



Ιόνιο Πανεπιστήμιο

Τμήμα Πληροφορικής

Πτυχιακή Εργασία

Δημιουργία Εκπαιδευτικής Άσκησης Ψηφιακής Εγκληματολογίας



Κωνσταντίνα Ηλιοπούλου (Α.Μ: Π2018070)

Τριμελής Εξεταστική Επιτροπή

1. Χριστόφορος Νταντογιάν (Επιβλέπων καθηγητής)
2. Ελένη Χριστοπούλου (Μέλος)
3. Άννα Σωτηροπούλου (Μέλος)

Κέρκυρα, 2023

Πίνακας Περιεχομένων

Περίληψη.....	3
Abstract.....	4
Κεφάλαιο 1^ο : Εισαγωγή.....	5
1.1: Σκοπός και Αντικείμενο Μελέτης.....	5
1.2: Δομή Διπλωματικής Εργασίας.....	5
1.3: Ψηφιακή Εγκληματολογία.....	5
1.4: Αντί – Εγκληματολογία.....	10
1.5: Σχετική Έρευνα.....	12
Κεφάλαιο 2^ο : Νομικό Πλαίσιο.....	14
2.1: Γενικό Πλαίσιο.....	14
2.2: Ισχύουσα κατάσταση στην Ελλάδα.....	16
2.3: Αρχή ιδιωτικότητας στον χώρο εργασίας.....	18
Κεφάλαιο 3^ο : Προστασία ιδιωτικότητας σε περιβάλλον ψηφιακής εγκληματολογίας.....	20
3.1: Ψηφιακά Πειστήρια.....	21
3.2: Ιδιωτικότητα κατά την εύρεση ψηφιακών πειστηρίων.....	21
3.3: Παραδεκτό ψηφιακών πειστηρίων.....	24
3.4: Διαδικασία συλλογής ψηφιακών πειστηρίων.....	25
Κεφάλαιο 4^ο : Στάδια ψηφιακής εγκληματολογικής ανάλυσης.....	28
4.1: Εντοπισμός Συσκευών.....	28
4.2: Εξαγωγή και Διατήρηση Δεδομένων.....	28
4.3: Αξιολόγηση και Ανάλυση της Σκηνής Εγκλήματος.....	29
4.4: Τεκμηρίωση της Σκηνής Εγκλήματος.....	29
4.5: Παρουσίαση.....	30
Κεφάλαιο 5^ο : Εργαλεία Ψηφιακής Εγκληματολογίας.....	31
5.1: Εργαλεία Συλλογής και Ανάλυσης Ψηφιακών Αποτυπωμάτων.....	31
5.2: Εμπορικά Προϊόντα.....	32
5.3: Ελεύθερου Λογισμικού.....	34
Κεφάλαιο 6^ο : Σενάριο.....	37
Κεφάλαιο 7^ο : Βιβλιογραφία.....	46

Περίληψη

Ως άνθρωποι με κρίση και εν συναίσθηση, ανησυχούμε για εκείνους που αγαπάμε και κυρίως για εμάς τους ίδιους. Τι είναι όμως αυτό που μας κάνει να αντιδράμε έτσι; Φοβόμαστε για την υπόληψή μας; Για την περιουσία μας; Ή μήπως για την ίδια μας τη ζωή; Μπορούν να καταστραφούν όλα σε μια στιγμή;

Σήμερα, συχνό είναι το φαινόμενο να μοιράζουμε προσωπικές και μη στιγμές μας στο διαδίκτυο. Δυστυχώς, πολλοί είναι εκείνοι που εκμεταλλεύονται οποιαδήποτε ευάλωτη στιγμή μας, είτε με εκβιασμούς και απειλές ή ακόμα και με ψυχολογικές πιέσεις. Αυτομάτως, οι πράξεις αυτές χαρακτηρίζονται ως ηλεκτρονικά εγκλήματα και επιβάλλεται να αναφερθούν στην αρμόδια Αρχή, ώστε να αντιμετωπιστούν.

Η ομάδα αντιμετώπισης συνεργάζεται με τον ειδικό αναλυτή ψηφιακών εγκλημάτων, ο οποίος είναι υπεύθυνος για την αναγνώριση, τη διατήρηση, την ανάλυση και την παρουσίαση των ψηφιακών πειστηρίων για το έγκλημα που διαπράττεται. Σε αυτόν τον κλάδο επιστήμης, ψηφιακή εγκληματολογία, όπως λέγεται, ο ερευνητής πρέπει να είναι ιδιαίτερα προσεκτικός με τα πειστήρια που θα υποβάλλει, καθώς η τελική έκθεση θα περάσει από νομικό έλεγχο.

Στη συγκεκριμένη εργασία, έχουμε δημιουργήσει μια εκπαιδευτική άσκηση ψηφιακής εγκληματολογίας η οποία πραγματεύεται ένα σενάριο ηλεκτρονικού εγκλήματος. Η υπόθεση είναι βασισμένη σε αληθινά γεγονότα, αλλά οι χαρακτήρες, τα ονόματα, τα περιστατικά, οι τοποθεσίες και οι διάλογοι αποτελούν μυθοπλασία.

Abstract

As people of judgment and awareness, we worry about those we love and, above all, about ourselves. But what is it that makes us react this way? Do we fear for our reputation? For our property? Or is it our own lives? Can it all be destroyed in an instant?

Nowadays, it is common to share our personal and non-personal moments online. Unfortunately, there are many who take advantage of any of our vulnerable moments, either through blackmail and threats or even psychological pressure. Automatically, these acts are classified as cybercrimes and must be reported to the competent authority so that they can be dealt with.

The response team works with the dedicated digital crime analyst, who is responsible for identifying, preserving, analyzing and presenting the digital evidence of the crime committed. In this branch of science, digital forensics, as it is called, the investigators must be especially careful with the evidence they submit, as the final report will go through legal scrutiny.

In this paper, we have created a digital forensics training exercise which deals with a cybercrime scenario. The case is based on real events, but the characters, names, incidents, locations and dialogues are fiction.

Κεφάλαιο 1^ο : Εισαγωγή

1.1 Σκοπός και Αντικείμενο Μελέτης

Σκοπός αυτής της εργασίας είναι να παρουσιαστούν οι μέθοδοι ανάλυσης του ψηφιακού εγκλήματος από τη σκοπιά του ειδικού ερευνητή. Μέσα από την εργασία, θα γίνει κατανοητό το πόσο επικίνδυνο είναι να μοιραζόμαστε πληροφορίες στα κοινωνικά δίκτυα, καθώς το βρίσκουμε ως τον πιο εύκολο κι άμεσο παράγοντα διευκόλυνσης των σχέσεων μας. Θα εξετάσουμε την ανίχνευση του ψηφιακού εγκλήματος, καλύπτοντας θέματα όπως, διαδικτυακός εκφοβισμός και πορνογραφία.

Αντικείμενο της εργασίας είναι η ανάλυση ενός εγκλήματος στον κυβερνοχώρο, περιλαμβάνοντας ζωντανά και ελκυστικά χαρακτηριστικά, όπως παραδείγματα σε πλαίσια με μοναδικά γεγονότα και πρόσωπα, καθώς και αποσπάσματα από συνομιλίες και παραβατικές συμπεριφορές. Επιπλέον, στη σχετική βιβλιογραφία παρουσιάζεται ο τρόπος συλλογής αποδεικτικών στοιχείων που προκύπτουν από την υπόθεση.

1.2 Δομή Διπλωματικής Εργασίας

- Στο **1^ο κεφάλαιο** αναφέρονται το πλαίσιο και οι ερευνητικοί στόχοι της εργασίας.
- Στο **2^ο κεφάλαιο** παρατίθεται το νομικό πλαίσιο που ισχύει για τα ψηφιακά πειστήρια και την ισχύουσα κατάσταση στην χώρα μας.
- Το **3^ο κεφάλαιο** εστιάζει στην προστασία της ιδιωτικότητας στο περιβάλλον της ψηφιακής εγκληματολογίας.
- Στο **4^ο κεφάλαιο** εστιάζουμε στα στάδια της εγκληματολογικής ανάλυσης.
- Στο **5^ο κεφάλαιο** παρατίθενται τα σχετικά εργαλεία συλλογής ψηφιακών αποτυπωμάτων.
- Στο **6^ο κεφάλαιο** αναλύεται το σενάριο ψηφιακής εγκληματολογίας και οι πρακτικές μέθοδοι διερεύνησης του ηλεκτρονικού εγκλήματος.
- Στο **7^ο κεφάλαιο** παρουσιάζεται η σχετική βιβλιογραφία και τα συμπεράσματα της έρευνας.

1.3 Ψηφιακή Εγκληματολογία

Όπως και στα εγκλήματα που διαπράττονται στον φυσικό κόσμο, τις περισσότερες φορές οι δράστες μετά το πέρασμά τους αφήνουν, είτε γενετικό υλικό, είτε διάφορα άλλα ίχνη και στοιχεία, που είναι ικανά να οδηγήσουν τους ερευνητές στην λύση του εγκλήματος. Έτσι και στα ψηφιακά εγκλήματα οι διαφορές δεν είναι μεγάλες εκτός του ότι τα ίχνη είναι ηλεκτρονικά. Σε αυτό το σημείο ξεκινάει ο ρόλος της Ψηφιακής Εγκληματολογίας (Digital Forensics) που ασχολείται - εκτός των άλλων - και με την ανάκτηση χαμένων πληροφοριών, ανάλυση ψηφιακών αποδείξεων - ακόμα και αναπαράσταση του ψηφιακού εγκλήματος.

Ως Ψηφιακή Εγκληματολογία ορίζεται η χρήση επιστημονικά προερχόμενων και αποδεδειγμένων μεθόδων για τη διατήρηση, συλλογή, επικύρωση, αναγνώριση, ανάλυση, ερμηνεία, καταγραφή και παρουσίαση των ψηφιακών αποδείξεων που προέρχονται από ψηφιακές πηγές και έχουν ως σκοπό τη διευκόλυνση, ανακατασκευή και αναπαράσταση εγκληματικών ενεργειών. Ο όρος αυτός χρησιμοποιήθηκε στο πρώτο Digital Forensic Research Workshop (DRFWS) που διεξήχθη το 2001 στην Νέα Υόρκη θέλοντας να καλύψει όλα τα ψηφιακά μέσα που έχουν τη δυνατότητα να αποθηκεύσουν δεδομένα. Κάποια που εκείνη την εποχή είχαν αυτήν την ικανότητα ήταν τα κινητά τηλέφωνα, τα δίκτυα και οι ασύρματες συσκευές.

Με την εξέλιξη της τεχνολογίας και την όλο αυξανόμενη χρήση υπολογιστών, ψηφιακών συσκευών και δικτύων, η Ψηφιακή Εγκληματολογία έχει αναδειχθεί ως σημαντική επιστήμη για την ανάκτηση χρήσιμων ψηφιακών δεδομένων που θα οδηγήσουν τελικά στον εντοπισμό κακόβουλων ενεργειών. Για τη διασφάλιση ότι τα αποτελέσματα είναι αποδεκτά στο δικαστήριο, οι επιστήμες αυτού του είδους είναι υποχρεωμένες να ακολουθούν τις βασικές αρχές της τεχνολογίας μαζί με επικυρωμένες και διαδικασίες.

Ο όρος της ψηφιακής δικανικής (Digital Forensics) αρχικά χρησιμοποιήθηκε ως συνώνυμο του όρου της δικανικής υπολογιστών (Computer Forensics), στη συνέχεια, όμως, επεκτάθηκε ο ορισμός του καλύπτοντας όλες τις συσκευές οι οποίες είναι ικανές να αποθηκεύσουν ψηφιακά δεδομένα, περιλαμβάνοντας τις κινητές συσκευές, τις βάσεις δεδομένων και τα δίκτυα, και αυτή τη στιγμή ο όρος μπορεί να χρησιμοποιηθεί ώστε να περιγράψει το σύνολο του κλάδου της ψηφιακής εγκληματολογίας. Με τον όρο Digital Forensics εννοούμε το γνωστικό αντικείμενο που προσπαθεί να ανιχνεύσει αποδεικτικά στοιχεία για εγκληματικές πράξεις ερευνώντας ψηφιακά τεκμήρια. Τα εγκλήματα μπορεί να είναι είτε ψηφιακά (κλοπή κωδικών, hacking σε τραπεζικούς λογαριασμούς, παιδική πορνογραφία κτλ.) είτε τα κλασικά εγκλήματα που συνήθως εξετάζουμε (κλοπές, ληστείες, δολοφονίες, απαγωγές) τα οποία χρησιμοποιούν τους ηλεκτρονικούς υπολογιστές ως μέσο τέλεσης.

Ως κλάδος της εγκληματολογίας εμφανίστηκε τη δεκαετία του 1980 και έκτοτε αναπτύσσεται συνεχώς περνώντας από τους προσωπικούς υπολογιστές στα δίκτυα και πλέον στα κινητά τηλέφωνα. Οι Biros και Weiser (2006) ορίζουν την ψηφιακή εγκληματολογία ως «επιστημονικές γνώσεις και μεθόδους που εφαρμόστηκαν για τον εντοπισμό, τη συλλογή, διατήρηση, εξέταση και ανάλυση των πληροφοριών που αποθηκεύονται ή μεταδίδονται σε δυαδική μορφή κατά τρόπο νομικά αποδεκτό, με στόχο τη χρήση του σε δικαστηριακή διαδικασία». Η ψηφιακή εγκληματολογική έρευνα απαιτεί καθορισμένες διαδικασίες που συμμορφώνονται με τη βιομηχανική πρακτική, οργανωτική πρακτική και κατάλληλη νομοθεσία, είτε ως μέρος της ποινικής έρευνας ή ως μέρος μιας γενικότερης αντιμετώπισης περιστατικών ασφαλείας. Η τεχνική και τα εργαλεία που χρησιμοποιούνται από τους ερευνητές της ψηφιακής δικανικής μπορεί να ποικίλλουν, ωστόσο, η διαδικασία κατά κύριο λόγο περιλαμβάνει τον σχεδιασμό, την απόκτηση των δεδομένων-στοιχείων, τη διατήρησή τους, την ανάλυσή τους και την υποβολή εκθέσεων.

Η παρουσίαση των ψηφιακών αποδεικτικών στοιχείων είναι μια μοναδική νομική πρόκληση που αντιμετωπίζουν τεχνικοί της ψηφιακής δικανικής (Kenneally, 2002). Η ψηφιακή δικανική, τελικά, αποτελεί το μεγαλύτερο και πιο πολύπλοκο κομμάτι της δικανικής επιστήμης και αποτελεί επιταγή της συχνά χαρακτηριζόμενης ως «ψηφιακή» εποχής μας. Η ψηφιακή εγκληματολογία είναι απαραίτητη για την επιτυχή δίωξη των ψηφιακών εγκληματιών, οι οποίοι χρησιμοποιούν διαφορετικές ψηφιακές συσκευές, όπως συσκευές υπολογιστών, δικτύου, κινητές συσκευές και συσκευές αποθήκευσης. Η ψηφιακή εγκληματολογική έρευνα, προκειμένου να αποκτήσει τις αποδείξεις που θα είναι αποδεκτές στο δικαστήριο πρέπει να ακολουθήσει μια συγκεκριμένη χαρτογραφημένη διαδικασία.

Οι έρευνες που πραγματοποιούνται στο πλαίσιο της ψηφιακής δικανικής παρουσιάζουν μεγάλη ποικιλομορφία. Τυπικά περιλαμβάνουν αποδεικτικά στοιχεία που ανακτήθηκαν από υπολογιστικά συστήματα, από το διαδίκτυο, ή από διερευνήσεις εισβολών σε δίκτυα. Η ψηφιακή εγκληματολογία επικεντρώνεται στην ανάπτυξη αποδείξεων που σχετίζεται με τον ψηφιακό κόσμο για χρήση αυτών σε ποινικές ή και αστικές δικαστικές διαδικασίες και με σκοπό τη διευκόλυνση ή τη βελτίωση της ανασυγκρότησης των γεγονότων που αφορούν την υπόθεση. Επίσης, μπορεί να χρησιμοποιηθεί για να αναγνωρισθεί ένα έγκλημα, να ταυτοποιηθούν ύποπτοι, να επαληθευτούν ή μη οι ισχυρισμοί διαδίκων και μαρτύρων αλλά ακόμη και να αποδειχθεί η αυθεντικότητα των προσκομισθέντων ως «σχετικών» εγγράφων. Ερευνώντας σκληρούς δίσκους και email, οι ερευνητές συχνά καταφέρνουν να εξιχνιάσουν εγκληματικές ενέργειες. Η έρευνα μπορεί να περιλαμβάνει σκληρούς δίσκους, έλεγχο του υπολογιστή ενώ βρίσκεται σε λειτουργία (για να καταγραφεί π.χ. ο κωδικός πρόσβασης), ακόμη και διαγραμμένα αρχεία. Πολυάριθμες μέθοδοι έχουν προταθεί για την ψηφιακή εγκληματολογία, ωστόσο, όλες διαφέρουν μεταξύ τους, με μοναδικό κοινό τη διατήρηση της ακεραιότητας του πρωτοτύπου των αποδεικτικών στοιχείων και την εξαγωγή πληροφοριών που έχουν αξία για την εκάστοτε υπόθεση. Αξιοσημείωτο είναι δε, ότι σε κάθε μεθοδολογία επικρατεί η αντίληψη ότι το αρχικό αποδεικτικό υλικό είναι τεράστιο σε μέγεθος, αλλά η «σημαντική» πληροφορία είναι ένα υποσύνολο, συχνά ένα πολύ μικρό υποσύνολο των αρχικών αποδείξεων.

Από τεχνικής απόψεως, έχουν αναπτυχθεί αρκετά εργαλεία προκειμένου να υποστηρίξουν τις έρευνες ψηφιακής εγκληματολογίας, μερικά από τα οποία είναι τα εξής : EnCase, Forensic Toolkit και το Sleuth Kit, όπως θα παρουσιαστούν σε επόμενη ενότητα. Τα περισσότερα εργαλεία χρησιμοποιούν τη δομή file system, file type, string searches, και hash value συγκρίσεις, ενώ επίσης έχουν προταθεί και κάποιες καινοτόμες προσεγγίσεις, όπως η εξόρυξη δεδομένων (data mining) και η ανάλυση των κοινωνικών δικτύων. Σε όλες τις μεθοδολογίες, τα ψηφιακά κομμάτια εντάσσονται στο πλαίσιο της υπόθεσης, σε κάθε περίπτωση, όμως, η συλλογή τους χρειάζεται να είναι σύννομη.

Αξιοσημείωτο είναι ότι στις Ηνωμένες Πολιτείες, η αποδοχή των επιστημονικών αποδείξεων στην ακροαματική διαδικασία συνδέεται με έναν μάρτυρα πραγματογνώμονα, ο οποίος παρουσιάζει τα αποδεικτικά στοιχεία στο δικαστήριο. Το στοιχείο αυτό το παρατηρούμε και στην ελληνική έννομη τάξη. Ένα εκτεταμένο σώμα της αμερικάνικης νομοθεσίας ασχολείται με τη σχέση μεταξύ των αποδεικτικών στοιχείων, του εξεταστή και τη μαρτυρία. Δύο σημαντικά στοιχεία είναι η εμπειρική

φύση της διαδικασίας της εξέτασης από τη μία πλευρά και η ικανότητα του εξεταστή να εξηγήσει τη μέθοδο που εφάρμοσε για να συλλέξει τα αποδεικτικά στοιχεία. Στο παραδοσιακό αυτό μοντέλο, είναι σημαντικό η διαδικασία της εξέτασης να διεξάγεται σε ένα «forensically sound» τρόπο, δηλαδή, όλες οι διεργασίες που έλαβαν χώρα θα πρέπει να μπορούν να αποδειχθούν. Το πεδίο της ψηφιακής εγκληματολογίας, σε γενικές γραμμές δεν έχει αλλάξει, οι έρευνες, δηλαδή, κατά κύριο λόγο εκτελούνται από το προσωπικό επιβολής του νόμου με κάποιο τυπικό τεχνολογικό υπόβαθρο. Εν ολίγοις, η ψηφιακή δικανική είναι η διαδικασία αναγνώρισης, διατήρησης, ανάλυσης, και παρουσίασης των αποδείξεων κατά τρόπο νομικά αποδεκτό.



Εικόνα 1 «Αναλυτής Ψηφιακών Εγκλημάτων – Digital Forensics Analyst»

1.4 Δραστική Ψηφιακή Εγκληματολογία

Η δραστική ψηφιακή εγκληματολογία αφορά την έρευνα που λαμβάνει χώρα μετά από ένα περιστατικό επίθεσης. Τα πειστήρια αφορούν τη μη «ενεργή» εγκληματολογία («dead» forensics). Η δραστική ψηφιακή εγκληματολογία περιλαμβάνει τέσσερις στόχους:

- Προσδιορίζει τα αίτια της εγκληματικής ενέργειας.
- Γίνεται σύνδεση των συμβάντων – αποδεικτικών στοιχείων με τους πιθανούς δράστες.
- Ελαχιστοποιούνται οι επιπτώσεις της επίθεσης, έτσι ώστε να συνεχισθεί η εύρυθμη λειτουργία των επιχειρησιακών διαδικασιών.
- Τελευταίος στόχος είναι η επιτυχής έρευνα του περιστατικού.

Η δραστική ψηφιακή εγκληματολογία περιλαμβάνει έξι φάσεις κατά τις οποίες εφαρμόζονται τεχνικές για τη διαφύλαξη, την ταυτοποίηση, την εξόρυξη, την τεκμηρίωση, την ανάλυση και τέλος, την ερμηνεία των ψηφιακών μέσων, τα οποία αποθηκεύονται στην ψηφιακή τους μορφή και αποτελούν αποδεικτικά στοιχεία, με στόχο τη διευκόλυνση και την ανασυγκρότηση των ψηφιακών πειστηρίων της επίθεσης.

Οι έξι φάσεις που εντάσσονται στη δραστική ψηφιακή εγκληματολογία είναι οι εξής:

Πρώτη φάση: Στο αρχικό στάδιο γίνεται αντιμετώπιση του περιστατικού και η επιβεβαίωση ότι το πληροφοριακό σύστημα έχει δεχτεί ψηφιακή επίθεση. Η φάση αυτή περιλαμβάνει τα ακόλουθα βήματα: την ανίχνευση του συμβάντος, την αναφορά του περιστατικού, την επιβεβαίωσή του, τη διατύπωση της υπόθεσης για το τι έχει συμβεί. Επιπλέον, χορηγείται άδεια για περαιτέρω έρευνα, διαμορφώνεται το πλάνο της έρευνας, κατανέμονται οι πόροι για τη διεξαγωγή της έρευνας και τέλος, γίνεται η κοινοποίηση της διαδικασίας του ελέγχου.

Δεύτερη φάση: Στη δεύτερη φάση γίνεται φυσική έρευνα του περιβάλλοντος. Πολλές φορές κρίνεται απαραίτητο σε μια ψηφιακή έρευνα να συμπεριληφθεί φυσική εγκληματολογική έρευνα, ώστε να συλλεχθούν όσο περισσότερες πληροφορίες για την επιτυχή διερεύνηση του εγκλήματος. Αρχικά, εξασφαλίζεται το φυσικό περιβάλλον που έλαβε χώρα το έγκλημα, πραγματοποιείται έρευνα στον χώρο του εγκλήματος για πιθανά αποδεικτικά στοιχεία, ακολουθεί συλλογή και ανάλυση των στοιχείων αυτών, εντοπίζονται πιθανές ψηφιακές ενδείξεις, ανακατασκευάζονται τα γεγονότα, διατυπώνεται το αντίστοιχο πόρισμα σύμφωνα με τα πειστήρια που συλλέχθηκαν και τέλος, αποθηκεύονται τα αποδεικτικά στοιχεία.

Τρίτη φάση: Η τρίτη φάση αναφέρεται στην ψηφιακή έρευνα της επίθεσης. Για την επιτυχή ψηφιακή διερεύνηση ακολουθούνται τα εξής βήματα:

- Εντοπισμός και συλλογή των αποδεικτικών στοιχείων.
- Ανάλυση δεδομένων. Η ομάδα επανεξετάζει το σχέδιο έρευνας και διατυπώνει ένα υποθετικό σενάριο, το οποίο στη συνέχεια, εφαρμόζεται δοκιμαστικά με στόχο την ανακατασκευή της επίθεσης που δέχθηκε το πληροφοριακό σύστημα.
- Αποκατάσταση υπηρεσιών. Στο σημείο αυτό, οι ερευνητές εγκλημάτων συνεργάζονται με την ομάδα διαχείρισης κινδύνων (risk management), ώστε να αποκατασταθούν τα συστήματα.

Τέταρτη φάση: Σε αυτή τη φάση, οι ερευνητές παραθέτουν μια τεκμηριωμένη έκθεση με τα ψηφιακά πειστήρια της έρευνας.

Πέμπτη φάση: Σε αυτό το στάδιο, περιλαμβάνεται η παρουσίαση των ευρημάτων. Η ερευνητική ομάδα θα προετοιμάσει την υπόθεση λαμβάνοντας υπόψη τις νομικές απαιτήσεις, θα συμπεριλάβει το χρονοδιάγραμμα όλης της υπόθεσης κι τέλος, θα παρουσιάσει τα στοιχεία που περιγράφουν την υπόθεση.

Έκτη φάση: Στην τελευταία φάση, γίνεται η ανακοίνωση των αποτελεσμάτων της έρευνας και το κλείσιμο της υπόθεσης.

1.5 Αντί – Εγκληματολογία

Ο Rogers (2006) προτείνει ότι υπάρχουν τέσσερις βασικές κατηγορίες: απόκρυψη δεδομένων, εξάλειψη αντικειμένων, συσκοτίσεις, και επιθέσεις.

Απόκρυψη δεδομένων

Η απόκρυψη δεδομένων μπορεί να επιτευχθεί με διάφορους τρόπους. Η κρυφή γραφή (δηλ. η στενογραφία) υπάρχει εδώ και χιλιάδες χρόνια. Τα εργαλεία ψηφιακής στενογραφίας είναι διαθέσιμα τουλάχιστον από τα μέσα της δεκαετίας του 1990 και το stego λογισμικό είναι διαθέσιμο για κάθε λειτουργικό σύστημα στον υπολογιστή. Οποιαδήποτε μορφή ψηφιακής πληροφορίας μπορεί να αποθηκευτεί μέσα σε πολλούς τύπους αρχείων, συμπεριλαμβανομένων αρχείων εικόνας, ήχου και βίντεο.

Οι μέθοδοι stego μπορούν επίσης να χρησιμοποιηθούν για να παρεμποδίσουν την εγκληματολογική έρευνα. Για παράδειγμα, ένα άτομο μπορεί να κρύψει μια εικόνα, έναν πίνακα ή μια λίστα κειμένου πίσω από μια φωτογραφία. Για παράδειγμα, τα μηνύματα κώδικα Μορς μπορούν να ενσωματωθούν σε μια εικόνα. Μπορούν να χρησιμοποιηθούν πολλές άλλες μορφές stego χαμηλής τεχνολογίας που κανένα αυτοματοποιημένο εργαλείο δεν μπορεί να εντοπίσει.

Εξάλειψη αντικειμένων

Τα εργαλεία εξάλειψης αντικειμένων είναι διαθέσιμα εδώ και πολλά χρόνια. Το αυτοματοποιημένο λογισμικό διαγραφής αντικειμένων είναι διαθέσιμο, φαινομενικά, για να επιτρέψει στον χρήστη να ανακτήσει τον αποθηκευτικό χώρο – και να προστατεύσει την ιδιωτική του ζωή -- αφαιρώντας τα αχρεία στα προσωρινά αρχεία που γεμίζουν τον σκληρό δίσκο. Τα εργαλεία εξάλειψης αντικειμένων δυσχεραίνουν την ανάλυση για τους εγκληματολόγους. Τα περισσότερα από τα προγράμματα αφήνουν αναγνωρίσιμα ίχνη της διαγραφής και πολλά δεν είναι τόσο πλήρη όσο διαφημίζουν ότι είναι, αφήνοντας συχνά υπολείμματα των ίδιων των πραγμάτων που υποτίθεται ότι διαγράφουν.

Κάλυψη «μονοπατιών»

Επιθέσεις άρνησης παροχής υπηρεσιών (DOS) και κατανεμημένες επιθέσεις DOS εξαρτώνται από την επιτυχή παραποίηση διευθύνσεων IP και έχουν κάνει τις εισβολές στο δίκτυο πιο δύσκολες να διερευνηθούν. Πράγματι, η άμυνα σε τέτοιες επιθέσεις αφορά περισσότερο την πρόληψη, την αντίδραση και την ανάκαμψη και όχι την ανίχνευση του επιτιθέμενου, αν και έχουν επινοηθεί ορισμένες μέθοδοι εντοπισμού IP, προκειμένου να εντοπίζονται τα πακέτα στο δίκτυο μέχρι την πηγή τους. Υπάρχουν διάφοροι τρόποι για να μπερδευτούν οι έρευνες ηλεκτρονικού ταχυδρομείου. Οι ανωνυμίες σε διεύθυνση ηλεκτρονικού ταχυδρομείου παρέχουν φαινομενικά προστασία της ιδιωτικής ζωής, εμποδίζοντας έναν ερευνητή να προσδιορίσει την πηγή ενός αποσταλμένου μηνύματος ηλεκτρονικού ταχυδρομείου. Η απόκρυψη ίχνους μπορεί επίσης να επιτευχθεί με τη διαγραφή ή/και την αλλοίωση των αρχείων καταγραφής διακομιστή ή/και των αρχείων συμβάντων συστήματος, ή την αλλαγή των ημερομηνιών διαφόρων αρχείων. Ένας κακός χάκερ που μπορεί να εισβάλει σε έναν διακομιστή πολύ πιθανότατα έχει τη γνώση να κρύψει τα ίχνη του και/ή να αφήσει ψευδή στοιχεία τροποποιώντας αυτά τα αρχεία.

Επιθέσεις στα πληροφοριακά συστήματα

Ο Palmer (2001) περιγράφει έξι φάσεις στη διαδικασία της ψηφιακής εγκληματολογίας – όλες είναι ανοικτές σε επιθέσεις:

- Η ταυτοποίηση αναφέρεται στη μέθοδο με την οποία ένας ερευνητής μαθαίνει ότι υπάρχει κάποιο περιστατικό που θέλει διερεύνηση. Αυτή η φάση μπορεί να υπονομευθεί με την απόκρυψη του περιστατικού ή την απόκρυψη της σχέσης μεταξύ του ψηφιακής συσκευής και του υπό διερεύνηση συμβάντος.
- Η διατήρηση περιγράφει τα βήματα με τα οποία διατηρείται η ακεραιότητα των αποδεικτικών στοιχείων. Η φάση αυτή μπορεί να υπονομευθεί με την καταστροφή των αποδείξεων ή την αμφισβήτηση της ακεραιότητάς τους.
- Η συλλογή είναι η διαδικασία με την οποία αποκτώνται δεδομένα από το αποδεικτικό μέσο. Το στάδιο αυτό μπορεί να είναι υπονομευθεί περιορίζοντας την πληρότητα των δεδομένων που συλλέγονται ή θέτοντας υπό αμφισβήτηση το υλικό, το λογισμικό και τις διαδικασίες με τις οποίες συλλέγονται τα αποδεικτικά στοιχεία.
- Η εξέταση αφορά τον τρόπο με τον οποίο εξετάζονται τα δεδομένα των αποδεικτικών στοιχείων. Αυτό το μέρος της διαδικασίας μπορεί να υπονομευθεί δείχνοντας ότι τα ίδια τα εργαλεία είναι ανεπαρκή, ελλιπή ή με άλλο τρόπο επιστημονικά μη έγκυρα.
- Η ανάλυση είναι το μέσο με το οποίο ο ερευνητής εξάγει συμπεράσματα από τα αποδεικτικά στοιχεία. Η φάση αυτή βασίζεται στα εργαλεία, την ερευνητική ικανότητα του εξεταστή και τα υπόλοιπα στοιχεία που βρέθηκαν. Εάν μια υπόθεση εξαρτάται αποκλειστικά από ψηφιακά αποδεικτικά στοιχεία, η ερμηνεία των αποδεικτικών στοιχείων είναι το μέρος που επιδέχεται τις περισσότερες επιθέσεις.
- Η παρουσίαση αναφέρεται στις μεθόδους με τις οποίες τα αποτελέσματα της ψηφιακής έρευνας παρουσιάζονται στο δικαστήριο, στους ενόρκους. Τα εργαλεία και οι μέθοδοι anti-forensics θα χρησιμοποιηθούν για να προσβάλουν την αξιοπιστία και τη σχολαστικότητα των εκθέσεων.

1.4 Σχετική Έρευνα

Η παρούσα διπλωματική εργασία σχετίζεται με τη διαδικασία δημιουργίας μιας άσκησης ψηφιακής εγκληματολογίας. Αποτελεί πρωτότυπη εφαρμογή πάνω σε αυτόν τον τομέα, καθώς είναι δικιά μου έμπνευσης. Ωστόσο, έχουν δημιουργηθεί παρόμοιες ασκήσεις – κυρίως στα πλαίσια πανεπιστημιακής έρευνας – οι οποίες συμβάλλουν τόσο στην πρακτική εξάσκηση του μαθητή όσο και στην ανάπτυξη ενός διαφορετικού σκεπτικού. Ενός σκεπτικού παρόμοιο με το σκεπτικό του κακόβουλης οντότητας. Παρακάτω, παρουσιάζονται οι σχετικές έρευνες και εργασίες στο πεδίο της ψηφιακής εγκληματολογίας.

Το πανεπιστήμιο του Princeton ανά καιρούς έχει δημοσιεύσει εκπαιδευτικές ασκήσεις ψηφιακής εγκληματολογίας. Συγκεκριμένα, τον Φθινόπωρο του 2016, δημιουργήθηκε μια άσκηση στην οποία οι μαθητές κλήθηκαν να υποδυθούν τον ψηφιακό ερευνητή, ώστε να εξιχνιάσουν την υπόθεση: *Στις 26 Νοεμβρίου 2009, στο Μίσιγκαν, η ζωή ενός νεαρού άνδρα κόπηκε πολύ νωρίς. Το άτυχο θύμα, σκοτώθηκε γύρω στα μεσάνυχτα εν ώρα εργασίας. Οι αστυνομικοί ανακάλυψαν ένα βελάκι, το οποίο φαίνεται, ανεξήγητα, να ήταν η αιτία θανάτου. Μετά από έρευνες, συνέλαβαν τον μοναδικό ύποπτο, τον Nefarious Criminal, και κατάσχεσαν τον υπολογιστή του. Δυστυχώς, ένας αρχάριος ερευνητής κρυπτογράφησε την εικόνα του δίσκου χωρίς να παρακολουθεί το κλειδί κρυπτογράφησης και ο εξοπλισμός επιστράφηκε στον Nefarious πριν γίνει αντιληπτό το λάθος. Τώρα, μετά από τέσσερα χρόνια μαντεψιών με ωμή βία, ο δίσκος έχει επιτέλους αποκρυπτογραφηθεί. Σκοπός της αποστολής, είναι να διεξαχθεί εγκληματολογική έρευνα του σκληρού δίσκου του Nefarious και να τεκμηριωθεί κάθε στοιχείο που σχετίζεται με τη δολοφονία του άτυχου θύματος.* (<https://www.cs.princeton.edu/courses/archive/fall13/cos432/homework/hw8.html>).

Τον Φθινόπωρο του 2017, οι φοιτητές κλήθηκαν να υλοποιήσουν ένα σενάριο δολοφονίας: *Τον Δεκέμβριο της ίδιας χρονιάς, καταγράφηκαν δύο τρομερά εγκλήματα. Σε έναν ποδοσφαιρικό αγώνα, οι μασκότε και των δύο ομάδων έπεσαν νεκρά μέσα σε χρονική στιγμή 30 δευτερολέπτων μεταξύ τους, παρόλη τη μεγάλη απόσταση. Η υπόθεση πήρε διαστάσεις όταν ο βασικός ύποπτος, ο Bobby McBobface, διέφυγε από τη χώρα και εξαφανίστηκε. Έτσι, οι ερευνητές πήραν θέση και κατάσχεσαν τον υπολογιστή του. Σκοπός του έργου είναι να διερευνήσουμε αυτή τη δολοφονία.* (https://www.cs.princeton.edu/courses/archive/fall17/cos432/assignments/a7/cos432_a7.pdf).

Την Άνοιξη του 2023, όπου είναι και η πιο πρόσφατη έρευνα του πανεπιστημίου, οι φοιτητές έπρεπε να παίζουν τον ρόλο ενός εγκληματολογικού αναλυτή που ερευνά μια δολοφονία. *Ο κατηγορούμενος είναι ο Bob, ο οποίος έχει φύγει από τη χώρα και έχει εξαφανιστεί. Οι αστυνομικοί έχουν κατασχέσει μια εικόνα του δίσκου του υπολογιστή του. Σκοπός και της συγκεκριμένης εκπαιδευτικής άσκησης, είναι η πραγματοποίηση μιας εγκληματολογικής εξέτασης της εικόνας του δίσκου και η τεκμηρίωσή της με τυχόν στοιχεία που σχετίζονται με την υπόθεση.* (<https://www.cs.princeton.edu/courses/archive/spring23/cos432/assignments/forensics/index.html>).

Χαρακτηριστικό των παραπάνω εκπαιδευτικών ασκήσεων του πανεπιστημίου του Princeton, εκτός από την πρωτοτυπία των σεναρίων τους, είναι ότι όλες υλοποιούνται στο λειτουργικό σύστημα Kali Linux. Αυτή είναι κι η μεγάλη διαφορά με την παρούσα πτυχιακή εργασία, αφού στη συγκεκριμένη, η υπόθεση είναι «χτισμένη» σε περιβάλλον Windows.

Κεφάλαιο 2^ο: Νομικό Πλαίσιο

2.1 Γενικό πλαίσιο

Η έρευνα επί των ψηφιακών μέσων καλύπτεται από εθνική και διεθνή νομοθεσία. Υπάρχουν συχνά περιορισμοί, οι οποίοι αφορούν στην παρακολούθηση ενός δικτύου, στην ανάγνωση προσωπικών επικοινωνιών και στην καταγραφή ψηφιακών πειστηρίων τα οποία περιλαμβάνουν προσωπικά δεδομένα τόσο των υπόπτων όσο και τρίτων ατόμων ως προς την εξεταζόμενη υπόθεση. Βάσει του Κανονισμού 679/2016 της Ε.Ε. για την προστασία δεδομένων προσωπικού χαρακτήρα *«Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία»* και *«...οι συγκεκριμένοι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς, νόμιμοι και προσδιορισμένοι κατά τον χρόνο συλλογής των δεδομένων προσωπικού χαρακτήρα»*. Επιπρόσθετα, στον ίδιο κανονισμό προσδιορίζονται γενικά τα προσόντα του ψηφιακού ερευνητή αναφέροντας ότι *«...οσάκις ανατίθενται σε εκτελούντα την επεξεργασία δραστηριότητες επεξεργασίας, ο Privacy in Digital Forensics σελ. 9 από 63 υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί μόνο εκτελούντες επεξεργασία οι οποίοι παρέχουν επαρκείς διαβεβαιώσεις, ιδίως από πλευράς εμπειρογνομosσύνης, αξιοπιστίας και πόρων, για την εφαρμογή τεχνικών και οργανωτικών μέτρων που θα ανταποκρίνονται στις απαιτήσεις του παρόντος κανονισμού, συμπεριλαμβανομένων εκείνων που αφορούν την ασφάλεια της επεξεργασίας.»* Ωστόσο, ο εν λόγω κανονισμός αναφέρεται γενικά στην επεξεργασία δεδομένων προσωπικού χαρακτήρα αποκλείοντας τις περιπτώσεις που αυτή είναι απαραίτητη για την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιπτώσεις που εξετάζονται και εξειδικεύονται από την Οδηγία 680/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Συγκεκριμένα, στην παράγραφο (34) αναφέρεται: *«Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, θα πρέπει να καλύπτει κάθε πράξη ή σύνολο πράξεων που εκτελείται επί δεδομένων προσωπικού χαρακτήρα ή συνόλων δεδομένων προσωπικού χαρακτήρα για αυτούς τους σκοπούς, είτε χρησιμοποιούνται αυτοματοποιημένα μέσα είτε άλλα, όπως η συλλογή, η αρχειοθέτηση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η αλλοίωση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η συσχέτιση ή ο συνδυασμός, ο περιορισμός της επεξεργασίας, η διαγραφή ή η καταστροφή»* και στην παράγραφο (35) *«Η εκτέλεση των καθηκόντων πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων η οποία ανατίθεται θεσμικά από τον νόμο στις αρμόδιες αρχές παρέχει σε αυτές τη δυνατότητα να απαιτούν από φυσικά πρόσωπα ή να δίνουν εντολή σε αυτά να συμμορφωθούν προς τα σχετικά αιτήματα. Σε μία τέτοια περίπτωση, η συγκατάθεση του υποκειμένου των δεδομένων όπως ορίζεται στον κανονισμό (ΕΕ) 2016/679 δεν θα πρέπει να παρέχει νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές»*.

Επιπρόσθετα, στην παράγραφο (38) αναφέρεται ότι «Σε κάθε περίπτωση, αυτή η επεξεργασία θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, όπως η πρόβλεψη για ειδική ενημέρωση του υποκειμένου των δεδομένων, το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, κυρίως το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να απαιτήσει αιτιολόγηση της απόφασης που ελήφθη κατόπιν της εν λόγω αξιολόγησης και το δικαίωμα αμφισβήτησης της απόφασης» και στην παράγραφο (43) «Ένα φυσικό πρόσωπο θα πρέπει να έχει δικαίωμα πρόσβασης σε δεδομένα τα οποία συνελέγησαν και το αφορούν και να μπορεί να ασκεί το δικαίωμα αυτό ευχερώς και σε εύλογα τακτά διαστήματα, προκειμένου να έχει επίγνωση της επεξεργασίας και να ελέγχει τη νομιμότητά της». Τέλος, στην παράγραφο (49) αναφέρεται ότι «Εάν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία στο πλαίσιο ποινικής έρευνας και ποινικής διαδικασίας ενώπιον δικαστηρίου, τα κράτη μέλη θα πρέπει να μπορούν να προβλέπουν ότι η άσκηση των δικαιωμάτων ενημέρωσης, πρόσβασης και διόρθωσης, διαγραφής και περιορισμού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα γίνεται σύμφωνα με τους εθνικούς κανόνες περί δικαστικών διαδικασιών». Privacy in Digital Forensics σελ. 10 από 63. Οι προαναφερθέντες κανονισμοί έχουν ενσωματωθεί στο ελληνικό δίκαιο με τον νόμο 4624/19 όπου στο άρθρο 24 αναφέρεται ότι «Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από δημόσιους φορείς για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, επιτρέπεται όταν η επεξεργασία αυτή είναι αναγκαία για την εκπλήρωση των καθηκόντων που τους έχουν ανατεθεί και εφόσον είναι ... β) αναγκαία για την αποτροπή κινδύνων για την εθνική ασφάλεια, εθνική άμυνα ή δημόσια ασφάλεια ή για τη διασφάλιση φορολογικών και τελωνειακών εσόδων γ) αναγκαία για τη δίωξη ποινικών αδικημάτων δ) αναγκαία για την αποτροπή σοβαρής βλάβης στα δικαιώματα άλλου προσώπου» και στο άρθρο 25 «Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από ιδιωτικούς φορείς για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, επιτρέπεται, εφόσον είναι απαραίτητη: ... β) για τη δίωξη ποινικών αδικημάτων ή γ) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, εκτός και εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα δεδομένα αυτά». Από την ανωτέρω ευρωπαϊκή και εθνική νομολογία γίνεται κατανοητό ότι ο ψηφιακός ερευνητής έχει πολλά τροχοπέδη στην εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία των προσωπικών δεδομένων καθώς πρέπει να λάβει υπόψη του την ανάγκη διαρκούς προστασίας των συλλεχθέντων προσωπικών δεδομένων καθ' όλη τη διάρκεια της επεξεργασίας αυτών με παράλληλη την απαίτηση διαρκούς ενημέρωσης για την επεξεργασία που αυτά υφίστανται. Για τη συλλογή στοιχείων που μπορεί να περιέχουν προσωπικά δεδομένα ο ψηφιακός ερευνητής πρέπει να λάβει ένταλμα έρευνας το οποίο απαιτεί επαρκής αιτιολόγηση για την έκδοσή του (και την κατ' επέκταση απαίτηση ύπαρξης ενοχοποιητικών στοιχείων που δικαιολογούν περαιτέρω έρευνα) και στο οποίο θα καθορίζονται με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν καθώς σε περίπτωση που αντληθούν ψηφιακά πειστήρια από αντικείμενα για τα οποία δεν έχει εκδοθεί ένταλμα έρευνας τα εν λόγω αποδεικτικά στοιχεία θα απορριφθούν κατά την ακροαματική διαδικασία. Κατά τη συλλογή όμως ψηφιακών πειστηρίων υπάρχει περίπτωση ο ψηφιακός ερευνητής να συλλέξει στοιχεία τρίτων ως προς την υπόθεση ατόμων, πολλά από αυτά να αποτελούν προσωπικά τους δεδομένα.

2.2 Ισχύουσα Κατάσταση στην Ελλάδα

Τα τελευταία χρόνια η χρήση των ηλεκτρονικών υπολογιστών προκάλεσε μια ανυπολόγιστη αύξηση των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή, αλλά οδήγησε και σε νέες μορφές εγκληματικής δράσης, με αποτέλεσμα να γίνονται προσπάθειες αντιμετώπισης της νέας αυτής εγκληματικότητας. Κρίνεται σκόπιμο να παρουσιαστεί το νομικό πλαίσιο σχετικά με το ηλεκτρονικό έγκλημα, όπως αυτό προβλέπεται στην ελληνική έννομη τάξη. Σε συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως με κεντρικό θέμα την προστασία των έννομων συμφερόντων των πολιτών έναντι των ηλεκτρονικών εγκλημάτων, έχει τεθεί το ζήτημα σαφούς ποινικής οριοθέτησης των αξιόποινων αυτών πράξεων, αλλά και αντιμετώπισής τους και εξιχνιάσής τους με σύννομες διαδικασίες.

Συγκεκριμένα, πραγματοποιήθηκε συνέδριο για το «Ηλεκτρονικό Έγκλημα» στη Βουδαπέστη και υπογράφηκε η συνθήκη, την 23-11-2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Τη συνθήκη αυτή υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας, χωρίς όμως η χώρα μας να την κυρώσει. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές ηλεκτρονικής εγκληματικότητας και είναι ως γνωστή ως «Convention on Cyber 2001».

Στην ελληνική έννομη τάξη, ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Στις μέρες μας έχει λάβει πολύ μεγάλες διαστάσεις το ιδιαίτερα σοβαρό ζήτημα της εκμετάλλευσης ανηλίκων για την παραγωγή πορνογραφικού υλικού και προκαλεί το έντονο ενδιαφέρον των ανθρώπων παγκοσμίως, καθόσον η «παιδική πορνογραφία» προσβάλλει την ατομική αξιοπρέπεια του ανηλίκου και θέτει σε κίνδυνο τη μετέπειτα εξέλιξή του. Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται το άρθρο 381Α «Φθορά ηλεκτρονικών δεδομένων, εισάγεται, δηλαδή, με το νόμο 4411/2016 το άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας, συμπληρώνοντας ένα σημαντικό νομικό κενό της ελληνικής έννομης τάξης που αφορούσε στην παράνομη διαγραφή, καταστροφή, αλλοίωση, απόκρυψη δεδομένων ενός πληροφοριακού συστήματος που δύναται να καταστήσει «ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο να αποκλείσει την πρόσβαση στα δεδομένα αυτά». Επίσης, με την παράγραφο 10 του δεύτερου άρθρου του νόμου 4411/2016, εισάγεται το άρθρο 381 Β Π.Κ., με αποτέλεσμα να εντάσσεται στην ελληνική νομοθεσία το άρθρο 7 της Οδηγίας, που αναφέρεται στην παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, κατοχή, ή διανομή : α) συσκευών ή προγραμμάτων υπολογιστή, σχεδιασμένων ή προσαρμοσμένων κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) συνθηματικών ή κωδικών πρόσβασης ή άλλων παρεμφερών δεδομένων με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Το άρθρο 386Α «Απάτη με υπολογιστή» καλύπτει τα κενά εφαρμογής των διατάξεων της κλασικής απάτης (386 ΠΚ «Απάτη»), ως προς την προσβολή της περιουσίας με την χρήση ηλεκτρονικού υπολογιστή. Με το νέο νόμο, στη διάταξη αυτή εισάγεται το άρθρο 8 της Σύμβασης και τώρα πια ρητά στους τρόπους πρόκλησης της ζημίας σε ξένη περιουσίας «είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα».

Στο άρθρο 216 ΠΚ ποινικοποιείται η πλαστογραφία που σχετίζεται άμεσα με το ηλεκτρονικό έγκλημα, λαμβάνοντας υπόψη την έννοια του εγγράφου στο στοιχ. γ) του άρθρου 13 ΠΚ, όπου έγγραφο θεωρείτε και «κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστή ή από περιφερειακή μνήμη υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο για εγγραφή αποθήκευση ή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό (πχ μαγνητοταινίες, CD, κινηματογραφικές ταινίες, βιντεοκασέτες κα), εφόσον τα μέσα και τα υλικά αυτά προσπορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία».

Αξιοσημείωτη είναι και η παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας. Το απαραβίαστο των επικοινωνιών αρχικά κατοχυρώνεται στο 21 Σύνταγμα με το άρθρο 19 όπου προστατεύεται η ελεύθερη επικοινωνία και ανταπόκριση. Η προστασία δεν αφορά μόνο τα γραπτά μηνύματα, αλλά και οποιαδήποτε άλλη μορφή ιδιωτικής επικοινωνίας (πχ οι επιστολές, τα τηλεγραφήματα, τα τηλεφωνήματα, τα τέλεξ, τα φαξ, τα e-mails) και η επικοινωνία αρχίζει από τη στιγμή που διατυπώνεται το μήνυμα από τον αποστολέα και τελειώνει μόλις λάβει γνώση του περιεχομένου της και ο παραλήπτης. Το έννομο αγαθό που προστατεύουν οι ποινικές διατάξεις των άρθρων 370 ΠΚ είναι το ιδιωτικό απόρρητο, μέσα στο οποίο εντάσσεται το άρθρο 19 Σ. Μέχρι το 1982, η ποινική προστασία του απορρήτου της επικοινωνίας, σύμφωνα με όσα ορίζει το άρθρο 370ΠΚ, περιορίζεται μόνο στο απόρρητο των γραπτών κειμένων. Όμως η χρήση της σύγχρονης τεχνολογίας για την παρακολούθηση ιδιωτικών συνομιλιών και την περαιτέρω χρησιμοποίηση του περιεχομένου τους ανάγκασε την επέκταση της ποινικής προστασίας και το απόρρητο των τηλεφωνημάτων. Έτσι θεσπίστηκε με το Ν.1291/1982 το αξιόποινο της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας με την ψήφιση του άρθρου 370ΑΠΚ για την. Η τελευταία τροποποίηση πραγματοποιήθηκε με τον Ν.3674/2008.

Το άρθρο 370 Γ ΠΚ (Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών) προστατεύει το λογισμικό και τα κάθε είδους προγράμματα ή στοιχεία υπολογιστών, καθώς επίσης και τα συναφή συστήματα τηλεπικοινωνιών. Σε αυτό το άρθρο μπορεί να υπαχθούν οι hackers και τα σχετικά περιστατικά hacking. Η διάταξη του άρθρου αυτού τροποποιήθηκε το νόμο 4411/2016, και με τη νέα διατύπωσή του, στη δεύτερη παράγραφο του τιμωρείται η παράνομη πρόσβαση «στο σύνολο ή τμήμα του πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του».

Ο ελληνικός νόμος για την προστασία των προσωπικών δεδομένων είναι ο Ν. 2472/1997 προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος υιοθετήθηκε προκειμένου να εφαρμοστεί στη χώρα μας η κοινοτική οδηγία 95/46/ΕΚ που αφορά τα προσωπικά δεδομένα. Ορίζει σε τι συνίσταται η επεξεργασία, παρέχει ασφαλιστικές δικλείδες και κυρώσεις σε περίπτωση παραβίασής τους. Επομένως, στο ως άνω νομοθετικό πλαίσιο θα βασιστούμε για να καθορίσουμε το περιθώριο επεξεργασίας των προσωπικών δεδομένων ακόμη και στο

χώρο εργασίας που μας απασχολεί στην προκειμένη περίπτωση. Ένα κρίσιμο ζήτημα, όμως, θέτει η αρχή της ιδιωτικότητας, δοθέντος ότι από τη μία πρέπει να οριοθετηθεί η επεξεργασία και συλλογή των προσωπικών δεδομένων προκειμένου να μην τίθεται ζήτημα παραβίασης της ιδιωτικότητας των εργαζομένων, από την άλλη όμως να μην περιορίζεται σε σημείο που να αποκλείεται η άσκηση του διευθυντικού δικαιώματος. Σε μια προσπάθεια να εξισορροπηθούν οι δύο αντικρουόμενες πλευρές και να προασπιστούν ισότιμα, στηρίζομαστε τόσο στο νόμο 2472/97 όσο και στην Οδηγία 115/2001 της Ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

2.3 Αρχή ιδιωτικότητας στον χώρο εργασίας

Σε αυτό το σημείο, σημαντικό είναι να προσδιοριστούν οι δύο πόλοι που τίθενται σε κίνδυνο από την πλευρά του εργαζομένου, ήτοι στα πλαίσια της εργασιακής σχέσης σημαντικό είναι να διαφυλάσσεται σφαιρικά η προσωπικότητά του, τόσο δηλαδή η έκφραση των ατομικών ελευθεριών του εργαζομένου μέσα στην επιχείρηση υπό την έννοια της εξωεπαγγελματικής σφαίρας όσο και η ίδια προσωπικότητα του εργαζομένου. Ένα σημαντικό άρθρο του ως άνω νόμου, είναι το 7Α παρ.1 το οποίο ορίζει τα πλαίσια απαλλαγής υποχρέωσης σε γνωστοποίηση και λήψη άδειας και συγκεκριμένα αναφέρει : «α) Όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί.» Ένα κρίσιμο σημείο είναι όταν έχει υποβληθεί αίτηση από τους υποψήφιους αλλά δεν έχει πραγματοποιηθεί η πρόσληψη. Σε αυτή την περίπτωση, οι εργοδότες χρειάζονται τη συγκατάθεση των υποψηφίων για την επεξεργασία των προσωπικών τους δεδομένων και καλούνται να γνωστοποιήσουν την ως άνω επεξεργασία. Η χρήση της τεχνολογικής υποδομής στο χώρο εργασίας είναι τόσο υπηρεσιακή όσο και προσωπική. Αυτό σημαίνει ότι οι εργαζόμενοι κάνουν χρήση του διαδικτύου τόσο στα πλαίσια των καθηκόντων τους όσο και για προσωπικούς λόγους. Σημαντικό είναι να καθοριστεί η έννοια της υπηρεσιακής χρήσης. Συγκεκριμένα, όταν γίνεται χρήση του διαδικτύου σχετική με τα καθήκοντα του εργαζομένου, όπως αυτά ορίζονται από σαφώς στη σύμβαση εργασίας, τότε αναμφισβήτητα η χρήση είναι υπηρεσιακή, ωστόσο, υπάρχουν κάποιες περιπτώσεις που πρέπει να προσεχθούν. Η χρήση δύναται να θεωρηθεί υπηρεσιακή ακόμη και αν πρόκειται για ιδιωτική επικοινωνία στην περίπτωση που ο εργαζόμενος θα προβεί σε κάποια ενέργεια ιδιωτικού περιεχομένου, ορμώμενη από κάποιο γεγονός στο εργασιακό περιβάλλον. Σε αυτή την περίπτωση, όπως χαρακτηριστικά αναφέρεται στην «Επιτήρηση και παρακολούθηση των τηλεπικοινωνιών στο χώρο εργασίας», του Ι.Γγλεζάκη «είναι δυνατό να θεωρηθεί υπηρεσιακή και επικοινωνία ιδιωτικής φύσης, όταν αυτή θα γίνει με αφορμή κάποιο υπηρεσιακό γεγονός, όπως για παράδειγμα όταν ο εργαζόμενος αναγκάζεται να ενημερώσει κάποιους δικούς του ανθρώπους για την αναβολή προγραμματισμένων σχεδίων επειδή θα πρέπει να παραμείνει στην εργασία του». Στις περιπτώσεις που ο εργαζόμενος χρησιμοποιεί για προσωπικούς λόγους την τεχνολογική υποδομή του εργασιακού του περιβάλλοντος και το διαδίκτυο, οφείλει να έχει προηγουμένως λάβει ρητή ή και σιωπηρή συγκατάθεση του εργοδότη του. Ως ρητή

θεωρείται η συγκατάθεση που περιλαμβάνεται στην έγγραφη σύμβαση εργασίας ή όταν ο εργοδότης παρέχει δύο ηλεκτρονικές διευθύνσεις, μία για τις προσωπικές του επικοινωνίες και μία για την εκπόνηση των εργασιακών του καθηκόντων. Από την άλλη πλευρά, σε κάποιες εταιρίες διατίθενται υπολογιστές, στους χώρους που πραγματοποιούνται τα διαλείμματα των εργαζομένων, τότε πρόκειται για μία σιωπηρή συγκατάθεση, που παρέχει τη δυνατότητα στους εργαζομένους να επικοινωνούν για προσωπικούς τους λόγους από συγκεκριμένους υπολογιστές κατά τη διάρκεια του διαλείμματος. Ένα σημαντικό ζήτημα που γεννάται όταν ο εργαζόμενος κάνει προσωπική χρήση στον επαγγελματικό υπολογιστή του, είναι η μεγάλη πιθανότητα πρόκλησης βλάβης στους ηλεκτρονικούς υπολογιστές, με τους γνωστούς ιούς. Συχνά, λοιπόν, σε πολλές εταιρίες και υπηρεσίες, η χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου παρακολουθείται προκειμένου να αποφευχθούν οι όποιοι κίνδυνοι, δημιουργώντας όμως σοβαρούς κλυδωνισμούς στην αρχή της ιδιωτικότητας.

Υπάρχουν συχνά περιορισμοί, οι οποίοι αφορούν την παρακολούθηση ενός δικτύου, την ανάγνωση προσωπικών επικοινωνιών και την καταγραφή ψηφιακών πειστηρίων τα οποία περιλαμβάνουν προσωπικά δεδομένα τόσο των υπόπτων όσο και τρίτων ατόμων ως προς την εξεταζόμενη υπόθεση. Ο ψηφιακός ερευνητής έχει πολλά τροχοπέδη στην εκτέλεση ψηφιακής δικανικής έρευνας με έμφαση στην προστασία των προσωπικών δεδομένων καθώς πρέπει να λάβει υπόψη του την ανάγκη διαρκούς προστασίας των συλλεχθέντων προσωπικών δεδομένων καθ' όλη τη διάρκεια της επεξεργασίας αυτών με παράλληλη την απαίτηση διαρκούς ενημέρωσης για την επεξεργασία που αυτά υφίστανται. Για τη συλλογή στοιχείων που μπορεί να περιέχουν προσωπικά δεδομένα ο ψηφιακός ερευνητής πρέπει να λάβει ένταλμα έρευνας το οποίο απαιτεί επαρκής αιτιολόγηση για την έκδοσή του (και την κατ' επέκταση απαίτηση ύπαρξης ενοχοποιητικών στοιχείων που δικαιολογούν περαιτέρω έρευνα) και στο οποίο θα καθορίζονται με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν καθώς σε περίπτωση που αντληθούν ψηφιακά πειστήρια από αντικείμενα για τα οποία δεν έχει εκδοθεί ένταλμα έρευνας τα εν λόγω αποδεικτικά στοιχεία θα απορριφθούν κατά την ακροαματική διαδικασία. Κατά τη συλλογή όμως ψηφιακών πειστηρίων υπάρχει περίπτωση ο ψηφιακός ερευνητής να συλλέξει στοιχεία τρίτων ως προς την υπόθεση ατόμων, πολλά από αυτά να αποτελούν προσωπικά τους δεδομένα.

Κεφάλαιο 3^ο: Προστασία ιδιωτικότητας σε περιβάλλον ψηφιακής εγκληματολογίας

3.1 Ψηφιακά Πειστήρια

Ως ψηφιακά πειστήρια ορίζουμε οποιαδήποτε πληροφορία είναι αποθηκευμένη σε ψηφιακό μέσο ή έχει μεταδοθεί μέσω αυτού και έχει αποδεικτική αξία σε μια δικαστική αίθουσα. Στην επιστήμη της ψηφιακής εγκληματολογίας, ο ειδικός ερευνητής αναλαμβάνει να ανακτήσει και να αναλύσει όλες τις ηλεκτρονικές πληροφορίες που μπορεί να σχετίζονται με μια κακόβουλη ενέργεια και τέλος να καταγράψει τα σχετικά ευρήματα σε μια έκθεση για δικαστική χρήση. Τα πειστήρια που θα συλλεχτούν θα πρέπει να είναι αυθεντικά, να προέρχονται δηλαδή, από την πηγή που εξετάστηκε χωρίς να χωρά καμιά αμφιβολία για το αντίθετο. Επίσης, να είναι αξιόπιστα, να χρησιμοποιούνται δηλαδή, τρόποι νομικά αποδεκτοί για τη συλλογή τους. Τέλος, η ακεραιότητα των δεδομένων αποτελεί ίσως το πιο ευαίσθητο σκέλος στη συλλογή των πειστηρίων, καθώς δεν γίνονται δεκτά από τις δικαστικές αρχές στοιχεία τα οποία είναι πιθανό να έχουν τροποποιηθεί ουσιαστικά. Επομένως, είναι απαραίτητο τα δεδομένα που συλλέγονται να είναι ίδια με εκείνα που αρχικά ανακαλύφθηκαν. Γενικά, τα ψηφιακά πειστήρια πρέπει να πληρούν τις παρακάτω προϋποθέσεις:

1. Να είναι σχετικές με το υπό κρίση ζήτημα, ήτοι να τελούν σε αιτιώδη συνάφεια με το υπό εξέταση αδίκημα.
2. Είναι σημαντικό να προέρχονται από νομικά αναγνωρισμένη επιστημονική μέθοδο η οποία να υποδεικνύεται και να υποστηρίζεται από κατάλληλη επικύρωση, ένταλμα ή εξουσιοδότηση.

Τα ψηφιακά δεδομένα μπορούν να αποθηκευτούν σε σκληρούς δίσκους και συνήθως όταν αναφερόμαστε σε κάποιον οργανισμό ή επιχείρηση, σε file servers και μεγάλα storage συστήματα. Επιπλέον, μπορούν να περιέχονται σε μέσα αποθήκευσης όπως cd-rom, usb flash μνήμες, backup disks, εξωτερικούς δίσκους, ακόμα και σε volatile μνήμες (RAM). Οι ειδικοί ψηφιακοί εγκληματολόγοι αναζητούν αποδείξεις σε αρχεία τα οποία μπορούν να βρεθούν:

1. Κρυπτογραφημένα με διάφορους αλγόριθμους κρυπτογράφησης (Ceasar cipher, Vigenère cipher). Αξίζει να αναφερθεί η μέθοδος της στενογραφίας (steganography) κατά την οποία μπορούν να κρυπτογραφηθούν δεδομένα μέσα σε ένα αρχείο εικόνας ή ένα αρχείο ήχου. Μάλιστα, στο σενάριο που θα παρουσιάσουμε σε παρακάτω ενότητα, χρησιμοποιείται στην πράξη η συγκεκριμένη μέθοδος.
2. Αρχεία που δημιουργούνται από τα πληροφοριακά συστήματα και αφορούν τις συναλλαγές και το αποτύπωμα των χρηστών σε διάφορες ενέργειές τους, όπως είσοδος – έξοδος σε μια ηλεκτρονική υπηρεσία, ποια αρχεία χρησιμοποίησαν και τροποποίησαν, αλλά και περιήγηση στο διαδίκτυο (cookies). Σημαντικές πληροφορίες, επίσης, μπορούν να εξαχθούν από την ηλεκτρονική αλληλογραφία των χρηστών. Στην παρούσα υπόθεση, γίνεται ιδιαίτερη έμφαση στις παραπάνω ενέργειες, καθώς ο κακόβουλος χρήστης δρα χρησιμοποιώντας αυτές τις μεθόδους.

3. Αρχεία που δημιουργούνται από το σύστημα και αφορούν υπηρεσίες, εφαρμογές και μεταφορά δεδομένων (κίνηση) σε ένα πληροφοριακό δίκτυο, όπως τα αρχεία καταγραφής συμβάντων, πίνακες δρομολόγησης, ARP cache εγγραφές.
4. Αρχεία που έχουν αποθηκευτεί εσκεμμένα στον unallocated χώρο ενός σκληρού δίσκου, δεδομένα που έχουν διαγραφεί και αποτελούν πειστήρια ή ακόμα και δεδομένα που έχουν δημιουργηθεί από την εκτέλεση ενός προγράμματος από έναν εξωτερικό δίσκο usb.

Ένας ψηφιακός ερευνητής, λοιπόν, ακολουθεί συγκεκριμένη μεθοδολογία, διακριτά βήματα σαφώς οριοθετημένα και θεσμοθετημένα για την εκτέλεση της ψηφιακής δικανικής. Οι ψηφιακές ενδείξεις πρέπει, επίσης, να έχουν όλα τα χαρακτηριστικά των συμβατικών στοιχείων, κάθε εργαλείο, μέθοδος ή διαδικασία που χρησιμοποιείται κατά τη διάρκεια της έρευνας χρειάζεται να πληρούν αυστηρές προδιαγραφές. Οι ερευνητές, επομένως, οφείλουν να διασφαλίσουν ότι η κατοχή και η πρόσβαση σε ηλεκτρονικές αποδείξεις είναι σύννομες, και σε κάθε περίπτωση οι διαδικασίες που εφαρμόζονται είναι συμβατές με την εκάστοτε νομοθεσία.

3.2 Ιδιωτικότητα κατά την εύρεση ψηφιακών πειστηρίων

Κατά τη διεξαγωγή μιας έρευνας σε ηλεκτρονικά δεδομένα, είναι σημαντικό να μην παραβιάζεται η ιδιωτικότητα του ατόμου κατά την εύρεση κάποιου ψηφιακού πειστηρίου. Κατόπιν τούτου, απαιτείται η χορήγηση εντάλματος που θα καθορίζει με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν. Μάλιστα, ακόμη και στην περίπτωση που ο ερευνητής θεωρήσει ότι μπορεί να αντλήσει στοιχεία και από άλλα αντικείμενα εκτός των καθορισμένων, τα στοιχεία αυτά δεν θα έχουν αποδεικτική αξία στη δικαστική αίθουσα και θα απορριφθούν. Γι' αυτό, κατά τη διάρκεια της εγκληματολογικής έρευνας, η χρήση μιας ακατάλληλης μεθοδολογίας ή παράνομης κατάσχεσης μπορεί να επηρεάσει αρνητικά το παραδεκτό των αποδεικτικών στοιχείων. Σε κάθε έρευνα, κρείσσονος σημασίας είναι σημαντικό να διασφαλίζεται η προστασία της ιδιωτικής ζωής του κατηγορούμενου, επομένως η νομική διαδικασία που επιβάλλεται να ακολουθηθεί για την αναζήτηση και την κατάσχεση στοιχείων, πρέπει να γίνεται κατόπιν εντάλματος, γεγονός που αντανάκλα το νομικό πλαίσιο που καλύπτει τις ως άνω διαδικασίες. Οι ερευνητές, επομένως, πρέπει όχι μόνο να εντοπίσουν, αλλά και να αρθρώσουν τα πιθανά αίτια στα οποία θα στηριχθεί η έκδοση εντάλματος έρευνας ή κατάσχεσης. Επιπλέον, σημαντικό είναι να γνωρίζουν τα όρια μέσα στα οποία μπορεί να διεξαχθεί μια έρευνα ή κατάσχεση κατόπιν εντάλματος. Ένα ωραίο παράδειγμα αποτελεί η κατάσχεση της ηλεκτρονικής αλληλογραφίας των κατηγορουμένων από τους τεχνικούς του Yahoo, με την κατηγορία της παιδικής πορνογραφίας κατόπιν βεβαίως έκδοσης του σχετικού εντάλματος. Ωστόσο, υπήρξαν δύο αντικρουόμενες αποφάσεις, ήτοι, το μεν πρωτοβάθμιο δικαστήριο έκρινε ότι η ανάκτηση των e-mails από τους τεχνικούς του Yahoo χωρίς την παρουσία της αστυνομίας ήταν παράνομη. Από την άλλη, το δευτεροβάθμιο δικαστήριο, έκρινε ότι η αναζήτηση των e-mails του κατηγορουμένου χωρίς την παρουσία αστυνομικού ήταν νομότυπη κατά την τέταρτη τροποποίηση της αμερικανικής νομοθεσίας και ως εκ τούτου τα δικαιώματα της ιδιωτικής ζωής του κατηγορούμενου δεν παραβιάστηκαν.

Τα ψηφιακά συστήματα (υπολογιστές, φορητές συσκευές) σχεδιάζονται πλέον με αυξημένες δυνατότητες προστασίας της ασφάλειας της συσκευής και της ιδιωτικότητας του χρήστη με την χρήση αυτών των δυνατοτήτων να επεκτείνεται και σε εύχρηστα λογισμικά τα οποία γίνονται συνεχώς αποτελεσματικότερα. Τα λογισμικά αυτά αποτελούν κομμάτι των τεχνολογιών PET (Privacy Enhancing Technologies) τα οποία χωρίς να επηρεάζουν αισθητά την λειτουργικότητα των συσκευών και των υπηρεσιών περιορίζουν τη χρήση και τη διακίνηση προσωπικών δεδομένων. Σκοπός των τεχνολογιών PET είναι η προστασία της ιδιωτικότητας των χρηστών με τον περιορισμό της χρήσης και της κοινοποίησης σε τρίτα άτομα των προσωπικών τους δεδομένων. Οι τεχνολογίες PET μολονότι χρησιμοποιούνται για την προστασία της ιδιωτικότητας των χρηστών αποτελούν πολλές φορές τροχοπέδη στον ψηφιακό ερευνητή κατά τη συλλογή των ψηφιακών πειστηρίων. Η δράση τους πολλές φορές εμποδίζει τα χρησιμοποιούμενα εργαλεία δικανικής ανάλυσης με αποτέλεσμα μαζί με έτερες τεχνικές που σκοπίμως δρουν με τέτοιο σκοπό να γίνεται λόγος για τον όρο Anti-Forensics. Ως Anti-Forensics χαρακτηρίζονται «οι πρακτικές που έχουν ως σκοπό την αλλοίωση και τον περιορισμό των διαθέσιμων ψηφιακών πειστηρίων καθώς και την παρεμπόδιση της εκτέλεσης της ψηφιακής δικανικής έρευνας» όπως επίσης και την αύξηση του χρόνου έρευνας του ψηφιακού ερευνητή έτσι ώστε είτε τα αποδεικτικά στοιχεία να καταστούν χρονικώς άκυρα είτε ο επιτιθέμενος να έχει τον απαιτούμενο χρόνο να καλύψει τα εν λόγω αποδεικτικά στοιχεία. Ωστόσο, τόσο η χρήση των PETs όσο και των τεχνικών Anti-Forensics δημιουργεί προβλήματα ιδιωτικότητας τρίτων χρηστών κατά την εκτέλεση της ψηφιακής δικανικής λόγω μη σωστής εφαρμογής τους, μη σωστής συντήρησής τους ή και λόγω κατασκευαστικών σφαλμάτων των χρησιμοποιούμενων εργαλείων.

Τα PETs όσο και τα Anti Forensics τυχαίνουν ευρείας αποδοχής και η χρήση τους ολοένα και αυξάνεται. Η χρήση τους ωστόσο ενέχει κινδύνους για την ιδιωτικότητα των χρηστών κατά τη συλλογή ψηφιακών πειστηρίων από τον ψηφιακό ερευνητή.

- Μερικοί από τους χρήστες που εγκαθιστούν εργαλεία Anti Forensics δεν τα χρησιμοποιούν σωστά με αποτέλεσμα σημαντικά προσωπικά δεδομένα να παραμένουν διαθέσιμα.
- Μερικά εργαλεία Anti-Forensics δεν λειτουργούν με τον τρόπο που διαφημίζονται αφήνοντας στοιχεία που μπορεί να οδηγήσουν στην ανάκτηση των δεδομένων.

Τα PETs που χρησιμοποιούνται σε μια ερευνητική διαδικασία θα πρέπει να έχουν τα εξής χαρακτηριστικά:

- Δεν πρέπει να επιβαρύνουν τον ερευνητή. Ο ερευνητής δεν θα πρέπει να χρειάζεται να εκτελεί σημαντικό αριθμό πρόσθετων καθηκόντων κατά τη διάρκεια της έρευνας.
- Θα πρέπει λογικά να αποκλείουν δεδομένα που προσδιορίζονται ως «άσχετα» με την έρευνα. Θα πρέπει να περιορίζουν συγκεκριμένα δεδομένα που αφορούν μέρη που δεν αποτελούν αντικείμενο έρευνας.
- Θα πρέπει να παρέχουν στον ερευνητή την ελευθερία πρόσβασης σε δεδομένα που θεωρούνται ψευδώς αρνητικά.

- Θα πρέπει να υποστηρίζουν τη λογοδοσία και τη διαφάνεια. Θα πρέπει να καταγράφουν τυχαίες και σκόπιμες προσβάσεις ιδιωτικών δεδομένων που δεν έχουν καμία σχέση με την έρευνα.
- Δεν θα πρέπει να υπονομεύουν μια έρευνα προσθέτοντας σημαντικές χρονικές καθυστερήσεις σε καθιερωμένες τεχνικές έρευνας, όπως φιλτράρισμα και εξόρυξη κειμένου.

Γίνεται κατανοητό λοιπόν, ότι κατά τη διαδικασία της εύρεσης και συλλογής των αποδεικτικών στοιχείων υφίσταται η πιθανότητα να παραβιαστούν προσωπικά δεδομένα κάποιου χρήστη. Ο ψηφιακός ερευνητής κατά την εκτέλεση της διαδικασίας συλλογής ψηφιακών πειστηρίων, θα αναζητήσει αρχεία τα οποία ενδέχεται να βρεθούν στις ακόλουθες μορφές:

- Κρυπτογραφημένα με αλγόριθμο κρυπτογράφησης ή με τεχνική Anti-Forensics και μπορεί να είναι φωτογραφίες, βίντεο και αρχεία κειμένου διάφορων ατόμων χωρίς τη δυνατότητα να ταυτοποιηθούν οι ιδιοκτήτες τους.
- Μετα-δεδομένα δραστηριότητας των χρηστών στο υπό εξέταση πληροφοριακό σύστημα (για παράδειγμα χρήση των εφαρμογών, είσοδος – έξοδος από εφαρμογές, cookies για το διαδίκτυο).
- Αρχεία καταγραφής δραστηριότητας και αρχεία καταγραφής συμβάντων όπου καταγράφεται η δικτυακή ροή όλων των χρηστών του εν λόγω συστήματος.

Τα μετα-δεδομένα της δραστηριότητας των χρηστών στο διαδίκτυο είναι διαθέσιμα στον ψηφιακό ερευνητή με τη χρήση των κατάλληλων εργαλείων δικανικής έρευνας (Forensic Tools) ακόμα και αν οι on – line συναλλαγές τους γίνουν με τη χρήση της incognito λειτουργίας των browsers καθιστώντας προσωπικά στοιχεία τρίτων ατόμων διαθέσιμα κατά τη διαδικασία της ψηφιακής δικανικής. Στο ίδιο άρθρο αναφέρεται ότι ακόμα και αρχεία κειμένου τα οποία ανήκουν στα άτομα για τα οποία έχει εκδοθεί ένταλμα έρευνας μπορεί να περιέχουν διαδραστικά δεδομένα τα οποία συσχετίζονται με τρίτα ως προς την υπόθεση άτομα. Επιπρόσθετα, από την ανωτέρω διαδικασία συλλογής ψηφιακών πειστηρίων ο ψηφιακός ερευνητής αποκτά το σύνολο των ψηφιακών μέσων αποθήκευσης που ανήκουν στον ύποπτο της υπό εξέταση υπόθεσης και τα οποία μπορεί να περιλαμβάνουν προσωπικά αρχεία (ιατρικά δεδομένα, οικογενειακές φωτογραφίες-βίντεο) τα οποία δεν συσχετίζονται με την υπόθεση και η απόκτηση και η επεξεργασία αυτών αποτελεί καταπάτηση της ιδιωτικότητάς του.

Λόγω των ανωτέρω τεχνικών όπου συνήθως είναι η πρακτική να λαμβάνονται πλήρη αντίγραφα του σκληρού δίσκου του υπό εξέταση συστήματος ώστε να διασφαλισθεί η ακεραιότητα των δεδομένων υφίσταται η πιθανότητα κατά την εξέταση των e-mail server, ο ψηφιακός ερευνητής να αποκτήσει πρόσβαση στα mail χιλιάδων χρηστών που δεν έχουν σχέση με την υπόθεση, ακόμα και αν η αναζήτηση για συγκεκριμένα mail έχει γίνει με τη χρήση προσδιορισμένων λέξεων-κλειδιών. Μία έτερη πρακτική είναι να λαμβάνεται κρυπτογραφημένο το πλήρες αντίγραφο του δίσκου με αποτέλεσμα ο ψηφιακός ερευνητής να μην μπορεί να εντοπίσει τα σχετικά με την υπόθεση δεδομένα. Υπάρχουν και οι περιπτώσεις όπου μπορεί να λάβει το κλειδί

αποκρυπτογράφησης με αποτέλεσμα τα προσωπικά δεδομένα τρίτων ως προς την υπόθεση ατόμων να παραβιάζονται.

Πέρα από τη διαδικασία που θα ακολουθηθεί για τη συλλογή των ψηφιακών πειστηρίων, το πρόβλημα της ιδιωτικότητας κατά τη συλλογή δεδομένων έγκειται και στην ακεραιότητα του ίδιου του ερευνητή. Βάσει των προγραμματισμένων διαδικασιών που ακολουθούνται κατά την έρευνα, ο ψηφιακός ερευνητής έρχεται συνήθως σε επαφή με πληροφορίες που δεν είναι άμεσα συσχετίσιμες με την υπό εξέταση υπόθεση. Είναι επιπλέον πιθανό κατά την έρευνα ο ψηφιακός ερευνητής να μην αποκαλύψει ορισμένα στοιχεία προσωπικού χαρακτήρα ώστε να τα χρησιμοποιήσει μετέπειτα για ιδίους σκοπούς. Αυτό ωστόσο δεν αποτελεί μόνο παραβίαση της ιδιωτικότητας των προσωπικών δεδομένων αλλά θέτει ενδεχομένως σε κίνδυνο και τον οργανισμό που δέχεται την ψηφιακή δικανική έρευνα καθώς η γνωστοποίηση παραβίασης των εν λόγω στοιχείων θα έχει αρνητικό αντίκτυπο στη φήμη του και θα του προσδώσει αρνητική δημοσιότητα.

3.3 Παραδεκτό ψηφιακών πειστηρίων

Για να είναι παραδεκτά στο δικαστήριο τα ψηφιακά αποδεικτικά στοιχεία πρέπει να είναι σχετικά επί του υπό κρίση ζητήματος και αξιόπιστα. Το αξιοσημείωτο είναι ότι η προϋπόθεση της αξιοπιστίας εξετάζεται σε μια άγνωστη για την ελληνική έννομη τάξη διαδικασία, το προδικαστικό «*Daubert ακροατήριο*». Ο δικαστής στην προδικαστική αυτή διαδικασία επιφορτίζεται με τον έλεγχο της μεθοδολογίας που αποφασίστηκε να ακολουθεί, ήτοι τα βήματα στη διεξαγωγή της έρευνας, καθώς επίσης και να διατυπώσει γνώμη επί της τεχνικής. Τόσο η μεθοδολογία όσο και η τεχνική πρέπει να δίνουν ακέραια και τελικά αξιόπιστα στοιχεία. Η διαδικασία Daubert καθορίζει τέσσερις κατευθυντήριες γραμμές που ακολουθούνται στην αξιολογική διαδικασία.

1. Δοκιμή: η διαδικασία πρέπει να έχει προηγουμένως δοκιμαστεί
2. Ποσοστό λάθους: Αφού έχει δοκιμαστεί θα δοθεί και το ποσοστό σφαλμάτων στα εξαγόμενα αποτελέσματα.
3. Δημοσίευση: Είναι σημαντικό να έχει δημοσιευθεί τόσο η μεθοδολογία όσο και η τεχνική (εργαλείο) και να έχει υποβληθεί σε μελέτες και πιθανόν σε διορθώσεις από την επιστημονική κοινότητα.
4. Αποδοχή: Η μεθοδολογία και το εργαλείο ψηφιακής εγκληματολογίας πρέπει σε κάθε περίπτωση να είναι αποδεκτά από την επιστημονική κοινότητα.

Η κατευθυντήρια γραμμή ορίζει ότι οι δοκιμές θα υποδείξουν εάν η εκάστοτε διαδικασία δύναται να παρέχει ακριβή αποτελέσματα. Οι δοκιμές επιμερίζονται σε δύο κατηγορίες, στις «*ψευδώς αρνητικές*» (false negative) και «*ψευδώς θετικές*» (false positive). Συγκεκριμένα, τα ψευδώς αρνητικά τεστ διασφαλίζουν ότι το χρησιμοποιούμενο εργαλείο παρέχει όλα τα δεδομένα. Με τις ψευδώς θετικές δοκιμές ελέγχεται ότι δεν εισάγονται νέα δεδομένα στο αποτέλεσμα. Η δεύτερη κατηγορία είναι δύσκολο να ελεγχθεί και συνήθως γίνεται με τη χρήση δεύτερου εργαλείου.

3.4 Διαδικασία συλλογής ψηφιακών πειστηρίων

Η διαδικασία χειρισμού των ηλεκτρονικών αποδεικτικών στοιχείων μπορεί να διαιρεθεί σε διάφορες φάσεις. Η πρώτη φάση περιλαμβάνει την ταυτοποίηση και τη συλλογή των στοιχείων, καταπολεμώντας τυχόν ιούς και προφυλάσσοντας τα στοιχεία, ενώ παράλληλα δημιουργούνται και έγγραφα. Στη δεύτερη φάση, προσδιορίζονται τα στοιχεία που είναι πιθανότερο να εξυπηρετήσουν τους σκοπούς της έρευνας, δίνοντας μεγαλύτερη έμφαση σε αυτά που δύνανται να αλλοιωθούν με την πάροδο του χρόνου. Κατά την τρίτη φάση τα ευρήματα αξιολογούνται και ερμηνεύονται, ενώ κατά την τέταρτη φάση παρουσιάζονται τα αποτελέσματα σε μια έκθεση, η οποία περιλαμβάνει πραγματικά περιστατικά, ερμηνεία και γνώμη ειδικού πραγματογνώμονα. Η έκθεση και η παρουσίαση συνιστούν βασικά βήματα στον κύκλο ζωής των ψηφιακών πειστηρίων, δεδομένου ότι το δικαστήριο εξετάζει την έκθεση και τα τεχνικά επιστημονικά ευρήματα όπως αυτά συνοδεύονται από τις ανάλογες αναφορές. Σε κάθε περίπτωση όλες οι ενέργειες και τα συμπεράσματα πρέπει να τεκμηριώνονται (πώς βρέθηκαν τα αποδεικτικά στοιχεία, σε τι κατάσταση βρέθηκαν, κλπ.).

Οι πρώτες κινήσεις που γίνονται από τον ερευνητή που ακολουθεί το μοντέλο του ινστιτούτου NIST είναι να αναγνωρίσει τις πηγές από τις οποίες μπορεί να αποκτήσει πληροφορίες και δεδομένα. Οι πηγές αυτές μπορεί να είναι εκατοντάδες. Οι πιο κοινές που ο καθένας μπορεί να φανταστεί είναι επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές, εξυπηρετητές, δίκτυα. Μέσω αυτών των ψηφιακών συσκευών και δεδομένων, ο ερευνητής θα φτάσει στο σκληρό δίσκο του συστήματος και σε θύρες USB που μπορεί να τις χρησιμοποιήσει για να εξάγει τις πληροφορίες που χρειάζεται να συλλέξει. Επίσης, οι οπτικοί δίσκοι, τα USB sticks, οι κάρτες μνήμης θεωρούνται μέσα εξωτερικής αποθήκευσης που περιέχουν σημαντικά δεδομένα. Εκτός από αυτά, δεδομένα υπάρχουν ακόμα και σε κινητά τηλέφωνα, mp3 players, iPods, ψηφιακές κάμερες. Ο ερευνητής κατά την διάρκεια της έρευνάς του οφείλει μέσα από την εμπειρία του να ξεχωρίσει οποιαδήποτε συσκευή μπορεί να του προσφέρει πληροφορία. Δεν πρέπει να παραβλέπεται πως χρήσιμα δεδομένα μπορούν να αποθηκευθούν ακόμα και στη μνήμη RAM του υπολογιστή ή στο δίκτυο, που σημαίνει πως στην επόμενη επανεκκίνηση ή στο κλείσιμο υπολογιστή αυτά θα χαθούν, άρα χρήζουν ιδιαίτερης προσοχής.

Κάποια άλλα σημεία που θα πρέπει να έχει στο νου ο ερευνητής είναι και σημεία που βρίσκονται εκτός του οργανισμού που ερευνάει. Τέτοια, σημεία μπορεί να είναι ο πάροχος Διαδικτύου που χρησιμοποιεί ο οργανισμός και από εκεί μπορεί να αποκτήσει τα logs, ούτως ώστε να μελετήσει την δραστηριότητα στο Διαδίκτυο. Για να αποκτήσει, ωστόσο κάποιος τα logs θα πρέπει να προηγηθεί δικαστική εντολή. Δεν είναι δυνατόν πάντα να συλλεχθούν πληροφορίες από τα μέσα που επιθυμεί ο ερευνητής για πρακτικούς λόγους. Για αυτό και πρέπει να είναι ικανός να βρει άλλους τρόπους να αποκτήσει τα δεδομένα που χρειάζεται. Από την στιγμή που η πρόληψη είναι η καλύτερη θεραπεία, οι εταιρείες και οι ειδικοί που δουλεύουν σε αυτές μπορούν να λάβουν κάποια μέτρα πρόληψης για να συλλέγουν χρήσιμα δεδομένα που θα χρειαστούν σε μια ψηφιακή εγκληματολογική έρευνα και θα διευκολύνουν τον ερευνητή σε περίπτωση που χρειαστεί. Τα πιο γνωστά λειτουργικά συστήματα, έχουν την δυνατότητα να ρυθμιστούν για να καταγράφουν τις αλλαγές που μπορεί να προκύψουν στις ρυθμίσεις ασφαλείας του συστήματος. Αυτά τα logs μπορούν να

αποδειχτούν ιδιαίτερα σημαντικά στο μέλλον για έναν οργανισμό. Όλα αυτά τα μέτρα βέβαια, θα πρέπει να σχεδιαστούν έχοντας ως βάση τον σεβασμό στην ιδιωτικότητα του εργαζόμενου ή γενικότερα του χρήστη.

Αφού ο ερευνητής εντοπίσει τις πιθανές πηγές, επόμενο βήμα είναι να αποκτήσει τα δεδομένα που χρειάζεται ώστε να τα μελετήσει. Το NIST διαχωρίζει αυτήν την διεργασία σε τρεις μικρότερες διεργασίες, τις οποίες θα δούμε παρακάτω:

- Σχεδιασμός: Ο Σχεδιασμός σύμφωνα με τις πιθανές πηγές είναι ένα σημαντικό βήμα, διότι ο ερευνητής σε αυτό το σημείο βασισμένος στα ψηφιακά μέσα που έχει εντοπίσει θα τα κατηγοριοποιήσει και θα τα διαχωρίσει. Οι παράγοντες που θα λάβει υπόψη του για να θέσει τις προτεραιότητες έχουν να κάνουν με την πιθανή αξία μιας πηγής και για το πόσο χρήσιμα θα είναι τα δεδομένα που μπορεί να προσφέρει. Ο ερευνητής σύμφωνα με την εμπειρία του και την φύση του συμβάντος θα μπορέσει να υπολογίσει πόσο σημαντική είναι η κάθε πηγή. Ακολουθεί, η ρευστότητα των δεδομένων. Στην ρευστότητα έχουμε αναφερθεί ήδη μιλώντας για την μνήμη RAM, η οποία μπορεί να έχει αποθηκευμένα δεδομένα τα οποία όμως μετά από τον τερματισμό του υπολογιστή θα χαθούν. Άρα καλό θα ήταν η συλλογή των δεδομένων αυτών να βρίσκεται πολύ ψηλά στην λίστα του ερευνητή και να προτιμώνται από τα υπόλοιπα δεδομένα. Ο τρίτος παράγοντας είναι η προσπάθεια που απαιτείται για τη συλλογή, αφού οι πηγές θα είναι πολλές και πιθανόν να πρέπει να εμπλακούν και άλλοι ειδικοί. Επίσης, η προσπάθεια που χρειάζεται για να αποκτήσει κάποιος πρόσβαση σε στοιχεία που μόνο ο πάροχος Διαδικτύου κατέχει, θα είναι σίγουρα πολύ μεγάλη και χρονοβόρα.
- Ανάκτηση Δεδομένων: Η ανάκτηση των δεδομένων προτείνεται να γίνει με εργαλεία της ψηφιακής εγκληματολογίας και να διατηρούνται στην αρχική μορφή τους. Η διαδικασία μπορεί να γίνει είτε τοπικά, είτε μέσω του δικτύου. Ο καλύτερος τρόπος ανάμεσα στους δύο είναι ο τοπικός επειδή οι πληροφορίες και το σύστημα ελέγχονται καλύτερα.
- Επαλήθευση των Δεδομένων: Μετά την ανάκτηση των δεδομένων, κρίνεται απαραίτητο να επαληθευτεί η ακεραιότητά τους. Αυτό γίνεται για νομικούς λόγους και έτσι ο ερευνητής επιβεβαιώνει πως δεν έχει τροποποιήσει ότι έχει συλλέξει. Και σε αυτό το βήμα η επαλήθευση θα γίνει με εργαλεία της ψηφιακής εγκληματολογίας, όπου μέσω της συνάρτησης κατακερματισμού θα συγκριθούν τα αρχικά στοιχεία με αυτά που απέκτησε ο ερευνητής κατά την διάρκεια της έρευνας.

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

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

Κεφάλαιο 4^ο: Στάδια ψηφιακής εγκληματολογικής ανάλυσης

4.1: Εντοπισμός Συσκευών

Τα στάδια της εγκληματολογικής ανάλυσης αποτελούν το σημαντικότερο μέρος της έρευνας, για την ανάκτηση δεδομένων και την απόκτηση πληροφοριών, έτσι ώστε οι ειδικοί ερευνητές να είναι σε θέση να τις χρησιμοποιήσουν στο δικαστήριο. Ωστόσο, πριν από αυτό το κομμάτι, είναι απαραίτητο για την έρευνα να συγκεντρωθούν όλα τα αποδεικτικά στοιχεία με ασφαλή τρόπο.

Σε αυτό το σημείο έχει νόημα ο εντοπισμός των συσκευών και των πόρων στα οποία περιέχονται τα δεδομένα που θα αποτελέσουν μέρος της έρευνας. Τα δεδομένα που εμπλέκονται σε μια έρευνα μπορεί να βρίσκονται σε συσκευές της εκάστοτε επιχείρησης, όπως υπολογιστές ή laptops, αλλά και σε προσωπικές συσκευές των χρηστών, όπως κινητά τηλέφωνα και tablets. Στη συνέχεια, οι συσκευές αυτές κατάσχονται και απομονώνονται, ώστε να εκμηδενιστεί κάθε πιθανότητα αλλοίωσης. Εάν τα δεδομένα βρίσκονται στον διακομιστή, στο δίκτυο ή ακόμα και στο cloud, ο ερευνητής ή η ίδια επιχείρηση πρέπει να διασφαλίσει ότι κανείς άλλος εκτός από την ομάδα έρευνας δεν έχει πρόσβαση σε αυτά.

4.2: Εξαγωγή και Διατήρηση Δεδομένων

Το επόμενο βήμα της εγκληματολογικής ανάλυσης είναι να διασφαλιστεί η ακεραιότητα και η καλή κατάσταση των δεδομένων. Σε αυτή τη φάση, αναφερόμαστε στη διατήρηση δεδομένων, για μια διαδικασία, δηλαδή, ασφαλούς φύλαξης των περιουσιακών στοιχείων χωρίς αλλοίωση ή αλλαγή του περιεχομένου των στοιχείων που βρίσκονται σε συσκευές και διαγραμμένα μέσα. Αποτελεί το πρώτο βήμα στην ανάκτηση ψηφιακών αποδεικτικών στοιχείων.

Η διατήρηση περιλαμβάνει την αναζήτηση, την αναγνώριση, την τεκμηρίωση και τη συλλογή αποδεικτικών στοιχείων που βασίζονται σε ηλεκτρονικά στοιχεία. Συγκεκριμένα, αφού κατασχεθούν οι συσκευές που εμπλέκονται σε μια έρευνα και αποθηκευτούν σε ασφαλή τοποθεσία, ο ερευνητής ψηφιακής εγκληματολογίας χρησιμοποιεί κατάλληλες τεχνικές για να εξάγει οποιαδήποτε δεδομένα που μπορεί να είναι σχετικά με την έρευνα και τα αποθηκεύει με ασφάλεια. Η διαδικασία αυτή μπορεί να περιλαμβάνει τη δημιουργία ψηφιακού αντιγράφου των σχετικών δεδομένων, το οποίο είναι γνωστό ως «εγκληματολογική εικόνα». Το αντίγραφο αυτό χρησιμοποιείται στη συνέχεια για ανάλυση και αξιολόγηση, ενώ τα πρωτότυπα δεδομένα και οι συσκευές τοποθετούνται σε ασφαλές μέρος, όπως ένα χρηματοκιβώτιο. Με τον τρόπο αυτό αποτρέπεται οποιαδήποτε αλλοίωση των αρχικών δεδομένων, ακόμη και αν η έρευνα τεθεί σε κίνδυνο. Η αποτυχία διατήρησης των αποδεικτικών στοιχείων στην αρχική τους κατάσταση θα μπορούσε να θέσει σε κίνδυνο ολόκληρη την έρευνα, χάνοντας ενδεχομένως πολύτιμες πληροφορίες που σχετίζονται με την υπόθεση.

4.3: Αξιολόγηση και Ανάλυση της Σκηνής Εγκλήματος

Οι εσφαλμένες διαδικασίες ή ο ακατάλληλος χειρισμός μιας κινητής συσκευής κατά τη διάρκεια της κατάσχεσης μπορεί να προκαλέσει απώλεια των ψηφιακών δεδομένων. Επιπλέον, οι παραδοσιακές εγκληματολογικές μεθόδους, όπως τα δακτυλικά αποτυπώματα ή η εξέταση DNA, μπορεί να χρειαστεί να εφαρμοστούν για να διαπιστωθεί η σύνδεση μεταξύ μιας κινητής συσκευής και του χρήστη της. Εάν η συσκευή δεν χειρίζεται σωστά, τα φυσικά αποδεικτικά στοιχεία ενδέχεται να αλλοιωθούν και να καταστούν άχρηστα. Παράλληλα, αφού εντοπιστούν και απομονωθούν οι εμπλεκόμενες συσκευές και τα δεδομένα αντιγραφούν κι αποθηκευτούν με ασφάλεια, οι ψηφιακοί εγκληματολόγοι χρησιμοποιούν διάφορες τεχνικές για να εξάγουν τις σχετικές πληροφορίες και να τις εξετάσουν, αναζητώντας ενδείξεις ή στοιχεία που παραπέμπουν σε αδίκημα. Αυτό συχνά περιλαμβάνει την ανάκτηση και εξέταση διαγραμμένων, κατεστραμμένων ή κρυπτογραφημένων αρχείων, χρησιμοποιώντας τεχνικές όπως:

- Αντίστροφη στενογραφία: τεχνική που χρησιμοποιείται για την εξαγωγή κρυμμένων δεδομένων εξετάζοντας το υποκείμενο hash ή τη σειρά χαρακτήρων που αντιπροσωπεύει μια εικόνα ή άλλο στοιχείο δεδομένων.
- Αναζήτηση αρχείων ή δεδομένων: εντοπισμός και ανάκτηση διαγραμμένων αρχείων με αναζήτηση των αποτυπωμάτων – μονοπατιών που μπορεί να αφήνουν τα διαγραμμένα αρχεία.
- Αναζήτηση με λέξεις-κλειδιά: χρήση λέξεων-κλειδιών για τον εντοπισμό και την ανάλυση πληροφοριών σχετικών με την έρευνα, συμπεριλαμβανομένων των διαγραμμένων δεδομένων.

Αυτές είναι μερικές μόνο από τις πολλές τεχνικές που χρησιμοποιούν οι ψηφιακοί εγκληματολόγοι για την αποκάλυψη αποδεικτικών στοιχείων.

4.4: Τεκμηρίωση της Σκηνής Εγκλήματος

Τα αποδεικτικά στοιχεία πρέπει να αναγνωρίζονται και να καταγράφονται με ακρίβεια. Μετά την ανάλυση, τα ευρήματα της έρευνας τεκμηριώνονται κατάλληλα με τρόπο που καθιστά εύκολη την οπτικοποίηση ολόκληρης της διαδικασίας έρευνας και των συμπερασμάτων της. Η σωστή τεκμηρίωση βοηθά στη διαμόρφωση ενός χρονοδιαγράμματος των δραστηριοτήτων που εμπλέκονται σε παραβάσεις, όπως υπεξαίρεση, διαρροή δεδομένων ή παραβιάσεις δικτύου. Μη ηλεκτρονικά υλικά όπως εγχειρίδια και υλικό συσκευασίας μπορεί να παρέχουν χρήσιμες πληροφορίες σχετικά με τις δυνατότητες της συσκευής, το δίκτυο που χρησιμοποιείται, πληροφορίες λογαριασμού και κωδικούς ξεκλειδώματος για το PIN. Η φωτογράφιση του τόπου του εγκλήματος σε συνδυασμό με την τεκμηρίωση μιας έκθεσης σχετικά με την κατάσταση κάθε ψηφιακής συσκευής και όλων των υπολογιστών που μετρήθηκαν, μπορεί να είναι χρήσιμη στην έρευνα, εφόσον προκύψουν ερωτήματα σχετικά με το περιβάλλον. Θα πρέπει να δημιουργηθεί ένα αρχείο όλων των δεδομένων. Όλες οι ηλεκτρονικές συσκευές, συμπεριλαμβανομένων των κινητών, τα οποία ενδέχεται να αποθηκεύουν δεδομένα, θα πρέπει να φωτογραφίζονται μαζί με όλα τα καλώδια των περιφερειακών συσκευών, τα διαγραμμένα μέσα και τις συνδέσεις. Ο ερευνητής θα πρέπει να

αποφεύγει να αγγίζει ή να αλλοιώνει την κινητή συσκευή κατά τη φωτογράφιση της και το περιβάλλον όπου βρέθηκε. Εάν η οθόνη της συσκευής είναι σε ορατή κατάσταση, τα περιεχόμενα της οθόνης θα πρέπει να φωτογραφίζεται και, εάν είναι απαραίτητο, να καταγράφεται χειροκίνητα, αποτυπώνοντας την ώρα, την κατάσταση της υπηρεσίας, στάθμη της μπαταρίας και άλλα εικονίδια που εμφανίζονται.

Παρακάτω, παρουσιάζονται πιο αναλυτικά τα βήματα που οφείλει να ακολουθεί ένας ειδικός ερευνητής ψηφιακών εγκλημάτων:

- Οφείλει να ακολουθεί την πολιτική της δικαιοδοσίας για την εξασφάλιση της σκηνής του εγκλήματος. Αυτό θα περιλαμβάνει τη διασφάλιση της απομάκρυνσης όλων των ατόμων από τον τόπο του εγκλήματος, άμεση περιοχή από την οποία πρόκειται να συλλεχθούν αποδεικτικά στοιχεία. Σε αυτό το σημείο της έρευνας μην αλλάξετε την κατάσταση οποιασδήποτε ηλεκτρονικής συσκευής: Εάν είναι απενεργοποιημένη, αφήστε την απενεργοποιημένη. Εάν είναι ενεργοποιημένη, αφήστε την ενεργοποιημένη.
- Οφείλει να προστατεύει τα ευπαθή δεδομένα φυσικά και ηλεκτρονικά. Τα ευπαθή δεδομένα μπορεί να βρίσκονται σε κουτιά αναγνώρισης κλήσεων, κινητά τηλέφωνα και άλλες παρόμοιες συσκευές. Ο πρώτος ανταποκριτής θα πρέπει να έχει πάντα κατά νου ότι οποιαδήποτε συσκευή που περιέχει ευπαθή δεδομένα πρέπει να ασφαρίζεται αμέσως, να τεκμηριωθεί ή/και να φωτογραφηθεί.

4.5: Παρουσίαση

Μόλις ολοκληρωθεί η έρευνα, τα πορίσματα παρουσιάζονται είτε σε ένα δικαστήριο είτε στην επιτροπή ή στην ομάδα που θα καθορίσει την έκβαση μιας αγωγής ή μιας εσωτερικής καταγγελίας. Οι ερευνητές ψηφιακής εγκληματολογίας μπορούν να ενεργήσουν ως ειδικοί μάρτυρες, συνοψίζοντας και παρουσιάζοντας τα στοιχεία που ανακάλυψαν και γνωστοποιώντας τα ευρήματά τους.

Κεφάλαιο 5^ο: Εργαλεία Ψηφιακής Εγκληματολογίας

Η ραγδαία εξέλιξη του κλάδου της Ψηφιακής Εγκληματολογίας έχει ως αποτέλεσμα και την ανάπτυξη πλήθους εργαλείων. Τα εργαλεία αυτά λειτουργούν τόσο σε περιβάλλον Windows (εμπορικά προϊόντα και ελεύθερου λογισμικού) όσο και σε περιβάλλον Linux (προϊόντα ανοιχτού - ελεύθερου λογισμικού). Στόχος των εργαλείων είναι να ανακαλύψουν και να ανασύρουν διαγραμμένα ή κατεστραμμένα αρχεία από ένα σκληρό δίσκο και να αποκαλύψουν την ύπαρξη και το περιεχόμενο αρχείων τα οποία είτε είναι κρυμμένα (hidden files) είτε προστατεύονται με κωδικό πρόσβασης.

5.1 Εργαλεία Συλλογής και Ανάλυσης Ψηφιακών Αποτυπωμάτων

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

Για να διασφαλίζουμε την ακεραιότητα των δεδομένων και της πηγής, και ότι δεν έχει αλλαχθεί ή αλλοιωθεί η αρχική πληροφορία, χρησιμοποιούμε της συναρτήσεις κατακερματισμού (*hash functions*). Αρχικά το αποθηκευτικό μέσο το οποίο αποτελεί την πηγή της πληροφορίας, περνάει από μια hash function και το αποτέλεσμα αποθηκεύεται. Ακολουθεί η διαδικασία της δημιουργίας αντιγράφου (*disk imaging*) και στη συνέχεια, το αντίγραφο περνάει από την ίδια hash function. Τέλος συγκρίνονται τα δυο αποτελέσματα των hash functions. Αν είναι ίδια, εξασφαλίζεται η ακεραιότητα και η αξιοπιστία τόσο της πηγής όσο και του αντιγράφου. Εξαιτίας της σημαντικότητας της διαδικασίας συλλογής των ψηφιακών αποτυπωμάτων, κάθε εργαλείο disk imaging θα πρέπει να πληροί συγκεκριμένες προδιαγραφές:

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

5.2 Εμπορικά Προϊόντα

FTK Imager:

Το FTK Imager είναι ένα εμπορικό εργαλείο που έχει δημιουργηθεί από την εταιρεία AccessData. Είναι γρήγορο, σταθερό και εύκολο στη λειτουργία του χάρη στο περιβάλλον του. Χρησιμοποιεί κατανεμημένη επεξεργασία και με αυτόν τον τρόπο αξιοποιεί πλήρως τους πολλούς πυρήνες των υπολογιστών. Έτσι, εκμεταλλεύεται πλήρως τις δυνατότητες του συστήματος για καλύτερο αποτέλεσμα. Το FTK Imager παρέχει ολοκληρωμένη επεξεργασία, με επακόλουθο το φιλτράρισμα και η αναζήτηση να γίνονται γρηγορότερα. Είναι βασισμένο σε βάση δεδομένων και χρησιμοποιεί μια βάση που είναι προσβάσιμη από τις ομάδες που δουλεύουν. Όλα τα δεδομένα αποθηκεύονται στην ίδια βάση, ασφαλή και έτσι όλοι έχουν πρόσβαση στα ίδια σημεία. Κατά αυτόν τον τρόπο υπάρχει μείωση του κόστους και της πολυπλοκότητας για την δημιουργία πολλών συνόλων με δεδομένα. Εξερευνεί τα περιεχόμενα αποθηκευτικών μέσων και δημιουργεί ακριβή αντίγραφά τους. Υποστηρίζει την ανάκτηση διαγραμμένων αρχείων. Τέλος, για τη διασφάλιση της ακεραιότητας, χρησιμοποιεί αλγορίθμους hashing, όπως ο MD5.

Blacklight:

Το Blacklight είναι ένα εμπορικό εργαλείο ανάλυσης που επιτρέπει στον ψηφιακό ερευνητή να εκτελέσει γρήγορα μια ψηφιακή έρευνα. Μπορεί να χρησιμοποιηθεί σε συσκευές που έχουν εγκαταστημένο λειτουργικό σύστημα MacOS, iOS συσκευές αλλά και σε συστήματα με Windows. Οι δυνατότητές του επεκτείνονται ακόμα και στα μέσα κοινωνικής δικτύωσης και σε υπηρεσίες ανταλλαγής μηνυμάτων.

XRY:

Το XRY είναι ένα λογισμικό φτιαγμένο από την εταιρεία MSAB. Χρησιμοποιείται σε λειτουργικά συστήματα Windows και δίνει στον χρήστη την δυνατότητα να εξάγει δεδομένα και πληροφορίες που μπορεί να του χρησιμεύσουν ως αποδείξεις από συσκευές που μπορεί να είναι έξυπνα κινητά τηλέφωνα, GPS, μόντεμ, tablets.

Internet Evidence Finder (IEF):

Το συγκεκριμένο εργαλείο είναι της εταιρείας magnetforensics. Είναι φιλικό προς τον χρήστη λόγω του γραφικού του περιβάλλοντος. Η ικανότητα του IEF έχει να κάνει με την εύρεση, ανάλυση και παρουσίαση των πειστηρίων από υπολογιστές, έξυπνα κινητά τηλέφωνα ακόμα και tablets. Αυτά μπορεί να είναι είτε στοιχεία από μηνύματα ή μέσα κοινωνικής δικτύωσης ή ακόμα και από πολλές πηγές. Τέλος, υποστηρίζει τα λειτουργικά συστήματα Windows, Linux, MacOSX.

EnCase:

Το EnCase είναι από τα πιο διαδεδομένα λογισμικά αυτού του είδους. Με το εργαλείο αυτό ο ερευνητής έχει την δυνατότητα να συλλέξει πληροφορίες από διάφορες ηλεκτρονικές συσκευές. Έχει ένα φιλικό προς τον χρήστη περιβάλλον και την ικανότητα να παράγει αυτόματη αναφορά. Εκτός από αυτά μπορεί να αποκρυπτογραφήσει στοιχεία που θα φανούν χρήσιμα κατά τη διάρκεια της έρευνας.

X-Ways forensics:

Υποστηρίζει μόνο τα λειτουργικά συστήματα Windows. Μπορεί να βρει διαγραμμένους φακέλους. Οι απαιτήσεις του όσον αφορά την εγκατάσταση είναι φυσιολογικές χωρίς να χρειάζεται κάτι ιδιαίτερο από άποψη υλικού. Δεν απαιτεί εγκατάσταση και εκτελείται απλά από μια USB συσκευή σε περίπτωση που ο χρήστης δεν επιθυμεί την εγκατάστασή του.

Oxygen Forensics Suite:

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

Acronis True Image:

Το TrueImage Echo Workstation παρέχεται από την εταιρεία Acronis και αποτελεί ένα από τα καλύτερα προγράμματα για επανάκτηση κατεστραμμένων τμημάτων του δίσκου αλλά και για τη δημιουργία κλώνου αυτού. Επίσης χρησιμοποιείται για τη δημιουργία back up των αρχείων, αλλά και επαναφορά των διαγραμμένων αρχείων. Μπορεί να δουλέψει σε Windows και Linux.

Forensics Assistant:

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

5.3 Ελεύθερου Λογισμικού

Digital Forensics Framework:

Είναι ένα λογισμικό ανοιχτού κώδικα γραμμένο σε C++, Python. Χρησιμοποιείται για τη συλλογή, διατήρηση και αποκάλυψη ψηφιακών πειστηρίων χωρίς να διακινδυνεύουν υπολογιστικά συστήματα και πληροφορίες. Επιπρόσθετα, ο χρήστης μπορεί να ανακτήσει κρυφά στοιχεία ή ακόμα και διαγραμμένα. Παρέχεται σε τρεις εκδόσεις: την DFF που είναι δωρεάν, την DFF Pro και την DFF Live. Οι δύο τελευταίες είναι εμπορικής χρήσης. Μπορούν να χρησιμοποιηθούν σε λειτουργικά συστήματα Windows και Linux.

The Sleuth Kit:

Είναι ένα λογισμικού ανοιχτού κώδικα γραμμένο σε C και Perl. Το Sleuth Kit είναι μια βιβλιοθήκη και μια συλλογή από εντολές που δίνουν τη δυνατότητα στον χρήστη να ερευνήσει τον δίσκο. Η βασική λειτουργία του προγράμματος επιτρέπει την ανάλυση μεγάλου όγκου δεδομένων και στοιχείων του συστήματος. Μπορεί επίσης, να ενσωματωθεί σε μεγαλύτερα εργαλεία ψηφιακής εγκληματολογίας και να οδηγήσει κατ' ευθείαν στην εύρεση πειστηρίων. Το Autopsy είναι μια πλατφόρμα που προσφέρει γραφικό περιβάλλον για το Sleuth Kit και παρέχει διαχείριση περιπτώσεων, αναζήτηση λέξεων-κλειδιά και πολλές άλλες αυτόματες λειτουργίες. Χρησιμοποιείται στα λειτουργικά συστήματα Windows και Linux.

Digital Evidence & Forensic Toolkit (DEFT):

Το DEFT είναι μια διανομή Linux. Σύμφωνα με τον κατασκευαστή του προγράμματος αποτελείται από GNU/Linux και την σουίτα Digital Advanced Response Toolkit (DART). Το συγκεκριμένο πρόγραμμα είναι μια λύση που βρίσκει εφαρμογή ακόμα και σε νομικές υπηρεσίες και η διανομή του είναι δωρεάν.

Sans Investigative Forensics Toolkit:

Το SIFT φτιάχτηκε βασισμένο στο Ubuntu. Είναι κυρίως δωρεάν ωστόσο κάποια plug-in κοστίζουν. Το λογισμικό είναι πολλαπλών χρήσεων και συνοδεύεται απ' όλα τα εργαλεία που μπορεί να χρειαστεί κάποιος.

Computer Aided Investigative Environment (CAINE):

Είναι ένα λογισμικό ανοιχτού κώδικα Linux διανομή με φιλικό προς τον χρήστη περιβάλλον και αντίστοιχα εργαλεία. Διανέμεται δωρεάν.

The Coroner's Toolkit:

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

SANS SIFT Workstation:

Πρόκειται για μια διανομή Linux σε VMware, η οποία αποτελεί πλήρες πακέτο για εγκληματολογική διερεύνηση σε ψηφιακά πειστήρια.

Lnix4n6:

Forensic boot CD που έχει δημιουργηθεί από την Βελγική αστυνομία, βασισμένο σε Knoppix και περιέχει λογισμικό ανοικτού τύπου για διερεύνηση ψηφιακών πειστηρίων.

SANTOKU:

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

Forevid:

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

Digital Evidence Investigator:

Πρόκειται για ένα εργαλείο ψηφιακής εγκληματολογίας για Windows, Linux και macOS. Το DEI συλλέγει ψηφιακά αποδεικτικά στοιχεία και τα παρουσιάζει σε προβολή χρονολογίου για να συνδέσει τον χρήστη με αρχεία και αντικείμενα.

Guymager:

Είναι ένα open source εργαλείο (forensic imager) για την απόκτηση πολυμέσων. Τα κύρια χαρακτηριστικά του είναι ότι υπάρχει εύκολη διεπαφή με τον χρήστη σε διάφορες γλώσσες. Είναι αρκετά γρήγορο, λόγω του pipelined σχεδιασμού του, αλλά και της συμπίεσης δεδομένων. Δημιουργεί εικόνες flat (dd), EWF (E01) και AFF, υποστηρίζει κλωνοποίηση δίσκων.

Paraben's Electronic Evidence Examiner:

Είναι μια ολοκληρωμένη ψηφιακή εγκληματολογική πλατφόρμα που έχει σχεδιαστεί για να χειρίζεται ένας πλήθος δεδομένων, πιο αποτελεσματικά, τηρώντας παράλληλα το παράδειγμα της Paraben για την εξειδικευμένη εστίαση ολόκληρης της διαδικασίας εγκληματολογικής εξέτασης. Η Paraben διαθέτει δυνατότητες σε:

- Desktop Forensics
- Email Forensics
- Smartphone Analysis
- Cloud Analysis
- IoT Forensics

Bulk Extractor:

Είναι ένα πρόγραμμα που εξάγει χαρακτηριστικά όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμούς πιστωτικών καρτών, διευθύνσεις URL και άλλους τύπους πληροφοριών από ψηφιακά αρχεία αποδεικτικών στοιχείων. Είναι ένα χρήσιμο εργαλείο για έρευνες κακόβουλου λογισμικού, έρευνες στον κυβερνοχώρο, καθώς και για ανάλυση εικόνων και σπάσιμο κωδικών πρόσβασης.

Forensic Explorer:

Είναι ένα ευέλικτο και εύχρηστο εργαλείο GUI με προηγμένη ταξινόμηση, φίλτρο, αναζήτηση με λέξεις-κλειδιά, ανάκτηση δεδομένων και τεχνολογία σεναρίων. Μπορεί να επεξεργάζεται γρήγορα μεγάλους όγκους δεδομένων, να αυτοματοποιεί σύνθετες εργασίες έρευνας, να παράγει λεπτομερείς αναφορές και να αυξάνει την παραγωγικότητα.

Dissect:

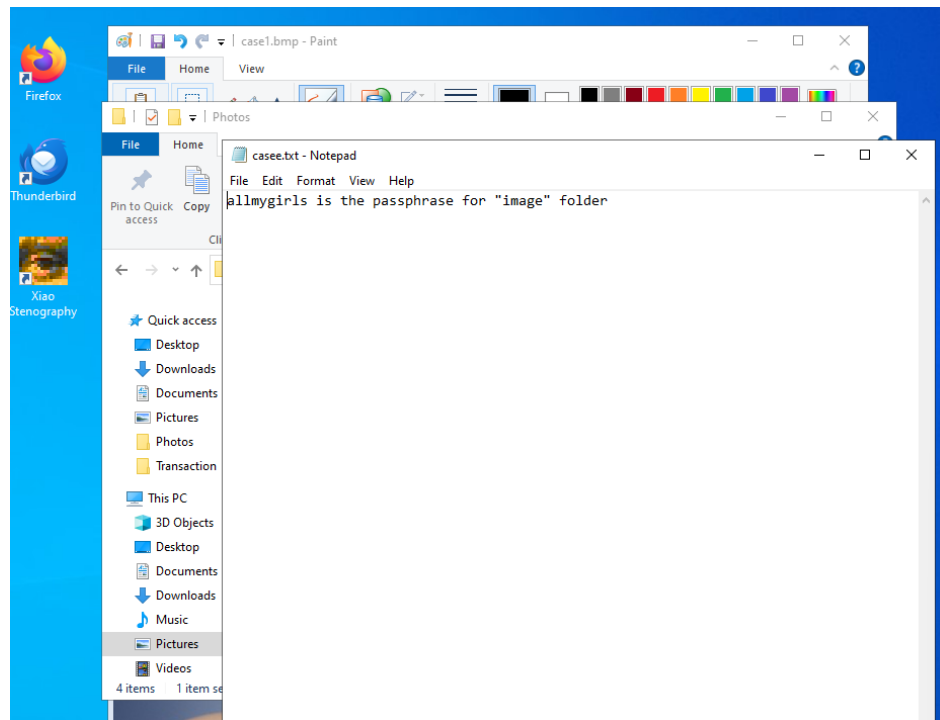
Είναι ένα σύνολο εργαλείων ψηφιακής εγκληματολογίας και αντιμετώπισης συμβάντων που μας επιτρέπει να έχουμε γρήγορη πρόσβαση και να αναλύουμε εγκληματολογικά αντικείμενα από διάφορες μορφές δίσκων και αρχείων.

Κεφάλαιο 6^ο: Σενάριο

Υπόθεση Άννας:

Μια νεαρή κοπέλα, η Άννα, είναι φοιτήτρια σε ένα δημόσιο πανεπιστήμιο της Ελλάδας. Αφού έλαβε μια σειρά μηνυμάτων σεξουαλικού περιεχομένου, ζητά τη βοήθεια των γονιών της. Από το περιεχόμενο των μηνυμάτων, φαίνεται ότι ο αποστολέας γνωρίζει σε ποιο πανεπιστήμιο σπουδάζει η Άννα, γνωρίζει τον κύκλο της, τους φίλους της και πολλές άλλες προσωπικές πληροφορίες. Η ταυτότητα του αποστολέα δεν αποκαλύπτεται στη συνομιλία τους. Καθώς ο πατέρας της Άννας ανησυχεί μήπως ο αποστολέας έχει δημοσιεύσει τις προσωπικές της πληροφορίες, αλλά και ανάρμοστο περιεχόμενο στο internet, αποφασίζει να κάνει διαδικτυακή έρευνα. Ανακαλύπτει, τελικά, ότι το όνομα της Άννας υπάρχει σε διάφορα σχόλια και αναρτήσεις σε ερωτικούς ιστοτόπους. Έτσι, αποφασίζει να απευθυνθεί στην αστυνομία της περιοχής, προκειμένου να «ξεφύγει» από αυτόν που την απειλεί. Η αστυνομία από τη μεριά της, έχει κατασχέσει τον προσωπικό υπολογιστή του ενόχου και ζητάει τη βοήθεια του αναλυτή ηλεκτρονικών εγκλημάτων (digital forensics analyst).

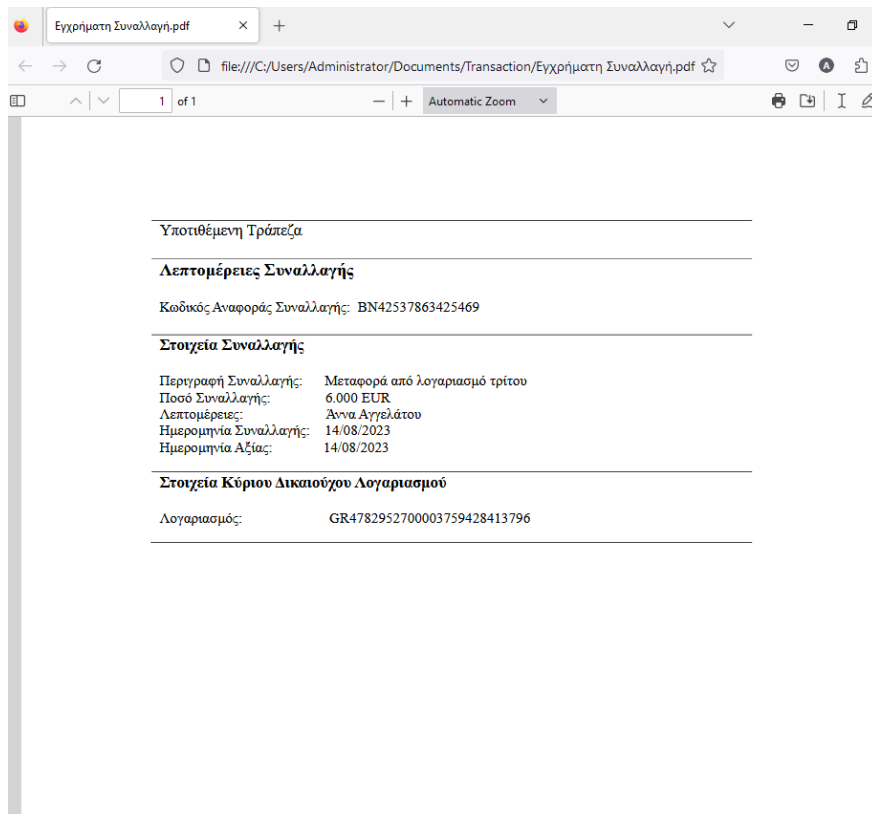
Ανοίγοντας το laptop του ενόχου, ο αναλυτής διαπιστώνει ότι για να αποκτήσει πρόσβαση, απαιτείται κωδικός. Χρησιμοποιεί το πρόγραμμα **Kon boot** εισέρχεται στα Windows OS χωρίς την ανάγκη χρήσης password. Στην επιφάνεια εργασίας, υπάρχουν ο κάδος ανακύκλωσης, το **firefox** ως προεπιλεγμένη επιλογή αναζήτησης, το **thunderbird** ως προεπιλεγμένο email και το πρόγραμμα **xiao stenography** για το οποίο ο αναλυτής καταλαβαίνει αμέσως ότι υπάρχει μία τουλάχιστον εικόνα που κρύβει κάποιο μήνυμα. Οπότε, αρχίζει να ψάχνει φωτογραφίες. Ανοίγοντας τον File Explorer (Εγγραφα), κατευθύνεται στην κατηγορία Pictures, μέσα στην οποία υπάρχουν δύο φάκελοι: Photos και case. Στον φάκελο Photos παρατηρεί ότι υπάρχουν 3 bmp files όπου απεικονίζουν 3 αντίστοιχες εικόνες μέσα από το πρόγραμμα paint των Windows. Αποφασίζει να αξιοποιήσει αυτή την πληροφορία. Με την εφαρμογή Xiao Steganography έχει τη δυνατότητα να «αποκωδικοποιήσει» τις εικόνες και να διαβάσει τα κρυμμένα μηνύματα. Ωστόσο, απαιτείται κωδικός για να ξεκλειδώσει το κάθε αρχείο. Ο κωδικός αναγράφεται στο όνομα του αρχείου. Επομένως, για το case1.bmp ο απαιτούμενος κωδικός είναι το case1. Το μήνυμα που εμφανίστηκε είναι το εξής: «**allmygirls** is the passphrase for “image” folder».



Εικόνα 1: «Εμφάνιση κρυμμένου μηνύματος από εικόνα.»

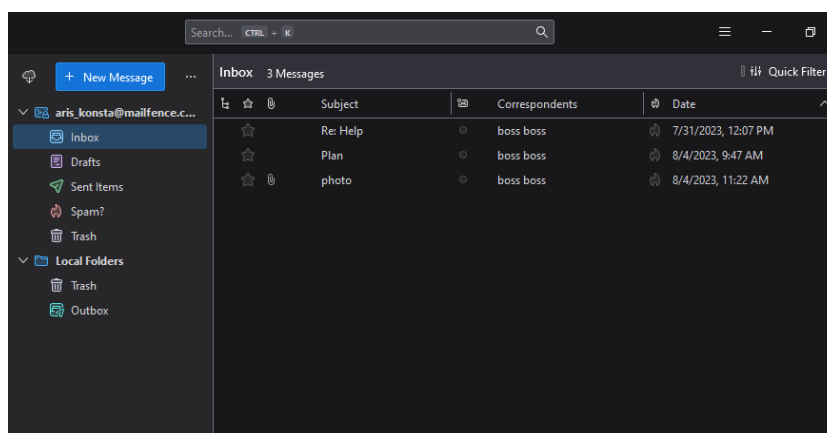
Το ίδιο μοτίβο ακολουθεί και με τα υπόλοιπα αρχεία και έτσι, ανακαλύπτει τους κωδικούς: «**!sharebody!**» για τον φάκελο naked και τον κωδικό «**&portraits**» για τον φάκελο girls. Στη συνέχεια, ο αναλυτής πρέπει να εξάγει τα αρχεία από τον φάκελο case για να βρει πληροφορίες. Χρησιμοποιεί τον ίδιο κωδικό με το όνομα του αρχείου και ξεκλειδώνει τον φάκελο. Με τα δεδομένα που έχει, ανοίγει τα images, naked και girls folders. Στο girls υπάρχει μια φωτογραφία της Άννας, ενώ στο naked, ακατάλληλες φωτογραφίες της.

Στην κατηγορία Documents, εμφανίζεται ένας φάκελος transaction ο οποίος περιέχει μια οικονομική συναλλαγή μεταξύ της Άννας και του κατηγορουμένου κι αποδεικνύει ότι του έχει στείλει το αναγραφόμενο ποσό.



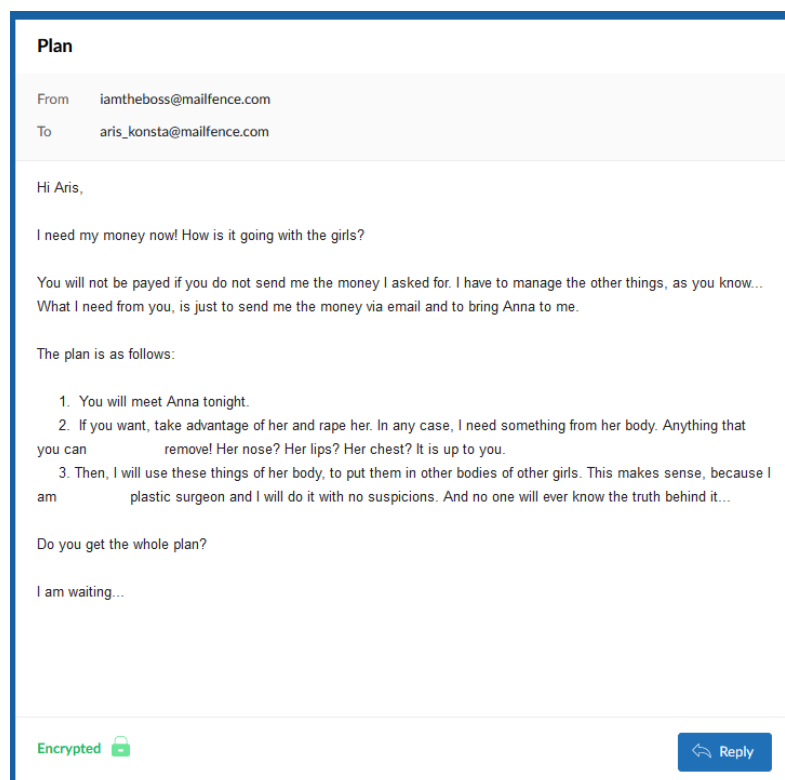
Εικόνα 2: «Εγχρήματη Συναλλαγή – Μεταφορά χρημάτων στον λογαριασμό του Άρη.»

Από την παραπάνω οικονομική συναλλαγή μπορούμε να διαπιστώσουμε ότι η Άννα, για κάποιο λόγο, έστειλε χρήματα στον Άρη. Εκκρεμεί, ως αναλυτές, να μάθουμε αυτόν τον λόγο. Η επόμενη κίνηση είναι να ερευνήσουμε το email του, ώστε να δούμε τι μηνύματα ανταλλάξε ο κατηγορούμενος και με ποιους. Σαν προεπιλεγμένο μέσο ηλεκτρονικού ταχυδρομείου, χρησιμοποιεί το thunderbird. Όπως παρατηρούμε από τα μηνύματα, ο Άρης έχει συνομιλήσει με μια οντότητα αναφερόμενη ως boss.



Εικόνα 3: «Ανταλλαγή μηνυμάτων με την οντότητα boss.»

Καταλαβαίνουμε από τα μηνύματα, ότι ο κατηγορούμενος έχει συχνή επικοινωνία με το boss. Έχουν ανταλλάξει μηνύματα στα οποία μας εξηγούν το «σχέδιο» και τις προθέσεις τους. Μάλιστα, σε ένα από τα μηνύματά τους, υπάρχει μια εικόνα με ένα κρυφό μήνυμα που μας βοηθάει στην αποκωδικοποίηση πληροφοριών. Ωστόσο, το μήνυμα στο οποίο αναγράφεται το πλάνο τους, είναι κρυπτογραφημένο κι απαιτεί passphrase για το ξεκλείδωμα και την ανάγνωσή του. Το passphrase είναι μία λέξη από τις πιο συνηθισμένες top 100.000 αγγλικές λέξεις, το «**pleasure**». Το αποκρυπτογραφημένο μήνυμα παρουσιάζεται παρακάτω:

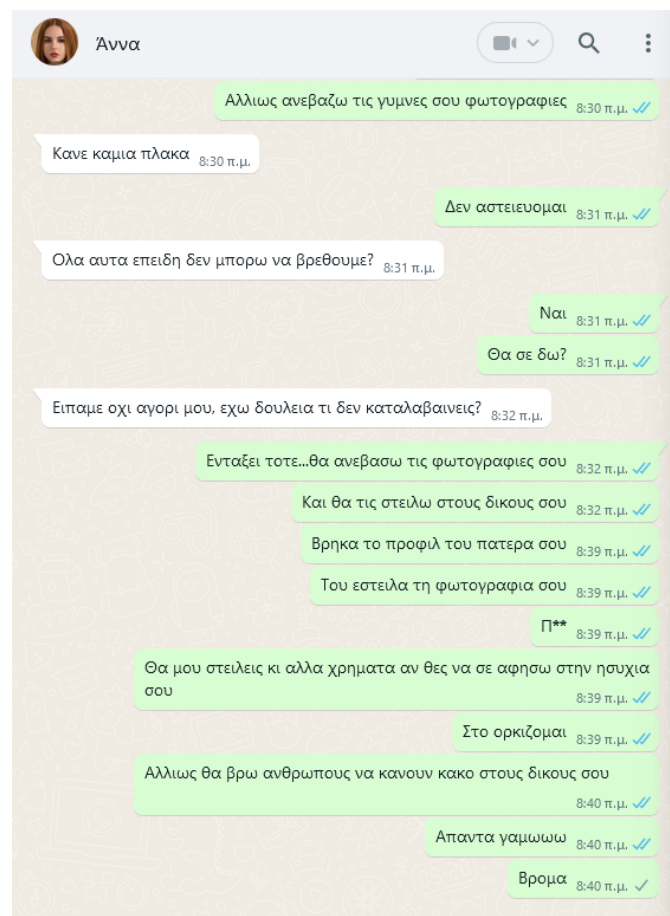


Εικόνα 4: «Σχέδιο κατηγορουμένου.»

Όπως φαίνεται από το μήνυμα, οι εντολές από το boss ήταν να εκμεταλλευτεί ο Άρης το σώμα της Άννας και να καταφέρει να αποκόψει κάποιο μέλος του σώματός της, ώστε να το χρησιμοποιήσουν έπειτα σε άλλες κοπέλες κάνοντας την αντίστοιχη χειρουργική επέμβαση. Αντιλαμβανόμαστε ότι το ανώτερο στέλεχος της οργάνωσης (boss) εργάζεται ως πλαστικός χειρουργός και πραγματοποιεί τέτοιες επεμβάσεις χωρίς να κινεί υποψίες.

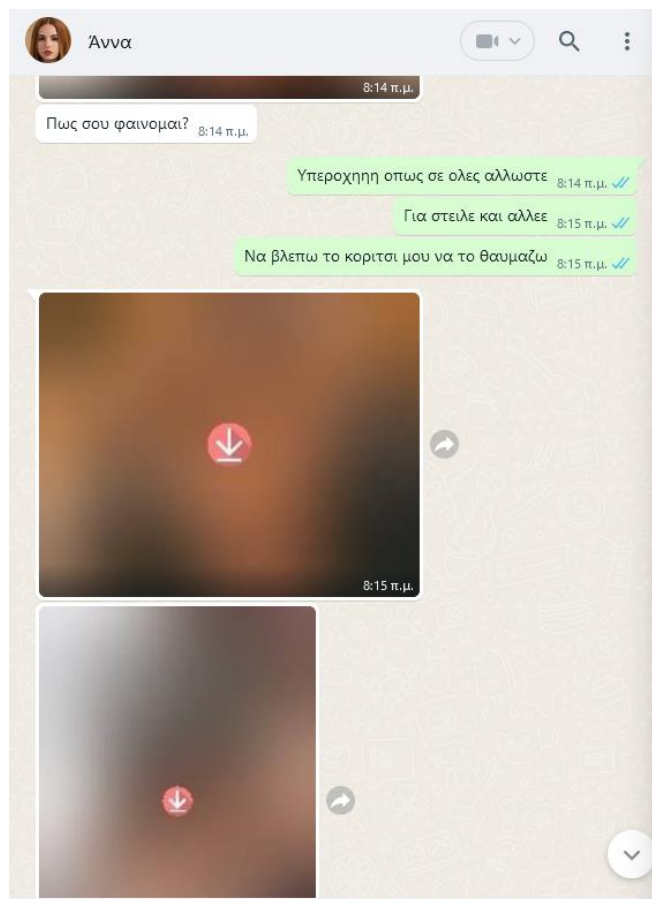
Ήρθε η ώρα να δούμε τα μηνύματα που αντάλλασσαν ο Άρης με την Άννα. Με μια γρήγορη ματιά διαπιστώνουμε ότι ο ένοχος δεν έχει «κατεβασμένη» κάποια εφαρμογή instant messaging. Οπότε καταλαβαίνουμε ότι συνομιλούσε μέσω online εφαρμογών. Κατευθυνόμαστε στο firefox. Με το που ανοίγουμε την αρχική σελίδα του συγκεκριμένου προγράμματος περιήγησης, βλέπουμε ότι υπάρχει σε ένα από τα bookmarks το **web.WhatsApp**. Αυτή είναι η εφαρμογή που ψάχνουμε! Την ανοίγουμε. Αμέσως βλέπουμε τη συνομιλία με την Άννα. Μετά από ανάγνωση της συζήτησης,

έχουμε συγκεντρώσει αρκετά στοιχεία με φωτογραφίες ανάρμοστου περιεχομένου και απεικονίσεις στιγμιότυπων με απειλές. Φαίνονται αναλυτικά παρακάτω:



Εικόνα 4: «Στιγμιότυπο απειλών.»

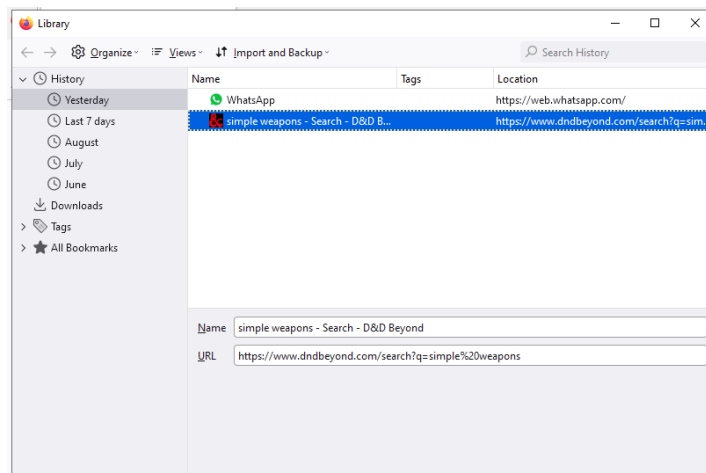
Εδώ όμως έχουμε μια ιδιαίτερη περίπτωση, καθώς ο κατηγορούμενος δεν «ανάγκασε» την Άννα να στείλει φωτογραφίες σεξουαλικού περιεχομένου, αλλά το έκανε από μόνη της.



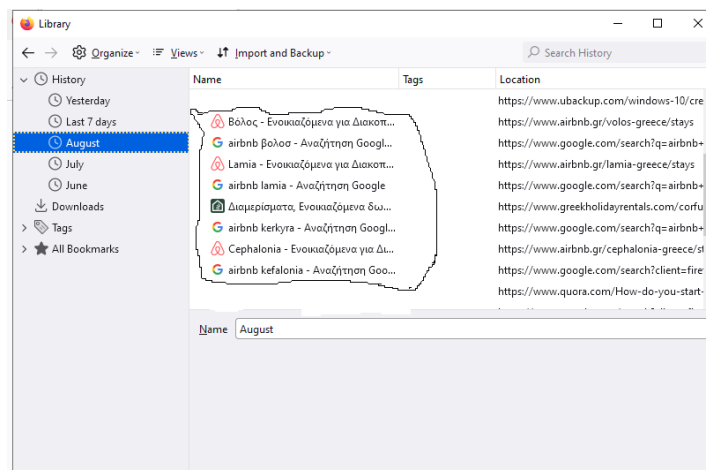
Εικόνα 5: «Στιγμιότυπο ανάρμωστον περιεχομένου.»

Σειρά έχει να δούμε το ιστορικό στο firefox του Άρη. Να μάθουμε τι αναζητήσεις έκανε, που κυμαινόταν, ώστε να καταλάβουμε τις προθέσεις του. Ανοίγουμε το Firefox History και ανακαλύπτουμε ότι ο κατηγορούμενος στις πρόσφατες αναζητήσεις του ενδιαφερόταν για όπλα. Συγκεκριμένα, έψαχνε για **simple weapons**. Αξιοσημείωτες επίσης, είναι οι αναζητήσεις που έχει κάνει για **ενοικιαζόμενα δωμάτια** σε Βόλο, Λαμία, Κέρκυρα και Κεφαλονιά. Ίσως ο Άρης σκεφτόταν να διαμείνει προσωρινά σε αυτά τα μέρη, ώστε να «ξεφύγει» από τις καταστάσεις.

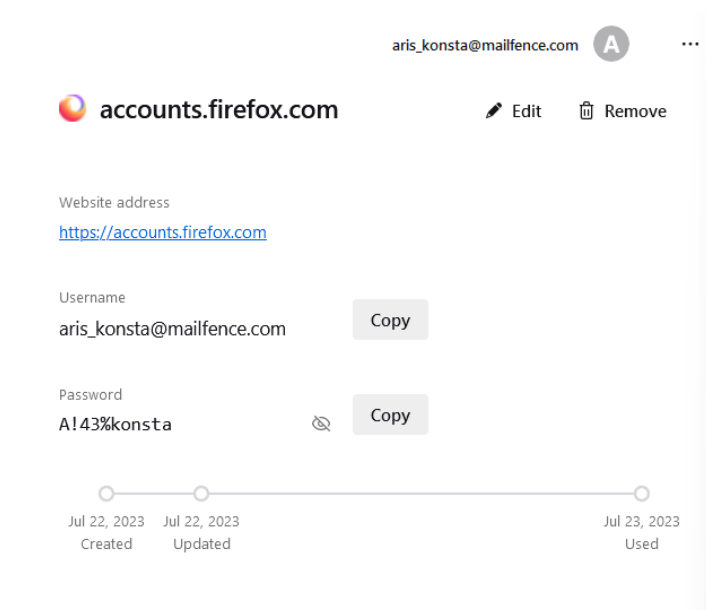
Εκτός από το ιστορικό των αναζητήσεων, ενδιαφέρον παρουσιάζουν τα **passwords**. Στο ιστορικό υπάρχει ένα account firefox με το αντίστοιχο username και password. Τα αποτελέσματα παρουσιάζονται παρακάτω:



Εικόνα 6: «Αναζήτηση για όπλα.»



Εικόνα 7: «Αναζήτηση για ενοικιαζόμενα δωμάτια.»



Εικόνα 8: «Κωδικοί για τον λογαριασμό στο firefox.»

Κεφάλαιο 7^ο : Επίλογος

Στη συγκεκριμένη πτυχιακή εργασία, έγινε λόγος για τη ψηφιακή εγκληματολογία. Σε μια σκηνή εγκλήματος, εκτός από τις Αρχές και τους εγκληματολόγους, αναλαμβάνουν δράση και οι ψηφιακοί ερευνητές. Αυτό συμβαίνει καθώς σε μια υπόθεση είναι πιθανό πληροφορίες και ίχνη ενός υπόπτου να περιέχονται σε τερματικές συσκευές, όπως υπολογιστή ή κινητό. Με αυτά τα δεδομένα που συλλέγει ο ψηφιακός αναλυτής, κρίνεται εάν ο ύποπτος είναι ένοχος ή αθώος σε μια δίκη. Η «υπόθεση της Άννας» αφορά τη διαδικτυακή πορνογραφία. Είναι σύνηθες σε τέτοια εγκλήματα, οι δράστες να απειλούν ή να εκφοβίζουν τα θύματά τους – γυναίκες στην πλειοψηφία – με σκοπό την αποστολή φωτογραφιών ανάρμοστου περιεχομένου. Στη συγκεκριμένη εργασία, ο δράστης έχει ήδη αποκτήσει τις φωτογραφίες του θύματος και ύστερα, απειλεί με βάση αυτές, με σκοπό την αποστολή χρημάτων. Σε ένα από τα κεφάλαια της εργασίας παρουσιάζεται το ολοκληρωμένο σενάριο εγκληματολογίας και η αντιμετώπισή του από τον ψηφιακό αναλυτή. Επιπλέον, γίνεται λόγος για το νομικό πλαίσιο που ισχύει στην Ευρώπη και στην Ελλάδα σχετικά με τα ψηφιακά εγκλήματα και τον τρόπο με τον οποίο τα πειστήρια του εγκλήματος γίνονται αποδεκτά νόμιμα σε μια δικαστική αίθουσα. Παρουσιάστηκαν διάφορα εργαλεία ανάλυσης και συλλογής αυτών των ψηφιακών πειστηρίων, καθώς και τα βήματα που ακολουθούνται σε μια ψηφιακή έρευνα. Μέσα σε όλη αυτή την κατάσταση, δεν θα μπορούσε να λείπει η έννοια της ιδιωτικότητας και τρόποι προστασίας της κατά τη διαδικασία των ερευνών και των αναλύσεων. Τέλος, αναφερθήκαμε στον ορισμό της Αντί – Εγκληματολογίας και των εργαλείων PETs όπου παρεμποδίζουν την έρευνα των ψηφιακών αναλυτών.

Συνοψίζοντας, αντικείμενο της παρούσας εργασίας είναι να κατανοηθούν οι μέθοδοι ανάλυσης του ψηφιακού εγκλήματος από τη σκοπιά του ειδικού ερευνητή. Μέσα από την εργασία, θα γίνει κατανοητό το πόσο επικίνδυνο είναι να μοιραζόμαστε πληροφορίες στα κοινωνικά δίκτυα, καθώς το βρίσκουμε ως τον πιο εύκολο κι άμεσο παράγοντα διευκόλυνσης των σχέσεων μας. Θα εξετάσουμε την ανίχνευση του ψηφιακού εγκλήματος, καλύπτοντας θέματα όπως, διαδικτυακός εκφοβισμός και πορνογραφία. Αντικείμενο της εργασίας είναι η ανάλυση ενός εγκλήματος στον κυβερνοχώρο, περιλαμβάνοντας ζωντανά και ελκυστικά χαρακτηριστικά, όπως παραδείγματα σε πλαίσια με μοναδικά γεγονότα και πρόσωπα, καθώς και αποσπάσματα από συνομιλίες και παραβατικές συμπεριφορές. Επιπλέον, στη σχετική βιβλιογραφία παρουσιάζεται ο τρόπος συλλογής αποδεικτικών στοιχείων που προκύπτουν από την υπόθεση.

Δυστυχώς, στην εποχή μας, λόγω της εξέλιξης της τεχνολογίας, «εξελίσσονται» και τα εγκλήματα. Πολλοί είναι εκείνοι που κινούνται διαδικτυακά. Εργάζονται διαδικτυακά, κάνουν τις αγορές τους διαδικτυακά, συνομιλούν διαδικτυακά. Κι αυτό είναι ένα φαινόμενο που παρατηρείται σε μεγάλο βαθμό όλο και πιο συχνά από τους νέους ανθρώπους. Σε ένα τέτοιο περιβάλλον, γίνονται πιο συχνά τα ψηφιακά εγκλήματα και οι διαδικτυακές επιθέσεις. Οι άνθρωποι εμπιστεύονται τα λάθος άτομα και καταλήγουν να μοιράζονται προσωπικές πληροφορίες σε αγνώστους με συνέπεια την εκμετάλλευση και τη δυσφήμιση τους. Δεν είναι λίγες οι φορές που οι επιτιθέμενοι εκφοβίζουν τα θύματά τους με την αποστολή ανάρμοστων φωτογραφιών στους

περίγυρους τους ή και εκτός στενού κύκλου. Σε αυτό το σημείο, αναλαμβάνουν οι ψηφιακοί εγκληματολόγοι. Με τις κατάλληλες αποδείξεις και πληροφορίες, έχουν τη δυνατότητα να ενοχοποιήσουν ή να αθώσουν τον εκάστοτε ύποπτο. Η ψηφιακή εγκληματολογία λοιπόν, κρίνεται απαραίτητη σε τέτοιες καταστάσεις. Είτε μέσω ιδιωτικών επιχειρήσεων συνεργαζόμενων με την αστυνομία, είτε μέσα στις αρχές, στη τμήμα δίωξης ηλεκτρονικού εγκλήματος, ο ψηφιακός ερευνητής είναι ένα επάγγελμα με απίστευτες προοπτικές και το κυριότερο, αποτελεί «χέρι βοηθείας» όσον αφορά τα ηλεκτρονικά εγκλήματα.

Κεφάλαιο 8^ο : Βιβλιογραφία

- [1] Κων/νος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, «Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και επικοινωνιών. Τεχνικά και νομικά θέματα», εκδόσεις Παπασωτηρίου, 2010.
- [2] Αθανασία Κούρμπαση, «Νομικό πλαίσιο εργαστηρίου ψηφιακής εγκληματολογίας σε στρατιωτικό περιβάλλον», Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς.
- [3] Νικόλαος Κασούμης, «Προσομοίωση σεναρίων ψηφιακής εγκληματολογίας στο διαδίκτυο των πραγμάτων με τον προσομοιωτή cupcarbon», Διπλωματική εργασία, Πανεπιστήμιο Μακεδονίας, 2018.
- [4] «Προστασία της Ιδιωτικότητας σε περιβάλλον Ψηφιακής Δικανικής Εγκληματολογίας (Privacy in Digital Forensics)», Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, 2022.
- [5] Brian Carrier, «Open Source Digital Forensics Tools: The Legal Argument», October 2002.
- [6] Cameron S.D. Brown, «Investigating and Prosecuting Cyber Crime. Forensic, Dependencies and Barriers to Justice», Intl. J. Cyber Criminology 83, January–June 2015.
- [7] C. Blackwell, G.Peterson & S.Shenoieds, «An Investigative Framework for Incident Analysis In Advances in Digital Forensics»,PartVII,22,2011.
- [8] Ioannis Iglezakis, Philippe Jogleux, Lilian Mitrou, Tatiana-Eleni Synodinou, «The Legal Regulation of Cyber Attacks».
- [9] ISACA, Information Security, Audit and Control Association (ISACA). COBIT 3rd Edition Control Objectives. <http://isaca.org>, July 2000.
- [10] Frank Y.W. Law et al, «Protecting Digital Data Privacy in Computer Forensic Examination», Systematic Approaches to Digital Forensic Engineering (SADFE), 2011.
- [11] Νόμος 4624/19 (ΦΕΚ 137/Α/29-8-2019): Προστασία δεδομένων προσωπικού χαρακτήρα.
- [12] Κανονισμός 679/2016 της Ε.Ε. για την προστασία δεδομένων προσωπικού χαρακτήρα.
- [13] Οδηγία 680/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

- [14] Van Solms, SH. and Lourens, CP. IFIP 11.9, «A Control Framework for Digital Forensics», 2006.
- [15] Maria Karyda and Lilian Mitrou, «Internet Forensics: Legal and Technical Issues».
- [16] Mark Pollitt, «Digital forensics as a surreal narrative».
- [17] Sydney Liles, Marcus Rogers and Marianne Hoebich, «A survey of legal issues facing digital forensic experts», Chapter 20.
- [18] Michael Kohn¹, JHP Eloff² and MS Olivier, «Framework for a Digital Forensic Investigation».
- [19] What is Digital Forensics? History, Process, Types, Challenges, online available: <https://www.guru99.com/digitalforensics.html#:~:text=Different%20types%20of%20Digital%20Forensics>.
- [20] Simson L. Garfinkel Valightml, Naval Postgraduate School, Monterey, USA, , «Digital forensics research: The next 10 years», 2 August 2010.
- [21] Wynand Staden, «Protecting Third Party Privacy in Digital Forensic Investigations», 9th International Conference on Digital Forensics (DF), Orlando, FL, United States. Jan 2013.
- [22] Caviglione, L., Wendzel, S. and Mazurczyk, W., «The future of digital forensics: Challenges and the road ahead», IEEE Security & Privacy, 2017.
- [23] «EC – Council Cybersecurity Exchange», online available: <https://www.eccouncil.org/cybersecurity-exchange/#:~:text=A%20digital%20forensic%20investigator%20is,i.e.%2C%20after>.
- [24] Suresh V.A, Venkatesh B. B and Anajaneyulu A.C, «Data Preservations by Using Digital Forensic Techniques», International Journal of Computer Systems (ISSN: 2394-1065), Volume 03– Issue 03, March, 2016.
- [25] Henseler, J. «Computer crime and computer forensics. In The encyclopedia of forensic science», 2000.
- [26] Karie, N. M., & Venter, H. S. «Taxonomy of challenges for digital forensics». Journal of forensic sciences, 2015.
- [27] Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. «Current Challenges and Future Research Areas for Digital Forensic Investigation». The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016). Florida, USA, 2016.
- [28] Mckemmish, R. «What is Forensic Computing? Trends and Issues in Crime and Criminal Justice», 1999.
- [29] Vlachopoulos, K., Magkos, E., & Chrissikopoulos, V. «A model for hybrid evidence investigation. Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security», 2013.

- [30] Zareen, M. S., Waqar, A., & Aslam, B. «Digital forensics: Latest challenges and response». In Information Assurance (NCIA), 2013 2nd National Conference.
- [31] Κωνσταντίνος Γεωργοκίτσος, «Mobile Device Forensics: Guidelines, Analysis and Tools.», Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, 2018.
- [32] Αποστολόπουλος Δημήτριος, «Digital Forensics: Case Studies. Ψηφιακή Εγκληματολογία: Μελέτη Πραγματικών Σεναρίων.», 2013.
- [33] Ανάργυρος Βελέντζας, «Κυβερνοέγκλημα σε Περιβάλλοντα Υπολογιστικού Νέφους Κρίσιμων Υποδομών», Διπλωματική εργασία, Πανεπιστήμιο Δυτικής Αττικής, 2021.
- [34] Christoforos Ntantogian, Dimitris Apostolopoulos, Giannis Marinakis, Christos Xenakis, «Evaluating the privacy of Android mobile applications under forensic analysis».
- [35] Παπουτσής Δημήτριος, «Ανασκόπηση και περιγραφή των μεθοδολογιών, προτύπων και εργαλείων που χρησιμοποιούνται για την ανάλυση ψηφιακών πειστηρίων διαδικτυακών υπηρεσιών. Επίδειξη κυριότερων ανοιχτών εργαλείων με συγκεκριμένες περιπτώσεις χρήσης», Διπλωματική εργασία, 2015.
- [36] Σταύρος Δημόπουλος, «Digital Evidence & forensics», Διπλωματική εργασία, Πανεπιστήμιο Πειραιώς, 2021.
- [37] Ιωάννης Στέλλιος, «Λειτουργικό σύστημα Android: Ασφάλεια & δοκιμές παρείσδυσης (Android Operating System: Security analysis and penetration testing)», 2016.
- [38] ERM Protect, «What Are the 5 Stages of a Digital Forensics Investigation?», <https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/>.
- [39] EC – Council, «What is Digital Forensics», online available at: <https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/>.
- [40] Team Spy Cloud, «70% Password Reuse: Password Security Needs a Forced Reset», 2022, online available at: <https://spycloud.com/blog/password-reuse/>.
- [41] Encyclopedia, «Password Reuse», online available at: <https://www.hypr.com/security-encyclopedia/password-reuse>.
- [42] Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis, «Delegate the smartphone user? Security awareness in smartphone platforms», 2013.
- [43] Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis, «Assessing Privacy Risks in Android: A User – Centric Approach», 2013.
- [44] Bhoopesh Kumar Sharma, Vipin Yadav, Mandeep Kaur Purba, Yogesh Sharma, «Challenges, Tools and Future of Mobile Phone Forensics», 2022.
- [45] Csid, «Consumer Survey: Password Habits», 2012.
- [46] Hashim Shaikh, «Practical android phone forensics», 2017.

- [47] Ninj@S3c, «Linux and disk forensics», 2013.
- [48] Linode, «Linux Users and Groups», 2023.
- [49] Vivek Gite, «Where are the passwords of the users located in Linux? », 2023.
- [50] Vivek Gite, «Understanding/ etc/shadow file format on Linux», 2023.
- [51] «How the ACSC can help during a cyber security incident», online available at: <https://www.cyber.gov.au/>.
- [52] Tessa Miller, «Do I really need to log out of webapps? », 2013, online available at: <https://lifelacker.com/do-i-really-need-to-log-out-of-webapps-1482782887>.
- [53] Man Pages, «GnuPG, online available at: <https://www.gnupg.org/documentation/manpage.html>».
- [54] Clemens Fruhwirth, «Luks on – disk Format Specification version 1.2.3», 2018.
- [55] «Linux Guide/Reset a forgotten root password», online available at: https://en.wikibooks.org/wiki/Linux_Guide/Reset_a_forgotten_root_password.
- [56] Ravi Saive, «How to encrypt and decrypt a partition in Linux», 2023.
- [57] Frank Rietta, «Introduction to OpenPGP: Decrypt this Message», 2014, online available at: <https://rietta.com/blog/the-openpgp-encrypted-message-exercise/>.
- [58] «Forensic Imaging Guide», 2016, online available at: https://its.idaho.gov/wp-content/uploads/sites/2/2016/12/forensic_imaging_guide.pdf
- [59] Juan Carlos Flores Cruz, Travis Atkinson, «Digital Forensics on a Virtual Machine», online available at: http://atkison.cs.ua.edu/papers/ACMSE11_JF.pdf
- [60] D. Bem, E. Huebner, «Computer Forensics Analysis in a Virtual Environment», *International Journal of Digital Evidence*, 2007.
- [61] Kruse II, W. G., & Heiser, J. G., «Computer Forensics: Incident Response Essentials: Addison Wesley Professional», 2002.
- [62] Nance K., Hay, B., Bishop, M., «Investigating the Implications of Virtual Machines Introspection for Digital Forensics», *International Conference on Availability, Reliability and Security*, 2009.
- [63] Zhang Y., Lin Y., «Research on the Key Technology of Secure Computer Forensics, Intelligent Information Technology and Security Informatics». *Third International Symposium*, 2010.
- [64] VMware, online available at: <https://www.vmware.com/products.html>
- [65] CyberSec_Sai, «Windows Forensic 101: How to Perform Forensic Investigation of Windows Machine?», online available at: <https://infosecwriteups.com/windows-forensic-101-how-to-perform-forensic-investigation-of-windows-machine-d1dfbea20254>

- [66] «Criminal Investigations», <https://forensicscience.llnl.gov/research/case-studies/investigations>
- [67] «Build Your Forensic Workstation», online available at: <https://bluecapesecurity.com/build-your-forensic-workstation/>
- [68] «Cyber Skills Live», online available at: <https://legacy.cyberskillslesson.com/hide-secret-messages-using-technology/#>
- [69] «Windows Forensics 1 | TryHackMe», online available at: <https://nehrunayak.medium.com/windows-forensics-1-tryhackme-873f732234d6>
- [70] «Data Forensics – Mozilla Firefox Forensics», online available at: <https://www.dataforensics.org/mozilla-firefox-forensics/>
- [71] «Mailxaminer – Mozilla Thunderbird Email Forensics», online available at: <https://www.mailxaminer.com/blog/mozilla-thunderbird-forensics/>
- [72] «Firefox Forensics», online available at: <https://www.forensicfocus.com/articles/firefox-forensics/>
- [73] «Browser Forensics: Firefox», online available at: <https://resources.infosecinstitute.com/topics/digital-forensics/browser-forensics-firefox/>
- [74] «Steganography Tutorial», online available at: <https://www.edureka.co/blog/steganography-tutorial#SteganographicTechniques>
- [75] «How to Password Protect a File or Folder in Windows 10», online available at: <https://www.avg.com/en/signal/how-to-password-protect-file-folder-in-windows>
- [76] «Digital Evidence and Forensics», *National Institute of Justice*, online available at: <https://nij.ojp.gov/digital-evidence-and-forensics>
- [77] «Forgot Windows password? Bypass it with KON-BOOT!», online available at: <https://kon-boot.com/>
- [78] Fabio R. Auffant II, «Computer Forensics I», *University at Albany*, <https://www.albany.edu/cyber/cdarea/syllabi/BFOR301%20-%20Computer-Forensics-I.pdf>
- [79] David Duggan, Bob Hutchinson, Lorie Liebrock, «Digital Forensics – lecture», online available at: <https://www.cs.nmt.edu/~df/lectures/DF%20Intro.pdf>
- [80] «Web Browser Forensics: Uncovering the Hidden Evidence in your Browser», online available at: <https://mcsi-library.readthedocs.io/articles/2022/05/web-browser-forensics-uncovering-the-hidden-evidence-in-your-browser/web-browser-forensics-uncovering-the-hidden-evidence-in-your-browser.html>