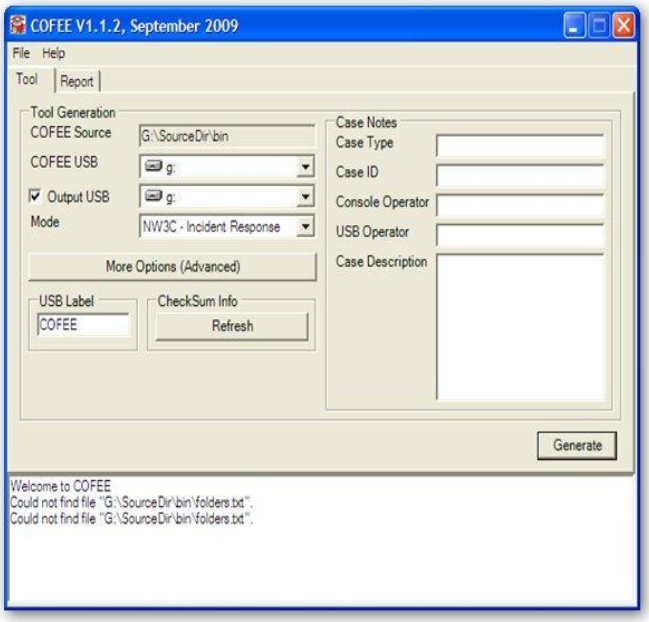
συμπεριλαμβανομένου ανενεργά ή διαγραμμένα αρχεία. Το SafeBack δεν γράφει ή τροποποιεί το αρχικό σύστημα και μπορεί να ξεκινήσει από μια δισκέτα εκκίνησης [79].

Συγκεκριμένα για το SafeBack 2.18, η αξιολόγηση του NIJ το 2003 υποδεικνύει ότι είναι κατάλληλο για τη δημιουργία bit-stream αντιγράφων ή εικόνων του αρχικού δίσκου ή μέρος του δίσκου. Κάποια προβλήματα παρουσιάστηκαν σε ειδικές περιπτώσεις όπου το σύστημα αρχείων ήταν FAT32, κάποιες πληροφορίες του συστήματος αρχείων είχαν μετατραπει, και με κάποιες ρυθμίσεις του BIOS που μπορεί να επηρεάσουν τη διαδικασία αντιγραφής και να μην εντοπιστούν κάποιο τομείς [35].

Άλλα εργαλεία δημιουργίας αρχεία εικονικών αντιγραφών για μετέπειτα ανάλυση και εξέταση είναι το SnapBack και dd, η δεύτερη όμως δεν παρέχει χρήσιμα χαρακτηριστικά των άλλων εργαλείων, όπως συλλογή μεταδεδομένων, διόρθωση λαθών κτλ [72].

6.7 COFEE

Το Computer Online Forensic Evidence Extractor (COFEE) είναι ένα εργαλείο σε USB συσκευή της Microsoft αποκλειστικά για χρήση από προσωπικό επιβολής νόμου. Περιέχει λειτουργίες για την εύκολη, γρήγορη και ασφαλή συλλογή δεδομένων που χάνονται μετά την απενεργοποίηση του υπολογιστή στο χώρο του συμβάντος. Η χρήση του δεν απαιτεί συγκεκριμένη εκπαίδευση, αρκούν βασικές γνώσεις στους υπολογιστές [82].



Εικόνα 15: COFEE

Ωστόσο, έχει αναπτυχθεί ένα εργαλείο για να εμποδίσει συγκεκριμένα τη λειτουργία του COFEE, το Detect and Eliminate Computer Acquired Forensics (DECAF). Κάποιες από τις ενέργειές του είναι ο καθαρισμός των καταγραφών του COFEE, η αποσύνδεση συσκευών USB

και επεξεργασία των MAC διευθύνσεων. Η χρήση τους όμως δεν εμποδίζει άλλα πιο εξελιγμένα εργαλεία forensics κατά την έρευνα [72].

6.8 OCFA

Το Open Computer Forensics Architecture (OCFA) είναι ένα κατανεμημένο εργαλείο forensics ανοιχτού κώδικα για την ανάλυση ψηφιακών μέσων σε εργαστηριακό περιβάλλον κατάλληλο για computer forensics. Αποτελείται από τρία βασικά μέρη, το OcfaLib, το OcfaArch και το OcfaModules [80].

Το πρώτο μέρος αποτελεί τη βιβλιοθήκη που αποτελεί κύριο στοιχείο για τη λειτουργία των άλλων δύο. Επιπλέον μπορεί να την εκμεταλλευτεί ο χρήστης για να δημιουργήσει νέες λειτουργίες προσαρμοσμένες στις ανάγκες του. Το δεύτερο μέρος, το OcfaArch, αποτελείται από τα κύρια στοιχεία του OCFA, ενώ το OcfaModules περιέχει διάφορους τύπους δευτερευόντων στοιχείων του OCFA.

6.9 SMART

Η ASR Data διαθέτει διάφορα εργαλεία forensics με κυριότερο το Storage Media Analysis Recovery Toolkit (SMART) το οποίο αποτελεί ένα λογισμικό και μεθοδολογία με σκοπό την κάλυψη κάθε τεχνικής και νομικής απαίτησης του χρήστη αποτελεσματικά και αποδοτικά. Είναι κατάλληλο τόσο για έρευνα στο χώρο του συμβάντος ή στο εργαστήριο και μπορεί να αναλύσει και ανενεργά συστήματα [81].



Εικόνα 16: ASR Data

Διαφορετικές εκδόσεις του SMART είναι [81]:

- SMART Linux[2]: είναι ένα live CD διανομής Linux κατάλληλο για forensics ψηφιακών δεδομένων, ηλεκτρονική έρευνα και απόκριση σε συμβάντα. Κάθε λειτουργία του SMART Linux έχει βελτιστοποιηθεί και διαμορφωθεί για την παραγωγή ενός

[2] Παρουσίαση του εργαλείου στο Παράρτημα Δ.

λειτουργικού συστήματος που προσφέρει ένα καθαρό, μη καταπατητικό περιβάλλον. Περιέχει πολλά εργαλεία forensic για αναζήτηση, ανάλυση και καταγραφή δεδομένων. Από τα βασικότερα πλεονεκτήματά του είναι ότι προσφέρει ένα πλήρες περιβάλλον εργασίας σε λιγότερο από 2 λεπτά για οποιοδήποτε λειτουργικό σύστημα, Windows-Linux-Macintosh.

- SmartMount: εγκαθιστά ή συνδέει τοπικά ή στο δίκτυο αρχεία EnCase, VMWareDisk, FTK, SMART ή dd, ή συνδέεται απευθείας με το σύστημα αρχείων τους χωρίς να χρειάζεται πάλι την ανάκτηση δεδομένων ή συσκευές προστασίας εγγραφής.
- Smart Acquisition Workshop (SAW): αποτελεί το τμήμα ανάκτησης δεδομένων ενός πλαισίου διαχείρισης μιας υπόθεσης κατάλληλα διαμορφωμένο για εκπληκτική απόδοση και οφέλη σε μεγάλες περίπλοκες ψηφιακές έρευνες.

6.10 Τα Linux ως εργαλείο forensic

Ένα οποιοδήποτε λειτουργικό σύστημα Linux μπορεί να μετατραπεί σε ένα ασφαλές περιβάλλον εργασίας για forensics με τις κατάλληλες τροποποιήσεις χάρης τη δυνατότητα αλλαγών σε οποιοδήποτε κομμάτι του λειτουργικού. Με τον έλεγχο των συνδέσεων εξωτερικών συσκευών, εφαρμογή προστασίας εγγραφής και άλλες ενέργειες παρέχεται ένα αξιόπιστο εργαλείο για την ανάκτηση δεδομένων σχεδόν από οποιοδήποτε υπολογιστικό σύστημα [55].

Ένας ερευνητής μπορεί να εκμεταλλευτεί τη πληθώρα εντολών που προσφέρεται από τα συστήματα Linux, τα οποία αν και δεν παρέχουν τόσο φιλικό περιβάλλον χρήσης όπως πιο δημοφιλή εργαλεία forensics (πχ EnCase), μπορούν όμως να εκτελέσουν οποιαδήποτε λειτουργία τόσο απευθείας στο χώρο του συμβάντος όσο και στο εργαστήριο, και σίγουρα το κόστος είναι πολύ μικρότερο σε σχέση με τα εμπορικά εργαλεία. Παρόλα αυτά απαιτείται ένας έμπειρος χρήστης, με άριστη γνώση των συστημάτων Linux, για να τεκμηριώσει αδιαμφισβήτητα τις ενέργειές του και τα τελικά αποτελέσματα.

6.11 Γλώσσα Python



Εικόνα 17 : Γλώσσα Python

Υπάρχουν εργαλεία για κάθε είδους λειτουργία που θα χρειαστεί σε μια έρευνα forensic, τα οποία καλύπτουν την εύρεση σχεδόν κάθε τύπου αρχείου σε οποιαδήποτε θέση του αποθηκευτικού μέσου. Ωστόσο, μπορεί να υπάρξουν περιπτώσεις όπου απαιτείται μια πιο ειδική αναζήτηση ή ο ερευνητής να θέλει να περιορίσει την έρευνά του σε συγκεκριμένα στοιχεία για την απόκτηση γρηγορότερων αποτελεσμάτων. Αυτό μπορεί να το επιτύχει δημιουργώντας τις δικές του μεθόδους με χρήση γλωσσών προγραμματισμού, όπως η Python, η οποία παρέχει κατάλληλες βιβλιοθήκες για λογισμικά εργαλεία forensics. Η Python είναι μια γλώσσα προγραμματισμού υψηλού επιπέδου, διαθέτει εκτενή βιβλιοθήκη και πακέτα για τη δημιουργία συναρτήσεων για τον εντοπισμό κρυπτογραφημένων αρχείων, μεταδεδομένων και άλλα, καθώς και για πιο την εξειδικευμένη εξέταση δεδομένων [48].

6.12 Αξιολόγηση Εργαλείων

Παρακάτω δίνεται ένας συνολικός πίνακας των εργαλείων που υποβλήθηκαν σε αξιολόγηση από το National Institute of Justice. Το τελικό αποτέλεσμα προκύπτει με βάση τις επιτυχημένες δοκιμασίες, δηλαδή τις περιπτώσεις που δεν εμφανίστηκαν ανωμαλίες, ως προς το σύνολο των δοκιμασιών που πραγματοποιήθηκαν. Η τιμή ένα (1) υποδεικνύει ελάχιστη ικανότητα να ανταπεξέλθει στις δοκιμασίες, ενώ τη μέγιστη ικανότητα υποδεικνύει η τιμή πέντε (5).

Όνομα	Χρονολογία Αξιολόγησης	Αριθμός συνολικών δοκιμών	Αριθμός επιτυχημένων δοκιμών	Τελική αξιολόγηση (1 έως 5)
EnCase 6.5	2009	11	7	3,2 / 5
FTK Imager 2.5.3.14	2008	9	6	3,3 / 5
Device Seizure 3.1	2009	10	5	2,5 / 5
SafeBack 2.18	2003	112	56	2,5 / 5

Πίνακας 1: Αξιολόγησης εργαλείων forensics

Από τον παραπάνω πίνακα φαίνεται μια σχετικά ικανοποιητική απόκριση των εργαλείων στις διάφορες δοκιμασίες που υποβλήθηκαν. Πρέπει όμως να σημειωθεί ότι από το σύνολο των δοκιμών αφαιρέθηκαν όχι μόνο αυτές που δεν κατάφεραν να ανταπεξέλθουν καθόλου τα εργαλεία, αλλά και όσες παρουσίασαν μικρά μεμονωμένα σφάλματα παρότι η γενική εικόνα του αποτελέσματος της δοκιμασίας ήταν αρκετά ικανοποιητική. Αυτού του είδους οι αποτυχίες ήταν το μεγαλύτερο ποσοστό, επομένως τα εργαλεία μπορούν να θεωρηθούν αποτελεσματικά και αξιόπιστα.

7 Εργαλεία AntiForensic

Τα εργαλεία antiforensic αναφέρονται σε αυτά που προσπαθούν να εμποδίσουν την εύρεση αποδεικτικών στοιχείων κατά τη διάρκεια μιας έρευνας όπως έχει αναλυθεί στο κεφάλαιο 4.4. Σε αυτό το κεφάλαιο παρουσιάζονται κάποια εργαλεία διαγραφής δεδομένων, κρυπτογράφησης, στεγανογράφησης και άλλα, τα οποία είναι αρκετά διαδεδομένα για την anti-forensic χρήση τους. Επιπλέον, αναλύονται τα μειονεκτήματα εργαλείων που διαγράφουν συγκεκριμένα αρχεία ή ένα αποθηκευτικό μέσο επειδή είναι μια από τις πιο διαδεδομένες anti-forensic ενέργειες και ακολουθεί μια αξιολόγησής τους.

Τα εργαλεία που θα παρουσιαστούν δεν έχουν κατεξοχήν στόχο την παρεμπόδιση μιας έρευνας ψηφιακών στοιχείων, είναι νόμιμα και συνήθως αξιοποιούνται για τη προστασία προσωπικών και ευαίσθητων δεδομένων. Ωστόσο, οι λειτουργίες που εκτελούν μπορούν να αξιοποιηθούν σε παράνομες δραστηριότητες.

7.1 Εργαλεία κρυπτογράφησης

Τα εργαλεία κρυπτογράφησης χρησιμοποιούνται για να αποκρύπτουν δεδομένα μέσω της μετατροπής τους με περίπλοκους αλγόριθμους. Παρότι δεν αποκρύπτεται η ύπαρξη των δεδομένων, απαιτείται η χρήση κατάλληλου κλειδιού για την αποκρυπτογράφηση και ανάκτησή τους.

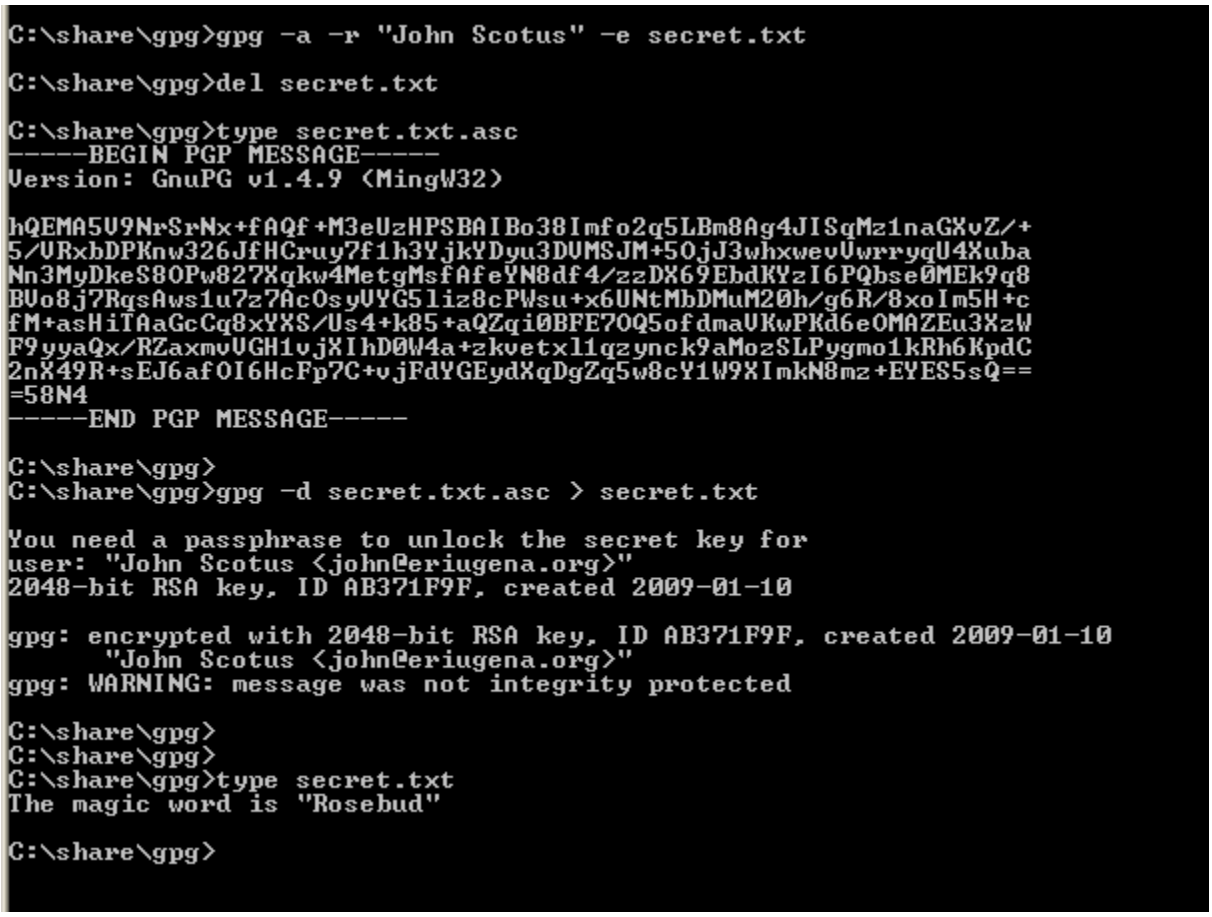
GnuPG



Εικόνα 18: Εργαλείο GnuPG

Το Gnu Privacy Guard (GnuPG) είναι μια ολοκληρωμένη και δωρεάν εφαρμογή του προτύπου OpenPGP (Pretty Good Privacy). Είναι ένα εργαλείο γραμμής εντολών το οποίο κρυπτογραφεί αρχεία και δεδομένα επικοινωνίας. Κυκλοφορεί σε δύο εκδόσεις, την 1.4.11 η οποία είναι μια φορητή και ανεξάρτητη έκδοση, και η πιο ενισχυμένη 2.0.17. Επιπλέον, η εφαρμογή Gpg4win παρέχει ένα φιλικό περιβάλλον εργασίας

κατάλληλο για Windows, και η Aegypten ανέπτυξε τη λειτουργία S/MIME (Secure/Multipurpose Internet Mail Extensions) για την GnuPG 2 [83].



Εικόνα 19: GnuPG Command Line

OpenSSL



Εικόνα 20: Εργαλείο OpenSSL

Το OpenSSL αποτελεί μια υλοποίηση των πρωτοκόλλων SSL (Secure Sockets Layer) και TLS (Transport Layer Security) καθώς και ολοκληρωμένων βιβλιοθηκών κρυπτογράφησης για γενική χρήση. Έχει Apache-style

άδεια, δηλαδή μπορεί να χρησιμοποιηθεί ελεύθερα για εμπορικούς και μη σκοπούς. Εργαλεία που βασίζονται στο OpenSSL είναι το Stunned και το OpenVPN (Virtual Private Network) τα οποία παρέχουν ασφαλές συνδέσεις στο διαδίκτυο [84, 85, 86].

TrueCrypt

Το TrueCrypt είναι ένα λογισμικό ανοιχτού κώδικα κρυπτογράφησης δίσκων. Είναι κατάλληλο για Windows, Linux και Mac. Τα κυριότερα χαρακτηριστικά του είναι η δημιουργία ενός εικονικού κρυπτογραφημένου δίσκου σε ένα αρχείο, η κρυπτογράφηση ολόκληρης αποθηκευτικής συσκευής όπως ένα σκληρό δίσκο ή συσκευή USB. Επιπλέον, δίνει τη δυνατότητα άρνησης σε περίπτωση που ο χρήστης αναγκαστεί να αποκαλύψει το κλειδί με την απόκρυψη τομέων ή ακόμα και λειτουργικών συστημάτων [87].



Εικόνα 21: TrueCrypt GUI

7.2 Εργαλεία στεγανογράφησης

Τα εργαλεία στεγανογράφησης ενσωματώνουν δεδομένα σε άλλα αρχεία με τρόπο που να μην είναι εμφανή. Για επιπρόσθετη ασφάλεια τα δεδομένα αυτά μπορούν να είναι κρυπτογραφημένα. Σε αντίθεση με τη κρυπτογράφηση, η στεγανογράφηση αποκρύπτει όχι απλά τα δεδομένα αλλά και την ύπαρξή τους γενικά. Ωστόσο, ο εντοπισμός των εργαλείων μπορεί να αποτελέσει στοιχείο για τον ερευνητή για την αναζήτηση στεγανογραφημένων αρχείων.

S-Tools

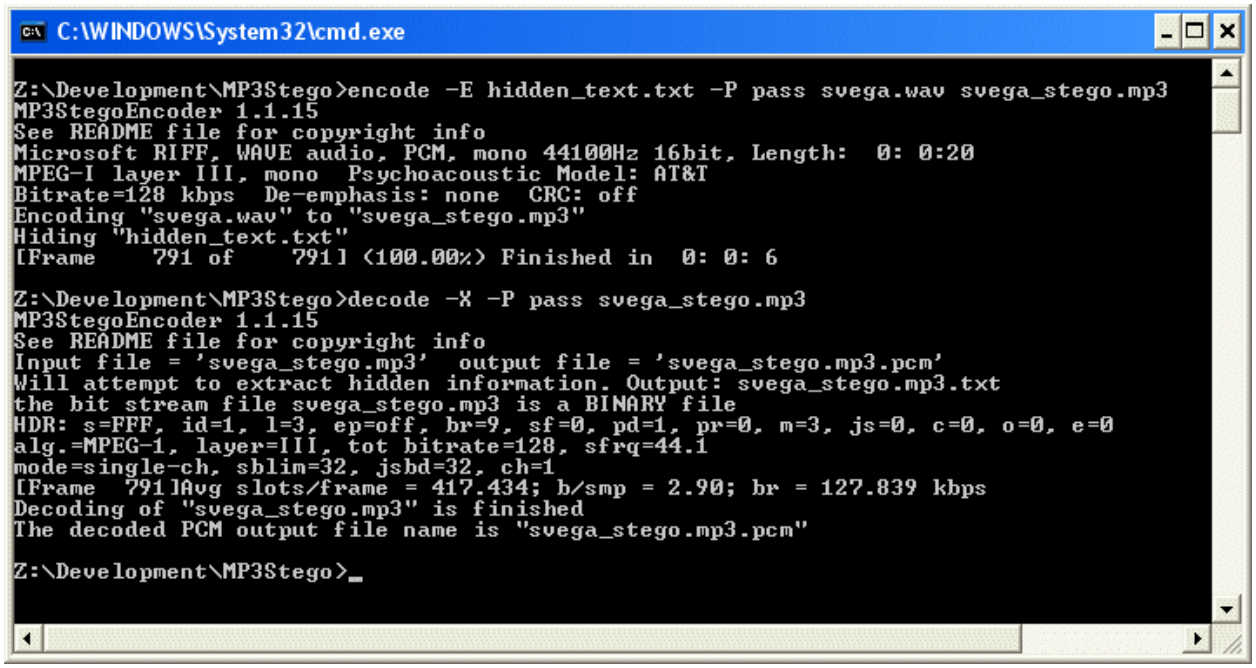
Το S-Tools είναι ένα εργαλείο στεγανογράφησης το οποίο κρύβει δεδομένα σε αρχεία εικόνας BMP (Bitmal Image File) και GIF (Graphics Interchange Format) και σε αρχεία ήχου WAV (Waveform Audio File Format). Τα δεδομένα που επιθυμεί ο χρήστης να κρύψει συμπιέζονται και μετά κρυπτογραφούνται πριν προστεθούν στο αρχείο ήχου ή εικόνας [88].



Εικόνα 22: S-Tools GUI

MP3Stego

Το εργαλείο λογισμικού MP3Stego κρύβει πληροφορίες σε αρχεία MP3 κατά τη διάρκεια της διαδικασίας συμπίεσης αφού πρώτα έχουν συμπιεστεί και κρυπτογραφηθεί τα δεδομένα που επιθυμεί ο χρήστης να τοποθετήσει στο αρχείο ήχου [89].



Εικόνα 23: MP3Stego

Invisible Secrets

Ένα άλλο εργαλείο στεγανογράφησης είναι το Invisible Secrets (Αόρατα Μυστικά). Είναι κατάλληλη για την ασφαλή αποθήκευση ή μεταφορά δεδομένων μέσω του διαδικτύου επειδή κρυπτογραφεί τα δεδομένα και τα τοποθετεί σε αρχεία ήχου, εικόνας ή σε ιστοσελίδες. Επιπλέον χαρακτηριστικά του είναι η παραγωγή τυχαίων κωδικών πρόσβασης και φύλαξή τους, προστασία εφαρμογών με κωδικούς και παροχή εικονικού πληκτρολογίου για την αποφυγή λογισμικών υποκλοπής [90].



Εικόνα 24: Invisible Secrets

7.3 Εργαλεία από τη Metasploit

Αρκετά εργαλεία και τεχνικές anti-forensic αναπτύχθηκαν από την Metasploit Anti – Forensics Investigation Arsenal (MAFIA) για την αφαίρεση αποδεικτικών στοιχείων από υπολογιστικά συστήματα και τον εντοπισμό αδυναμιών σε γνωστά εργαλεία forensics [91]. Κάποια από αυτά είναι:

- Timestomp: διαγράφει ή μετατρέπει πληροφορίες ενός αρχείου σχετικές ημερομηνία και ώρα,
- Slacker: κρύβει αρχεία στο νωθρό χώρο ενός NTFS συστήματος αρχείων,

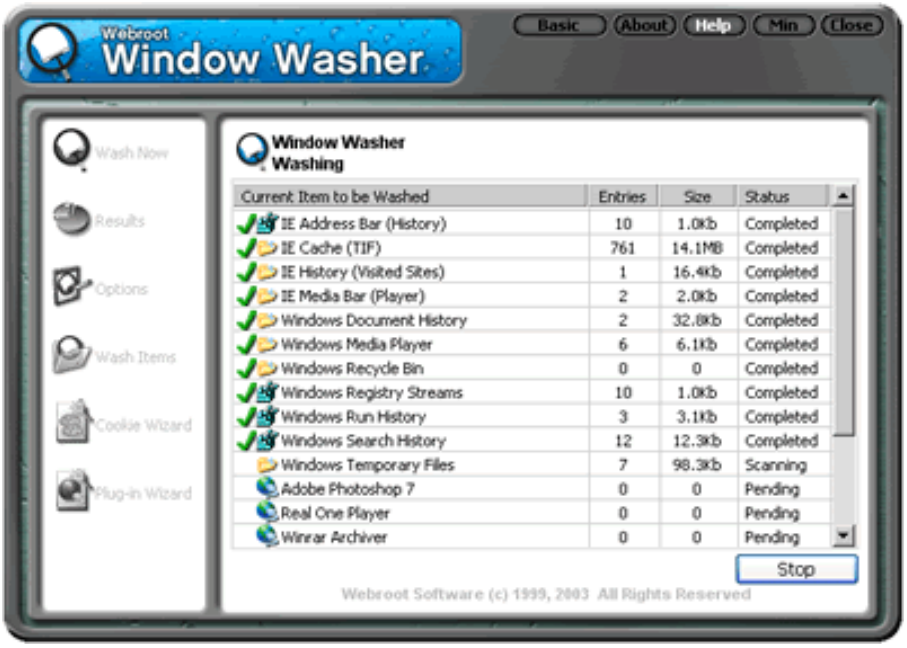
- Sam Juicer: μεταποθηκεύει τις τιμές hash από το αρχείο SAM (Security Accounts Manager), το οποίο περιέχει κωδικούς του χρήστη σε μορφή hash, χωρίς να αφήνει ίχνη στο δίσκο.
- Transmogrify: δίνει τη δυνατότητα στο χρήστη να καλύψει κάποιο αρχείο με οποιοδήποτε τύπο αρχείου, το οποίο δεν εντοπιζόταν από το EnCase.

7.4 Εργαλεία διαγραφής δεδομένων

Τα εργαλεία διαγραφής δεδομένων εγγράφουν τυχαία δεδομένα στο χώρου του δίσκου που βρίσκονται τα αρχεία που επιθυμεί να διαγράψει ο χρήστης εξαλείφοντας τη δυνατότητα επανάκτησής τους. Η νόμιμη χρήση τους αφορά τη προστασία προσωπικών δεδομένων, αλλά μπορεί να θεωρηθεί αδίκημα αν ο σκοπός είναι η διαγραφή αποδεικτικών στοιχείων μιας παράνομης δραστηριότητας. Ωστόσο, η χρήση των αναφερόμενων εργαλείων δεν πρέπει να επαναπαύει το χρήστη του εξαιτίας των πολλών αδυναμιών τους που θα αναλυθούν μετά τη παρουσίαση κάποιων από αυτά τα εργαλεία.

Window Washer

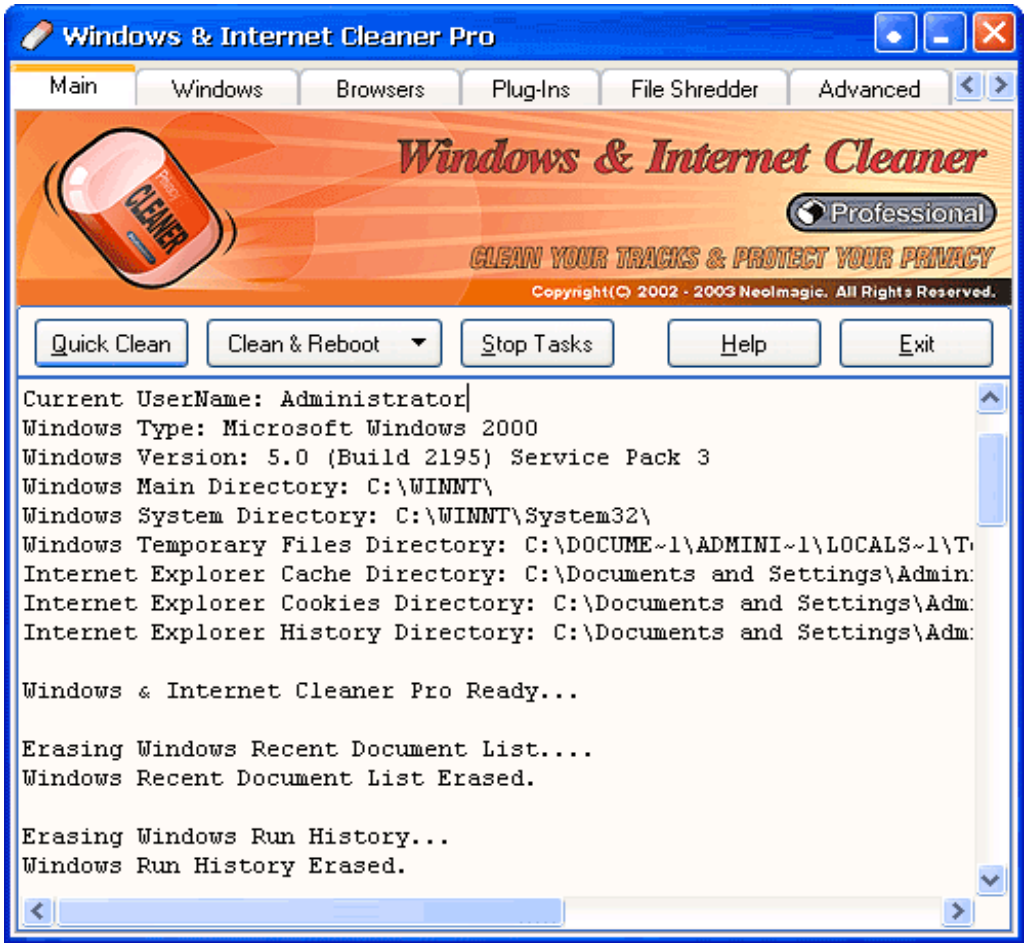
Το Window Washer της Webroot είναι ένα πρόγραμμα διαγραφής δεδομένων για τη προστασία της ιδιωτικότητας. Παρέχει ένα φιλικό περιβάλλον εργασίας για Windows το οποίο προστατεύει την ιδιωτική ζωή του χρήστη εύκολα και γρήγορα. Διαγράφει ίχνη από ιστοσελίδες που επισκέφτηκε ο χρήστης, δηλαδή το ιστορικό, διευθύνσεις, cookies και άλλα. Διαγράφει μόνιμα αρχεία και τα επικαλύπτει χρησιμοποιώντας τεχνικές κρυπτογράφησης για να αποτραπεί η επανάκτησή τους [92].



Εικόνα 25: Window Washer

Windows & Internet Cleaner Pro

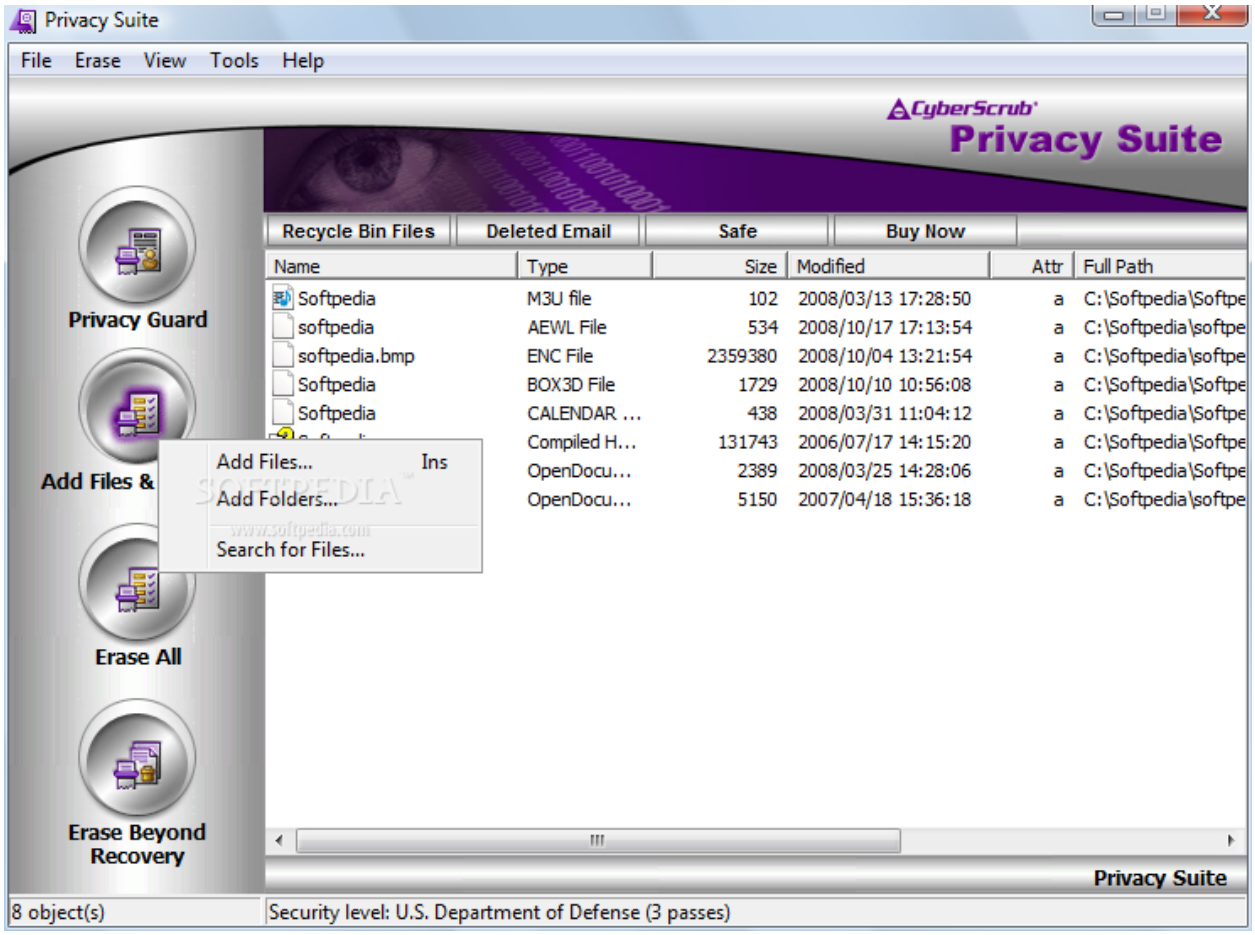
Η Neoimagic ανέπτυξε ένα εργαλείο, ειδικά για το περιβάλλον των Windows, με βασική λειτουργία τη διαγραφή από τον υπολογιστή αρχεία που βρίσκονται στη κρυφή μνήμη, ιστορικό, cookies, και άλλα ίχνη που αφήνονται από την περιήγηση στο διαδίκτυο αφήνοντας μόνο αυτά που επιθυμεί ο χρήστης. Επιπλέον, δίνεται η δυνατότητα αλλαγής μονοπατιών διάφορων φακέλων του συστήματος. Ο καθαρισμός του υπολογιστή μπορεί να γίνει αυτόματα κατά την εκκίνηση ή πριν την απενεργοποίησή του [95].



Εικόνα 26: Windows & Internet Cleaner Pro

CyberScrub

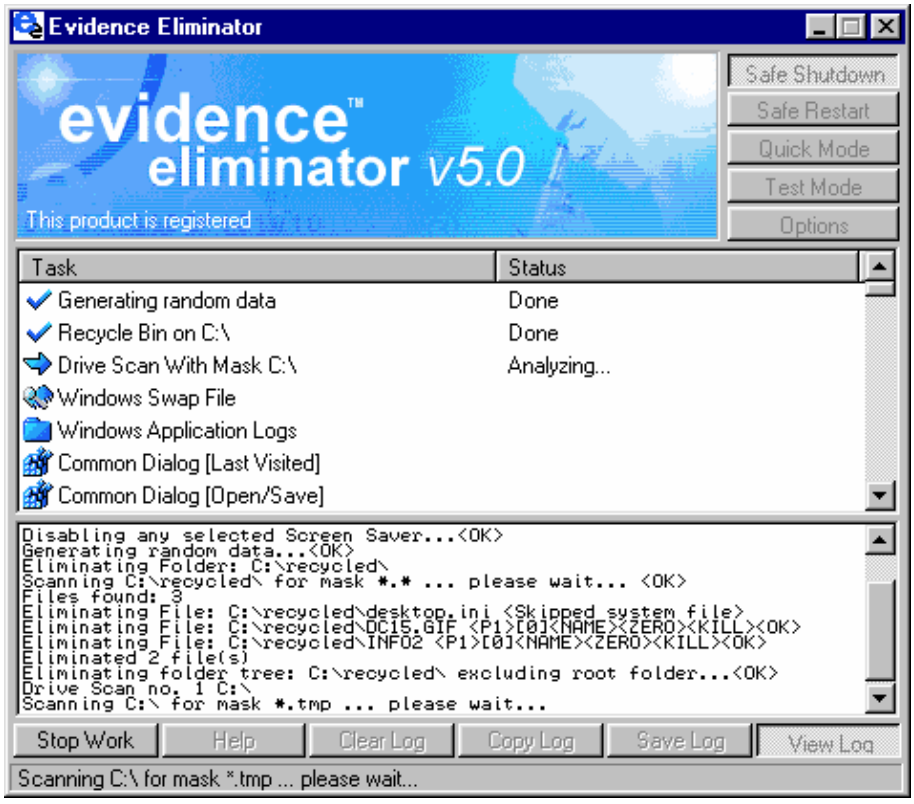
Η CyberScrub είναι μια εταιρία παραγωγής λογισμικού για την προστασία των δεδομένων και διασφάλιση της ιδιωτικότητας. Τα προϊόντα της απευθύνονται σε εταιρίες και δημόσιους οργανισμούς αλλά και σε ιδιώτες. Ανάμεσα στα προϊόντα που προσφέρει είναι το Privacy Suite, μια εφαρμογή για την ολοκληρωτική διαγραφή ευαίσθητων πληροφοριών και διαδικτυακής δραστηριότητας. Επίσης, το cyberCide διαγράφει δεδομένα από σκληρούς δίσκους, ενώ το Compliance Suite είναι κατάλληλο για τη διαχείριση μεγάλων δικτυακών επιχειρήσεων [93].



Εικόνα 27: CyberScrub

Evidence Eliminator

Το Evidence Eliminator είναι ένα δυνατό και εύκολο πρόγραμμα για τη πλήρη διαγραφή δεδομένων από το σκληρό δίσκο αλλά και ιστορικό από επισκέψεις στο διαδίκτυο. Είναι από τα λίγα προϊόντα που διαφημίζει ότι διαγράφει όλα τα δεδομένα από όλες τις πιθανές τοποθεσίες αποθήκευσης με αποτέλεσμα κανένα από τα γνωστά εργαλεία forensic, όπως το EnCase, να μην μπορεί να τα επανακτήσει [94].



Εικόνα 28: Evidence Eliminator

7.4.1 Μειονεκτήματα

Η αποτελεσματικότητα ενός εργαλείου διαγραφής δεδομένων εξαρτάται τόσο από τον κατασκευαστή του αλλά πολύ περισσότερο από τους ίδιους τους χρήστες. Ένας κοινός χρήστης με τυπικές γνώσεις χρήσης ενός απλού υπολογιστικού συστήματος εμπιστεύεται το πρόγραμμα που χρησιμοποιεί ότι θα κάνει τη δουλεία που υπόσχεται. Ένας έμπειρος χρήστης όμως μπορεί να προβλέψει κάποια από τα μειονεκτήματα που περιγράφονται παρακάτω.

Ένα από τα συνηθέστερα λάθη που κάνουν οι περισσότεροι χρήστες είναι να διατηρούν τις προεπιλεγμένες ρυθμίσεις του εργαλείου αυτούσιες, όμως έτσι πολλές ενέργειες παραλείπονται επειδή πρωτεύον στόχος είναι η γρηγορότερη εκτέλεση του προγράμματος. Η διαγραφή αρχείων από μη εντοπισμούς χώρους, τη περιοχή ανταλλαγής και άλλες τοποθεσίες, δεν πραγματοποιείται με συνέπεια της μείωσης της αποτελεσματικότητάς τους και τη διατήρηση αρκετών δεδομένων. Επιπλέον, δεν διαγράφονται δεδομένα που δημιουργήθηκαν από το λειτουργικό σύστημα ή από κάποια εφαρμογή. Για παράδειγμα το Office δημιουργεί προσωρινά

αντίγραφα ενός Word αρχείου αλλά το antiforensic εργαλείο δεν εντοπίζει αυτά τα αντίγραφα παρά μόνο το πρωτότυπο αρχείο που βρίσκεται μια συγκεκριμένη θέση την οποία προσπαθεί να επικαλύψει [43].

Μία άλλη παράβλεψη είναι η διαγραφή του μητρώου καταγραφής χρήσης που διατηρούν συνήθως τα λειτουργικά για τα λογισμικά που έχουν εγκατασταθεί. Οπότε ο ερευνητής μπορεί να πάρει πληροφορίες για προγράμματα που είχε προηγουμένως ο χρήστης εγκατεστημένα και για ποιο χρονικό διάστημα. Κάποια λειτουργικά συστήματα διατηρούν αντίγραφα ασφαλείας για τη δημιουργία σημείων επαναφοράς στη περίπτωση κατάρρευσης του συστήματος. Τα περισσότερα εργαλεία δεν λαμβάνουν υπόψη αυτά τα αντίγραφα παρέχοντας την ευκαιρία εντοπισμού ενδεχόμενων αποδεικτικών στοιχείων κατά την έρευνα [43].

Επιπρόσθετα, κάποιες φορές ζητείται η διαγραφή προγραμμάτων ή αρχείων που παράχθηκαν από ένα πρόγραμμα μιας συγκεκριμένης έκδοσης με αποτέλεσμα παλιότερες εκδόσεις και τα αντίστοιχα αρχεία να παραμένουν στο σύστημα και να εντοπίζονται από τους ερευνητές. Ακόμα, υπάρχουν ειδικές δομές αρχείων, όπως το Master File Table του NTFS, όπου δεν μπορούν να επέμβουν αυτά τα εργαλεία, συνεπώς είναι δυνατή η επαναφορά δεδομένων [43].

Τέλος, όλα τα antiforensic εργαλεία διατηρούν πληροφορίες σχετικά με τον χρήστη και τις ρυθμίσεις του, και πιθανόν να καταγράφουν τα αρχεία που διαγράφηκαν και πότε έγινε η διαγραφή. Υπάρχουν εργαλεία που διατηρούν απλό αρχείο κειμένου ή άλλου είδους αρχεία με το πλήρες όνομα και μονοπάτι των αρχείων που επικάλυψαν για την αποφυγή του εντοπισμού τους. Επακόλουθο είναι ακόμα και οι καταγραφές των ίδιων των εργαλείων να μπορούν να αποτελέσουν πηγή πληροφοριών και αποδείξεων παρά την προσπάθεια απόκρυψή τους [43].

7.4.2 Αξιολόγηση εργαλείων

Ο πίνακας που ακολουθεί παρακάτω στηρίζεται στην forensic αξιολόγηση εργαλείων διαγραφής δεδομένων των Matthew Geiger και Lorrie Faith Cranor, από το Institute for Software Research του Carnegie Mellon University. Έξι εργαλεία anti-forensic έλαβαν μέρος στις δοκιμασίες, ο στόχος ήταν η χρήση τους για τη διαγραφή δεδομένων και στη συνέχεια το Forensic Tool Kit 1.50 θα χρησιμοποιηθεί για τον εντοπισμό δεδομένων που έχουν απομείνει [43]. Η

συγκεκριμένη αξιολόγηση πραγματοποιήθηκε τον Ιούνιο 2005, επομένως είναι αναμενόμενο κάποια από τα αποτελέσματα να έχουν αλλάξει με τη βελτίωση των εργαλείων μέχρι τώρα.

Η βαθμολογία ξεκινάει από το μηδέν (0) που υποδηλώνει αδυναμία του εργαλείου να διαγράψει πλήρως συγκεκριμένα δεδομένα, ενώ το μέγιστο είναι το τρία (3) δηλαδή πλήρη διαγραφή χωρίς ίχνη.

	Window Washer	**Windows & Internet Cleaner**	**CyberScrub**	**Evidence Eliminator**
Διαγραφή μη καταχωρημένου χώρου	0	2	3	3
Διαγραφή αρχείων χρήστη και συστήματος	1	1	2	1
Διαγραφή καταγραφών χρήσης μητρώου	2,5	2	2	2,5
Αποτροπή ανάκτησης αρχείου μητρώου από το σημείο επαναφοράς του συστήματος	0	0	3	3
Διαγραφή δεδομένων από ειδικές δομές του συστήματος αρχείων	2	2	2	2
Απόκρυψη επιλογών του εργαλείου και αρχεία καταγραφής δραστηριότητάς του	2	2	2	2
Συνολική αποτελεσματικότητα εργαλείου	**1,25**	**1,5**	**2,3**	**2,25**

Πίνακας 2: Αξιολόγησης εργαλείων anti-forensics

Τα εργαλεία διαγραφής δεδομένων κατάφεραν να παρουσιάσουν μια καλή εικόνα στις δοκιμασίες. Τα πιο αποτελεσματικά ήταν το Evidence Eliminator και το CyberScrub, ενώ με αρκετή διαφορά ακολουθούν τα άλλα δύο. Από τα αποτελέσματα του πίνακα αξιολόγησης φαίνεται ότι δεν είναι δυνατόν να διαγραφούν επιτυχώς όλα τα δεδομένα του υπολογιστικού συστήματος και αναγκαστικά θα παραμείνουν κάποια ίχνη δεδομένων που μπορεί να εντοπίσει αργότερα ένας ερευνητής. Αξιοσημείωτο είναι και το γεγονός ότι κανένα εργαλείο δεν κατάφερε να αποκρύψει πλήρως τη δραστηριότητά του με αποτέλεσμα να υπάρχει πιθανότητα να έχει αφήσει ίχνη ακόμα και για δεδομένα που έχει διαγράψει επιτυχώς.

8 Ανάλυση Forensic σε Λειτουργικά Συστήματα

Ένα λειτουργικό σύστημα αποτελεί το βασικό λογισμικό ενός υπολογιστή για τη διαχείριση και τον συντονισμό εργασιών, και παρέχει μια διεπαφή μεταξύ του υλισμικού και τον χρήστη. Τα πιο διαδεδομένα λειτουργικά συστήματα που κυκλοφορούν είναι τα Microsoft Windows, διανομές με πυρήνα Linux, όπως RedHat/Fedora, Ubuntu, Slackware, SuSE, και το Mac OS της Apple.

Ένα από τα κύρια μέρη ενός λειτουργικού συστήματος που πρέπει να μελετήσει ένας ειδικός στα forensics είναι το Σύστημα Αρχείων (File System), επηρεάζει άμεσα τον τρόπο αποθήκευσης, προσπέλασης και διαγραφής των αρχείων και μπορούν να παρέχουν σημαντικές πληροφορίες κατά τη διάρκεια μιας έρευνας. Για κάθε λειτουργικό σύστημα είναι διαφορετικό και μπορεί να διαφέρει ακόμα και σε διανομές του ίδιου λειτουργικού συστήματος.

Το σύστημα αρχείων αντιστοιχεί φυσικές τοποθεσίες ενός τομέα με λογικές διευθύνσεις. Ένας τομέας (volume) αποτελείται από ένα ή περισσότερα τμήματα (partition) ενός ή περισσότερων δίσκων, όπου δίσκος σε αυτή τη περίπτωση θα θεωρείται κάθε φυσική αποθηκευτική συσκευή. Τα πιο γνωστά εργαλεία forensic, όπως το EnCase και το FTK, αναγνωρίζουν τις βασικές δομές των διαφορετικών συστημάτων αρχείων, ωστόσο πρέπει να δοθεί μεγαλύτερη προσοχή στις ιδιαιτερότητες του καθενός.

Εκτός από το σύστημα αρχείων, ένα λειτουργικό σύστημα διαθέτει αρχεία με πολλές πληροφορίες για τα προγράμματα που είναι εγκατεστημένα, τις δραστηριότητες των χρηστών τόσο τοπικά στο ίδιο το σύστημα, όσο και διαδικτυακά. Το σημαντικό είναι να γνωρίζει ο ερευνητής ποιες είναι οι πηγές σε κάθε λειτουργικό για να μπορέσει να τις αξιοποιήσει αναλόγως.

8.1 Microsoft Windows



Εικόνα 29: Windows

Το λειτουργικό σύστημα των Windows της Microsoft είναι λογισμικό κλειστού κώδικα και είναι από τα δημοφιλέστερα λειτουργικά, καλύπτοντας περίπου το 90% της αγοράς των προσωπικών υπολογιστών. Η

γραφική διεπαφή του λειτουργικού είναι φιλική προς τον χρήστη και διευκολύνει την εκτέλεση προγραμμάτων και τη διαχείριση αρχείων. Το πρώτο λειτουργικό σύστημα Windows εμφανίστηκε το 1985 ως προσθήκη στο MS-DOS. Από τότε ακολούθησαν πολλές εκδόσεις βελτιώνοντας σημαντικά τόσο το περιβάλλον εργασίας όσο και τις δυνατότητές του. Το 2009 παρουσιάστηκε η πιο πρόσφατη διανομή, τα Windows 7, τα οποία κυκλοφορούν σε διάφορες εκδόσεις για προσωπικούς υπολογιστές [72].

8.1.1 Σύστημα Αρχείων

Η εταιρεία Microsoft έχει αναπτύξει δύο κύρια συστήματα αρχείων για το λειτουργικό σύστημα των Windows. Τα πρώτα Windows χρησιμοποιούσαν ένα αρκετά απλό σύστημα αρχείων, το FAT, το οποίο στη συνέχεια αντικαταστήθηκε από το NTFS για να καλύψει τις συνεχόμενα αυξανόμενες ανάγκες των υπολογιστικών συστημάτων.

File Allocation Table (FAT)

Το File Allocation Table (FAT), αναπτύχθηκε στις αρχές της δεκαετίας ’80 αρχικά για δισκέτες και στη συνέχεια προσαρμόστηκε στις ανάγκες των νεότερων αποθηκευτικών μέσων όπως τους σκληρούς δίσκους. Υπάρχουν τρεις εκδόσεις, το FAT12, FAT16 και FAT32, με ουσιαστική διαφορά μεταξύ τους το μέγεθος των εγγραφών, δηλαδή στο FAT12 οι εγγραφές είναι μεγέθους 12 bit, και ούτω καθεξής [13]. Πλέον, το συγκεκριμένο σύστημα αρχείων χρησιμοποιείται κυρίως σε μικρές υπολογιστικές συσκευές λόγω της σταθερότητας και της απλότητάς του [5].

Μία εγγραφή στον πίνακα FAT γίνεται με τη δημιουργία ενός αρχείου ή φακέλου, περιέχει το όνομα του αρχείου ή φακέλου, χρονικές τιμές MAC (last Modified, last Accessed, Create), αριθμό αρχικής συστάδας (cluster), δηλαδή της πρώτης μονάδας που χρησιμοποιείται για την αποθήκευσης των δεδομένων του αρχείου, το μέγεθος του αρχείου και άλλα μεταδεδομένα. Το αρχείο του πίνακα βρίσκεται στην αρχή του δίσκου για τον άμεσο εντοπισμό του και υπάρχει πάντα ένα δεύτερο αντίγραφο σε περίπτωση που μια κακόβουλη πράξη αχρηστέψει το αρχικό [52, 5, 13].

Για τον εντοπισμό ενός αρχείου το FAT υποδεικνύει την αρχική συστάδα που είναι αποθηκευμένο. Όταν το αρχείο είναι αρκετά μεγάλο και διαμοιράζεται σε περισσότερες συστάδες, το σύστημα FAT τα συνδέει με μια αλυσίδα συστάδων όπου το τέλος της μίας συστάδας υποδεικνύει την αμέσως επόμενη. Το βασικό μειονέκτημα αυτής της τεχνικής είναι ότι δεν υπήρχε τρόπος να εντοπιστεί η προηγούμενη συστάδα αλλά μόνο η επόμενη. Ωστόσο εργαλεία forensics εφοδιασμένα με κατάλληλους αλγόριθμους μπορούν να εντοπίσουν και τις προηγούμενες συστάδες [5, 2].

Κατά τη διαδικασία της διαγραφής ενός αρχείου το FAT αλλάζει στη δεκαεξαδική συμβολοσειρά E5 το πρώτο byte στην αντίστοιχη εγγραφή του πίνακα για να δηλωθεί ως αχρησιμοποίητη και οι εγγραφές για τις συστάδες μηδενίζονται [5, 2]. Τα Windows διατηρούν τη πρώτη συστάδα της αλυσίδας για να είναι δυνατή η ανάκτηση του αρχείου τουλάχιστον μέχρι να εγγραφούν νέα δεδομένα στις συστάδες [13].

Κάποιο από τα ελαττώματα του συστήματος FAT είναι ότι αφήνει αρκετό χώρο αχρησιμοποίητο σε μια συστάδα σε περιπτώσεις που το αρχείο είναι μικρότερου μεγέθους με αποτέλεσμα να μένει χώρος ανεκμετάλλευτος και να προσφέρονται μέρη για απόκρυψη άλλων δεδομένων [5]. Επιπλέον, σε κάποιες διαδικασίες, όπως αντιγραφής ή μετονομασίας, κάποια μεταδεδομένα αλλάζουν ενώ άλλα όχι, δημιουργώντας πιθανές ασυνέπειες, για παράδειγμα ο χρόνος δημιουργίας να είναι μεγαλύτερος από το χρόνο τελευταίας μετατροπής του αρχείου [13].

New Technology File System (NTFS)

Το NTFS αποτελεί το νεότερο σύστημα αρχείων της Microsoft και έχει χρησιμοποιηθεί στις τελευταίες εκδόσεις των Windows. Είναι αρκετά πιο περίπλοκο σύστημα σε σχέση με το FAT για να καλύψει νέες αλλά και μελλοντικές απαιτήσεις. Παρέχει περισσότερη ασφάλεια και σταθερότητα σε σχέση με το προηγούμενο, υποστηρίζει μεγαλύτερα ονόματα αρχείων και εκμεταλλεύεται με βέλτιστο τρόπο μεγάλο αποθηκευτικό χώρο. Δεν χρησιμοποιείται πλέον ο πίνακας κατανομής αρχείων (FAT), αλλά ο πίνακας κύριων αρχείων (Master File Table - MFT) [5, 52, 13].

Το μέγεθος των εγγραφών του MFT είναι 1KB όπου τα πρώτα 42 bytes περιέχουν τις κύριες πληροφορίες ενώ τα επόμενα χρησιμοποιούνται για την αποθήκευση άλλων χαρακτηριστικών. Η

πρώτη εγγραφή είναι για τον ίδιο τον πίνακα αφού στην ουσία αποτελεί αρχείο του συστήματος και περιέχει τη θέση που είναι αποθηκευμένος στο δίσκο [13]. Οι επόμενες εγγραφές περιέχουν τα μεταδεδομένα των αρχείων συμπεριλαμβανομένου και πληροφορίες σχετικά με τη προστασία του αρχείου. Αρχικά ο MFT ορίζει λογικούς αριθμούς συστάδων (logical cluster numbers - LCN) σε όλο το δίσκο ή κομμάτι του δίσκου (partition), και στη συνέχεια ο κάθε αριθμός συνδέεται με ένα εικονικό αριθμό συστάδας για να δίνεται η δυνατότητα επέκτασης του αρχείου πέρα από τον ελεύθερο χώρο του δίσκου. Οι αριθμοί αυτοί βοηθάνε το λειτουργικό σύστημα να διαβάσει και να γράψει δεδομένα στο δίσκο [52].

Όταν γίνεται εισαγωγή νέων αρχείων, το MFT εκμεταλλεύεται τις αχρησιμοποίητες εγγραφές διαγραμμένων αρχείων πρώτα και μετά προσθέτει νέες εφόσον χρειαστεί. Άμεση συνέπεια είναι η δυσκολία ανάκτησης παλιότερων δεδομένων επειδή αντικαθιστούνται γρήγορα. Επιπλέον, ο κατάλογος εγγραφών του MFT είναι ταξινομημένος με βάση το όνομα, οπότε με κάθε διαγραφή πραγματοποιείται μια διαδικασία ταξινόμησης όπου χαμηλότερες εγγραφές καλύπτουν τις διαγραμμένες και χάνεται η σύνδεση των ονομάτων των αρχείων με τα δεδομένα στο δίσκο [2].

Κατά τη διαδικασία όμως της διαγραφής ο χρήστης μεταφέρει το αρχείο στο φάκελο του κάδου ανακύκλωσης από τη γραφική διεπαφή των Windows. Το αρχείο αλλάζει όνομα και γίνεται μια εγγραφή στο αρχείο Info2 το οποίο περιέχει κάποια από τα μεταδεδομένα του αρχείου, όπως το μονοπάτι και χρονικές σημάνσεις. Αρκετά εργαλεία forensic έχουν τη δυνατότητα να ανακτούν τις πληροφορίες του Info2 και να εντοπίζουν την προέλευση διαγραμμένων αρχείων ειδικά αν συνδέονται με εξωτερικά μέσα αποθήκευσης [5].

Ακόμα, η δυναμική αύξηση του μεγέθους του MFT παραχωρεί ένα επιπλέον τρόπο απόκρυψης δεδομένων. Ο χρήστης μπορεί να δημιουργήσει νέα αρχεία για να προστεθούν νέες εγγραφές στο πίνακα και στη συνέχεια να τα διαγράψει οπότε μένουν ελεύθερες οι εγγραφές. Με αυτό τον τρόπο μπορεί να προσθέσει δεδομένα που θέλει να κρύψει στο χώρο του πίνακα που δεν χρησιμοποιείται πλέον, αν και υπάρχει ο κίνδυνος να επικαλυφθούν από άλλες δραστηριότητες του συστήματος [13].

Μία άλλη ιδιότητα του νέου συστήματος είναι ο καθορισμός αδειών πρόσβασης στους χρήστες ή ομάδες χρηστών για κάθε αρχείο και φάκελο καθώς και το επίπεδο πρόσβασης είτε από τον τοπικό υπολογιστή ή μέσω κάποιου δικτύου [52]. Η λίστα ελέγχου πρόσβασης (access control

list - ACL) καταγράφει τα δικαιώματα ανάγνωσης, εγγραφής και εκτέλεσης των αρχείων και φακέλων, ενώ το αρχείο $Secure αποθηκεύει λεπτομερής πληροφορίες ιδιοκτησίας και πρόσβασης. Τα αρχεία αυτά βοηθάνε τον ερευνητή να προσδιορίσει ποιοι χρήστες είχαν πρόσβαση σε ποια δεδομένα [3].

Επιπρόσθετα, για τη παροχή καλύτερης ασφάλειας αναπτύχθηκε το κρυπτογραφημένο σύστημα αρχείων (encrypting file system - EFS) το οποίο συνδυάζει συμμετρική κρυπτογράφηση με τεχνολογίες δημοσίου κλειδιού έτσι ώστε μόνο οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση σε αρχεία και φακέλους [52]. Το σύστημα κρυπτογράφησης συσχετίζει το κλειδί κρυπτογράφησης με πληροφορίες από το λογαριασμό του χρήστη για να γίνεται η διαδικασία κρυπτογράφησης ή αποκρυπτογράφησης στο επίπεδο συστήματος [5].

Ως συμπληρωματικό στη λειτουργία του EFS, στα Windows Vista εμφανίστηκε για πρώτη φορά το BitLocker το οποίο σε αντίθεση με το EFS δεν κρυπτογραφεί αρχεία αλλά ολόκληρους αποθηκευτικούς τομείς (volumes). Είναι σχεδιασμένο να λειτουργεί με ένα μικροεπεξεργαστή, το Trusted Platoform Module (TPM) το οποίο αποθηκεύει τα κλειδιά κρυπτογράφησης Full Volume Encryption Keys (FVEK) και τα αποδεσμεύει όταν επαληθευτεί η ακεραιότητα των δεδομένων εκκίνησης. Στη περίπτωση που ο ερευνητής δεν εντοπίσει το BitLocker τότε δεν θα μπορέσει να αποκτήσει πρόσβαση στα δεδομένα από το εικονικό αντίγραφο που θα έχει δημιουργήσει. Για να αποφευχθεί αυτό πρέπει να ελεγχθεί το τμήμα εκκίνησης του τόμου το οποίο υποδεικνύει αν είναι κρυπτογραφημένος ο τομέας ή όχι [3].

Οι εναλλακτικές ροές δεδομένων (Alternate Data Streams - ADS) είναι ένα σημαντικό στοιχείο που πρέπει να λαμβάνεται υπόψη κατά τη διάρκεια μιας έρευνας. Το σύστημα NTFS επιτρέπει σε ένα αρχείο, εκτός από τη βασική ανώνυμη ροή, να σχετίζεται και με άλλες διαφορετικές ροές δεδομένων, δηλαδή διαφορετική σειρά bytes. Με αυτό τον τρόπο οι εφαρμογές μπορούν να δημιουργήσουν μια ροή δεδομένων με κάποιο όνομα για ένα αρχείο και να χρησιμοποιούν αυτό το όνομα για να αποκτήσουν πρόσβαση. Ο αρχικός λόγος δημιουργίας τους ήταν για ύπαρξη συμβατότητας με τα συστήματα Macintosh. Οι ADS δεν είναι ορατές στο σύστημα αρχείων και έχουν τη δυνατότητα να κρύψουν άλλα δεδομένα εν γνώση του χρήστη ή όχι [52, 5].

Ένα ακόμα νέο χαρακτηριστικό του NTFS σε σχέση με το FAT είναι η καταγραφή κάθε ενέργειας του συστήματος αρχείων στο αρχείο $Logfile για τη γρήγορη διόρθωση μετά από

βλάβη. Σε αυτό το αρχείο καταγράφεται κάθε αλλαγή στα μεταδεδομένα που σχετίζονται με τα αρχεία, όχι όμως στα δεδομένα τους. Το συγκεκριμένο αρχείο μπορεί να περιέχει κρίσιμες πληροφορίες για έναν ερευνητή forensics σχετικά με τις δραστηριότητες του χρήστη και τη κατάσταση του συστήματος [2, 5, 13].

8.1.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών

Από τις πρώτες πηγές που πρέπει να ελεγχθούν σε μια έρευνα είναι το μητρώο των Windows (Windows Registry). Είναι η βάση που περιέχει όλες τις ρυθμίσεις για λογισμικό και υλισμικό, προτιμήσεις των χρηστών, αρχικές ρυθμίσεις συστήματος καθώς και πληροφορίες για κωδικούς πρόσβασης. Επιπλέον, ένας ερευνητής μπορεί να βρει πληροφορίες σχετικά με ασύρματες συνδέσεις, ιστορικό από περιήγηση στο διαδίκτυο ή και για μη αναγνωσμένα ηλεκτρονικά μηνύματα αλληλογραφίας [52, 5].

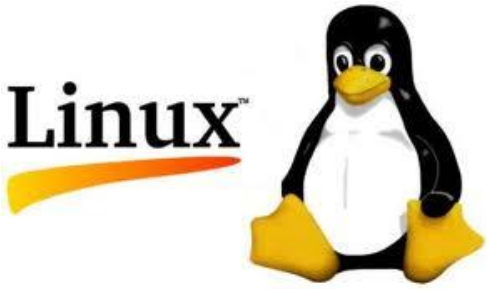
Πηγές πληροφοριών αποτελούν και τα αρχεία καταγραφής γεγονότων των Windows τα οποία περιέχουν δραστηριότητες του χρήστη και του συστήματος. Για παράδειγμα, στα Windows XP το αρχείο AppEvent.evt σχετίζεται με το λογισμικό που είναι εγκατεστημένο, το SecEvent.evt έχει πληροφορίες σχετικά με θέματα ασφάλειας και πρόσβασης σε δεδομένα, και Internet.evt καταγράφει στοιχεία σχετικά με το διαδίκτυο. Οι πληροφορίες αυτές είναι χρήσιμες σε μια έρευνα επειδή μπορεί να προσδιοριστεί η αιτία ενός συμβάντος καθώς και ονόματα χρηστών που είχαν συνδεθεί, IP διευθύνσεις και άλλα [3].

Επίσης, οι δραστηριότητες του χρήστη σε ένα υπολογιστικό σύστημα προκαλούν την εκτέλεση ενεργειών εν αγνοία του. Από κάποιες ενέργειες καταγράφονται πληροφορίες οι οποίες είναι χρήσιμες για έναν ερευνητή. Για παράδειγμα, η δημιουργία και διαγραφή λογαριασμών χρηστών καταγράφεται σε αρχεία που μπορούν αργότερα να παρέχουν σημαντικές πληροφορίες. Επιπρόσθετα, καταγράφεται η είσοδος του χρήστη στο λειτουργικό σύστημα, πότε έγινε και με ποιο τρόπο, για να εντοπιστούν οι υπεύθυνοι μιας δράσης ή τυχόν παράνομης πρόσβασης. Ακόμα και η εμφάνιση προειδοποιητικών μηνυμάτων αποθηκεύεται και ίσως υποδεικνύει πιθανές παράνομες ενέργειες [3].

Τέλος, τα προγράμματα που είναι εγκατεστημένα στο σύστημα και πληροφορίες όπως ημερομηνία εγκατάστασης αποτελούν στοιχεία μιας έρευνας. Σχεδόν όλα τα προγράμματα βρίσκονται στον φάκελο Program Files, αλλά μπορεί κάποιες πληροφορίες ή ακόμα και άλλα προγράμματα να βρίσκονται στο προφίλ του χρήστη. Συνήθως κατά τη διαγραφή ενός προγράμματος τα δεδομένα που είναι στο προφίλ του χρήστη παραμένουν και αποτελούν στοιχεία για την ύπαρξή του. Ωστόσο, ένα πρόγραμμα μπορεί να έχει εγκατασταθεί από άλλο χρήστη και να έχει επιλεχθεί εγκατάσταση σε όλους τους χρήστες, οπότε η κάθε πληροφορία θα πρέπει να ελέγχεται [3].

8.2 Linux

Το λειτουργικό σύστημα Linux είναι ένα ελεύθερο λογισμικό τύπου Unix. Κυκλοφορούν διάφορες διανομές, κάποιες από τις οποίες παρέχουν ένα φιλικό περιβάλλον εργασίας για τις συχνές δραστηριότητες ενός κοινού χρήστη, ενώ άλλες διανομές είναι πιο εξειδικευμένες για τη κάλυψη λειτουργιών όπως συστημάτων ανίχνευσης εισβολών. Είναι λογισμικό ανοιχτού κώδικα επομένως ο χρήστης έχει πρόσβαση σε όλα τα αρχεία του συστήματος και δικαιώματα μετατροπής τους με βάσης τις ανάγκες του [3].



Εικόνα 30: Linux

8.2.1 Σύστημα αρχείων

Σε αρκετές διανομές Linux τα συνηθέστερα συστήματα αρχείων είναι το δεύτερο και τρίτο επεκταμένο σύστημα αρχείων (second and third extended filesystem), το Ext2 και το μεταγενέστερο Ext3, τα οποία βασίζονται στο σύστημα αρχείων των Unix (UNIX File System - UFS). Άλλα γνωστά συστήματα είναι το ReiserFS, XFS και το JFS, αλλά θα περιγραφούν τα Ext2-3 καθώς αποτελούν τα πιο δημοφιλή στην κοινότητα των Linux.

Second and Third Extended File System (Ext2 – Ext3)

Τα περισσότερα τωρινά συστήματα Linux χρησιμοποιούν το σύστημα αρχείων Ext3 το οποίο είναι απόγονος του Ext2. Διατηρεί τα βασικά χαρακτηριστικά του προηγούμενου αλλά επιπλέον διαθέτει τη δυνατότητα καταγραφής ημερήσιας δραστηριότητας (journaling) για την γρηγορότερη ανάκαμψη του συστήματος μετά από εμφάνιση βλάβης, ωστόσο μπορεί να αναγνωριστεί από το υπολογιστικό σύστημα ως Ext2 με χρήση κατάλληλης εντολής [13].

Το σύστημα αρχείων ξεκινάει με μια προαιρετικά διατηρημένη περιοχή και το υπόλοιπο διαχωρίζεται σε τμήματα που ονομάζονται σύνολα ομάδων (block groups). Όλα τα σύνολα ομάδων εκτός από το τελευταίο περιέχουν τον ίδιο αριθμό ομάδων και χρησιμοποιούνται για την αποθήκευση ονομάτων αρχείων, μεταδεδομένων και περιεχόμενο των αρχείων. Βασικές πληροφορίες σχετικά με τη δομή του δίσκου είναι αποθηκευμένες σε μια δομή δεδομένων υπερ-ομάδας (superblock) στην αρχή του συστήματος αρχείων, ενώ το περιεχόμενο των αρχείων είναι αποθηκευμένο σε ομάδες (blocks), δηλαδή σύνολα διαδοχικών τομέων [13, 3].

Τα μεταδεδομένα των αρχείων και ευρετηρίων, όπως τον αριθμό bytes του αρχείου, χρονικές σημάνσεις, τον αριθμό των blocks που καταλαμβάνει καθώς και αναγνωριστικούς αριθμούς των χρηστών ή ομάδων, είναι αποθηκευμένα σε κόμβους του πίνακα περιεχομένων (index nodes), για συντομία θα αναφέρονται ως inodes [13, 3]. Το superblock διαχειρίζεται το σύστημα αρχείων με το να παρακολουθεί τα inodes και τις καταστάσεις όλων των blocks της αποθηκευτικής συσκευής [5].

Άλλα βασικά στοιχεία του συστήματος είναι η ομάδα εκκίνησης (Boot block) που περιέχει τη τοποθεσία του κώδικα εκκίνησης του συστήματος και η ομάδα δεδομένων (Data block) η οποία περιέχει τις λογικές διευθύνσεις στις οποίες είναι αποθηκευμένα τα δεδομένα στην συσκευή. Ακόμα, το Bad Block Inode (BBI) παρακολουθεί βλαβερές ή κατεστραμμένες περιοχές τις αποθηκευτικής συσκευής και τις καταγράφει. Το BBI μπορεί να μετατραπεί ώστε να περιέχει και καλές περιοχές οπότε κάποιος που θέλει να κρύψει δεδομένα σε μια περιοχή μπορεί να την παρουσιάσει ως κατεστραμμένη [5].

Κατά τη διαγραφή ενός αρχείου τα συστήματα Ext2 και Ext3 ενεργούν διαφορετικά. Το Ext3 μηδενίζει το μέγεθος του αρχείου και διαγράφει τους δείκτες στα inodes και στις άλλες ομάδες δεδομένων, ενώ το Ext2 δεν διαγράφει τις τιμές των inodes κάνοντας πιο εύκολη την

επανάκτηση των αρχείων. Και στα δύο συστήματα οι χρονικές σημάνσεις αλλάζουν ώστε να δείχνουν τη στιγμή της διαγραφής. Ουσιαστικά, με τη διαγραφή αποκρύπτεται η καταχώρηση του αρχείου και το σύστημα ορίζει τη σχετική inode διαθέσιμη για χρήση. Τα δεδομένα του αρχείου και οι αντίστοιχες καταχωρήσεις παραμένουν στο δίσκο μέχρι να καλυφθούν από νέα δεδομένα. Για την ανάκτηση διαγραμμένων αρχείων ο πιο αποτελεσματικός τρόπος είναι η εξέταση των διαγραμμένων inodes καθώς περιέχουν χρήσιμα μεταδεδομένα όπως ημερομηνίες, χαρακτηριστικά και τοποθεσίες των δεδομένων στο δίσκο [3, 13, 2].

Άλλο σημαντικό χαρακτηριστικό είναι οι άδειες χρήσης των αρχείων (file permissions) καθώς δίνουν τη δυνατότητα στον ερευνητή να εξακριβώσει ποιος έχει πρόσβαση και ποιος όχι σε κάποιο αρχείο και τι δικαιώματα έχει στο αρχείο. Επιπλέον, συνήθως τα συστήματα Linux αποθηκεύουν αρχεία παρόμοιων τύπων στην ίδια περιοχή του δίσκου. Αυτό το χαρακτηριστικό ευνοεί την αναζήτηση διαγραμμένων αρχείων με το περιορισμό της σε συγκεκριμένες περιοχές [3].

8.2.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών

Τα συστήματα Linux έχουν πολλά αρχεία καταγραφής με πληροφορίες για συνδέσεις και αποσυνδέσεις χρηστών από το σύστημα καθώς και για γεγονότα που έχουν συμβεί κατά τη διάρκεια μιας σύνδεσης. Κάθε εφαρμογή αφήνει ίχνη στο σύστημα μέσω προσωρινών αρχείων ή στο χώρο swap. Ανάμεσα στα αρχεία που πρέπει να ερευνούνται είναι το etc/passwd επειδή περιέχει όλους τους χρήστες του συστήματος και πληροφορίες σχετικά με το μονοπάτι του προσωπικού τους ευρετηρίου [2, 3].

Επιπλέον, γίνεται καταγραφή δικτυακών κινήσεων του συστήματος, όπως συνδέσεις με εξυπηρετητές και ασύρματες συνδέσεις (WiFi). Διατηρούνται αρχεία και με το ιστορικό εκτέλεσης εντολών από τους χρήστες, τα οποία είναι απαραίτητα για τον εντοπισμό μη θεμιτών πράξεων στο σύστημα από κάποιο χρήστη ή παράνομη πρόσβαση και εκτέλεση ενεργειών από εισβολείς. Ιδιαίτερη προσοχή απαιτείται στις προγραμματισμένες ενέργειες (scheduled tasks) και στα ανάλογα αρχεία συστήματος επειδή είναι πιθανό να περιέχουν κάποιου είδους παγίδας από το χρήστη για την απόκρυψη ή καταστροφή δεδομένων [3].

Το περιβάλλον εργασίας κάποιων εκδόσεων Linux, όπως το Gnome, και εφαρμογές όπως το OpenOffice, διατηρούν λίστες των πρόσφατα χρησιμοποιημένων αρχείων. Ακόμα, κατά τη διαδικασία της εκτύπωσης δημιουργούνται αρχεία με τα περιεχόμενα και τα μεταδεδομένα του αρχείου που πρόκειται να εκτυπωθεί. Επίσης, πολλά προγράμματα προσφέρονται για διαδικτυακή δραστηριότητα είτε με κάποιο γραφικό περιβάλλον εργασίας είτε μέσω της γραμμής εντολών, και παρέχουν πληροφορίες για παράδειγμα από το ιστορικό περιήγησης, τα cookies, την ηλεκτρονική αλληλογραφία και άλλα [3].

8.3 Mac OS



Εικόνα 31: Mac OS

Το λειτουργικό σύστημα Mac OS αναπτύχθηκε από την Apple για υπολογιστικά συστήματα τύπου Macintosh. Το πρώτο λειτουργικό εμφανίστηκε το 1984 παρόλο που τότε ήταν γνωστό ως λογισμικό του Συστήματος. Η πιο πρόσφατη διανομή είναι το Mac OS X, αποτελεί ένα Unix λειτουργικό σύστημα βασισμένο στο NeXTSTEP και στο πυρήνα Mach, και κυκλοφορούν εκδόσεις για προσωπικούς υπολογιστές και εξυπηρετητές. Το γραφικό περιβάλλον του χρήστη είναι στο ύφος της Apple, ωστόσο οι λειτουργίες και εντολές είναι αυτές ενός Unix συστήματος, οπότε είναι απαραίτητο ο ερευνητής forensics να έχει γνώσεις για τέτοια συστήματα [51].

8.3.1 Σύστημα Αρχείων

Το πρώτο σύστημα αρχείων της Apple ήταν το Macintosh File System (MFS) το 1984 για δισκέτες, το οποίο σύντομα αντικαταστήθηκε από το Ιεραρχικό Σύστημα Αρχείων (Hierarchical File System - HFS) για τη διαχείριση αποθηκευτικών μέσων μεγάλου μεγέθους. Το τελευταίο σύστημα αρχείων είναι το HFS Plus (HFS+), μια βελτιωμένη έκδοση του HFS.

Hierarchical File System (HFS)

Η Apple ανέπτυξε το Ιεραρχικό Σύστημα Αρχείων (Hierarchical File System - HFS) για τη διαχείριση αρχείων σε δισκέτες, σκληρούς δίσκους καθώς και σε CDs. Ένα από τα κύρια χαρακτηριστικά του είναι ο διαχωρισμός των δεδομένων και των μεταδεδομένων ενός αρχείου. Για τον εντοπισμό όλων των αρχείων και των φακέλων ενός τομέα χρησιμοποιεί ένα κατάλογο αρχείων [5].

Ο κατάλογος αυτός διατηρεί διάφορα ήδη δεδομένων με σημαντικότερο τη καταχώρηση του αρχείου. Οι πληροφορίες που βρίσκονται στη περιοχή καταχώρησης του αρχείου είναι ένας μοναδικός αριθμός αναγνώρισης CNID (catalog node identification), το μέγεθος του αρχείου, χρόνοι δημιουργίας, μετατροπής και αποθήκευσης, ο χώρος που το πρώτο κομμάτι του αρχείου είναι αποθηκευμένο στο τομέα και δείκτες για τους χώρους που είναι τα μεταδεδομένα [5].

Τα κύρια αρχεία του HFS είναι τα Catalog και Extents Overflow. Το πρώτο περιέχει εγγραφές για κάθε αρχείο και φάκελο του συστήματος με τα χαρακτηριστικά τους όπως χρονικές σημάνσεις. Οι εγγραφές αυτές έχουν ένα μοναδικό αριθμό, το αναγνωριστικό κόμβων καταλόγου (catalog node ID - CNID), και είναι αποθηκευμένες σε ένα ισορροπημένο δέντρο (B-tree) το οποίο ευνοεί την αποτελεσματική αναζήτηση. Υπάρχουν τέσσερα ήδη εγγραφών, οι φάκελοι, τα αρχεία, τα νήματα αρχείων και τα νήματα φακέλων (file and folder threads). Το HFS χρησιμοποιεί τα νήματα αρχείων και φακέλων για να συνδέει τα ονόματα με τις αντίστοιχες εγγραφές αρχείων ή φακέλων χρησιμοποιώντας το μοναδικό CNID [2].

Ακόμα, οι εγγραφές των νημάτων περιέχουν αναφορές στους φάκελους γονέων (parent folders) που χρησιμοποιούνται για τη δόμηση της ιεραρχίας του συστήματος αρχείων. Τα αρχεία σε ένα τομέα HFS έχουν δύο διχάλες, μία διχάλα δεδομένων (data fork) που αποθηκεύεται το περιεχόμενο του αρχείου και μια διχάλα πόρων (resource fork) με ιδιαίτερη δομή δεδομένων για πληροφορίες όπως εικονίδια και μενού. Οι πρώτες οχτώ συστάδες κάθε περιοχής είναι απαριθμημένες σε κάθε εγγραφή αρχείου στο Catalog, οποιεσδήποτε επιπλέον περιοχές (extents) αποθηκεύονται στο αρχείο Extents Overflow [2].

Όταν ένα αρχείο διαγράφεται, μεταφέρεται στο φάκελο απορριμμάτων (trash folder) αλλά δεν σημειώνεται ως διαγραμμένο παρά μόνο όταν αδειάσει ο συγκεκριμένος φάκελος. Τα δεδομένα παραμένουν στο δίσκο μέχρι να καλυφθούν από νέα. Ένα αρχείο δηλώνεται διαγραμμένο όταν η

σχετική τιμή μεγέθους στη βάση του Catalog σημειωθεί ως μηδέν. Επιπλέον, η εγγραφή στο Catalog διαγράφεται με την απομάκρυνση κάθε αναφοράς στα δεδομένα του δίσκου [2, 51].

Η ανάκτηση διαγραμμένων αρχείων σε ένα σύστημα HFS είναι αρκετά δύσκολη επειδή οι κόμβοι σε αρχείο Catalog επανεγγράφονται αρκετά συχνά κυρίως εξαιτίας της διατήρησης της δομής B-tree του αρχείου. Κάποιες βασικές τεχνικές ανάκτησης δεδομένων μπορούν να χρησιμοποιηθούν αλλά μόνο για την απόκτηση των περιεχομένων ενός αρχείου [3].

Hierarchical File System Plus (HFS+)

Το νεότερο σύστημα αρχείων της Apple είναι το HFS+ το οποίο παρέχει αρκετές νέες βελτιώσεις σε σχέση με το HFS, όπως τη χρήση του προτύπου Unicode για τα ονόματα αρχείων και υποστηρίζει πολλαπλές διχάλες δεδομένων (data forks) ανά αρχείο. Από τα πιο βασικά αρχεία του HFS+ συστήματος είναι το αρχείο καταλόγου (catalog file), περιγράφει την ιεραρχία των φακέλων και αρχείων σε ένα τομέα και περιέχει μεταδεδομένα για όλα τα αρχεία, όπως σημάνσεις χρόνου, αναγνωριστικό του αρχείου και πληροφορίες του χρήστη [51].

Για την ανάκτηση διαγραμμένων αρχείων είναι απαραίτητες η διχάλα δεδομένων (data fork) και οι διχάλες πόρων (resource forks). Η πρώτη περιέχει πληροφορίες σχετικά με τη τοποθεσία που είναι αποθηκευμένο το περιεχόμενο του αρχείου και το μέγεθός του, ενώ οι δεύτερες παρέχουν πληροφορίες σχετικά με τους πόρους και τα μεταδεδομένα εφαρμογών [51].

8.3.2 Πληροφορίες από δραστηριότητες χρηστών και εφαρμογών

Το λειτουργικό Mac OS X περιέχει αρκετές εφαρμογές που μπορούν να παρέχουν σε ένας ερευνητή πληροφορίες σχετικά με τις δραστηριότητες του χρήστη. Κάποιες από αυτές είναι το Apple Mail, διαχειρίζεται την ηλεκτρονική αλληλογραφία, το Safari, περιηγητής στο διαδίκτυο, και το iChat για την αποστολή και λήψη άμεσων μηνυμάτων. Μια άλλη πηγή πληροφοριών είναι το τερματικό, ή αλλιώς ονομαζόμενο γραμμή εντολών, όπου εκτελούνται εντολές Unix και διατηρούνται αρχεία ιστορικού που περιέχουν τις τελευταίες εντολές του χρήστη [51].

Επιπρόσθετα, διατηρούνται λίστες με τις πρόσφατα χρησιμοποιημένες εφαρμογές και αρχεία για την εύκολη πρόσβαση στα πιο συχνά χρησιμοποιημένα στοιχεία. Όσο αφορά τη δικτυακή δραστηριότητα, οι παλιότερες εκδόσεις δεν ήταν κατάλληλα σχεδιασμένες για συνδέσεις στο διαδίκτυο και δεν διατηρούσαν αρχεία καταγραφών. Οι νέες όμως εκδόσεις όπως το MacOS 9 και το MacOS X παρέχουν αρχεία τα οποία καταγράφουν τη διαδικτυακή δραστηριότητα και την ηλεκτρονική αλληλογραφία που έχει σταλθεί ή παραληφθεί. Ανάμεσα στις πληροφορίες που περιέχουν είναι το ιστορικό περιήγησης σε ιστοσελίδες και σύνδεσης σε πρόσφατους εξυπηρετητές [2].

Ο κώδικας και τα απαραίτητα αρχεία ενός προγράμματος βρίσκονται όλα μαζί σε ένα φάκελο επιτρέποντας με αυτό τον τρόπο την εύκολη εγκατάστασή τους και απεγκατάσταση, αλλά και τον γρήγορο εντοπισμό χρήσιμων αρχείων. Οι περισσότερες διαδικασίες καταγράφονται σε αρχεία αλλά κάποια από αυτά διατηρούνται για περιορισμένο χρονικό διάστημα ή καταλαμβάνουν μέχρι κάποιο συγκεκριμένο χώρο στο δίσκο. Άλλες πληροφορίες για τους χρήστες προέρχονται από τη βάση δεδομένων των χρηστών, από τα αρχεία του προσωπικού τους λογαριασμού και από άλλα δεδομένα στο δίσκο [3].

9 Νομικά Ζητήματα

Η εξάπλωση των ηλεκτρονικών εγκλημάτων έχει οδηγήσει στη θέσπιση νέων νόμων αλλά και την προσαρμογή παλαιοτέρων για την καταπολέμησή τους. Οι νόμοι αυτοί έχουν σκοπό την πλαισίωση μιας νόμιμης έρευνας και απόκτησης αποδεικτικών στοιχείων καθώς και τη προστασία των πολιτών και της ιδιωτικότητάς τους από παράνομες πράξεις αλλά και από παραβιάσεις των δικαιωμάτων τους κατά τη διάρκεια των ερευνών.

Όμως, η νομική αντιμετώπιση των ηλεκτρονικών εγκλημάτων και γενικά παράνομων δραστηριοτήτων συναντά πολλά εμπόδια και δυσκολίες λόγω του ιδιαίτερου χαρακτήρα τους. Η εξάλειψη των συνόρων μέσω του διαδικτύου ευνοεί την εκτέλεση εγκλημάτων σχεδόν οπουδήποτε. Επιπλέον, με τη διαφορετική νομοθεσία που έχει θεσπίσει κάθε χώρα για την νομική αντιμετώπιση τέτοιου είδους εγκλημάτων είναι πολύ δύσκολο να ασκηθεί μια κοινή πολιτική στον τρόπο δίωξή τους [2].

9.1 Προστασία Ιδιωτικότητας

Η προστασία της ιδιωτικής ζωής αποτελεί αναφαίρετο δικαίωμα κάθε ανθρώπου. Αφορά τη δυνατότητα διατήρησης της ανωνυμίας του, τη προστασία των προσωπικών και ευαίσθητων δεδομένων του, αλλά και τη προστασία του ατόμου από ανεπιθύμητες επαφές και παράνομες εισβολές στη καθημερινή του ζωή με οποιοδήποτε τρόπο [2].

Ωστόσο, η επεξεργασία προσωπικών δεδομένων ενός ατόμου είναι αδύνατον να αποφευχθεί. Η ένταξη ενός ατόμου στη κοινωνία απαιτεί τη διεκπεραίωση διαδικασιών από διάφορες υπηρεσίες δημόσιες, υγείας, ασφάλισης, οι οποίες καταγράφουν και επεξεργάζονται συνεχώς προσωπικές πληροφορίες των πολιτών. Με την επέκτασή τους κιόλας στο διαδίκτυο παρέχονται νέες υπηρεσίες και διευκολύνσεις με αντάλλαγμα τη δημιουργία προφίλ των χρηστών και τη παρακολούθηση των κινήσεών τους [41].

Παρότι πολλοί χρήστες θεωρούν ότι μέσω της χρήσης του διαδικτύου διατηρούν την ανωνυμία τους, με κάθε τους ενέργεια καταγράφονται πληροφορίες στον υπολογιστή τους αλλά και σε περιοχές άλλων, για παράδειγμα στους εξυπηρετητές που συνδέονται. Επίσης, οι πάροχοι

υπηρεσιών διαδικτύου αποθηκεύουν πληροφορίες σχετικά με τη σύνδεση των χρηστών και τις διατηρούν για όσο χρόνο επιβάλλεται από το νόμο.

Η διατήρηση προσωπικών δεδομένων από διάφορους φορείς είναι απαραίτητη για τη πιθανή χρησιμοποίηση τους ως πηγές αποδεικτικών στοιχείων σε μια ψηφιακή έρευνα. Η χρήση τεχνικών Forensics κρίνεται αναγκαία αν και παραβιάζει την ιδιωτική ζωή του υπόπτου, αλλά μπορεί να έχει και ως παράπλευρη απώλεια την ιδιωτικότητα άλλων ανθρώπων. Πληροφορίες όπως οι επαφές ενός χρήστη, συχνές ιστοσελίδες που επισκέπτεται που μπορεί να υποδεικνύουν το τρόπο ζωής και τις προτιμήσεις του, μέχρι και η ηλεκτρονική του αλληλογραφία μπορεί να γνωστοποιηθούν κατά τη διάρκεια μιας έρευνας [41].

Μια από τις πιο αμφιλεγόμενες περιπτώσεις καταπάτησης ιδιωτικότητας είναι η παρακολούθηση μιας μετάδοσης επικοινωνίας του υπόπτου, κατά τη διάρκεια της οποίας είναι πολύ πιθανή η καταγραφή πληροφοριών που δεν σχετίζονται με την υπόθεση της έρευνας και μπορεί να αποτελούν προσωπικές πληροφορίες άλλων ατόμων [2]. Τα δεδομένα που συλλέγονται διακρίνονται σε αυτά που έχουν αναχαιτισθεί ή όχι, αλλιώς αν είναι πρόσφατα ή παλιότερα δεδομένα. Για τον περιορισμό της καταπάτησης συνήθως πραγματοποιείται κατάσχεση αποθηκευμένων επικοινωνιών παρά η άμεση παρακολούθηση [2, 21].

Παρόλα αυτά η παρακολούθηση χρησιμοποιείται ευρέως με το πρόσχημα της αντιμετώπισης της τρομοκρατίας και καθημερινά συλλέγονται κάθε ειδών δεδομένα από πολλούς ανυποψίαστους πολίτες. Για παράδειγμα στην Αμερική εφαρμόζεται το Total Information Awareness (TIA), ή αλλιώς γνωστό ως Terrorism Information Awareness, το οποίο δημιουργεί προφίλ ατόμων με τεχνικές εξόρυξης δεδομένων από βάσεις δεδομένων του δημόσιου και ιδιωτικού τομέα για τη πιθανή αναγνώριση τρομοκρατών και τον εντοπισμό τρομοκρατικών ενεργειών [2, 41].

Με βάση τα παραπάνω, η θέσπιση νόμων για την προστασία των προσωπικών δεδομένων των πολιτών και την οριοθέτηση των δικαιωμάτων και υποχρεώσεων των ατόμων επιβολής νόμου είναι απαραίτητη για τη διαφύλαξη των βασικών δικαιωμάτων. Ωστόσο, η κάθε χώρα ορίζει τους δικούς της νόμους για την προστασία των πολιτών της οι οποίοι μπορεί να διαφέρουν αρκετά και να εμποδίζουν μια κοινή διεθνή αντιμετώπιση ενός εγκλήματος. Για την αντιμετώπιση αυτού το προβλήματος οι Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) και η Ευρωπαϊκή

Ένωση (ΕΕ) δημιούργησαν κοινά νομικά πλαίσια για τα μέλη τους τα οποία θα αναλυθούν στη συνέχεια.

9.1.1 Νομικό Πλαίσιο στις Η.Π.Α.

Στην Αμερική, η ιδιωτικότητα των πολιτών προστατεύεται με το Fourth Amendment με βάση το οποίο απαγορεύεται η χωρίς λόγο έρευνα και κατάσχεση οπουδήποτε είδους προσωπικών στοιχείων. Για να είναι νόμιμη μια έρευνα πρέπει να ακολουθούνται αυστηρές διαδικασίες, όπως η έκδοση κατάλληλου εντάλματος έρευνας, το οποίο περιγράφει τη πιθανή αιτία, ή να επικρατούν ειδικές συνθήκες για την άμεση διεξαγωγή της [2, 41].

Για να μπορέσει ένα άτομο να ισχυριστεί ότι έχει παραβιαστεί παράνομα η ιδιωτική του ζωή πρέπει να έχει προβεί στις κατάλληλες ενέργειες που υποδηλώνουν προσπάθεια προστασίας προσωπικών δεδομένων και να κριθεί εύλογη η προσδοκία ιδιωτικότητας που επικαλείται [2]. Ωστόσο, οι περιορισμοί ισχύουν μόνο για άτομα επιβολής νόμου και όχι για ιδιώτες εφόσον δεν ενεργούν εκ μέρους του κράτους ή κρατικής υπηρεσίας [4].

Σε κάποιες συγκεκριμένες καταστάσεις όμως που δεν υπάρχουν εύλογες προσδοκίες ιδιωτικότητας θεωρείται ότι δεν έχει γίνει παραβίαση [4]. Για παράδειγμα η εικόνα στην οθόνη του υπολογιστή, τα δεδομένα που στέλνονται από ένα δημόσιο δίκτυο ή είναι αποθηκευμένα σε ένα υπολογιστή που έχουν πολλά άτομα πρόσβαση χωρίς κάποιο κωδικό δεν θεωρείται ότι προστατεύονται με αποτέλεσμα νομικά να μην υπάρχει παραβίαση [33].

9.1.2 Νομικό Πλαίσιο στην Ε.Ε και Ελλάδα

Στην Ευρωπαϊκή Ένωση ισχύει το άρθρο 8 της Ευρωπαϊκής Συνθήκης και το άρθρο 7 των Θεμελιωδών Δικαιωμάτων για τη προστασία της ατομικής ιδιωτικότητας των πολιτών της ΕΕ. Σύμφωνα με αυτά τα άρθρα ο καθένας έχει δικαίωμα στο σεβασμό της ιδιωτικής του και οικογενειακής του ζωής, κατοικίας και επικοινωνίας. Η αρχή της αναλογικότητας είναι η βάση στην οποία στηρίζονται οι ευρωπαϊκοί νόμοι, δηλαδή τα μέτρα που θα ληφθούν πρέπει να είναι

κατάλληλα για την επίτευξη του στόχου τους και οι αρνητικές συνέπειες της παρέμβασης να αντισταθμίζονται από τα θετικά αποτελέσματα [41].

Επίσης, στις χώρες της Ευρωπαϊκής Ένωσης έχει ενσωματωθεί η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για τη προστασία προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και τη διασφάλιση της μεταφοράς τους στις χώρες μέλη όπου προστατεύονται τα βασικά ατομικά δικαιώματα ιδιαίτερα της ιδιωτικότητας. Όσον αφορά τη μετάδοση σε χώρες εκτός της ΕΕ, η τρίτη χώρα πρέπει να εξασφαλίζει ένα ικανοποιητικό επίπεδο προστασίας των δεδομένων διαφορετικά τα κράτη μέλη πρέπει να λάβουν μέτρα για την αποφυγή διαβίβασης των δεδομένων στη συγκεκριμένη χώρα εκτός αν συντρέχουν συγκεκριμένες προϋποθέσεις [2, 66].

Αργότερα, εκδόθηκε η οδηγία 2002/58/ΕΚ συγκεκριμένα για τη προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, σύμφωνα με την οποία ισχύει το απόρρητο των επικοινωνιών αλλά δεν εμποδίζει την τεχνική αποθήκευση η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας. Επιπλέον, επιτρέπει τη καταγραφή συνδιαλέξεων και συναφών δεδομένων κίνησης όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης έρευνας με σκοπό τη παροχή αποδεικτικών στοιχείων [67].

Πιο συγκεκριμένα στην Ελλάδα, με βάση το Άρθρο 9Α του Συντάγματος "ο καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει" [68]. Επιπρόσθετα, ο νόμος Ν.2472/97 ενσωματώνει την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για τη προστασία των προσωπικών δεδομένων και συνίσταται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με στόχο την εποπτεία της εφαρμογής του συγκεκριμένου νόμου και τη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων [69].

Ο ίδιος νόμος επίσης ορίζει με το άρθρο 5, παράγραφος 2δ, τις προϋποθέσεις για την επεξεργασία προσωπικών δεδομένων, σύμφωνα με το οποίο επιτρέπεται μόνο σε περιπτώσεις δημόσιου συμφέροντος ή εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από Δημόσια Αρχή ή μπορεί να την αναθέσει είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο. Πιο αυστηρές είναι οι προϋποθέσεις για την επεξεργασία ευαίσθητων δεδομένων, οι οποίες ορίζονται από το άρθρο 7, παράγραφος 2ε. Η επεξεργασία τους επιτρέπεται μόνο για λόγους εθνικής ασφάλειας,

αντιμετώπιση εγκληματικών πράξεων, προστασία δημόσιας υγείας, δημόσιο φορολογικό έλεγχο ή έλεγχο κοινωνικών παροχών και εκτελείται μόνο από Δημόσια Αρχή [69].

Επιπρόσθετα, με βάση το άρθρο 5, παράγραφος 2ε, του νόμου Ν.2472/97, επιτρέπεται η επεξεργασία και ανακοίνωση των δεδομένων σε τρίτους, εφόσον είναι απολύτως αναγκαία για την ικανοποίηση έννομου συμφέροντος που επιδιώκεται και υπερέχει των δικαιωμάτων των ατόμων που αναφέρονται τα δεδομένα χωρίς να θίγονται οι θεμελιώδεις ελευθερίες τους. Με αυτό τον τρόπο θεμελιώνεται η συνεργασία αρχών για την αντιμετώπιση εγκληματικών ενεργειών [69].

Ακόμα, ο νόμος 3471/2006 ενσωματώνει την οδηγία 2002/58/ΕΚ για τη προστασία της ιδιωτικής ζωής και τη θέσπιση προϋποθέσεων για την επεξεργασία προσωπικών δεδομένων καθώς και τη διασφάλιση του απορρήτου των επικοινωνιών στο τομέα των ηλεκτρονικών επικοινωνιών. Τέλος, με βάση το νόμο Ν.3783/2009 απαιτείται η ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας αλλά μόνο για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

9.2 Δικαιοδοσία

Σε πολλές περιπτώσεις ψηφιακής έρευνας έχουν εμφανιστεί δυσκολίες στην ανάθεση δικαιοδοσίας κυρίως εξαιτίας του αμφιλεγόμενου γεωγραφικού προσδιορισμού στο διαδικτυακό χώρο. Σε εγκληματικές υποθέσεις είναι συνήθως ο τόπος εκτέλεσης ή/και ο τόπος που επήλθε το αποτέλεσμα του εγκλήματος. Αντίθετα, σε αστικές υποθέσεις προσδιορίζεται ακόμα πιο δύσκολα καθώς οι επιπτώσεις μπορεί να εμφανίζονται σε πολλές χώρες [2].

Ειδικά ο τόπος επέλευσης του αποτελέσματος είναι δυσκολότερο να προσδιοριστεί καθώς ουσιαστικά είναι το διαδίκτυο και κάθε χώρα που μπορεί να έχει πρόσβαση στα ανάλογα δεδομένα που σχετίζονται με τη παράνομη πράξη. Ο τόπος εκτέλεσης θεωρείται το μέρος όπου βρισκόταν ο δράστης τη στιγμή που πραγματοποιούσε τη παράνομη δραστηριότητα ακόμα κι αν ουσιαστικά η εκτέλεση γινόταν σε πολλές χώρες μέσω κάποιου δικτυακού προγράμματος.

Μια χώρα έχει δικαίωμα δίωξης των υπαιτίων ενός συμβάντος εφόσον μπορεί να αποδείξει την ύπαρξη αξιόλογης σχέσης μεταξύ της χώρας και του δράστη ή και του αποτελέσματος της παράνομης ενέργειας. Μπορεί να αναλάβει τη δικαιοδοσία σε περιπτώσεις όπου ο δράστης έδρασε σε αυτή τη χώρα, ή το υπολογιστικό σύστημα που χρησιμοποιήθηκε ήταν εκεί κατά τη διάρκεια του συμβάντος, ή ήταν το θύμα, ή όταν η πρόθεση του δράστη ήταν να παρανομήσει σε βάρος της συγκεκριμένης χώρας [2].

Οι δράστες που γνωρίζουν τα νομοθετικά συστήματα και δεν έχουν κάποια συγκεκριμένη τοποθεσία ως στόχο, επιλέγουν χώρες που είναι περισσότερο νομικά ευνοϊκές. Οι περισσότερες χώρες αντιμετωπίζουν με διαφορετικό τρόπο το ηλεκτρονικό έγκλημα και την αποδοχή ψηφιακών αποδείξεων. Ως αποτέλεσμα, ο δράστης αναλόγως με το τόπο μπορεί τα ίχνη που θα αφήσει να μην γίνουν αποδεκτά ή να μην είναι αρκετά για την επίτευξη καταδίκης, αλλά ακόμα κι αν είναι, η ποινή ίσως είναι πιο ελαφριά σε σχέση με τις ποινές μιας άλλης χώρας [41].

Επίσης, ο προσδιορισμός αρμόδιας αρχής για την έρευνα ενός εγκλήματος ή καταγγελιών μπορεί να είναι δύσκολος όταν εμπλέκονται παραπάνω από μια υπηρεσία σε μια υπόθεση. Σε αυτές τις περιπτώσεις ένα αρμόδιο νομικό πρόσωπο μπορεί να καθορίσει ποιος θα την αναλάβει. Όταν όμως εμπλέκεται ένα ηλεκτρονικό έγκλημα ή κυβερνοέγκλημα όπου ο τόπος τέλεσης και εμφάνισης αποτελεσμάτων είναι το διαδίκτυο δεν μπορεί να οριστεί αυτόματα ποια χώρα είναι αρμόδια για την δίωξη του εγκλήματος. Γι’ αυτό το λόγο απαιτείται μια κοινή πολιτική παγκοσμίως για την αποφυγή διαμαχών στο θέμα της δικαιοδοσίας.

Μία από τις πρώτες προσπάθειες εφαρμογής μια κοινής πολιτικής έγινε το 2001 όπου χώρες εντός και εκτός της Ευρωπαϊκής Ένωσης συμμετείχαν σε σύναψη διεθνούς σύμβασης για το έγκλημα στον κυβερνοχώρο με σκοπό την άσκηση παρόμοιων νομοθεσιών σε αυτό το τομέα, θέτοντας κοινούς ορισμούς σε βασικές έννοιες και εφαρμόζοντας βασικούς κανόνες και αρχές στη ψηφιακή έρευνα. Για την αποδοχή όμως έρευνας σε διαφορετική χώρα, που έχει αποδεχτεί τη Σύμβαση για το Κυβερνοέγκλημα, πρέπει τα δεδομένα να είναι δημόσια διαθέσιμα και στη περίπτωση που έχουν ληφθεί από χώρο εκτός δικαιοδοσίας πρέπει να έχει γίνει με τη νόμιμη συναίνεση του ατόμου που είναι υπεύθυνο για τα συγκεκριμένα δεδομένα [73, 41].

Στην Ελλάδα, σύμφωνα με το άρθρο 16 του Ποινικού Κώδικα, τόπος τέλεσης θεωρείται ο τόπος που ο δράστης διέπραξε ολικά ή μερικά την αξιόποινη πράξη, καθώς και ο τόπος που επήλθε ή

θα μπορούσε να επέλθει, σε περίπτωση που δεν ολοκληρώθηκε η ενέργεια του δράστη, το αξιόποινο αποτέλεσμα. Με αυτόν τον ορισμό διευρύνεται η δυνατότητα εφαρμογής του ελληνικού δικαίου πέρα των γεωγραφικών ορίων. Οι ελληνικοί νόμοι μπορούν να εφαρμοστούν σε συγκεκριμένες περιπτώσεις σε άλλες χώρες είτε ο δράστης έχει ελληνική υπηκοότητα είτε όχι, αλλά και σε αλλοδαπούς που βρίσκονται στην Ελλάδα [70].

Συνήθως εφαρμόζεται η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία αρμόδιο είναι το κράτος στο οποίο εκδηλώθηκε το έγκλημα κατά την κύρια σημασία του. Ωστόσο, λόγω της φύσης του διαδικτύου, σε κάποιες καταστάσεις ο προσδιορισμός του τόπου τέλεσης είναι σχετικά δύσκολος, ειδικά όσον αφορά τα κυβερνοεγκλήματα, καθώς μπορεί να θεωρηθούν πολλαπλοί τόποι ή και να είναι διαφορετικοί οι τόποι εμφάνισης του αποτελέσματος και εντοπισμού αποδεικτικών στοιχείων.

9.3 Νόμιμη Έρευνα και Κατάσχεση

Για να πραγματοποιηθεί μια έρευνα και κατάσχεση απαιτείται η έκδοση κατάλληλου εντάλματος από ένα αρμόδιο νομικό πρόσωπο. Το ένταλμα είναι μια ένορκη έγγραφη δήλωση και περιγράφει τη πιθανή αιτία, το χώρο έρευνας, τα αντικείμενα που θα κατασχεθούν ή άτομα που θα συλληφθούν. Σε κάποιες περιπτώσεις δίνεται μια περιγραφή του σχεδίου ή της στρατηγικής έρευνας που θα εφαρμοστεί για τη παροχή εγγύησης ότι θα ακολουθηθούν όλες οι νόμιμες ενέργειες [4, 2].

Στην έρευνα ψηφιακών αποδείξεων δεν είναι πάντα γνωστό εκ το προτέρων το είδος των πληροφοριών και των συσκευών που μπορεί να τις περιέχουν. Στο ένταλμα έρευνας δίνεται περιγραφή των συσκευών που μπορεί να περιέχουν ψηφιακές πληροφορίες ή περιγραφή των πληροφοριών που αναζητούν και ορίζεται τι γίνεται προσπάθεια να εντοπιστεί για τη συγκεκριμένη υπόθεση [4].

Για να μην προκληθεί καμία αλλαγή στα αρχικά δεδομένα κατά τη διάρκεια κατάσχεσης αποδεικτικών στοιχείων πρέπει να γίνεται από κατάλληλο αρμόδιο άτομο ειδικευμένο στα forensics, ο οποίος φέρει όλη την ευθύνη για όσο διάστημα κατέχει τις αποδείξεις και μεταβιβάζεται στο επόμενο άτομο που θα τις αναλάβει. Επίσης, κάθε ενέργεια έρευνας και

κατάσχεσης θα πρέπει να καταγράφεται λεπτομερώς για μετέπειτα αξιολόγηση από τρίτα άτομα [21].

Ωστόσο, κάτω από ειδικές συνθήκες είναι δυνατή η πραγματοποίηση έρευνας ή κατάσχεσης χωρίς το ανάλογο ένταλμα. Για παράδειγμα σε επείγουσες καταστάσεις όπου η καταστροφή ή μετατροπή των αποδείξεων μπορεί να προκληθεί πολύ εύκολα από οποιαδήποτε κίνηση κάποιου που έχει άμεση πρόσβαση ή τα δεδομένα είναι εξαιρετικά ευμετάβλητα ή εύκολα να μετακινηθούν. Αν και μπορεί να γίνει η κατάσχεση στις προαναφερθείσες καταστάσεις, απαιτείται έκδοση εντάλματος για την μετέπειτα έρευνα και ανάλυσής τους [5, 33].

Δεν θεωρείται απαραίτητο το ένταλμα σε περιπτώσεις που έχει δώσει ο ιδιοκτήτης τη συγκατάθεση του να γίνει η έρευνα. Άλλες εξαιρέσεις είναι για στοιχεία που βρίσκονται σε κοινή θέα ή σε καταστάσεις που ο ερευνητής δρούσε με καλή πίστη θεωρώντας ότι ήταν νόμιμες οι πράξεις τους, για παράδειγμα όταν ένα ένταλμα έρευνας δεν είναι σαφές σε κάποια σημεία ή υπάρχουν εσφαλμένες παραλείψεις [33].

Αλλά, εξαιτίας των ιδιαίτερων χαρακτηριστικών των ψηφιακών δεδομένων είναι δύσκολο να διευκρινιστεί πότε μια έρευνα ή κατάσχεση είναι παράνομη ή όχι. Η δημιουργία αντιγραφών των δεδομένων μπορεί να θεωρηθεί ότι δεν αποτελεί κατάσχεσή τους και εφαρμογή κάποιων τεχνικών στο αντίγραφο μπορεί να μην θεωρηθεί έρευνα από κάποιους ειδικούς. Η πρώτη περίπτωση μπορεί να υποστηριχθεί επειδή δεν παραλαμβάνονται τα αρχικά στοιχεία και ο ιδιοκτήτης έχει ακόμα τα δεδομένα στην κατοχή του. Στη δεύτερη περίπτωση, η χρήση τεχνικών, για παράδειγμα hashing, οι οποίες δεν επεξεργάζεται το περιεχόμενο των αρχείων υποστηρίζεται ότι δεν αποτελεί έρευνα στα δεδομένα [33].

9.4 Νομική Ισχύς Αποδείξεων

Ο σκοπός μιας έρευνας είναι ο εντοπισμός αποδεικτικών στοιχείων που θα υποδηλώνουν αν ένα γεγονός είναι αληθινό ή όχι, ή θα αποδεικνύουν την ακεραιότητα μιας άλλης απόδειξης. Οι αποδείξεις που θα χρησιμοποιηθούν μπορεί να είναι άμεσες ή έμμεσες, μια έμμεση μαρτυρία, αποδεικτικά έγγραφα, αντικείμενα που κατασχέθηκαν και αποτελούν απόδειξη, ή και καταθέσεις

ειδικών. Όλες πρέπει να είναι αυθεντικές, αξιόπιστες και να αποτελούν τις καλύτερες αποδείξεις που μπορούν να παρουσιαστούν [52, 27].

Οι ψηφιακές αποδείξεις είναι "οποιαδήποτε πληροφορία με πιθανή αξία η οποία είναι είτε αποθηκευμένη ή μεταδίδεται σε ψηφιακή μορφή". Αναλόγως με την υπόθεση αποδείξεις μπορεί να αποτελούν διαφορετικά τα ψηφιακά στοιχεία, για παράδειγμα το περιεχόμενο ενός μηνύματος ηλεκτρονικής αλληλογραφίας αποτελεί αποδεικτικό έγγραφο, αρχεία καταγραφών και πληροφορίες συστήματος αποτελούν έμμεσα αποδείξεις και άλλα [27].

Η σύνδεση όμως των ψηφιακών στοιχείων με ένα συγκεκριμένο άτομο δεν είναι σχεδόν ποτέ εφικτή επειδή δεν περιέχουν φυσικά αποτυπώματα του ατόμου που τα παρήγαγε. Μπορούν να συνδεθούν μόνο σε περιπτώσεις που τα δεδομένα έχουν καταγράψει φυσικά χαρακτηριστικά όπως με την καταγραφή ομιλίας ή φωτογραφίες, ή συνοδεύονται από ψηφιακή υπογραφή ή άλλο κρυφό στοιχείο γνωστό μόνο στον συγκεκριμένο άτομο [27]. Αλλά ακόμα και τότε μπορεί να υποστηριχτεί ότι είναι κατασκευασμένες αποδείξεις ή το κρυφό στοιχείο τύπου ψηφιακής υπογραφής έγινε γνωστό σε τρίτο άτομο.

Η ισχύ των αποδείξεων μπορεί να είναι διαφορετική ανάλογα με την υπόθεση. Σε εγκληματικές υποθέσεις οι αποδείξεις πρέπει να είναι αξιόπιστες πέρα από κάθε λογική αμφιβολία, ενώ σε αστικές αρκεί οι αποδείξεις ενός γεγονότος να υπερτερούν από τις αυτές που υποστηρίζουν το αντίθετο. Δύο είναι τα βασικά χαρακτηριστικά τους, η σχέση που έχουν με την υπόθεση και η βαρύτητά τους, δηλαδή πόσο επηρεάζουν τη πιθανότητα ισχύς ή όχι του γεγονότος [27].

Η βαρύτητα των αποδείξεων εξαρτάται από το πόσο πιθανές είναι οι αποδείξεις αν το γεγονός είναι πραγματικό ή όχι. Αν το αποδεικτικό στοιχείο μπορεί να οφείλεται ισοδύναμα λόγω του γεγονότος ή κάποιος να το κατασκεύασε τότε δεν έχει αποδεικτική αξία. Για να διατηρηθεί η βαρύτητα των στοιχείων η πιθανότητα μετατροπής πρέπει να μειωθεί στο ελάχιστο για να διασφαλίσει την ακεραιότητά τους [27].

Επίσης, για να γίνουν αποδεκτά τα στοιχεία σε ένα δικαστήριο αρχικά ελέγχονται για το πώς αποδεικνύεται η σχέση τους με τα γεγονότα και τι επιπτώσεις έχουν σε αυτά. Η πιθανή αξία τους πρέπει να ξεπερνάει κάθε αρνητική επίδραση που ίσως προκαλέσει. Τα αποδεικτικά στοιχεία πρέπει να έχουν ληφθεί με νόμιμους και επιστημονικά αποδεκτούς τρόπους διαφορετικά δεν γίνονται αποδεκτά ανεξαρτήτως της σημαντικότητάς τους [27, 21].

Σε όλων των ειδών αποδείξεων ισχύει ο κανόνας παρουσίασης των καλύτερων αποδεικτικών στοιχείων (best evidence) σύμφωνα με τον οποίο δεν γίνονται αποδεκτά δευτερεύουσες αποδείξεις, όπως αντίγραφα, εφόσον υπάρχουν οι αρχικές και είναι διαθέσιμες. Όσο αφορά όμως τις ψηφιακές αποδείξεις δεν είναι πάντα εφικτή η παρουσίασή τους στην αρχική μορφή. Συνεπώς, η εκτυπωμένη μορφή των αποδείξεων γίνεται αποδεκτή ως ισάξια με τη ψηφιακή, αλλά και τα αντιγραμμένα δεδομένα μπορούν να γίνουν αποδεκτά σε ένα δικαστήριο εφόσον δεν αμφισβητηθεί η ακρίβειά τους σε σχέση με τα αρχικά δεδομένα [21].

Σε αντίθεση με τις φυσικές αποδείξεις, στις ψηφιακές χρησιμοποιούνται ειδικές τεχνικές για τη συλλογή τους και την ανάλυση τους, συνεπώς πρέπει και οι τεχνικές αυτές να γίνουν αποδεκτές. Το δικαστήριο του Daubert, USA όρισε κάποια κριτήρια για να προσδιορίσει την επιστημονική εγκυρότητα μιας κατάθεσης εμπειρογνώμονα. Σύμφωνα με αυτά τα κριτήρια για να θεωρηθεί αξιόπιστη μια θεωρία ή τεχνική που χρησιμοποίησε ο ερευνητής πρέπει να έχει ελεγχθεί, να έχει υπολογιστεί το πιθανό ποσοστό σφάλματος και τα πρότυπα που ακολουθήθηκαν, ή να έχει αξιολογηθεί, δημοσιευθεί και να είναι ευρέως αποδεκτή [27, 21].

Οι νομοθεσίες των ευρωπαϊκών χωρών αποδέχονται στοιχεία οποιασδήποτε μορφής σε νομικές διαδικασίες και επιτρέπουν την ελεύθερη παρουσίαση και αξιολόγηση δεδομένων ενός υπολογιστικού συστήματος. Τα αποδεικτικά στοιχεία που θα παρουσιαστούν σε μια νομική διαδικασία πρέπει να είναι ακέραια όπως και η διαδικασία έρευνας, στοιχεία που έχουν συλλεχθεί χωρίς τη τήρηση αρχών και κανόνων δεν μπορούν να γίνουν αποδεκτά [41]. Συγκεκριμένα στην Ελλάδα, με βάση το άρθρο 19, παράγραφος 3 του Συντάγματος απαγορεύεται η χρήση αποδεικτικών στοιχείων που έχουν αποκτηθεί παραβιάζοντας το απόρρητο δεδομένων επικοινωνίας και προσωπικών δεδομένων [68].

10 Επίλογος

Η εξάπλωση και ανάπτυξη των υπολογιστικών συσκευών και συστημάτων έχουν διευκολύνει τη καθημερινή ζωή του ανθρώπου σε πολλούς τομείς, όμως κάποιοι μπορούν να εκμεταλλευτούν τις δυνατότητές τους για μη θεμιτούς σκοπούς. Η συνεχόμενη αύξηση των παράνομων δραστηριοτήτων με χρήση ψηφιακών μέσων οδήγησε στη λήψη μέτρων για την αντιμετώπισή τους, και συγκεκριμένα στην ανάπτυξη μιας νέας επιστήμης των Computer Forensics.

Τα Computer Forensics έχουν ως στόχο την εύρεση, συλλογή, ανάλυση και παρουσίαση ψηφιακών αποδεικτικών στοιχείων με τρόπο που θα είναι αποδεκτά σε μια νομική διαδικασία. Επομένως, είναι αναγκαία η χρήση μεθόδων και εργαλείων που θεωρούνται αξιόπιστα από την επιστημονική κοινότητα των Computer Forensics, με σημαντικότερο χαρακτηριστικό τη προστασία της ακεραιότητας των δεδομένων σε όλη τη διαδικασία της έρευνας.

Διαδεδομένες τεχνικές του τομέα της πληροφορικής, όπως ο κατακερματισμός και τεχνικές εξόρυξης δεδομένων, συμβάλουν στην ανακάλυψη αποδεικτικών στοιχείων και στην αντιμετώπιση ενεργειών του υπόπτου για την απόκρυψή τους μέσω κρυπτογράφησης ή άλλων τεχνικών. Επιπλέον, χρησιμοποιούνται για τη προστασία των στοιχείων και την αποφυγή μετατροπών. Πολλά εργαλεία, ανοιχτού και κλειστού κώδικα, έχουν σχεδιαστεί για την εφαρμογή αυτών των τεχνικών και για τη διευκόλυνση του ερευνητή στη συλλογή και ανάλυση δεδομένων.

Εντούτοις, συναντώνται αρκετά προβλήματα κατά τη διάρκεια μιας ψηφιακής έρευνας. Οι δυνατότητες που έχει ο ύποπτος για την απόκρυψη ή καταστροφή δεδομένων, τις επονομαζόμενες τεχνικές anti-forensic, είναι πολυάριθμες και κάποιες φορές δύσκολα εντοπίσιμες. Επιπρόσθετα, οι σημάνσεις χρόνου αποτελούν ένα σημαντικό χαρακτηριστικό των αρχείων για τη δημιουργία ενός χρονοδιαγράμματος του συμβάντος. Η τυχόν τροποποίησή τους δημιουργεί σύγχυση στην έρευνα και μπορεί να οδηγήσει ακόμα και στην κατάρριψη της υπόθεσης.

Ένας ερευνητής για να χρησιμοποιήσει αποτελεσματικά τα εργαλεία forensics αλλά και για να αντιμετωπίσει επιτυχώς τις τεχνικές anti-forensic που μπορεί να έχει εφαρμόσει ο χρήστης του υπολογιστικού συστήματος που αναλύεται, πρέπει όχι μόνο να γνωρίζει επαρκώς τα εργαλεία που χρησιμοποιεί, αλλά και τα χαρακτηριστικά τουλάχιστον των πιο γνωστών λειτουργικών

συστημάτων και των συστημάτων αρχείων που χρησιμοποιούν. Επιπλέον, οι επαρκείς γνώσεις λογισμικών που χρησιμοποιούσε ο ύποπτος και σχετίζονται με τις αποδείξεις που ερευνούνται μπορούν να βοηθήσουν στον εντοπισμό επιπλέον στοιχείων. Η πιστοποίηση των γνώσεών του αποτελεί ένα σημαντικό πλεονέκτημα για την αναγνώρισή του ως αξιόπιστο εμπειρογνώμονα.

Παρότι τα Computer Forensics αναπτύχθηκαν σχετικά πρόσφατα, έχουν ήδη παρουσιαστεί αρκετοί μέθοδοι για την έρευνα και συλλογή αποδεικτικών στοιχείων. Περιγράφουν φάσεις ή βήματα για τη διαδικασία ψηφιακής έρευνας, όπου κάποια από αυτά είναι λεπτομερή ενώ άλλα πιο αφηρημένα για να προσαρμόζονται ευκολότερα σε μελλοντικές εξελίξεις του τομέα. Όμως, η δημιουργία μεθόδων για ειδικές περιπτώσεις είναι σημαντική για τη γρήγορη ανταπόκριση του ερευνητή αλλά και για τον προσδιορισμό μιας κοινής αποδεκτής αντιμετώπισης η οποία αν επιτύχει να προτυποποιηθεί θα είναι κατάλληλη για εφαρμογή σε διεθνής υποθέσεις.

Επίσης, τα Computer Forensics διαθέτουν και νομική πλευρά εφόσον τα αποτελέσματα της έρευνας πρέπει να παρουσιαστούν σε μια νομική διαδικασία. Οπότε όποια μέθοδος, τεχνική ή εργαλείο χρησιμοποιηθεί για την εύρεση αποδείξεων πρέπει να πληρούν κάποιες προδιαγραφές για να θεωρούνται έγκυρα και αξιόπιστα.

Ωστόσο, προβληματισμό έχει προκαλέσει η παρέμβαση στην ιδιωτική ζωή των ατόμων που εμπλέκονται, ή μπορεί και όχι, στην υπόθεση που διερευνάται. Έχουν θεσπιστεί νόμοι για τη προστασία προσωπικών δεδομένων αλλά δεν είναι πάντα εφικτή η αποφυγή επεξεργασίας πληροφοριών τρίτων ατόμων. Όλα τα μέτρα που θα ληφθούν πρέπει να καταγράφονται και να τεκμηριώνονται για να διασφαλιστεί η τήρηση των νόμων και κανονισμών.

Το ηλεκτρονικό έγκλημα, και ιδιαίτερα το κυβερνοέγκλημα, δεν γνωρίζει σύνορα και γεωγραφικούς περιορισμούς, με αποτέλεσμα η συχνή εμφάνιση συμβάντων που είναι δύσκολος ο προσδιορισμός του τόπου εγκλήματος και ο καθορισμός δικαιοδοσίας. Η χρήση προτύπων και διεθνών κανόνων συμβάλουν στην αποτελεσματικότερη συνεργασία χωρών και στην απόδοση δικαιοσύνης ανεξάρτητα από την αρχή που θα λάβει τη δικαιοδοσία.

Συμπερασματικά, η επιστήμη των Computer Forensics παρέχει κατάλληλες μεθόδους για τη συλλογή, επεξεργασία και παρουσίαση ψηφιακών αποδεικτικών στοιχείων παρόλη τη συνεχή εξέλιξη των ψηφιακών τεχνολογιών που αναγκάζει την κατ’ εξακολούθηση προσαρμογή στα νέα δεδομένα δυσκολεύοντας την ανάπτυξη προτύπων. Ωστόσο, η επιστημονική κοινότητα

αυτού του τομέα καταφέρνει να ανταπεξέρχεται επιτυχώς στις ανάγκες που προκύπτουν με τη παρουσίαση αξιόπιστων μεθόδων και εργαλείων, αν και ακόμα υπάρχει αρκετό πρόσφορο έδαφος για την περαιτέρω ανάπτυξη και βελτίωσή τους με στόχο τη κάλυψη μελλοντικών απαιτήσεων, όπως για παράδειγμα την ψηφιακή έρευνα σε συστήματα cloud computing.

Παράρτημα Α

Ερωτήσεις προς τη Δίωξη Ηλεκτρονικού Εγκλήματος

1. Ποια είναι τα συχνότερα ηλεκτρονικά εγκλήματα που εμφανίζονται στην Ελλάδα;

2. Ποια είναι τα βασικά χαρακτηριστικά των ηλεκτρονικών εγκλημάτων;

3. Τι μέθοδοι εφαρμόζονται και ποια εργαλεία χρησιμοποιούνται συνήθως; Είναι προτιμητέα η χρήση ελεύθερου λογισμικού ή εμπορικού και γιατί;

4. Τι εκπαίδευση έχουν λάβει τα μέλη της ομάδας έρευνας ηλεκτρονικών εγκλημάτων (γνώσεις υπολογιστών και δικτύων, νομικά κτλ);

5. Είναι ικανοποιητικοί οι πόροι που διαθέτονται για μια αποτελεσματική έρευνα; Ποιο είναι το ποσοστό επιτυχίας;

6. Ποιες δυσκολίες εμφανίζονται συχνότερα σε μια έρευνα ψηφιακών στοιχείων;

7. Μπορείτε να αναφέρετε ένα παράδειγμα μιας υπόθεσης και του τρόπου αντιμετώπισής της;

8. Τι μέτρα λαμβάνουν συνήθως οι δράστες για την απόκρυψη ενοχοποιητικών στοιχείων και πόσο εύκολα ή δύσκολα μπορούν να παρακαμφθούν;

9. Ποιες ενέργειες ακολουθούνται για να γίνουν οι ψηφιακές αποδείξεις αποδεκτές σε ένα δικαστήριο;

10. Μπορεί να αντιμετωπίσει επιτυχώς υποθέσεις ηλεκτρονικού εγκλήματος και κυβερνοεγκλήματος η ισχύουσα νομοθεσία στη Ελλάδα;

11. Πως αντιμετωπίζονται εγκλήματα όπου ο δράστης βρίσκεται στην Ελλάδα αλλά οι συνέπειες των πράξεων του εμφανίζονται σε άλλη χώρα; Και αντιστρόφως, αν ο δράστης βρίσκεται εκτός Ελλάδος αλλά ο στόχος του είναι σε ελληνικό έδαφος;

12. Το τελευταίο καιρό έχουν δημοσιευτεί αρκετές τρομοκρατικές ενέργειες και συλλήψεις τρομοκρατών. Συνέβαλε με κάποιο τρόπο η δίωξη ηλεκτρονικού εγκλήματος στην έρευνα;

13. Αν ναι με ποιο τρόπο; Κατά την έρευνα χρειάστηκε να γίνει επεξεργασία προσωπικών δεδομένων άλλων ατόμων;

14. Τι μέτρα λαμβάνονται για τη προστασία της ιδιωτικής ζωής των ελλήνων πολιτών κατά τη διάρκεια έρευνας ψηφιακών αποδείξεων για παράδειγμα στο διαδίκτυο;

15. Μπορεί να θεωρηθεί απόκρυψη πληροφοριών μέτρα που λαμβάνουν οι χρήστες για να προστατέψουν τα δεδομένα τους και διωχθούν ποινικά;

16. Εκτός από εγκληματικές υποθέσεις αναλαμβάνονται και άλλου είδους υποθέσεων όπως καταγγελίες από πολίτες ή εταιρίες;

17. Αν ναι, είναι διαφορετικός ο τρόπος αντιμετώπισής τους σε σχέση με τις εγκληματικές υποθέσεις;

18. Γίνονται συχνά στόχοι ηλεκτρονικών επιθέσεων ελληνικές εταιρίες, τράπεζες, δημόσιοι οργανισμοί;

19. Αν ναι, είναι προετοιμασμένοι για τη προστασία τους αλλά και για τη διατήρηση ψηφιακών αποδείξεων που θα διευκολύνουν μια πιθανή έρευνα;

20. Τι συμβουλές θα δίνατε στους απλούς χρήστες για να προστατευθούν από επιθέσεις στο διαδίκτυο;

Παράρτημα Β

Πίνακας Εργαλείων Forensics

Εργαλείο	Περιγραφή
COFEE	Σύνολο εργαλείων της Microsoft
Coroner's Toolkit	Σύνολο εργαλείων
dd	Δημιουργία εικονικών αντιγραφών
Device Seizure	Ανάλυση φορητών συσκευών
DIBS	Δημιουργία εικονικών αντιγραφών
DIBS Portable Evidence Recovery Unit	Δημιουργία εικονικών αντιγραφών
Digital Intelligence	Προστασία εγγραφής
EasyTimeline	Αναπαράσταση χρονοδιαγραμμάτων
EnCase	Σύνολο εργαλείων
Forensic ToolKit	Σύνολο εργαλείων
Helix	Αναπαράσταση χρονοδιαγραμμάτων
NetMap	Εργαλείο αναπαράστασης συνδέσμων
OCFA	Σύνολο εργαλείων
P2 Commander	Σύνολο εργαλείων
ProDiscover	Δημιουργία εικονικών αντιγραφών
Rapid Action Imaging Device	Δημιουργία εικονικών αντιγραφών
SafeBack	Δημιουργία εικονικών αντιγραφών
SMART	Σύνολο εργαλείων
SmartSector Imaging	Δημιουργία εικονικών αντιγραφών
The Sleuth Kit	Σύνολο εργαλείων
TULP	Ανάλυση φορητών συσκευών
Zeitline	Αναπαράσταση χρονοδιαγραμμάτων
ZERP	Ανάλυση φορητών συσκευών

Παράρτημα Γ

Πίνακας Εργαλείων Anti-Forensics

Εργαλείο	**Περιγραφή**
CyberScrub	Διαγραφή αρχείων
Evidence Eliminator	Διαγραφή αρχείων
Gnu Privacy Guard	Κρυπτογράφηση
Invisible Secrets	Στεγανογράφηση
MP3Stego	Στεγανογράφηση
NCovert	Απόκρυψη δεδομένων δικτύων
Onion Routing	Απόκρυψη δεδομένων δικτύων
OpenSSL	Κρυπτογράφηση
Sam Juicer	Απόκρυψη hash τιμών του αρχείου SAM
Slacker	Απόκρυψη δεδομένων στο χώρο slack
S-Tools	Στεγανογράφηση
Timestomp	Μετατροπή Χρονικών σημάνσεων
Transmogrify	Απόκρυψη αρχείων από το EnCase
TrueCrypt	Κρυπτογράφηση
Window Washer	Διαγραφή αρχείων
Windows & Internet Cleaner Pro	Διαγραφή αρχείων

Παράρτημα Δ

Παρουσίαση Εργαλείου Forensic, SMART for Linux

Σε αυτό το σημείο παρουσιάζονται κάποιες από τις βασικές δυνατότητες του εργαλείου SMART της ASR Data. Συγκεκριμένα χρησιμοποιείται η ειδική έκδοση αξιολόγησης SMART for Linux, το SMART – Ubuntu 2011/01, σε μια εικονική μηχανή VMware Player 3.0.1.

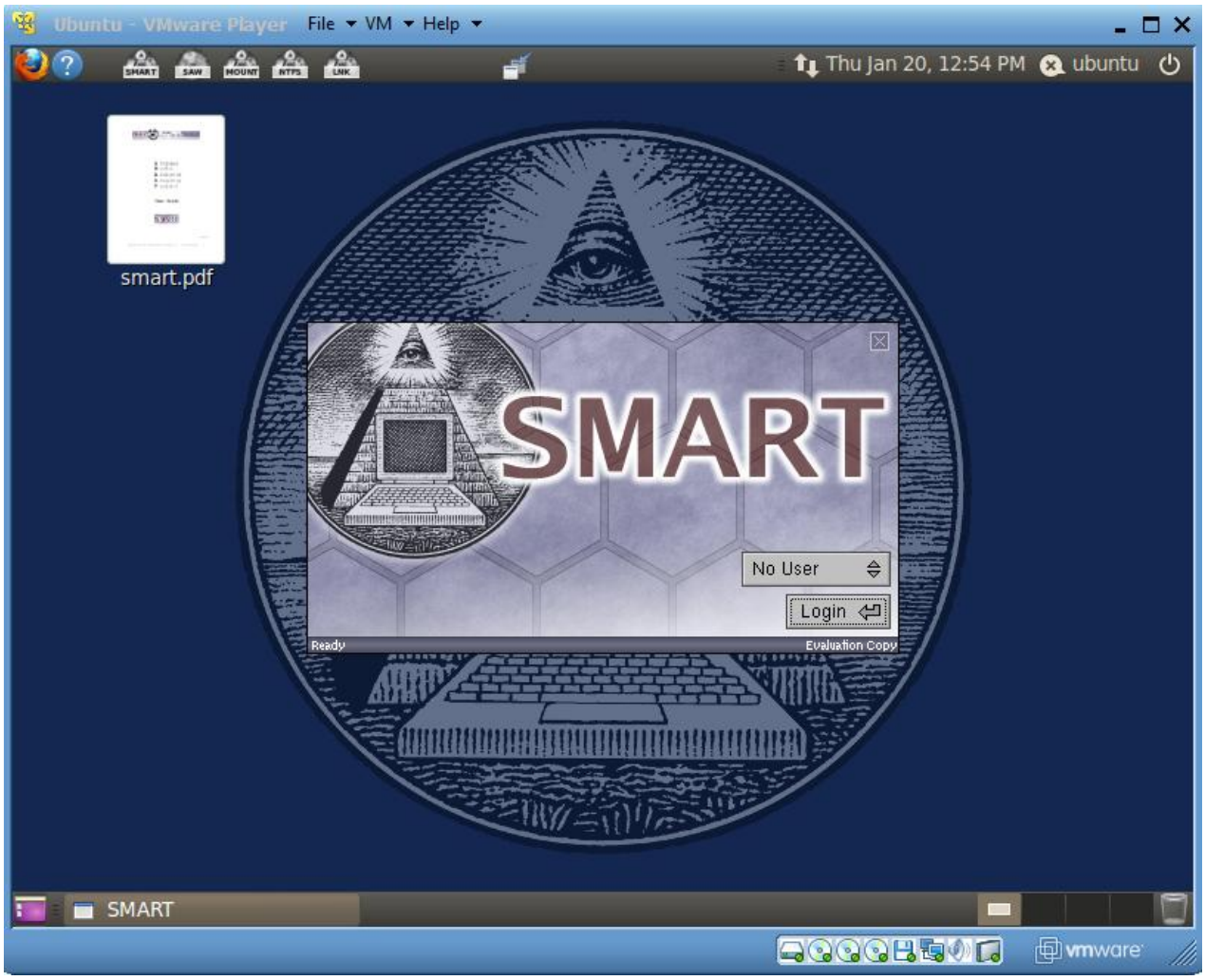
Στα πλαίσια της εργασία χρησιμοποιήθηκε ένα εξωτερικό USB flash drive 1GB της Transcend για την ανάλυσή του από το εργαλείο SMART.

Εκκίνηση του SMART

Η εκκίνηση του προγράμματος γίνεται μέσω του λειτουργικού Ubuntu στο οποίο είναι ενσωματωμένο. Το λειτουργικό εκτός από τα βασικά προγράμματα που συναντώνται σχεδόν σε κάθε διανομή Linux, περιέχει και τα SMART, SAW, MOUNT, NTFS και LNK τα οποία αποτελούν εργαλεία forensic.

Αρχικά θα χρησιμοποιηθεί το εργαλείο SMART που εκτελεί τις κύριες λειτουργίες μιας ψηφιακής έρευνας.

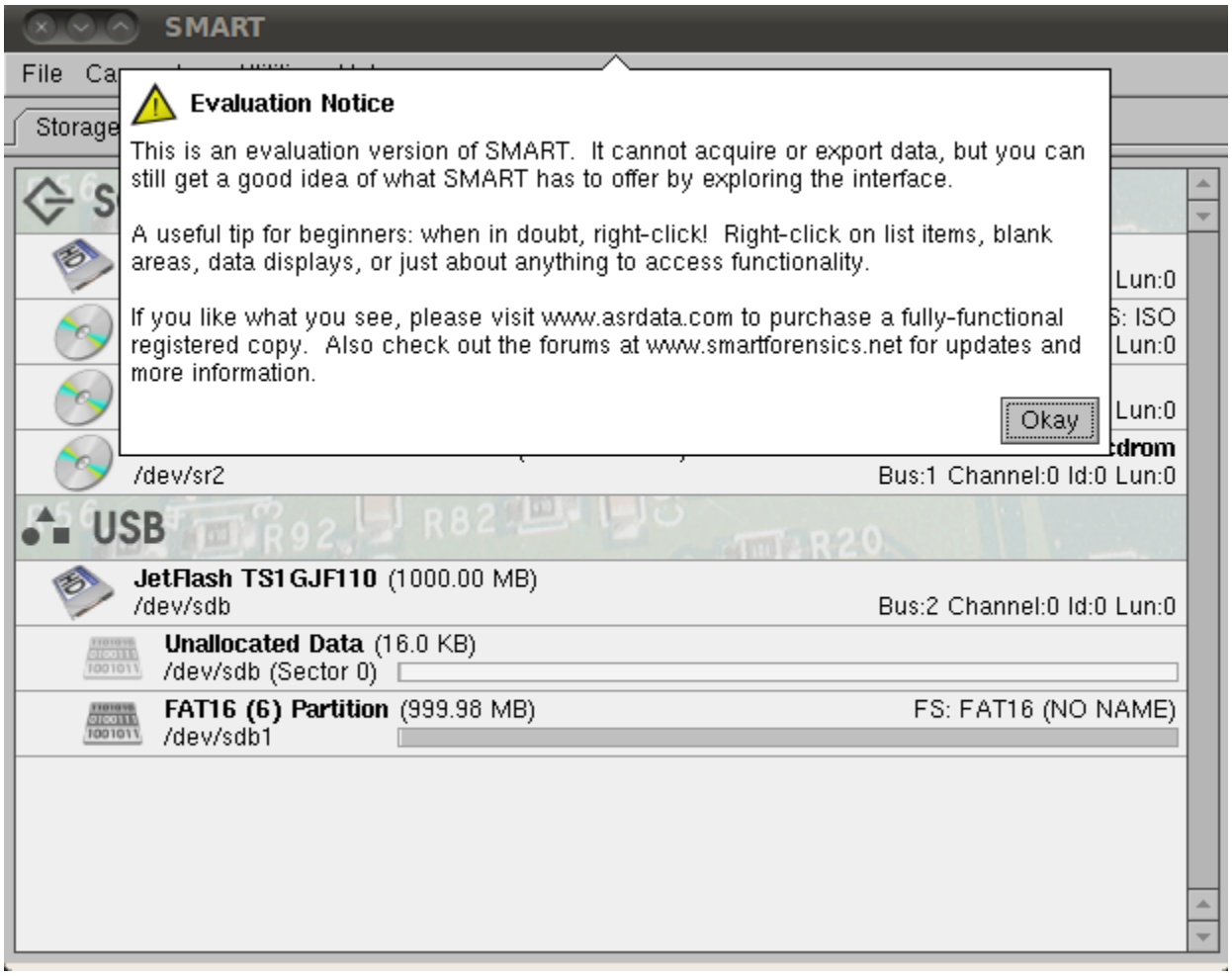
Κατά την έναρξη του προγράμματος ζητείτε να επιλεχθεί κάποιος χρήστης ή να δημιουργηθεί ένας νέος ή να γίνει σύνδεση χωρίς χρήστης (No User) το οποίο επιλέγεται σε αυτή τη περίπτωση.



Εικόνα 1: Smart for Linux

Παρουσίαση διαθέσιμων αποθηκευτικών μέσων

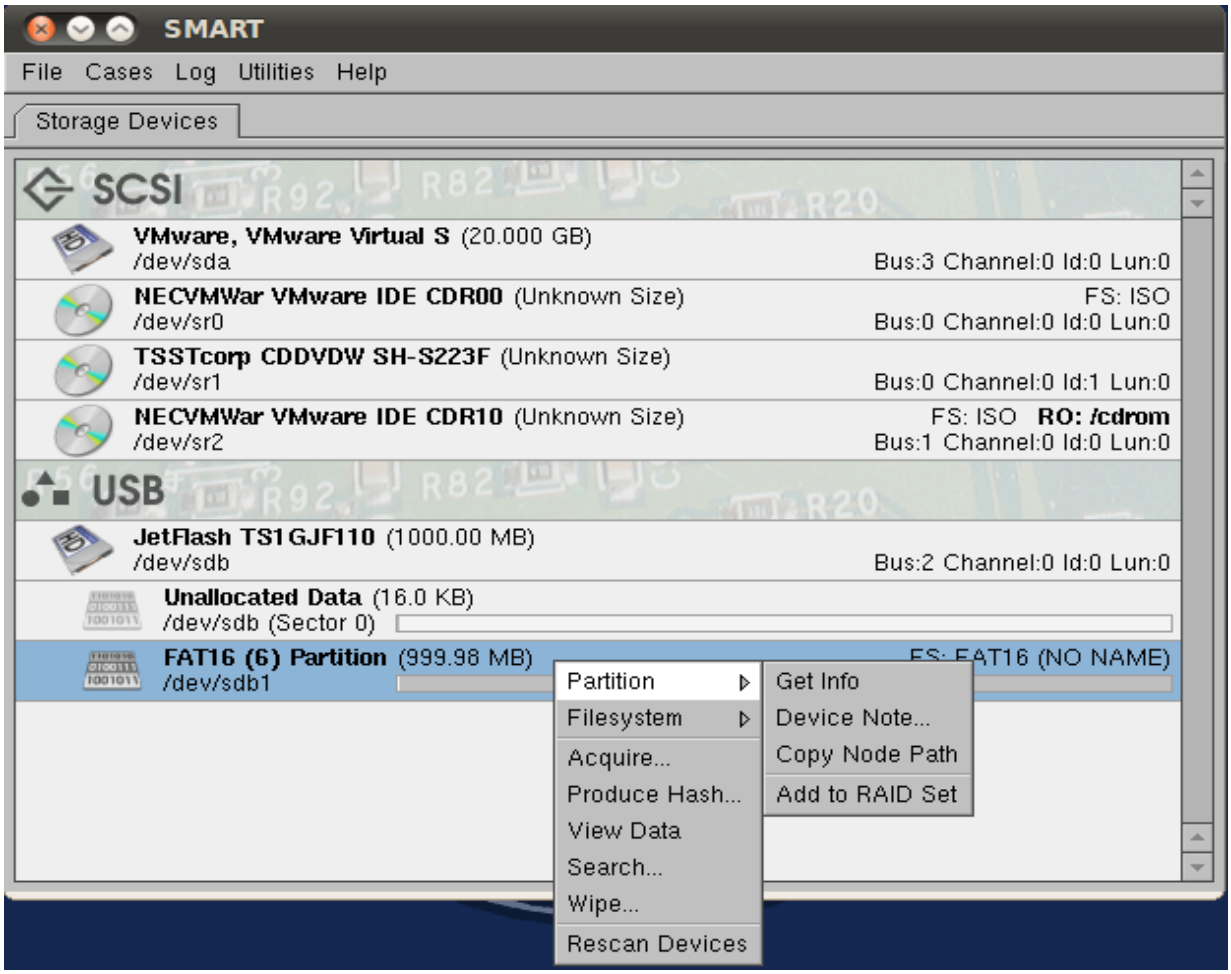
Μετά την σύνδεση ακολουθεί ένα παράθυρο με όλες τις αποθηκευτικές συσκευές που έχουν εντοπιστεί. Παρακάτω βλέπουμε και το αρχικό μήνυμα που παρουσιάζει για προειδοποίηση του περιορισμού των δυνατοτήτων του λόγω της συγκεκριμένης έκδοσης του.



Εικόνα 2: Storage Devices

Λόγω της χρήσης εικονικής μηχανής δεν υπάρχει κάποιος σκληρός δίσκος με λειτουργικό σύστημα, επομένως θα επικεντρωθούμε στα αρχεία της USB συσκευής.

Από τα πρώτα στοιχεία που εμφανίζονται είναι το μέγεθος της συσκευής και το σύστημα αρχείων του το οποίο στη συγκεκριμένη αποθηκευτική συσκευή είναι το FAT16.



Εικόνα 3: Storage Device - USB

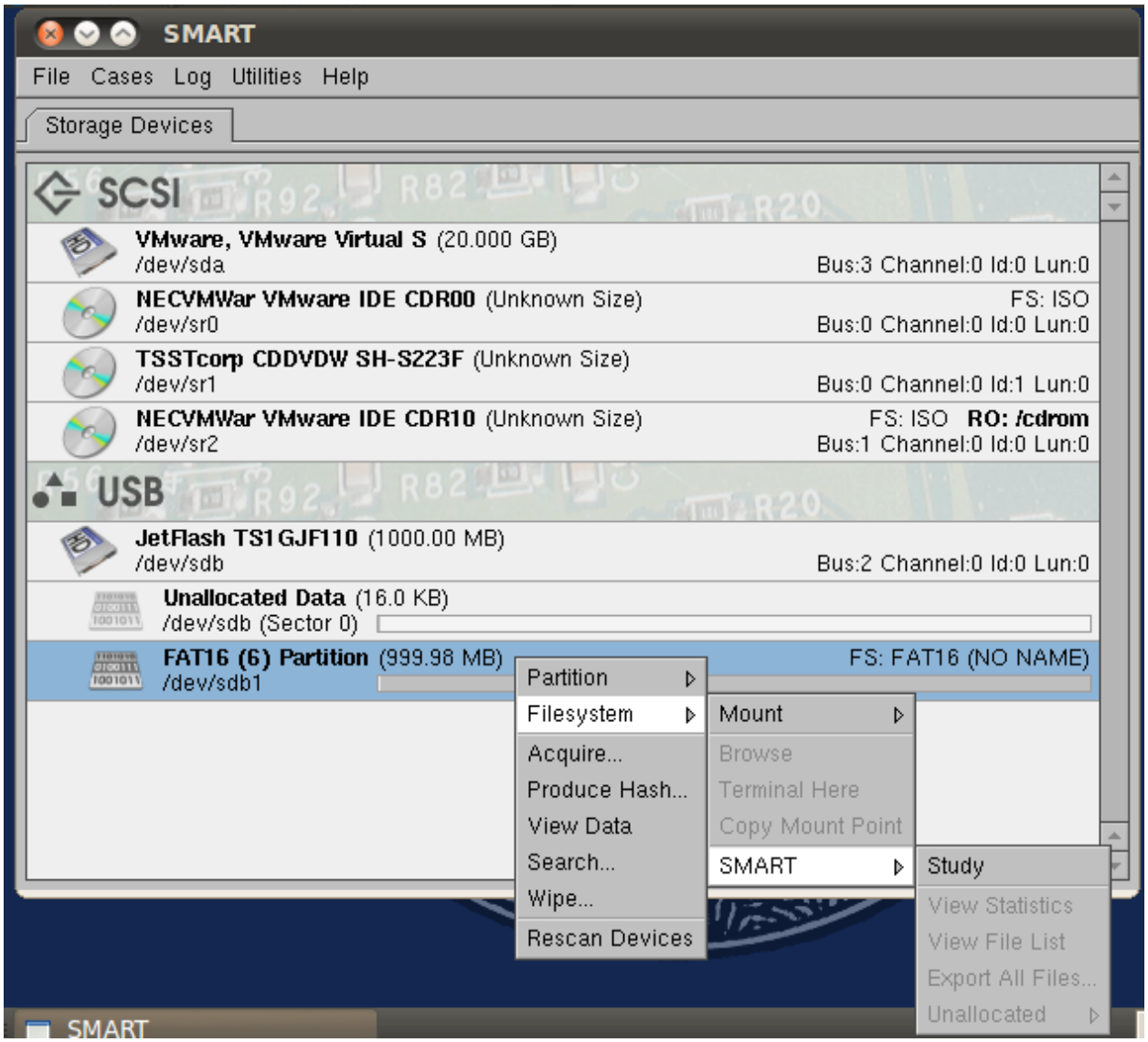
Περισσότερες πληροφορίες εμφανίζονται με την επιλογή Partition → Get Info. Πιο αναλυτικά, εκτός από το σύστημα αρχείων, εμφανίζεται το μέγεθος σε MB και Bytes, ο αριθμός των τομέων του δίσκου και άλλα χαρακτηριστικά.



Εικόνα 4: Πληροφορίες Συσκευής

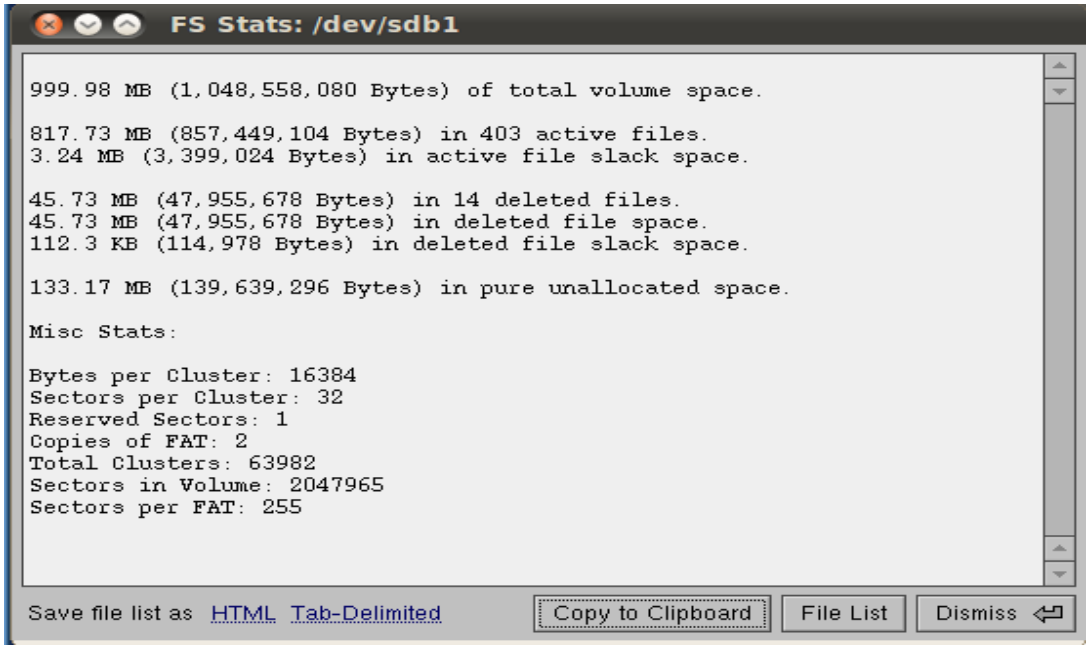
Ανάλυση Συσκευής

Η ανάλυση της συσκευής από το SMART για τον εντοπισμό ενεργών και διαγραμμένων δεδομένων γίνεται μέσω της επιλογής Filesystem →SMART → Study.

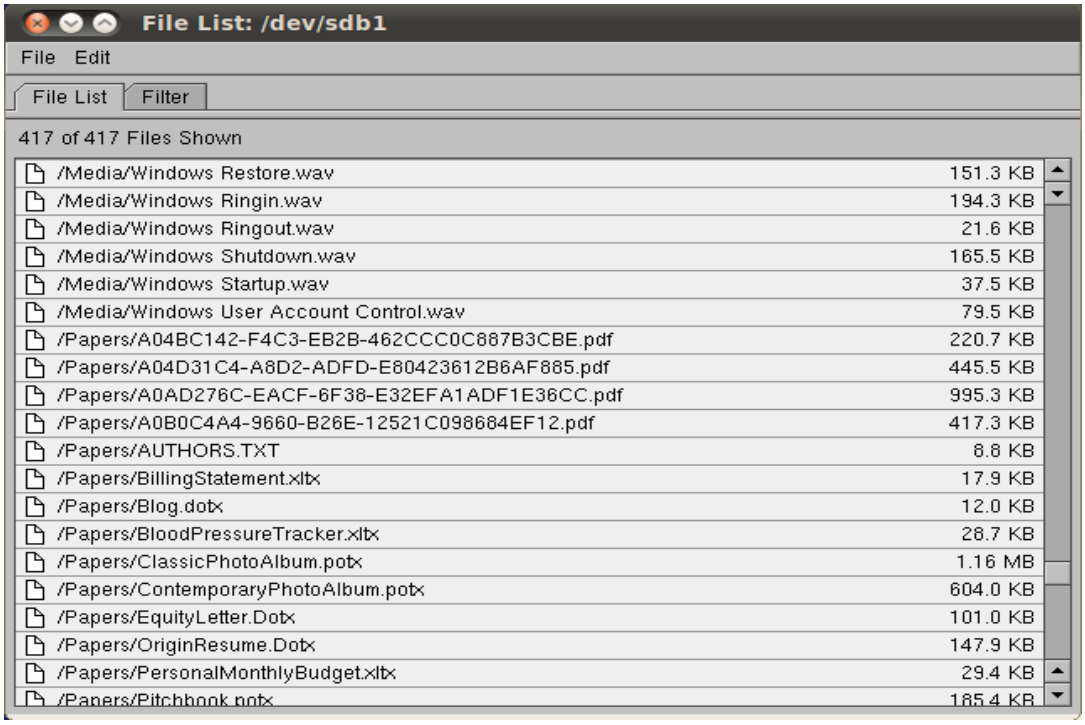


Εικόνα 5: SMART - Study

Μετά την ανάλυση έχουν υπολογιστεί κάποια στατιστικά στοιχεία για τη συσκευή και δημιουργήθηκε μια λίστα με το σύνολο των αρχείων που εντοπίστηκαν.

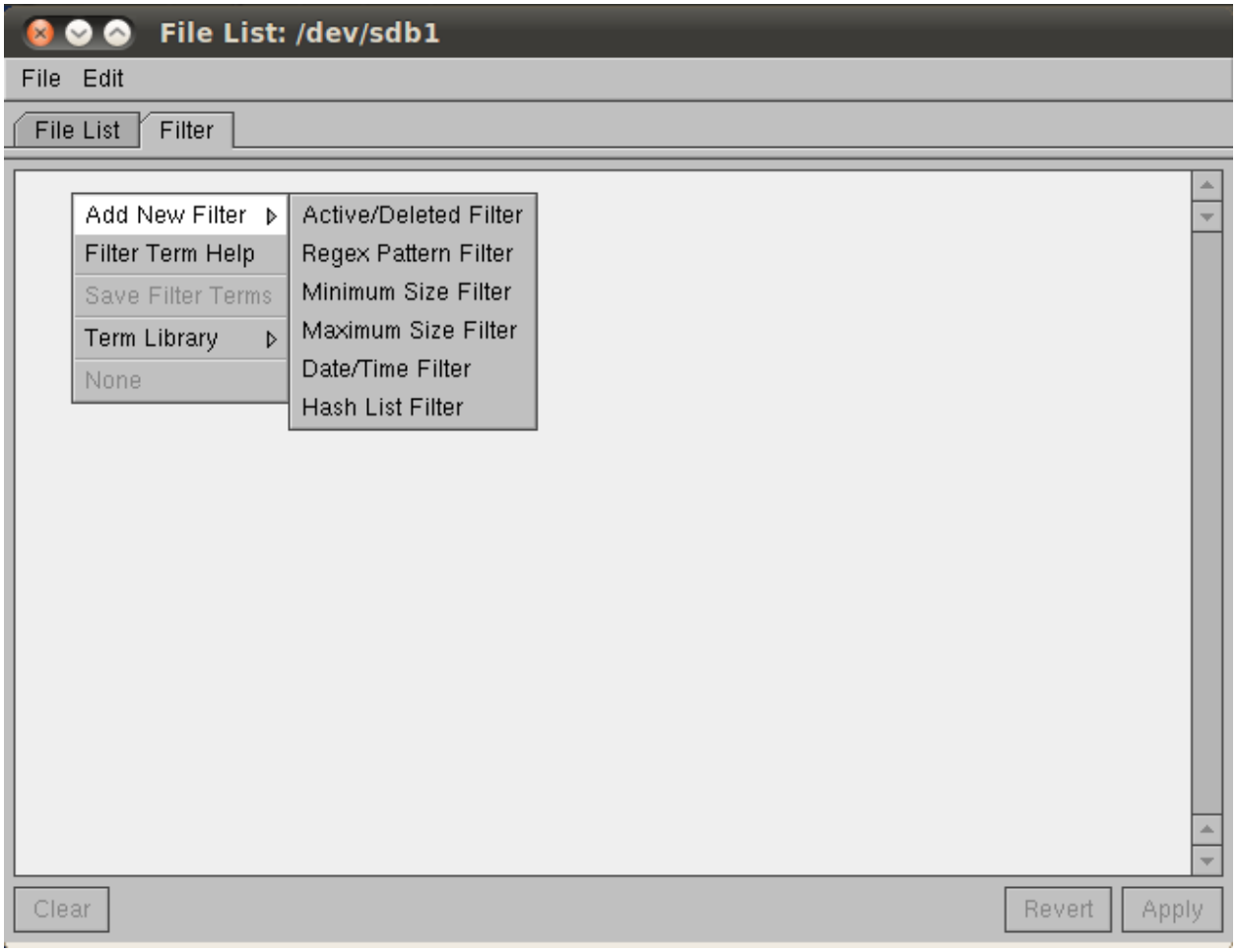


Εικόνα 6: Στατιστικά συσκευής



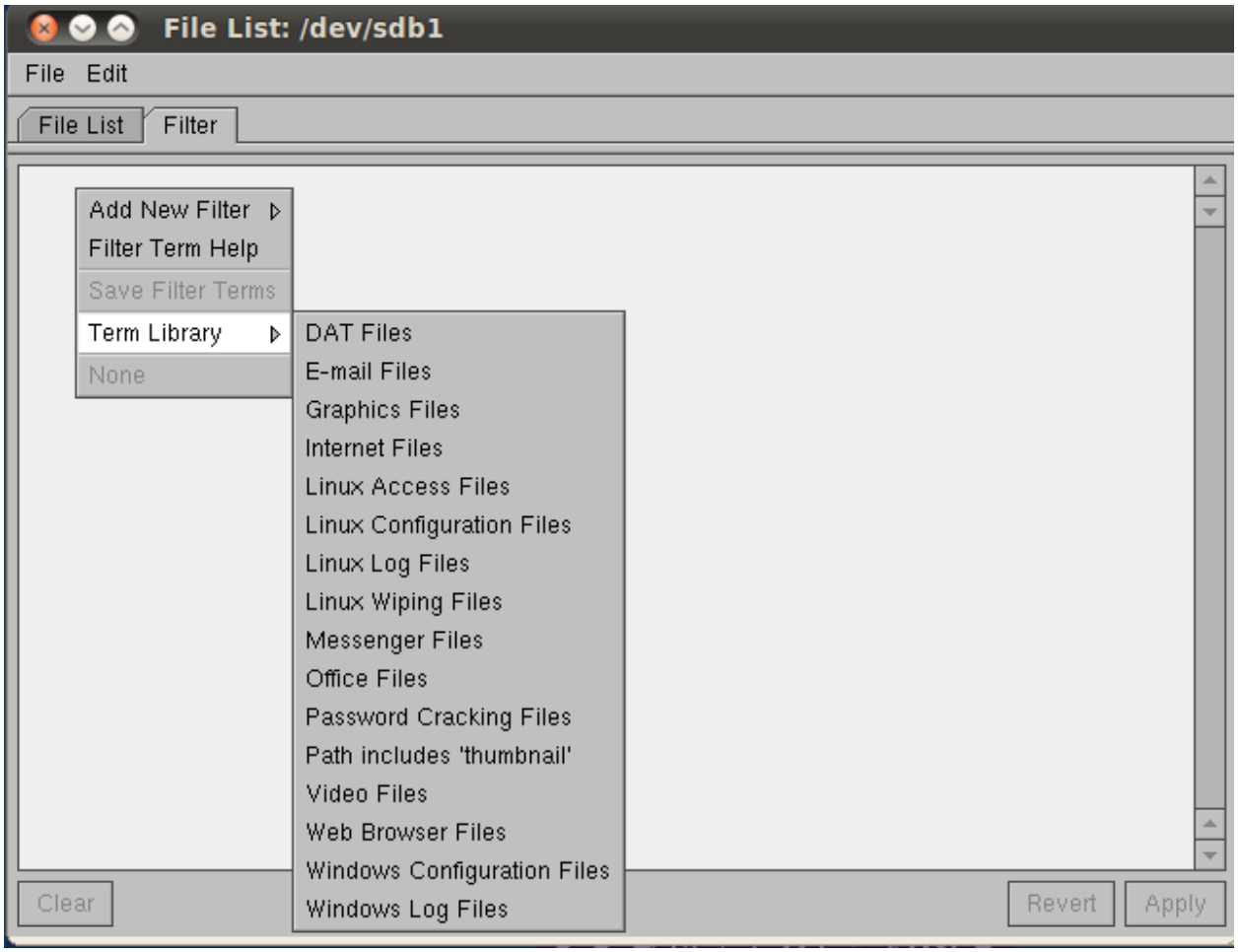
Εικόνα 7: Λίστα αρχείων

Η λίστα των αρχείων μπορεί να φιλτραριστεί, είτε με βάση κάποια χαρακτηριστικά του αρχείου όπως αν είναι διαγραμμένα ή ενεργά, με βάση το μέγεθος, τις χρονικές σημάνσεις του αρχείου και άλλα.



Εικόνα 8: Φιλτράρισμα αρχείων με βάση χαρακτηριστικών

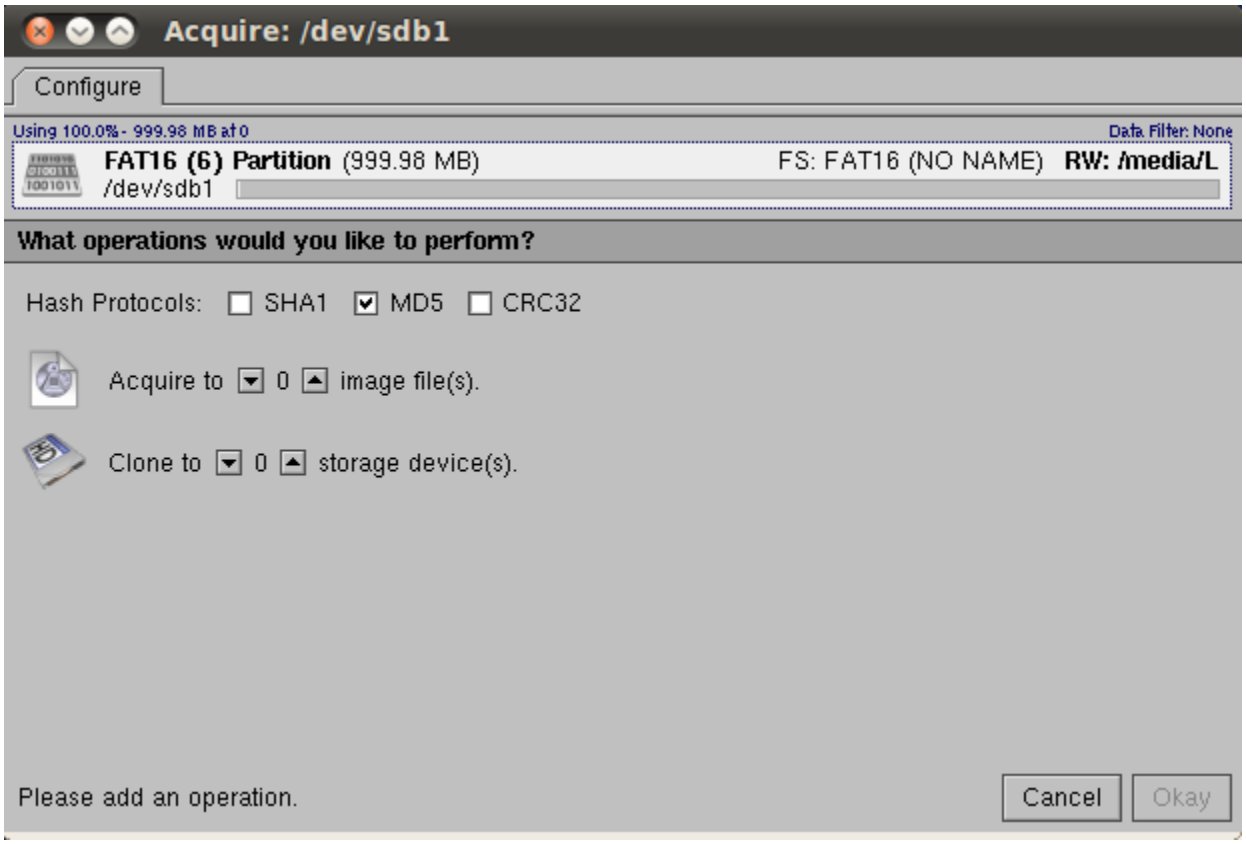
Επιπλέον, μπορεί να γίνει φιλτράρισμα με βάση όρους μιας βιβλιοθήκης που περιλαμβάνει είδη αρχείων, για παράδειγμα εικόνες, βίντεο και άλλα.



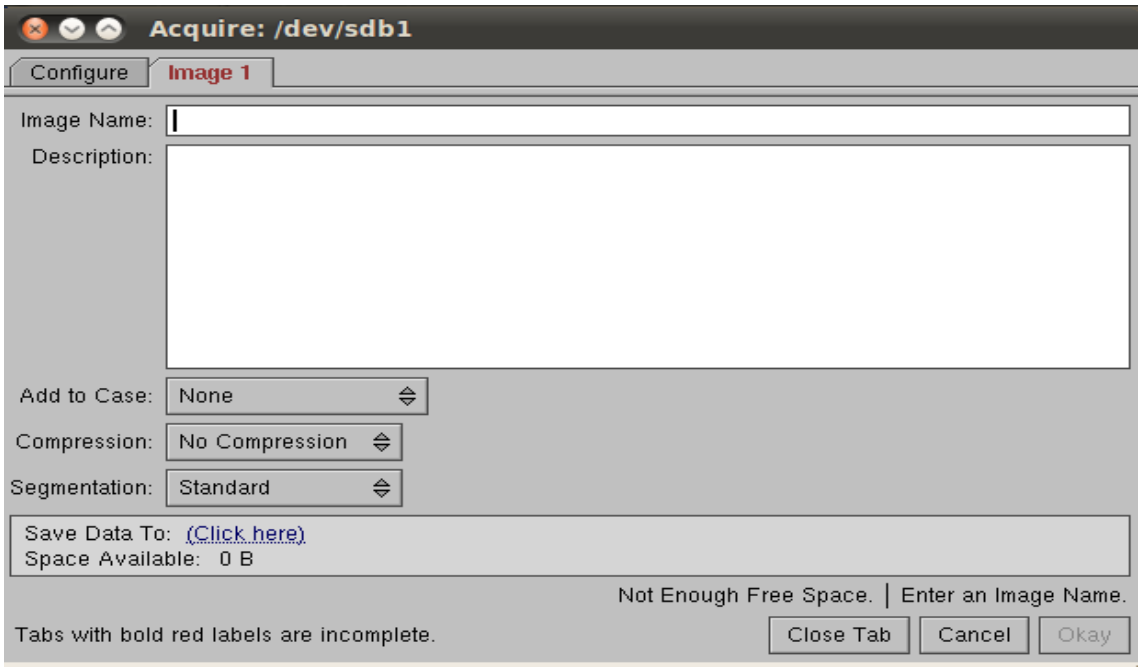
Εικόνα 9: Φιλτράρισμα με βάση το είδος του αρχείου

Διαδικασία αντιγραφής

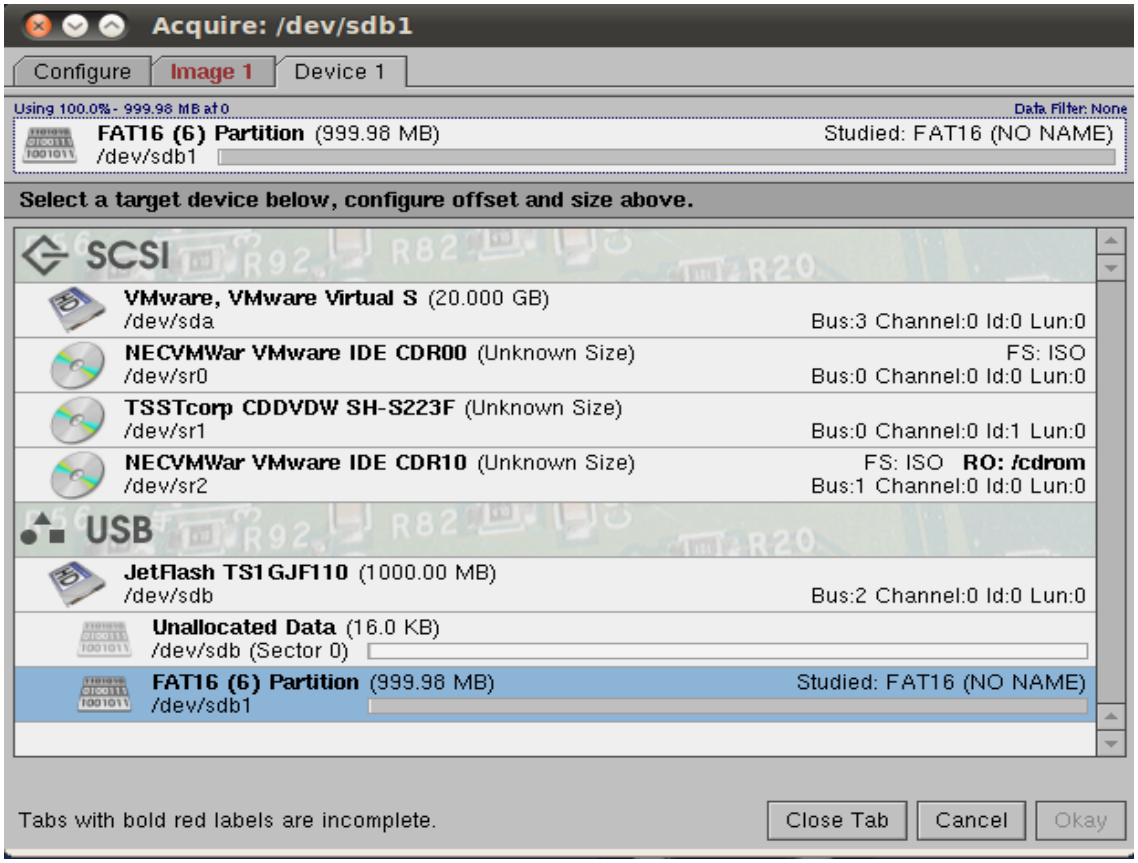
Η απόκτηση των δεδομένων πρέπει να γίνεται με ειδικές διαδικασίες για να αποφευχθεί οποιαδήποτε μεταβολή στα δεδομένα. Το SMART δίνει δύο επιλογές, την απόκτηση μέσω ενός εικονικού αντίγραφου (image file) ή τη «κλωνοποίηση» μιας συσκευής (clone storage device).



Εικόνα 11: Απόκτηση δεδομένων



Εικόνα 12: Image File

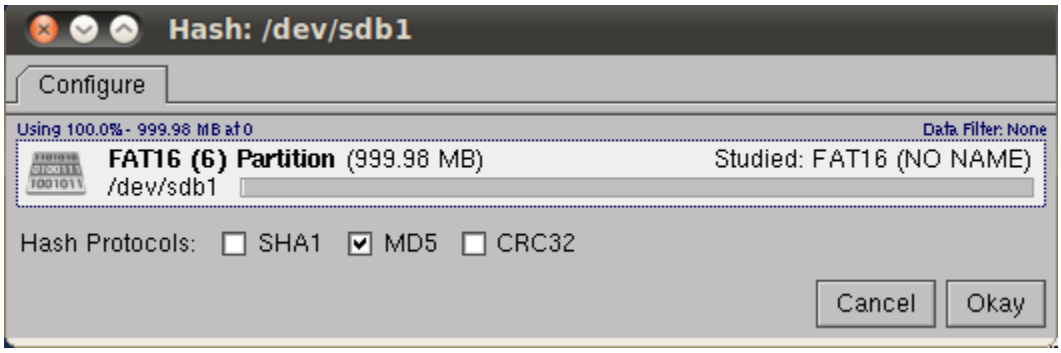


Εικόνα 13: Clone Storage Device

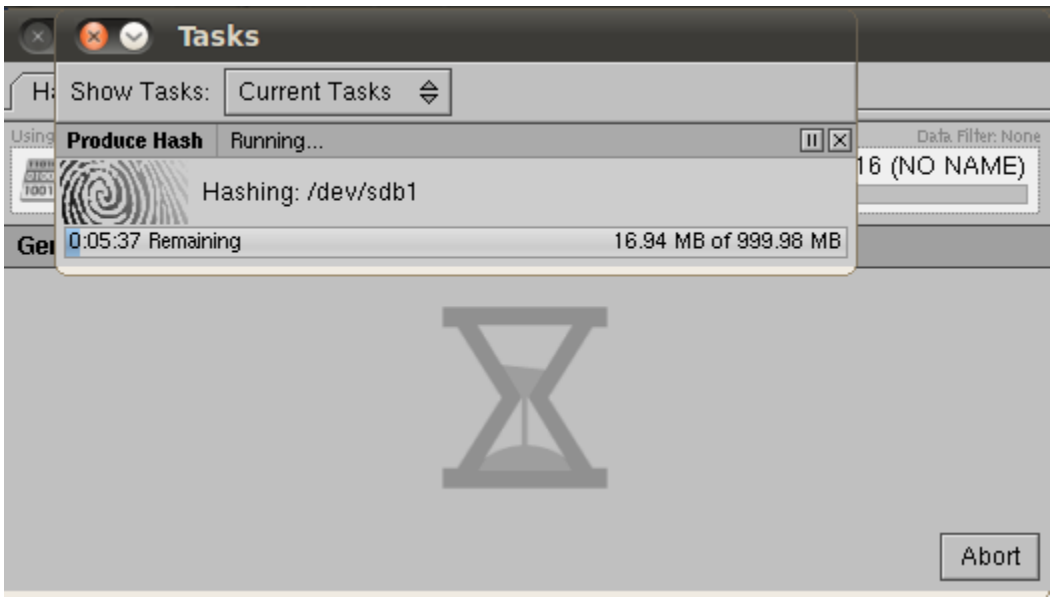
Διαδικασία παραγωγής τιμής hash

Απαραίτητη λειτουργία είναι η παραγωγή μιας τιμής hash της συσκευής για τη μετέπειτα επαλήθευση της ακεραιότητας της ίδιας και των αντιγράφων της.

Αρχικά επιλέγεται ποιο πρωτόκολλο θα ακολουθηθεί για την δημιουργία της τιμής hash. Το SMART δίνει τη δυνατότητα παραγωγής της τιμής με βάση το SHA-1, MD5 και το CRC32. Για αυτό το παράδειγμα επιλέχθηκε το MD5.

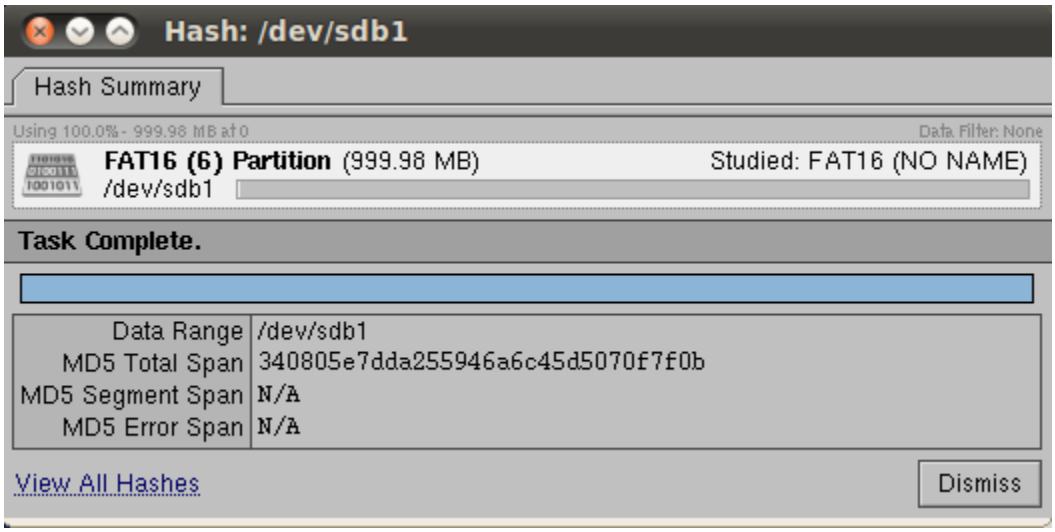


Εικόνα 14: Επιλογή πρωτοκόλλου Hash



Εικόνα 15: Δημιουργία τιμής hash

Μετά την ολοκλήρωση της διαδικασίας κατακερματισμού (hashing) έχει παραχθεί μια τιμή hash 32 χαρακτήρων η οποία είναι αποκλειστική για το συγκεκριμένο σύνολο δεδομένων.



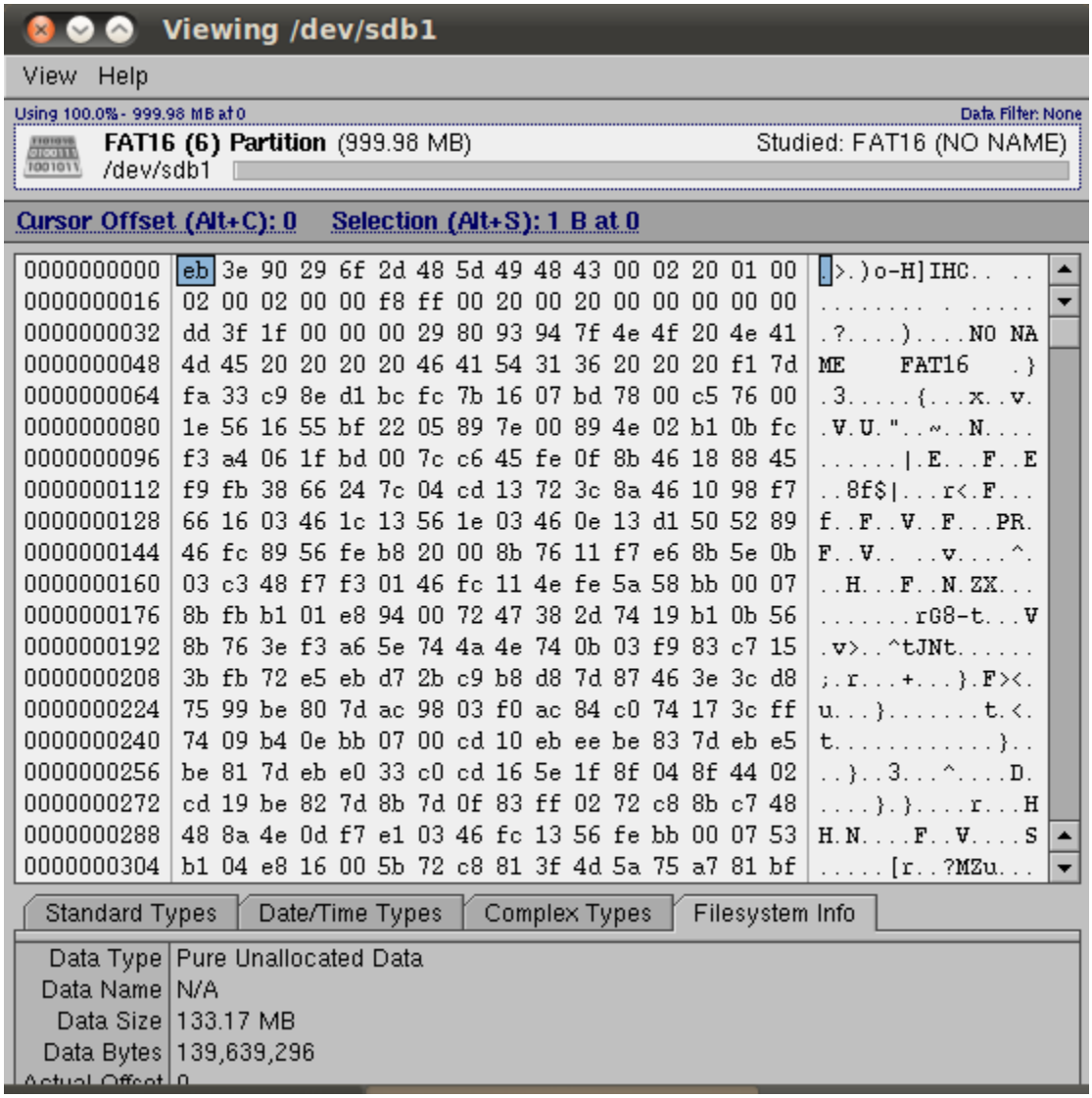
Εικόνα 16: Ολοκλήρωση διαδικασίας hashing



Εικόνα 17: Τιμή Hash

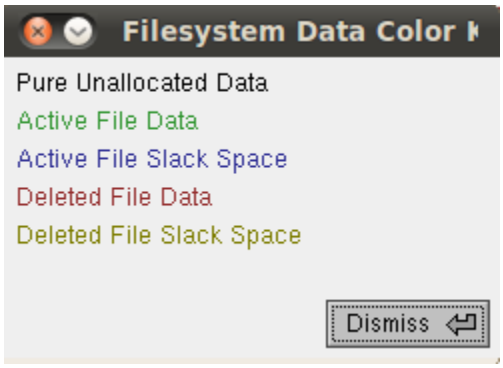
Εμφάνιση δεδομένων

Τα δεδομένα εμφανίζονται σε δεκαεξαδική μορφή (hex) και ως μη επεξεργασμένα (raw data). Το χρώμα των δεδομένων αντιπροσωπεύει τη κατάσταση των δεδομένων, για παράδειγμα στην παρακάτω εικόνα το μαύρο υποδηλώνει ότι τα συγκεκριμένα δεδομένα είναι σε καταχωρημένο χώρο.

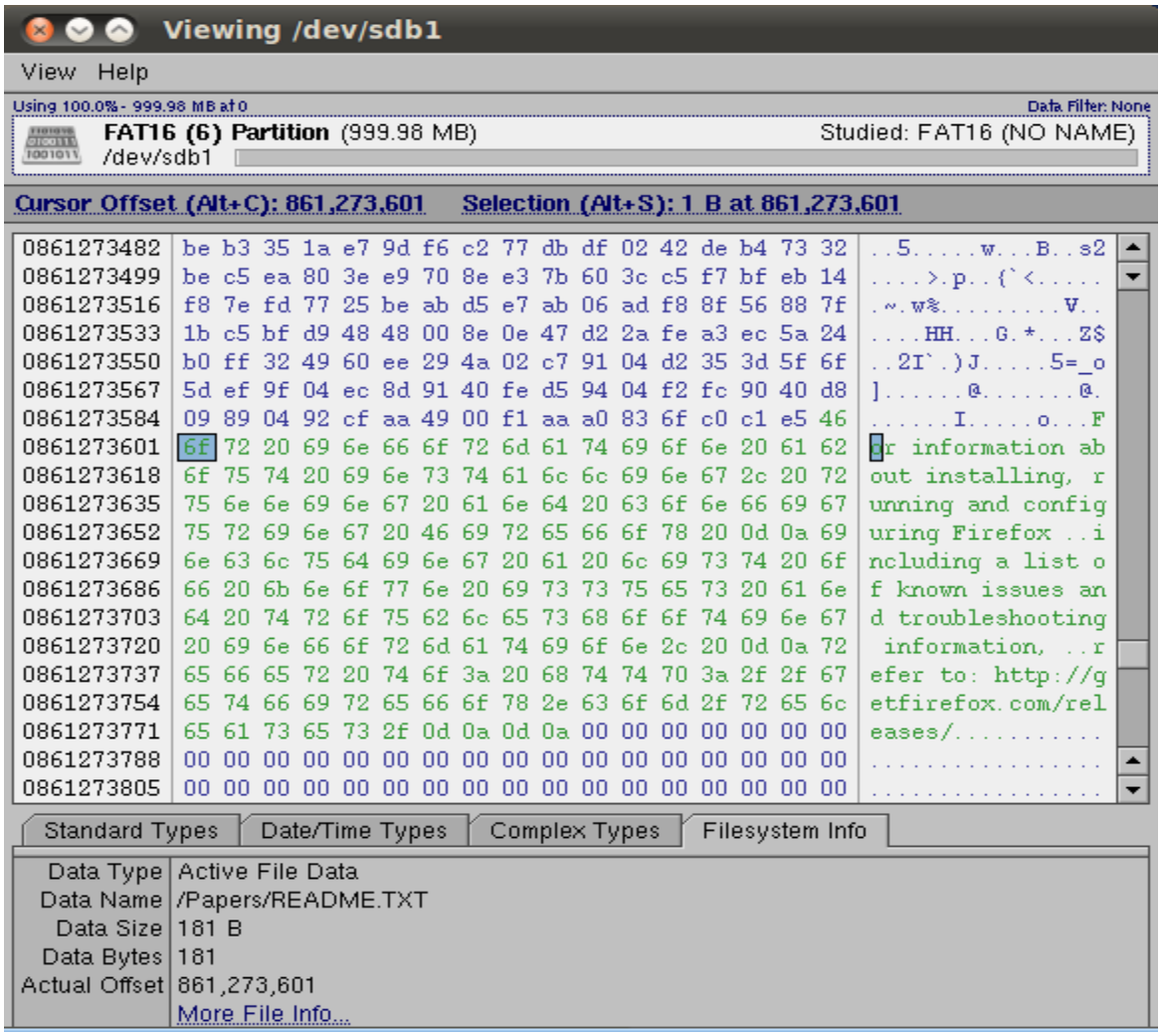


Εικόνα 18: Μη καταχωρημένα δεδομένα

Στο παρακάτω πίνακα παρουσιάζεται τι αντιπροσωπεύει ο διαφορετικός χρωματισμός των δεδομένων για τον ευκολότερο διαχωρισμό τους κατά την εξέτασή τους.



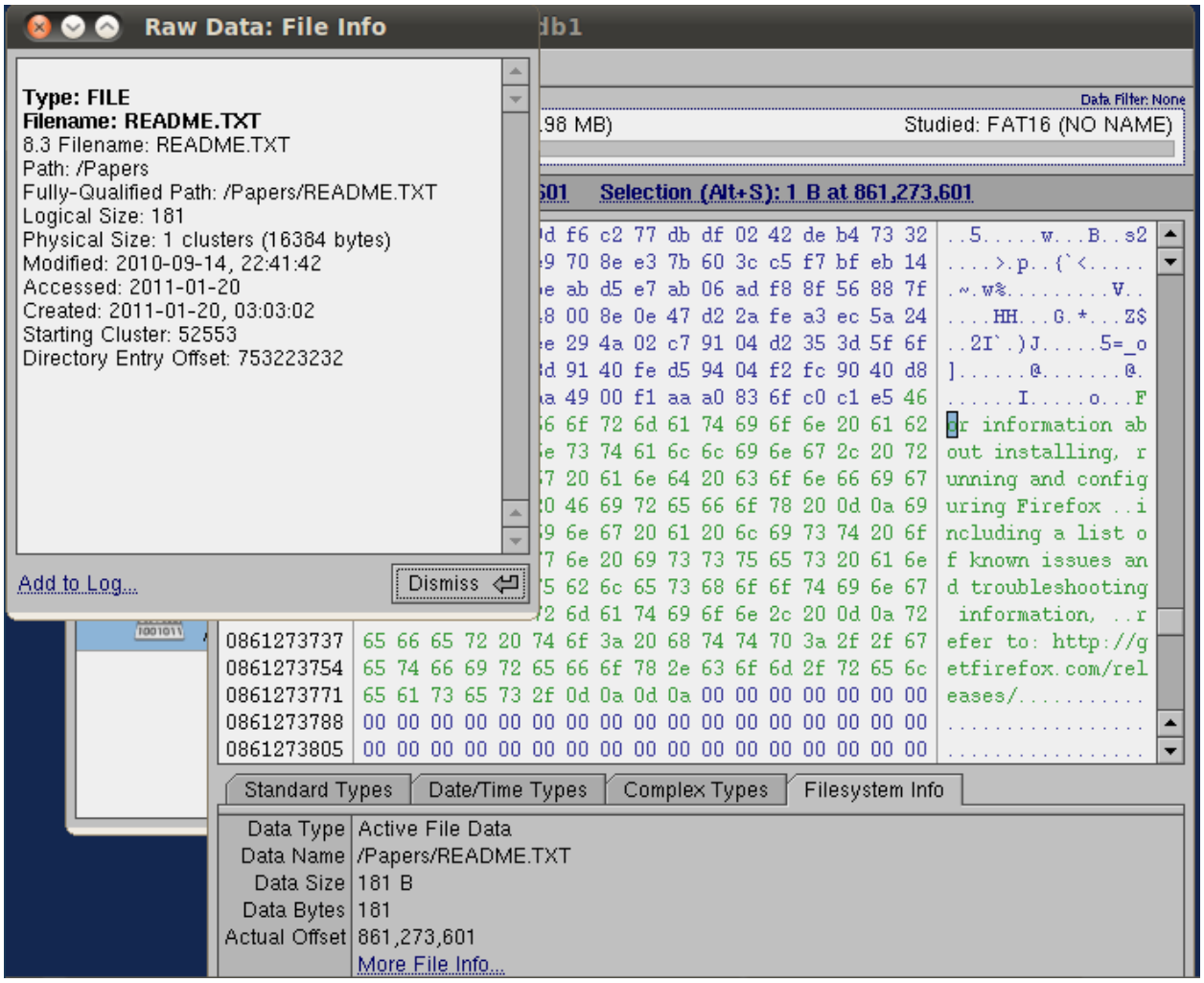
Εικόνα 19: Χρωματικός διαχωρισμός των αρχείων



Εικόνα 20: Ενεργά δεδομένα

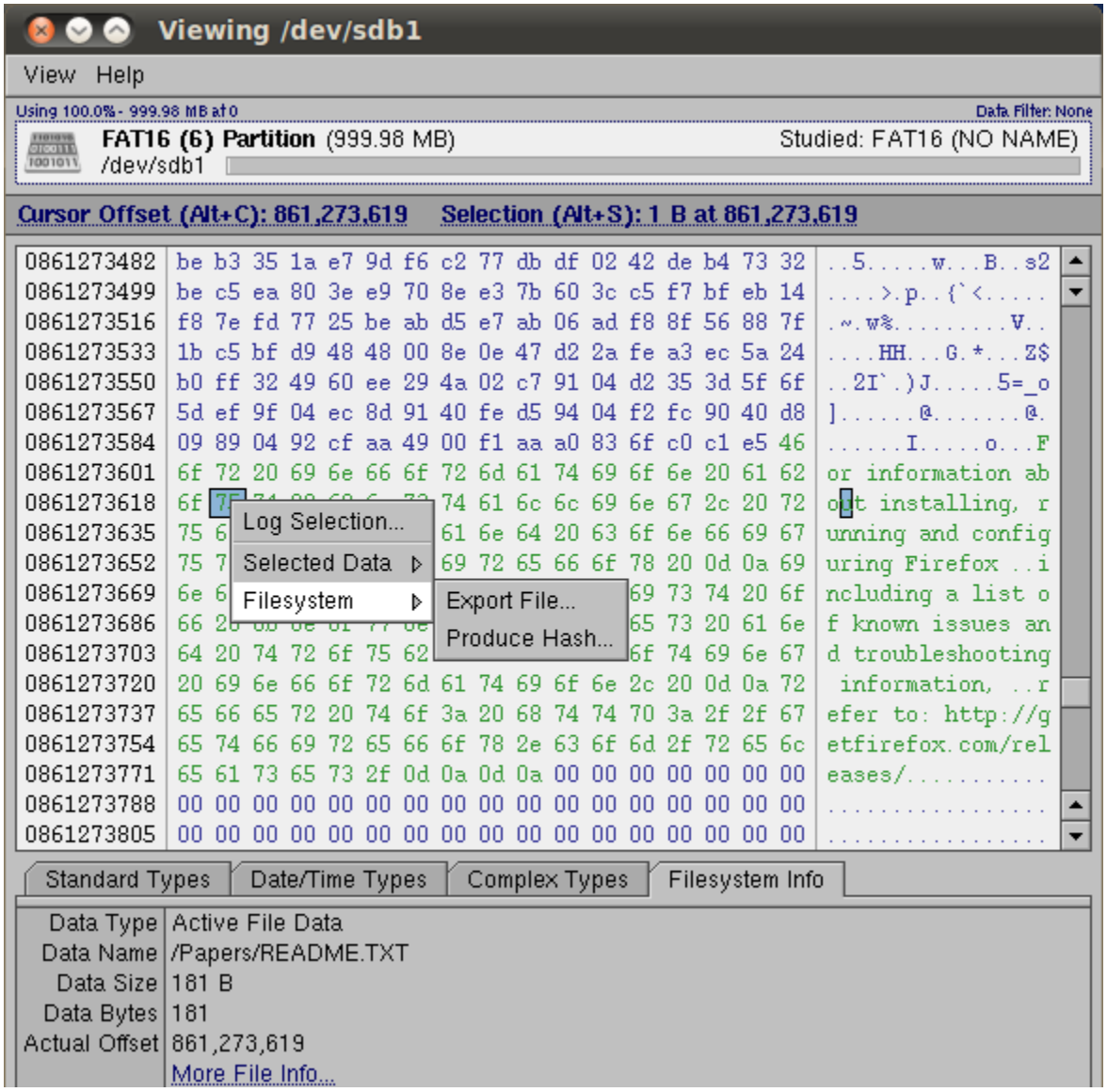
Στη παραπάνω εικόνα έχει εντοπιστεί ένα αρχείο απλού κειμένου όπου το περιεχόμενό του μπορεί να παρουσιαστεί σε αναγνώσιμη μορφή.

Με την επιλογή κάποιου μέρους του αρχείου μπορούν να εμφανιστούν πληροφορίες για το αρχείο όπως βλέπουμε παρακάτω.



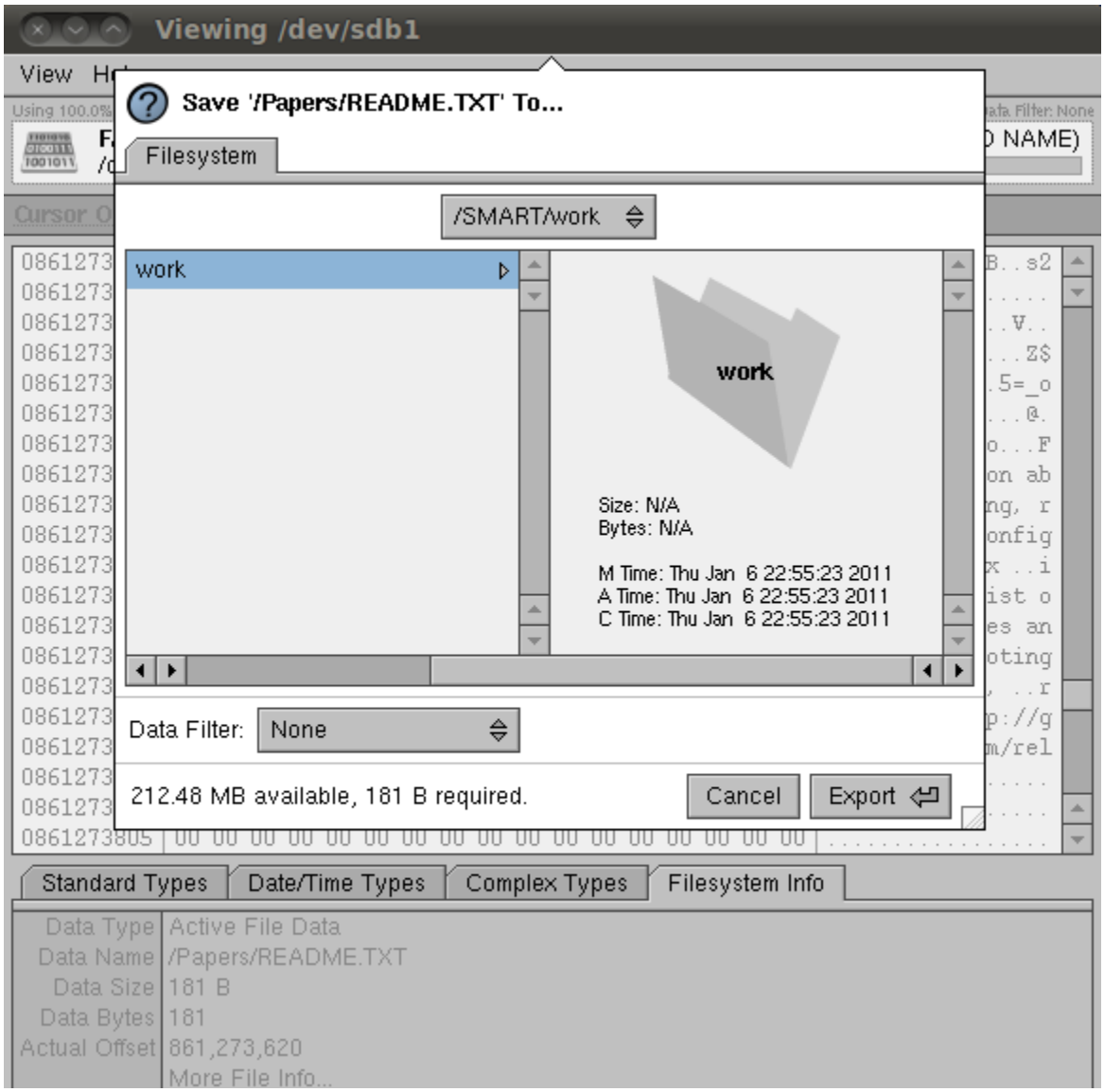
Εικόνα 21: Στοιχεία αρχείου

Από την επιλογή Filesystem →Produce Hash, μπορεί να παραχθεί μια τιμή hash αποκλειστικά για αυτό το αρχείο, ενώ με την επιλογή Export File γίνεται εξαγωγή του αρχείου για περαιτέρω ανάλυση.



Εικόνα 22: Επιλογές επεξεργασίας αρχείου

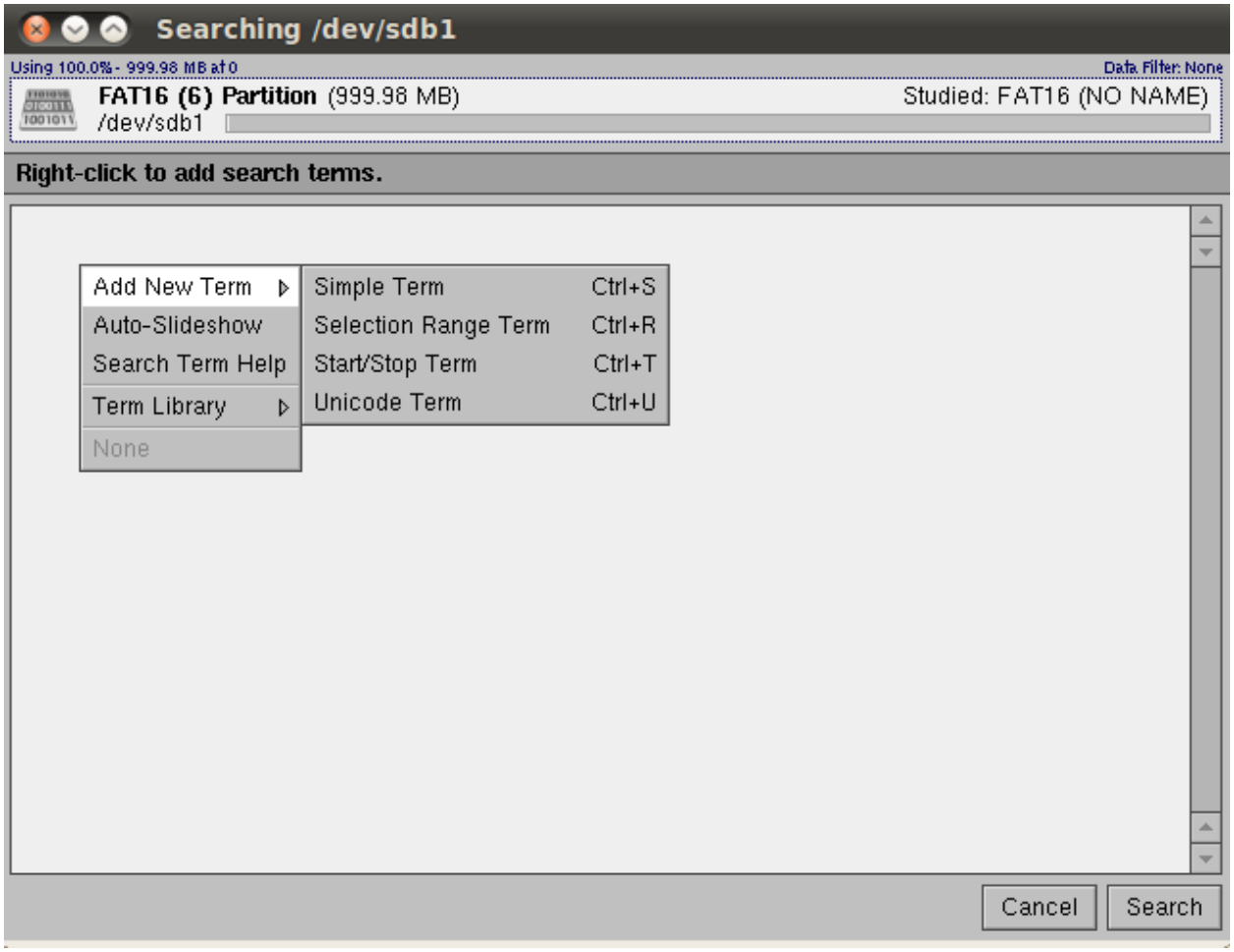
Το αρχείου που θέλουμε να εξάγουμε αποθηκεύεται σε έναν επιλεγμένο αποθηκευτικό χώρο, συνήθως στο χώρο εργασίας που δημιουργήθηκε από το εργαλείο για τη συγκεκριμένη ανάλυση.



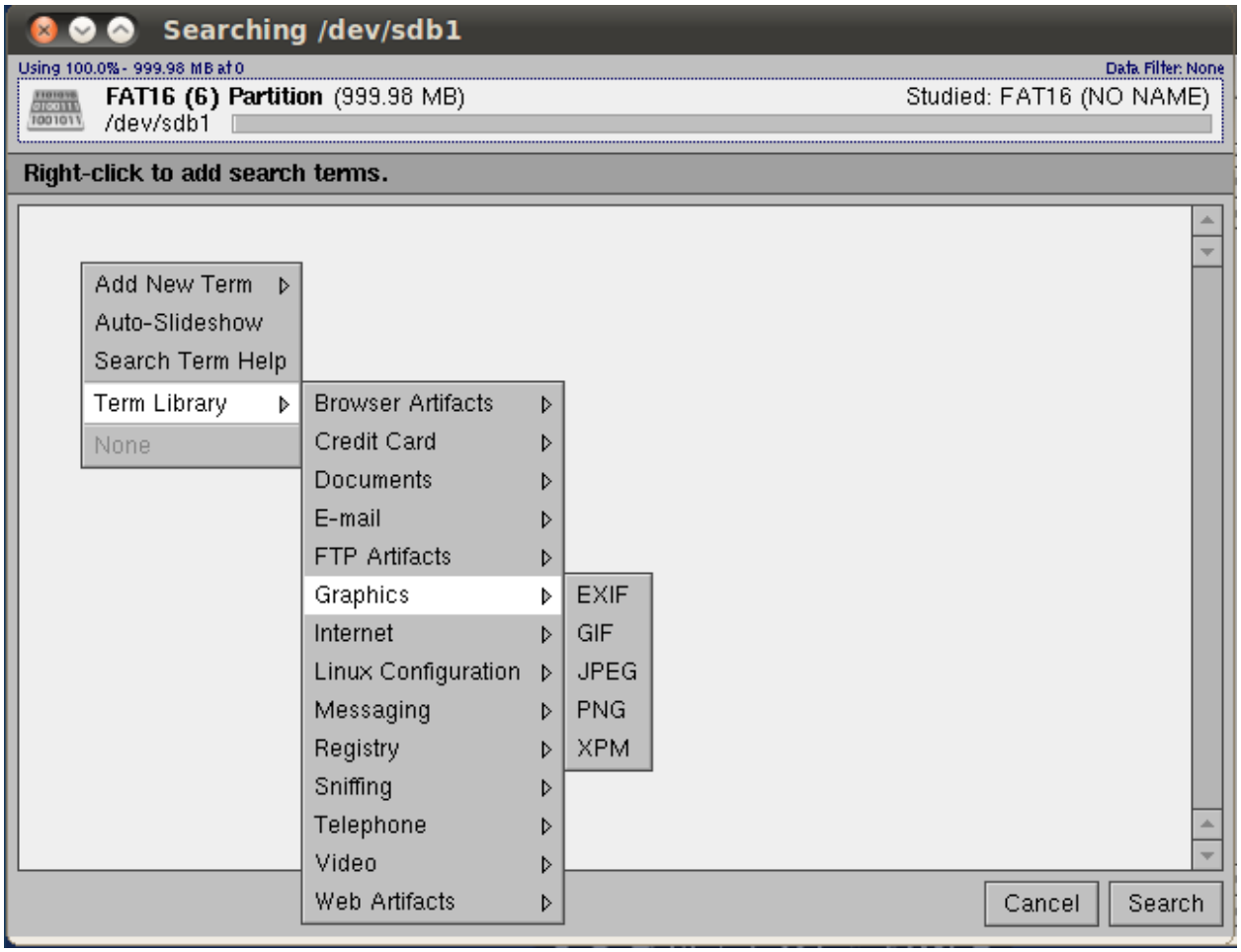
Εικόνα 23: Εξαγωγή αρχείου

Αναζήτηση αρχείων

Με την επιλογή της Αναζήτησης ο χρήστης μπορεί να επικεντρωθεί στα αρχεία που τον ενδιαφέρουν περισσότερο. Μπορεί να πραγματοποιηθεί είτε με την εισαγωγή μιας ή παραπάνω λέξεων που πιθανόν να περιέχεται σε κάποιο αρχείο ή με την επιλογή συγκεκριμένου όρου από τη βιβλιοθήκη όρων που διατίθεται.

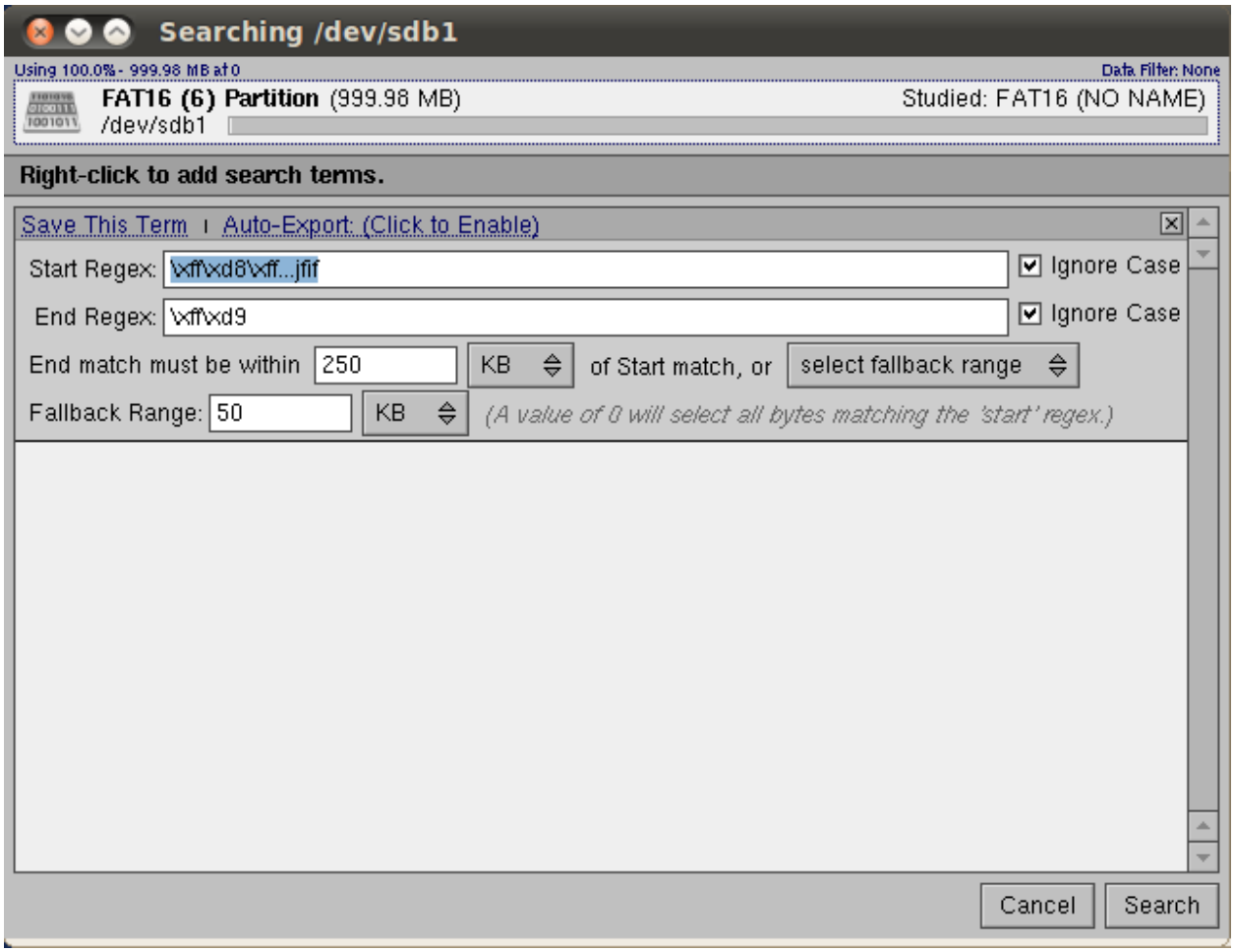


Εικόνα 24: Αναζήτηση με την εισαγωγή λέξης από τον χρήστη

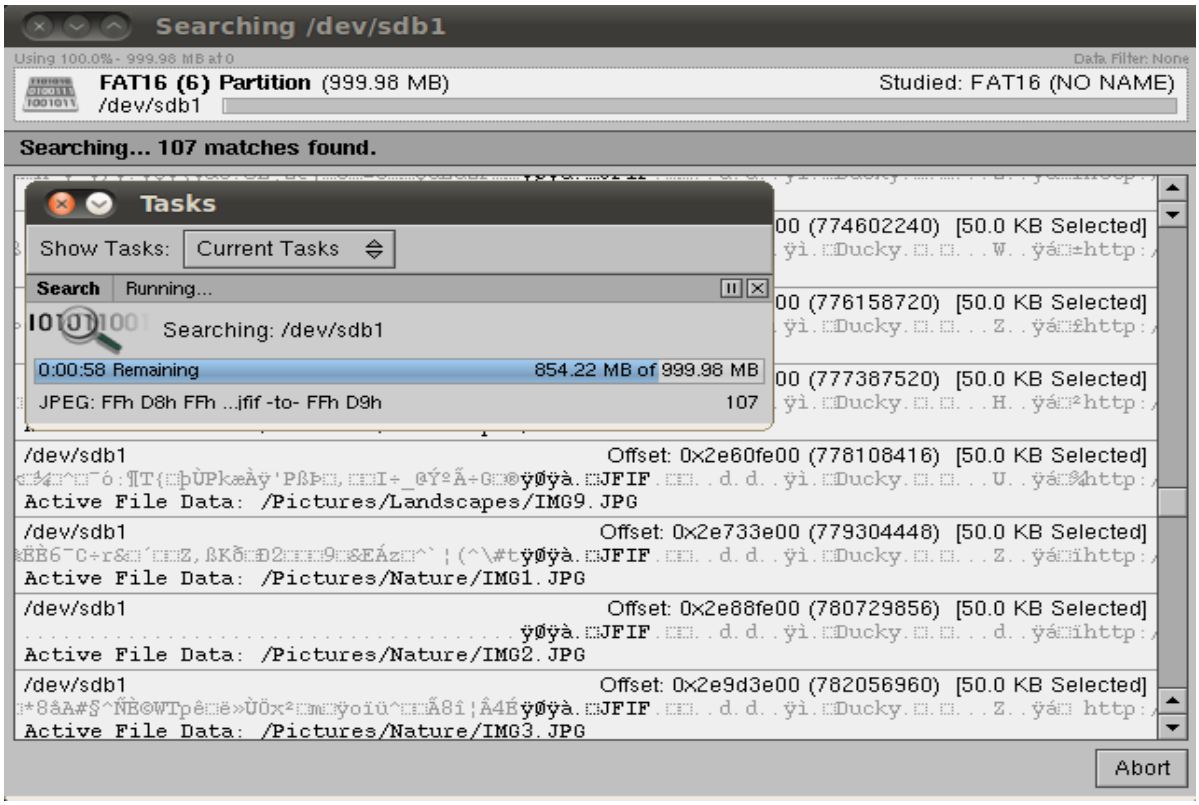


Εικόνα 25: Αναζήτηση συγκεκριμένου είδους αρχείου

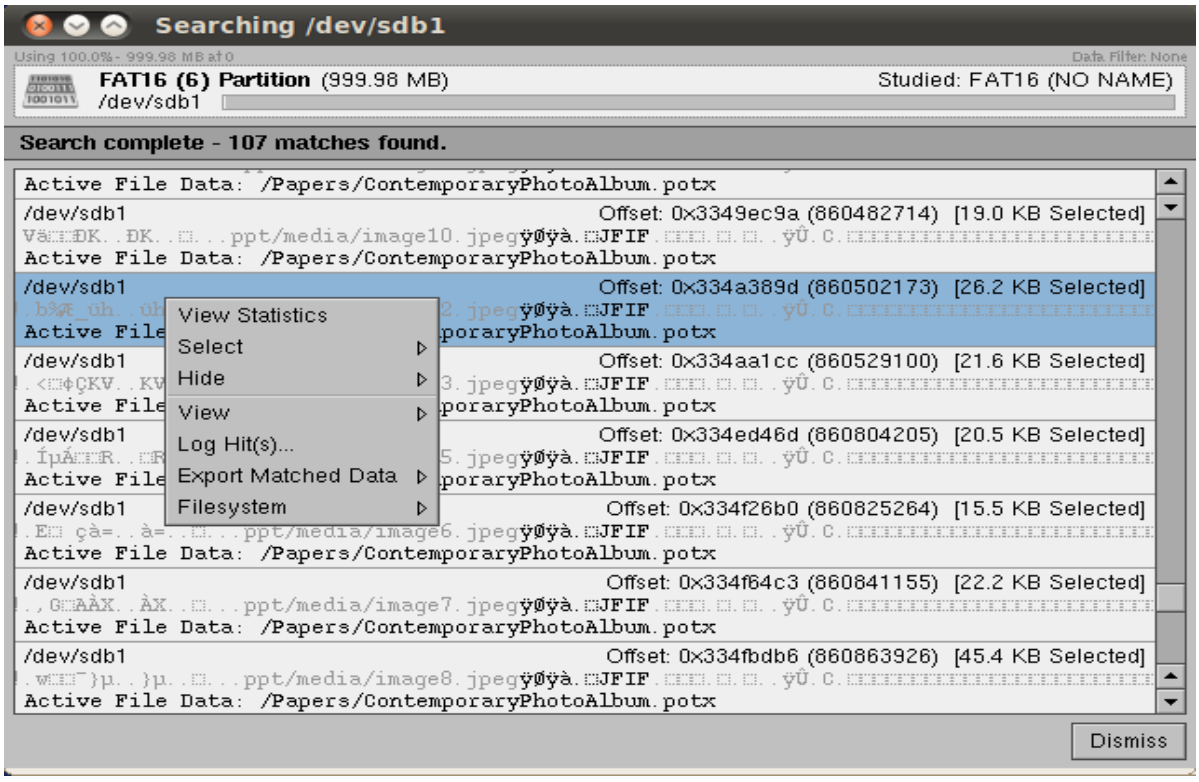
Στο συγκεκριμένο παράδειγμα επιλέχθηκε να γίνει αναζήτηση όλων των αρχείων εικόνας τύπου JPEG.



Εικόνα 26: Αναζήτηση αρχείων JPEG

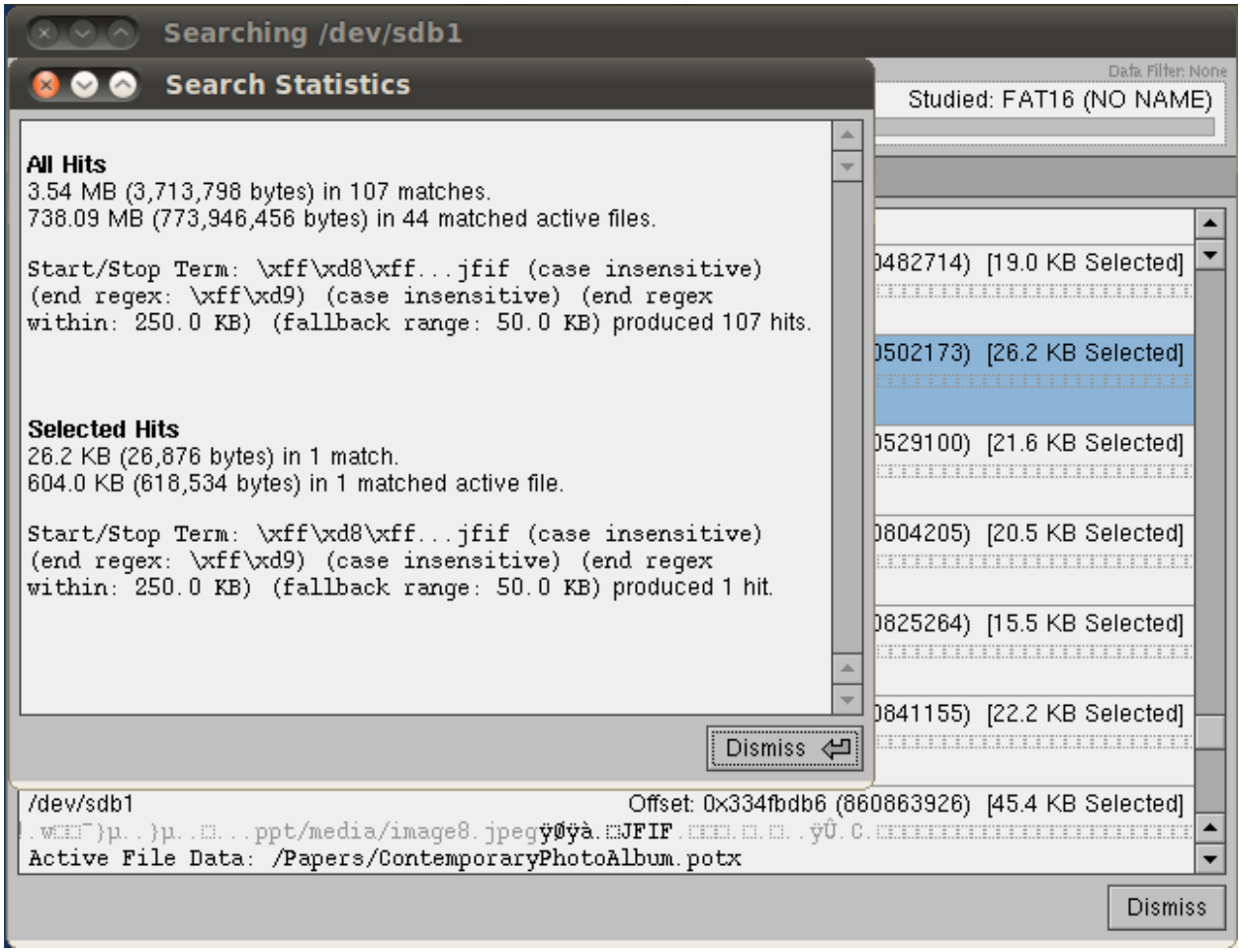


Εικόνα 27: Πραγματοποίηση αναζήτησης



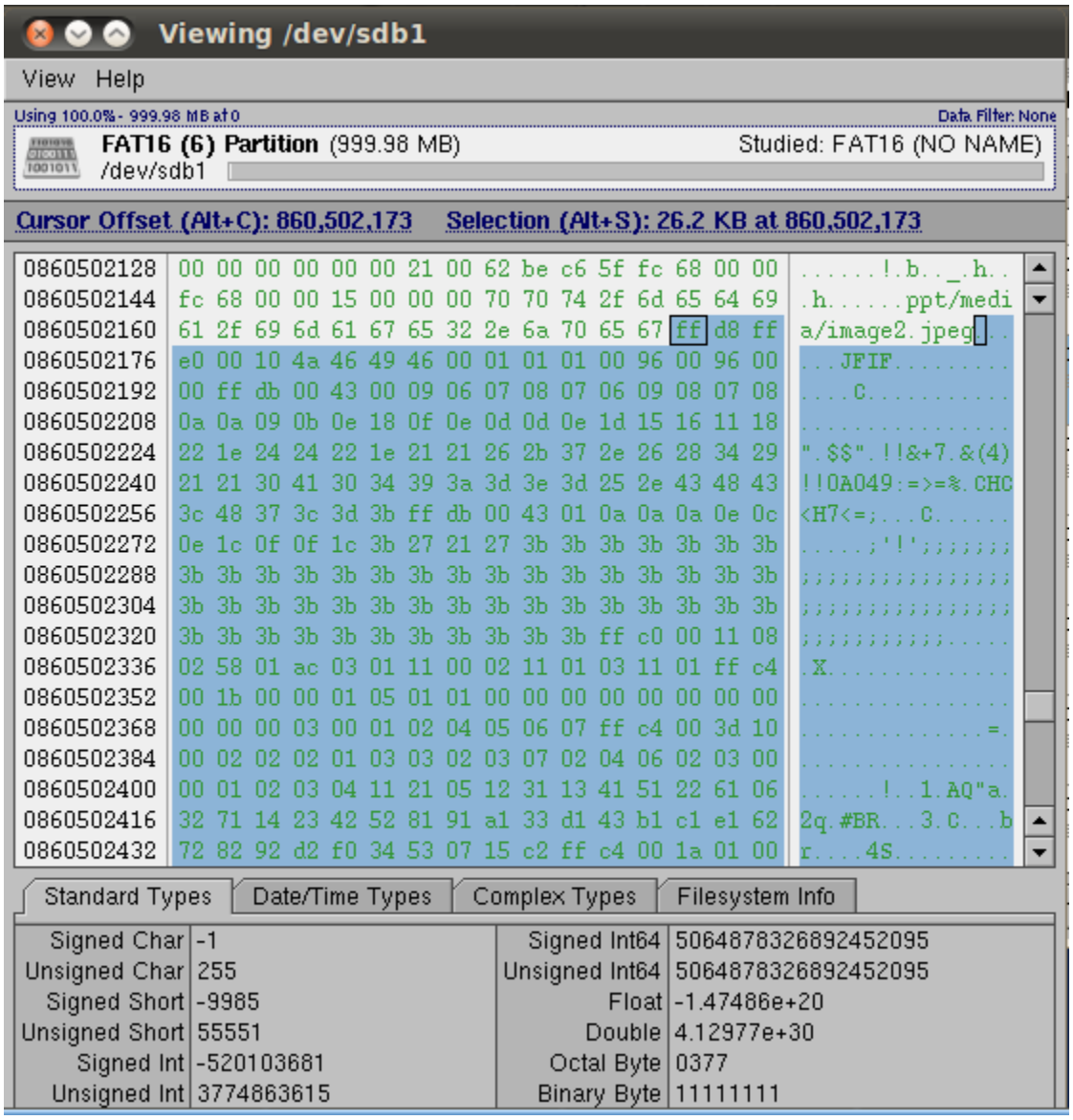
Εικόνα 28: Αποτελέσματα αναζήτησης

Μετά την ολοκλήρωση της αναζήτησης παρέχονται στατιστικές πληροφορίες με βάση τα αποτελέσματά της.



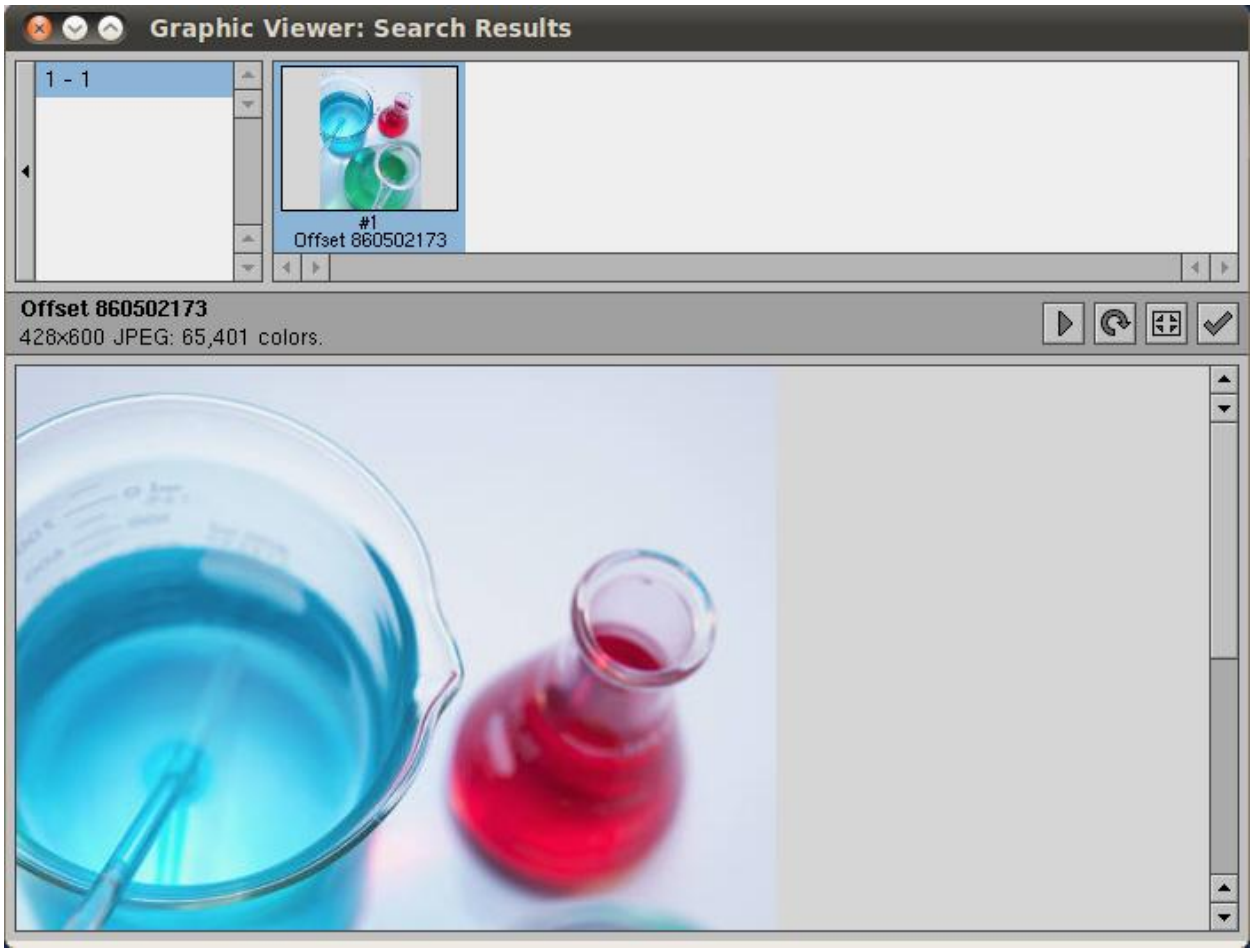
Εικόνα 29: Στατιστικά αναζήτησης

Η εμφάνιση ενός αρχείου από τα αποτελέσματα της αναζήτησης μπορεί να γίνει με τη μορφή που είναι αποθηκευμένο στο δίσκο όπου φαίνεται και η ακριβής θέση του.



Εικόνα 30: Εμφάνιση αρχείου ως Raw Data

Αλλά, δίνεται και η δυνατότητα εμφάνισης του αρχείου σε γραφική μορφή εφόσον είναι εφικτό.



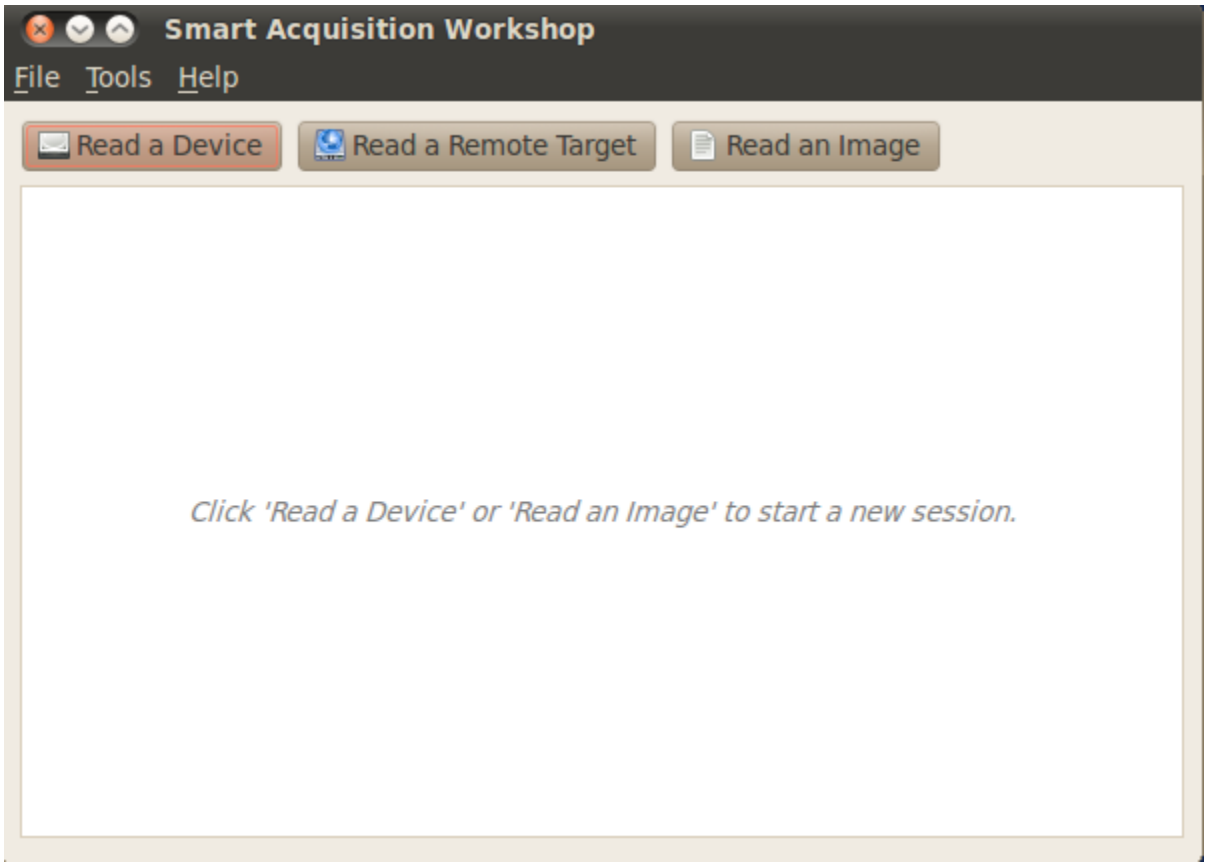
Εικόνα 31: Εμφάνιση αρχείου ως Graphic Data

Το SMART for Linux, εκτός από το βασικό εργαλείο SMART, περιέχει και τα:

- Smart Acquisition Workshop (SAW)
- SMART – Mount
- Grok – NTFS (NTFS visualization tool)
- Grok – LNK (NTFS link file analyzer)

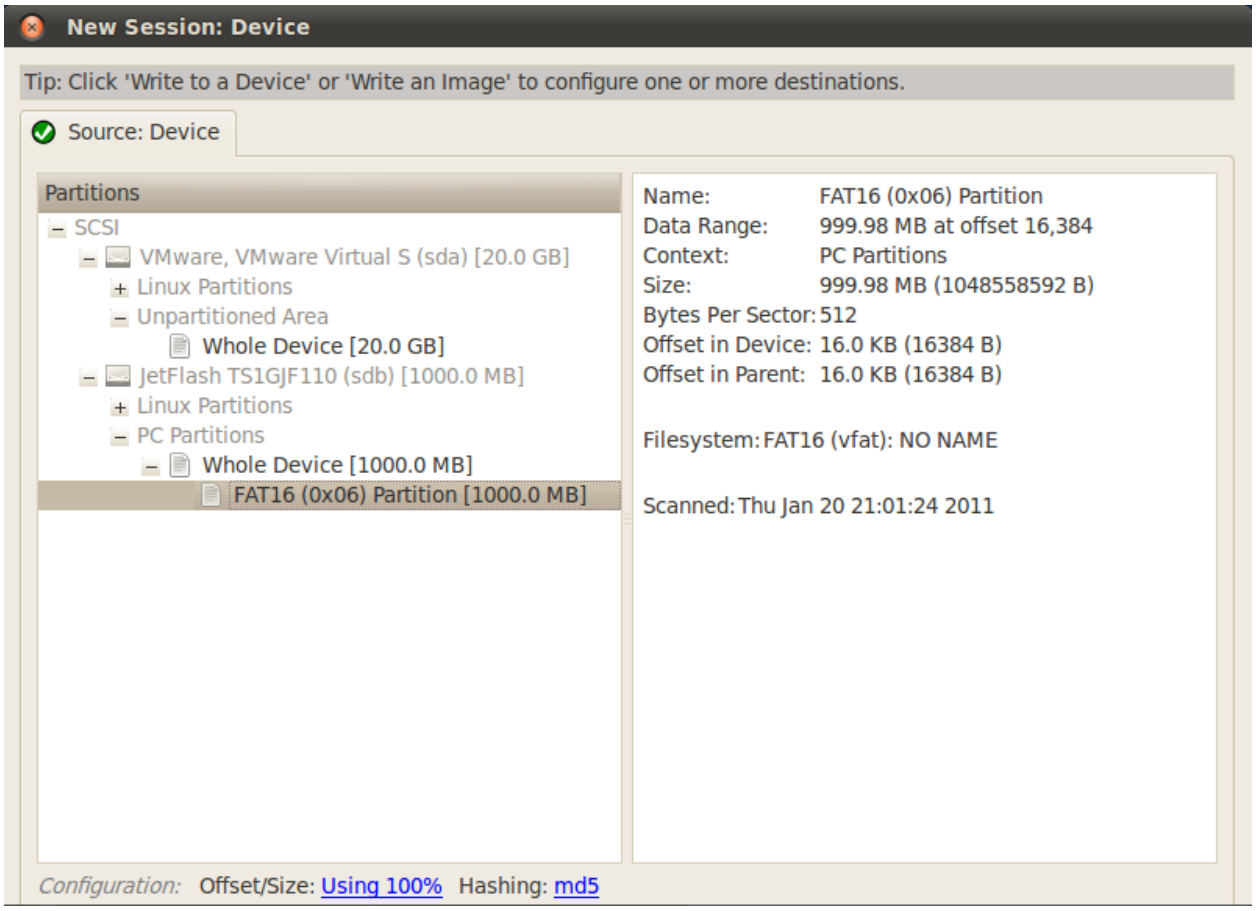
Παρακάτω δίνεται ένα δείγμα μόνο των δύο πρώτων εργαλείων, καθώς για τα δυο τελευταία δεν υπήρχε κατάλληλο NTFS σύστημα για τη δοκιμή τους.

Παρουσίαση Smart Acquisition Workshop



Εικόνα 32: SAW

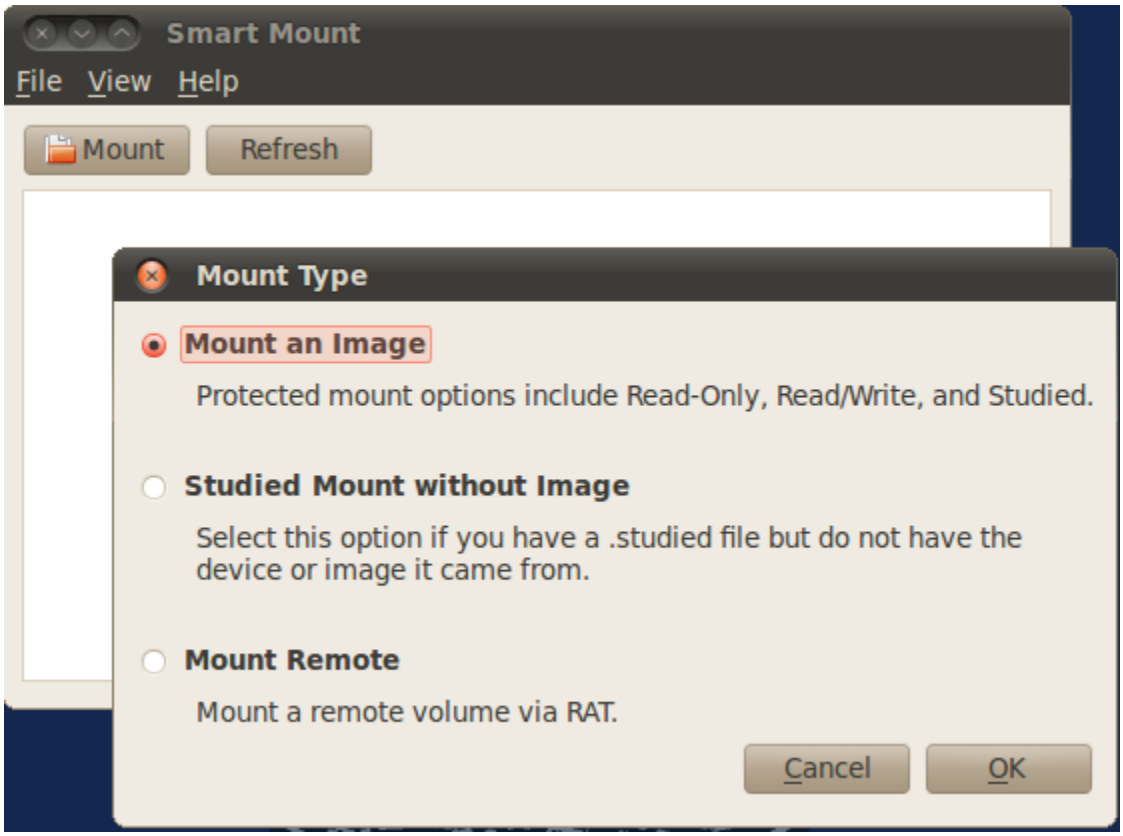
Με την επιλογή «Read a Device» γίνεται απόκτηση δεδομένων από μια αποθηκευτική συσκευή, στη συγκεκριμένη περίπτωση από τη συσκευή USB.



Εικόνα 33: Read a Device

Παρουσίαση Smart Mount

Επιλογή τύπου αρχείου για σύνδεση με το SMART.



Εικόνα 34: Smart Mount

Βιβλιογραφία

Βιβλία

1. **Βαζιργιάννης Μιχάλης, Χαλκίδη Μαρία. 2006.** *Εξόρυξη Γνώσης Από Βάσεις Δεδομένων Και Τον Παγκόσμιο Ιστό.* Αθήνα : τυπωθήτω - Γιώργος Δαρδανός, 2006.

2. **Casey, Eoghan. 2004.** *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* s.l. : Academic Press , 2004.

3. **Casey, Eoghan. 2010.** *Handbook of Digital Forensics and Investigation.* United States of America : Elsevier Inc, 2010.

4. **Johnson, Thomas A. 2005.** *Forensic Computer Crime Investigation.* s.l. : CRC Press, 2005.

5. **Linda Volonino, Reynaldo Anzaldua. 2008.** *Computer Forensics for Dummies.* Indianapolis, Indiana : Wiley Publishing, Inc, 2008.

6. **Shinder, Debra Littlejohn. 2002.** *Scene of the Cybercrime - Computer Forensics Handbook.* s.l. : Syngress Publishing, Inc., 2002.

Επιστημονικά Άρθρα

7. **Angela Orebaugh, Jeremy Allnutt. 2009.** *Classification of Instant Messaging Communications for Forensics Analysis.* s.l. : The International Journal of Forensic Computer Science, 2009.

8. **Boris Kovalerchuk, Evgenii Vityaev, Robert Holtfreter.** *Correlation of complex evidence in forensic accounting using data mining.* s.l. : Central Washington University Ellensburg, Russian Academy of Science.

9. **Bradley Schatz, George Mohay, Andrew Clark. 2006.** *A correlation method for establishing provenance of timestamps in digital evidence.* s.l. : Elsevier, 2006.

10. **Brian D. Carrier, Eugene H. Spafford. 2003.** *Getting Physical with the Digital Investigation Process.* s.l. : International Journal of Digital Evidence, 2003.

11. **Brian D. Carrier, Eugene H. Spafford . 2005.** *Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence.* New Orleans, LA : Digital Forensic Research Workshop, 2005.

12. **Brian D. Carrier, Eugene H. Spafford. 2004.** *An Event-Based Digital Forensic Investigation Framework.* s.1.: Purdue University, 2004

13. **Brian D. Carrier. 2005.** *File System Forensic Analysis.* s.l. : Addison Wesley Professional, 2005.

14. **Brian D. Carrier. September 2003.** *Open Source Digital Forensics Tools.* September 2003.

15. **Buchholz, Florian. 2007.** *An Improved Clock Model for Translating Timestamps.* s.l. : James Madison University, 2007.

16. **Christian S.J. Peron, Michael Legary.** *Digital Anti-Forensics: Emerging trends in data transformation techniques.*

17. **Ciardhuáin, Séamus Ó. 2004.** *An Extended Model of Cybercrime Investigations.* s.l. : International Journal of Digital Evidence, 2004.

18. **Cloppert, Michael. 2008.** *Ex-Tip: An Extensible Timeline Analysis Framework in Perl.* s.l. : SANS Institute, 2008.

19. *Computer Forensics - Part 1: An Intoduction to Computer Forensics.* s.1. : Information Security and Forensics Society (ISFS), 2004

20. *Computer Forensics - Part 2: Best Practices*. s.1. : Information Security and Forensics Society (ISFS), 2004

21. **Daniel J. Ryan, Gal Shpantzer.** *Legal Aspects of Digital Forensics.* s.l. : The George Washington University.

22. **Eric H. Holder, Eric H. Holder, John H. Laub. 2009.** *Test Results for Mobile Device Acquisition Tool:Paraben Device Seizure 3.1.* s.l. : National Institute of Justice, 2009.

23. **Eric H. Holder, Laurie O. Robinson, Kristina Rose. 2009.** *Test Results for Digital Data Acquisition Tool: EnCase 6.5.* s.l. : National Institute of Justice, 2009.

24. **Florian Buchholz, Brett Tjaden. 2007.** *A brief study of time.* s.l. : Elsevier, 2007.

25. **Forte, Dario. 2002.** *Analyzing the Difficulties in Backtracing Onion Router Traffic.* s.l. : International Journal of Digital Evidence, 2002.

26. **Georgios Pangalos, Vasilios Katos. 2009.** *Information Assurance and Forensic Readiness.* Greece : s.n., 2009.

27. **Gladyshev, Pavel. 2004.** *Formalising Event Reconstruction in Digital Investigations - Legal view of digital evidence.* 2004.

28. *Good Practice Guide for Computer-Based Electronic Evidence.* s.l. : Association of Chief Police Officers.

29. **Harris, Ryan. 2006.** *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem.* USA : Elsevier, 2006.

30. **Hosmer, Chet. 2002.** *Proving the Integrity of Digital Evidence with Time.* s.l. : International Journal of Digital Evidence, 2002.

31. **Hurlbut, Dustin. 2009.** *Fuzzy Hashing for Digital Forensic Investigators.* s.l. : AccessData, 2009.

32. **J. Philip Craiger, Mark Pollitt, Jeff Swauger. 2005.** *Law Enforcement and Digital Evidence.* s.l. : Handbook of Information Security, 2005.

33. **Jekot, Wayne. 2007.** *Computer Forensics, Search, Strategies and the Particularity Requirement.* s.l. : University of Pittsburgh Journal of Technology Law & Policy, 2007.

34. **Jens Olsson, Martin Boldt. 2009.** *Computer forensic timeline visualization tool.* s.l. : Elsevier, 2009.

35. **John Ashcroft, Deborah J. Daniels, Sarah V. Hart. 2003.** *Test Results for Disk Imaging Tools: SafeBack 2.18.* s.l. : National Institute of Justice, 2003.

36. **Kessler, Gary C.** *An Overview of Steganography for the Computer Forensics Examiner.* s.l. : Champlain College Burlington.

37. **Kessler, Gary C.** *Anti-Forensics and the Digital Investigator.*

38. **Kerr, Orin S. 2005.** *Digital evidence and the new criminal procedure*

39. **Lyle, James R. 2003.** *NIST CFTT: Testing Disk Imaging Tools.* s.l. : International Journal of Digital Evidence, 2003.

40. **Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota. 2006.** *Computer Forensics Field Triage Process Model.* s.l. : Conference on Digital Forensics, Security and Law, 2006.

41. **Maria Karyda, Lilian Mitrou.** *Internet Forensics: Legal and Technical Issues.* s.l. : University of the Aegean.

42. **Mark Reith, Clint Carr, Gregg Gunsch. 2002.** *An Examination of Digital Forensic Models.* s.l. : International Journal of Digital Evidence, 2002.

43. **Matthew Geiger, Lorrie Faith Cranor. 2005.** *Counter-Forensic Privacy Tools - A Forensic Evaluation.* s.l. : Carnegie Mellon University, 2005.

44. **Matthew Meyers, Marc Rogers.** *Computer Forensics: The Need for Standardization and Certification.* s.1.: International Journal of Digital Evidence

45. **April 2006.** *MD5 Collisions - The Effect on Computer Forensics.* s.l. : AccessData Corp., April 2006.

46. **Michael B. Mukasey, Jeffrey L. Sedgwick, David W. Hagy. 2008.** *Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14.* s.l. : National Institute of Justice, 2008.

47. **Nicole Lang Beebe, Jan Guynes Clark. 2005.** *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process.* s.l. : Digital Investigations Process Framework, 2005.

48. **OConnor, T.J. 2010.** *Grow Your Own Forensic Tools: A Taxonomy of Python Libraries Helpful for Forensic Analysis.* s.l. : SANS Institute, 2010.

49. **Panigrahi, P.K. 2006.** *Discovering Fraud in Forensic Accounting Using Data Mining Techniques.* s.l. : The Chartered Accountant, 2006.

50. **Pavel Gladyshev, Ahmed Patel. 2005.** *Formalising Event Time Bounding in Digital Investigations.* s.l. : International Journal of Digital Evidence, 2005.

51. **Philip Craiger, Paul K. Burke.** *Mac Forensics: Mac OS X and the HFS+ File System.*

52. **Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits. March 2005.** *First Responders Guide to Computer Forensics.* s.l. : CERT Training and Education, March 2005.

53. **Roussev Vassil, Golden G. Richard III.** *Digital Forensics*

54. **Rowlingson, Robert. 2004.** *A Ten Step Process for Forensic Readiness.* s.l. : International Journal of Digital Evidence, 2004.

55. **Rude, Thomas. 2003.** *Building a Linux Super Kernel for Data Forensics.* 2003.

56. **Salgado, Richard P. 2005.** *Fourth Amendment Search and the Power of the Hash.* s.l. : Harvard Law Review Association, 2005.

57. **Saudi, Madihah Mohd. 2001.** *An Overview of Disk Imaging Tool in Computer Forensics.* s.l. : SANS Institute, 2001.

58. **Venansius Baryamureeba, Florence Tushabe. 2004.** *The Enhanced Digital Investigation Process Model.* s.l. : Institute of Computer Science, Makerere University, 2004.

59. **Weil, Michael C. 2002.** *Dynamic Time & Date Stamp Analysis.* s.l. : International Journal of Digital Evidence, 2002.

60. **Willassen, Svein Yngvar. 2008.** *Finding Evidence of Antedating in Digital Investigations.* s.l. : Norwegian University of Science and Technology, 2008.

61. **Willassen, Svein Yngvar. 2008.** *Timestamp evidence correlation by model based clock hypothesis testing.* s.l. : Norwegian University of Science and Technology, 2008.

62. **Zeno Geradts, Jurrien Bijhold.** *Data Mining in Forensic Image Databases.* s.l. : Netherlands Forensic Institute.

63. **Morgan, Carrie M. 2002.** *An Historical Perspective of Digital Evidence: A Forensic Scientist's View.* s.1: International Journal of Digital Evidence, 2002

64. **Chisholm, Colin. 2010.** *Integrating Forensic Investigation Methodology into eDiscovery*. SANS Institute, 2010

Νομικό Πλαίσιο

65. Οδηγία 2002/58/ΕΚ. s.l. : Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων

66. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

67. 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)

68. Σύνταγμα της Ελλάδας, όπως αναθεωρήθηκε με το Ψήφισμα της 27ης Μαΐου 2008 της Η' Αναθεωρητικής Βουλής των Ελλήνων

69. Νόμος 2472/1997 για τη προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τροποποιήσεις

70. Ποινικός Κώδικας

Σύνδεσμοι

71. Scientific Working Group on Digital Evidence, http://www.swgde.org/
72. Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Main_Page
73. Convention On Cybercrime, Budapest 23.11.2001, Council Of Europe, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
74. Forensics Wikipedia, http://www.forensicswiki.org/wiki/Main_Page

Σύνδεσμοι για Εργαλεία Forensic

75. Access Data – Forensic Toolkit (FTK), http://accessdata.com/
76. Guidance Software – EnCase, http://www.guidancesoftware.com/
77. Paraben – P2 Commander, Device Seizure, http://www.paraben.com/index.html
78. The Sleuth Kit, http://www.sleuthkit.org/
79. Forensics intl – SafeBack, http://www.forensics-intl.com/safeback.html
80. Open Computer Forensics Architecture – OCFA, http://sourceforge.net/apps/trac/ocfa/wiki
81. ASR Data – SMART, http://www.asrdata.com/
82. Microsoft - Computer Online Forensic Evidence Extractor, http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

Σύνδεσμοι για Εργαλεία Anti - Forensic

83. The GNU Privacy Guard, http://www.gnupg.org/
84. OpenSSL Project, http://www.openssl.org/
85. OpenVPN, http://openvpn.net/
86. Stunnel – Multiplatform SSL tunneling proxy, http://www.stunnel.org/

87. True Crypt – Free open-source on-the-fly encryption, http://www.truecrypt.org/
88. Spychecker – S-Tools, http://www.spychecker.com/program/stools.html
89. Mp3 Stego, http://www.petitcolas.net/fabien/steganography/mp3stego/index.html
90. Invisible Secrets 4, http://www.invisiblesecrets.com/
91. Metasploit Anti-Forensics Project, http://www.metasploit.com/research/projects/antiforensics/
92. Webroot Window Washer, http://www.webroot.com/En_US/consumer-products-windowwasher.html
93. CyberScrub, http://www.cyberscrub.com/en/
94. Evidence Eliminator, http://www.evidence-eliminator.com/
95. Neoimagic - Windows & Internet Cleaner Pro, http://www.neoimagic.com/windows-internet-cleaner/