ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Συγκριτική αξιολόγηση open source εργαλείων Digital Forensics: Μελέτη περίπτωσης σε Android»

Σχήμα 1 Digital Forensics

Της φοιτήτριας
Τσόκανη Ειρήνη
Αρ. Μητρώου: 185421

Επιβλέπων
Ονοματεπώνυμο κ. Ηλιούδης
Χρήστος
Βαθμίδα Καθηγητής

Ημερομηνία Σεπτέμβριος 2023

Τίτλος Π.Ε.«Συγκριτική αξιολόγηση open source εργαλείων Digital Forensics: Μελέτη περίπτωσης σε Android»

Κωδικός Π.Ε. 23177

Ονοματεπώνυμο φοιτητή/τών Τσόκανη Ειρήνη

Ονοματεπώνυμο εισηγητή κ. Ηλιούδης Χρήστος

Ημερομηνία ανάληψης Π.Ε. 29/03/2023

Ημερομηνία περάτωσης Π.Ε. 10/09/2023

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

«Αφιερώνω αυτή την πτυχιακή στην οικογένεια μου για την αγάπη και την υποστήριξη που μου προσέφερε καθ' όλη τη διάρκεια αυτής της πορείας.»

Πρόλογος

Τα τελευταία χρόνια, η ψηφιακή εγκληματολογία αποτελεί ένα ιδιαίτερα κρίσιμο πεδίο στον τομέα της κυβερνοασφάλειας. Παρά την άρρηκτη συσχέτισή της με την τεχνολογία, στην πραγματικότητα, το εκτεταμένο της αντίκτυπο επεκτείνεται και στην κοινωνία. Καθώς τα smartphone, πρωτίστως, αλλά και άλλες ψηφιακές συσκευές έχουν έντονη παρουσία στην καθημερινή ζωή, η πιθανότητα για ψηφιακά εγκλήματα και παραβιάσεις δεδομένων έχει αυξηθεί σημαντικά. Για αυτό το λόγο, καθίσταται αναγκαία η χρήση αξιόπιστων ψηφιακών εγκληματολογικών εργαλείων. Η αυξανόμενη ζήτηση για τα εργαλεία αυτά, έχει οδηγήσει σε πολλαπλασιασμό των εργαλείων στην αγορά, και πιο συγκεκριμένα, των εργαλείων ανοιχτού κώδικα. Με βασικά χαρακτηριστικά τους την διαφάνεια και την προσβασιμότητα, προσφέρουν την οικονομικά αποδοτικότερη εναλλακτική λύση για την συλλογή, την εξαγωγή και την ανάλυση διαφορετικών ψηφιακών δεδομένων, ενισχύοντας το υψίστης σημασίας έργο των ερευνητών της ψηφιακής εγκληματολογίας.

Περίληψη

Η παρούσα πτυχιακή με τίτλο «Συγκριτική Ανάλυση Open Source Εργαλείων Digital Forensics: Μελέτη περίπτωσης σε Android» παρουσιάζει μια ολοκληρωμένη αναλυτική μελέτη με σκοπό την διερεύνηση, την αξιολόγηση και την σύγκριση εργαλείων ανοιχτού κώδικα που χρησιμοποιούνται σε εγκληματολογικές έρευνες. Η ραγδαία εξέλιξη της ψηφιακής εγκληματολογίας, έχει αναδείξει τη σημασία της ύπαρξης και της εφαρμογής αποτελεσματικών τεχνικών και μεθόδων στοχεύοντας στη διερεύνηση και στην ανάλυση ψηφιακών δεδομένων.

Η εργασία στοχεύει στην επίτευξη και διεξαγωγή μιας ολοκληρωμένης συγκριτικής ανάλυσης εργαλείων ψηφιακής εγκληματολογίας ανοιχτού κώδικα με απώτερο σκοπό την ενημέρωση και καθοδήγηση των ερευνητών στην επιλογή των ιδανικών εργαλείων. Στο πλαίσιο αυτο, θα παρουσιαστεί μια αναλυτική σύγκριση ποικίλων παραγόντων, συμπεριλαμβανομένης της λειτουργικότητας, της χρηστικότητας, της αξιοπιστίας, της συμβατότητας και των δυνατοτήτων τους, σε σχέση με τα καθιερωμένα εγκληματολογικά πλαίσια και πρότυπα.

Κατά τη διεξαγωγή της έρευνας, η μεθοδολογία που θα χρησιμοποιηθεί ακολουθεί μια συστηματική προσέγγιση, που περιλαμβάνει την επιλογή κατάλληλων εργαλείων. Με αυτόν τον τρόπο, θα διερευνηθεί η αποτελεσματικότητα και η απόδοση αυτών των εργαλείων κατά την εξαγωγή και την ανάλυση διαφορετικών τύπων δεδομένων. Με την εφαρμογή μιας δομημένης μεθοδολογίας η οποία βασίζεται στην τυποποιημένη διαδικασία εξαγωγής και ανάλυσης δεδομένων, πραγματοποιήθηκε μια μελέτη περίπτωσης στα πλαίσια της αξιολόγησης των δυνατοτήτων ενος εγκληματολογικού εργαλείου ανοιχτού κώδικα.

Τα συμπεράσματα που προκύπτουν απο την συγκριτική ανάλυση στοχεύουν στην πληροφόρηση για τα χαρακτηριστικά των εργαλείων ψηφιακής εγκληματολογίας ανοιχτού κώδικα. Η παρούσα εργασία αποσκοπεί στην παροχή σημαντικών ενδείξεων για την επιλογή των κατάλληλων εργαλείων για τους ερευνητές της ψηφιακής εγκληματολογίας, συμβάλλοντας στην βελτίωση της διαδικασίας ανάλυσης ψηφιακών δεδομένων και, κατ επεκταση, στην ενίσχυση και εξελιξη του γνωστικού πεδίου. Με αυτόν τον τρόπο, διευκολύνεται η βελτίωση και η ανάπτυξη εργαλείων ψηφιακής εγκληματολογίας ανοιχτού κώδικα.

«Comparative Analysis of Open Source Digital Forensics Tools on Android»

«Eirini Tsokani»

Abstract

With the advent of digital devices such as Android Smartphones nowadays it has become vital to have sturdy Digital Forensic techniques in place, that can investigate and analyze Digital Evidence efficiently. An increasing number of organizations are using Open Source Tools in Digital Forensic Investigations due to their transparency, accessibility and collaborative development features. In this thesis we aim to provide a comprehensive evaluation report on Open Source Digital Forensic Tools designed specifically for android devices by comparing different aspects like functionality ease-of-use reliability compatibility etc., We adopt a systematic methodology which involves tool selection, experimentation, data acquisition, analysis interpretation etc., Our comparison assessment covers key dimensions such as extraction and analysis of different types of data typically encountered during android forensic investigations; call logs messages, multimedia files, application data, device artifacts and evaluates each tool's performance accuracy and reliability through controlled experiments and real-world case scenarios. We also delve into the open-source tools' integration capabilities with established forensic frameworks and standards to ensure interoperability and compatibility.

This thesis conducts an extensive investigation of the methodology, usability and effectiveness of open source digital forensics tools, taking into account various factors such as probative strength, data security efficiency and frequency of updates. Additionally, it explores the integration of these tools with established forensic frameworks and standards, aiming to ensure seamless compatibility with established investigative practices. The research findings provide valuable insights into the features, capabilities, and challenges faced by open source digital forensics tools, helping to expand knowledge in the field. Digital forensic investigators and researchers can benefit from the outcomes of this study, as it offers a useful resource for selecting appropriate open source tools tailored for Android-based investigations.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κ. Ηλιούδη, για την ανεκτίμητη καθοδήγηση και την υποστήριξη του κατά την διάρκεια αυτής της πτυχιακής εργασίας.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία

Κεφάλαιο 1ο: Εισαγωγή

1.1 Αντικείμενο της πτυχιακής εργασίας

Η παρούσα πτυχιακή εργασία επικεντρώνεται στην διεξαγωγή μιας διεξοδικής παρουσίασης των κλάδων της ψηφιακής εγκληματολογίας και στην σχολαστική συγκριτική ανάλυση των εργαλείων τους, με ιδιαίτερη έμφαση στα εργαλεία ανοιχτού κώδικα καθώς επίσης και στην χρήση τους στις ψηφιακές συσκευές. Δεδομένης της εκθετικής εξάπλωσής τους σε διάφορους τομείς της καθημερινής ζωής, η ανάγκη για ισχυρά και αποτελεσματικά εργαλεία ψηφιακής εγκληματολογίας καθίσταται ολοένα και πιο επιτακτική καθώς οι ερευνητές βασίζονται ιδιαίτερα σε αυτά για την εξαγωγή, την ανάλυση και την ερμηνεία κρίσιμων δεδομένων.

Ως εκ τούτου, επιδιώκεται η αντιμετώπιση της ανάγκης για μια ολοκληρωμένη ανάλυση με έμφαση στα δυνατά σημεία και στους περιορισμούς που προκύπτουν από τη χρήση των εργαλείων ανοιχτού κώδικα, ιδιαίτερα κατά την εφαρμογή τους στον κλάδο της εγκληματολογίας κινητών συσκευών. Συνεπώς, στοχεύει να εμβαθύνει στο εκτεταμένο ερευνητικό πεδίο των εργαλείων ανοιχτού κώδικα, εξετάζοντας την εφαρμογή, τις λειτουργικές δυνατότητες και τη συνολική απόδοση τους στο πλαίσιο ψηφιακών ερευνών.

1.2 Στόχοι πτυχιακής εργασίας

Η εργασία στοχεύει να προσφέρει πρακτικές και εφαρμόσιμες γνώσεις για την αποτελεσματική αξιοποίηση των εργαλείων ανοιχτού κώδικα, παρέχοντας καθοδήγηση σχετικά με τη βέλτιστη επιλογή τους αναλογα τον εγκληματολογικό κλαδο διερεύνησης. Παρουσιάζοντας λοιπόν τις βέλτιστες πρακτικές και στρατηγικές επιλογής εργαλείων, δίνεται η δυνατότητα στους επαγγελματίες ερευνητές να εξορθολογίσουν τις ερευνητικές τους διαδικασίες.
Επιπρόσθετα, αναλύεται εκτενώς ο τομέας της ψηφιακής εγκληματολογίας των κινητών συσκευών, προσδιορίζοντας τα δυνατά και αδύνατα σημεία των εργαλείων, γεγονός που επιτεύχθηκε με την διεξαγωγή μιας μελέτης περίπτωσης η οποία έχει ως στόχο την βαθύτερη κατανόηση των δυνατοτήτων τους.
Καθόλη τη διάρκεια της έρευνας, δίνεται έμφαση στον τρόπο με τον οποίο αυτά τα εργαλεία αντιμετωπίζουν αποτελεσματικά τις μοναδικές προκλήσεις που παρουσιάζονται στον τομέα της ψηφιακής εγκληματολογίας.

1.3 Επιτεύγματα

Η παρούσα πτυχιακή εργασία αποτελεί μια σημαντική συνεισφορά στον τομέα της ψηφιακής εγκληματολογίας με κεντρικό πυρήνα τα εγκληματολογικά εργαλεία. Μέσω μιας πλήρους και διεξοδικής παρουσίασης και συγκριτικής ανάλυσης, αποτυπώνονται οι σημαντικές δυνατότητες και οι περιορισμοί που απορρέουν από τη χρήση ψηφιακών εργαλείων.

Η διεξοδική ανάλυση των λειτουργιών, των δυνατοτήτων και της απόδοσης των εργαλείων που επισημαίνονται, αποτελούν πολύτιμη ενημερωτική πηγή για τους επαγγελματίες και τους ερευνητές του τομέα της ψηφιακής εγκληματολογίας και της κυβερνοασφάλειας.

Επιπλέον, η εργασία προσφέρει συγκρίσιμα αποτελέσματα και πρακτικές προτάσεις, οι οποίες μπορούν να βελτιστοποιήσουν τις ψηφιακές έρευνες όλων των κλάδων, καθώς και να ενισχύσουν την αξιοπιστία και αποτελεσματικότητά τους. Κατα συνέπεια, βελτιστοποιούν την κατανόηση του εύρους των διαθέσιμων εργαλείων καθώς επίσης και την ανάλυση και διαχείριση των ψηφιακών δεδομένων που προκύπτουν. Τα επιτεύγματα αυτά μπορούν να συνεισφέρουν στην προώθηση της επιστήμης της ψηφιακής εγκληματολογίας αποτελώντας πολύτιμη βάση για μελλοντικές έρευνες και προάγοντας καινοτόμες προσεγγίσεις στον συνεχώς εξελισσόμενο αυτό τομέα.

1.4 Διάρθρωση

Η εργασία ακολουθεί ένα εμπεριστατωμένο πλαίσιο για την παρουσίαση των διαφόρων ψηφιακών εγκληματολογικών κλάδων και των εργαλείων τους, κυρίως ανοιχτού κώδικα, με συνοχή. Η εισαγωγή παρέχει ένα σαφές πλαίσιο, διευκρινίζοντας τη σημασία και τον σκοπό της μελέτης εργαλείων ψηφιακής εγκληματολογίας. Μέσα από μια εκτενή βιβλιογραφική ανασκόπηση, διερευνώνται μεθοδολογίες και εξελίξεις στα εργαλεία αυτά.

Το ερευνητικό μοντέλο της μεθοδολογίας της ψηφιακής εγκληματολογίας χρησιμεύει ως το θεμελιώδες πλαίσιο, περιγράφοντας τα βασικά βήματα και τις τεχνικές για τη διεξαγωγή ερευνών. Οι λειτουργίες, οι μετρήσεις απόδοσης και οι δυνατότητες ενσωμάτωσης των εγκληματολογικών εργαλείων παρουσιάζονται συστηματικά, στοχεύοντας στην ολοκληρωμένη πληροφόρηση για τα αντίστοιχα δυνατά και αδύνατα σημεία τους.

Επιπλέον, εμβαθύνει στους διαφορετικούς κλάδους της ψηφιακής εγκληματολογίας και στα εργαλεία τους καθώς επίσης και στις συγκεκριμένες προκλήσεις που παρουσιάζονται, υπογραμμίζοντας τον τρόπο με τον οποίο αντιμετωπίζουν τις εκάστοτε προκλήσεις. Στη συνέχεια αναλύονται οι τύποι των ψηφιακών αποδεικτικών στοιχείων και η μεθοδολογία για την διαδικασία της συλλογής και της ανάλυσή τους.

Έπειτα, πραγματοποιείται μια σύγκριση χαρακτηριστικών του ανοιχτού και του εμπορικού κώδικα, η οποία βασίζεται στα πλεονεκτήματα και τα μειονεκτήματά τους και στη συνέχεια μια εκτεταμένη αναφορά σε ορισμένα εργαλεία ανοιχτού κώδικα, η οποία ακολουθείται απο μια συγκριτικη αναλυση.

Στην συνέχεια, διεξάγεται μια εκτενή ανάλυση της κινητής εγκληματολογίας, και των μοναδικών προκλήσεων που αντιμετωπίζει, ενώ παράλληλα παρουσιάζονται οι αναδυόμενες τάσεις του τομέα. Αναλύονται εκτενώς εργαλεία που συναντώνται και χρησιμοποιούνται στις εγκληματολογικές έρευνες, με ιδιαίτερη έμφαση στη διατήρηση της ακεραιότητας των αποδεικτικών στοιχείων.

Επιπρόσθετα, η εργασία περιλαμβάνει μια μελέτη περίπτωσης που επικεντρώνεται στην διεξαγωγή εγκληματολογικής έρευνας σε κινητή συσκευή με λειτουργικό Android. Η μελέτη περίπτωσης παρουσιάζει ένα πραγματικό σενάριο όπου εφαρμόζονται εργαλεία ανοιχτού κώδικα και μεθοδολογίες ψηφιακής εγκληματολογίας για την ανάλυση στοιχείων που εξάγονται από μια συσκευή Android.

Στο τελευταίο κεφάλαιο, εξάγονται γενικά συμπεράσματα και προσφέρονται πρακτικές συστάσεις στον τομέα της ψηφιακής εγκληματολογίας. Η έρευνα θεσπίζει βασικά κριτήρια για τη συστηματική αξιολόγηση των εργαλείων ψηφιακής εγκληματολογίας, διασφαλίζοντας την αντικειμενικότητα σε όλη τη διαδικασία αξιολόγησης.

1.5 Σε ποιους απευθύνεται

Η παρούσα πτυχιακή εργασία χρησιμεύει ως ένας ανεκτίμητος πόρος που εξυπηρετεί ένα ευρύ φάσμα αναγνωστών με ενδιαφέρον στον τομέα της ψηφιακής εγκληματολογίας. Οι επαγγελματίες ερευνητές της εγκληματολογίας και της κυβερνοασφάλειας μπορούν να επωφεληθούν σε μεγάλο βαθμό από τις περιεκτικές πληροφορίες που παρουσιάζονται, κατανοώντας τις δυνατότητες και τους περιορισμούς των εργαλείων ανοιχτού κώδικα. Η εργασία μπορεί να αποτελέσει αναφορά για αυτούς, καθώς εμβαθύνει στα διακριτά χαρακτηριστικά τους αλλά και στους κινδύνους που εγκυμονούν.

Επιπρόσθετα, ενθαρρύνεται η περαιτέρω διερεύνηση και πρόοδο στον κλάδο, καθώς παρουσιάζει τις μελλοντικές επεκτάσεις τους, ενισχύοντας την καινοτομία και τη βελτίωση στις μεθοδολογίες ψηφιακής έρευνας.

Τέλος, οι φοιτητές που επιδιώκουν σπουδές ή και διερεύνηση στον τομέα της ψηφιακής εγκληματολογίας θα αποκομίσουν εξίσου σημαντικά οφέλη από αυτήν την εργασία, καθώς ενισχύει τις ακαδημαϊκές τους αναζητήσεις. Ως αποτέλεσμα, αυτή η εργασία τους δίνει έμμεσα τη δυνατότητα να συνεισφέρουν στο πεδίο της ψηφιακής εγκληματολογίας.

Κεφάλαιο 2ο: Digital Forensics, κλάδοι και προκλήσεις

2.1 Ορισμός

Η ψηφιακή εγκληματολογία περιλαμβάνει την ανάκτηση, την ανάλυση και την διατήρηση ψηφιακών δεδομένων, όπως ήχου, εικόνας, βίντεο, αρχείου κλήσεων κλπ., που συλλέγονται κατόπιν διεξοδικής εξέτασης ηλεκτρονικών συσκευών[1]. Τα δεδομένα αυτά μπορούν να προκύψουν από ψηφιακές συσκευές όπως σκληρούς δίσκους υπολογιστών, κινητά τηλέφωνα, έξυπνες συσκευές, συστήματα πλοήγησης οχημάτων. Οι αποθηκευτικές δυνατότητες αυτών των συσκευών αυξάνονται μέρα με τη μέρα. Για αυτόν τον λόγο, είναι ζωτικής σημασίας τα δεδομένα τους να παραμένουν αναλλοίωτα κατά την εγκληματολογική ανάλυση, διασφαλίζοντας ότι τα ληφθέντα αποτελέσματα μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία[2].

2.2 Ερευνητικό Μοντέλο Μεθοδολογίας Ψηφιακής Εγκληματολογίας

Η ψηφιακή εγκληματολογία αποτελεί ένα ισχυρό εργαλείο για την ανακάλυψη και την ανάλυση πολυάριθμων περιστατικών που συνδέονται τόσο με την ασφάλεια στον κυβερνοχώρο όσο και με τη φυσική ασφάλεια[3]. Η διαδικασία αντιμετώπισης περιστατικών αφορά τον εντοπισμό παραβιάσεων, τον προσδιορισμό των υποκείμενων αιτιών και των προσώπων που εμπλέκονται και τη συλλογή αποδεικτικών στοιχείων. Μολονότι τα εγκληματικά σενάρια μπορεί να διαφέρουν, οι διαδικασίες που ακολουθούν είναι πάντοτε οι εξής: ταυτοποίηση στοιχείων, συλλογή, εξαγωγή και διατήρηση, ανάλυση, τεκμηρίωση και τέλος, αναφορά[1].

Ταυτοποίηση: Το πρώτο στάδιο του ερευνητικού μοντέλου αφορά τον προσδιορισμό των στόχων και των πόρων που είναι απαραίτητοι για την διεξαγωγή μιας αποτελεσματικής έρευνας[4]. Σε αυτούς, περιλαμβάνονται το ερευνητικό προσωπικό, τα διαθέσιμα εργαλεία, οι φυσικοί πόροι και τα νομικά ζητήματα. Στη συνέχεια, οι ερευνητές προσδιορίζουν τον τύπο δεδομένων που αντλούνται από τις συσκευές αποθήκευσης. Η προέλευση και ο τύπος των δεδομένων ποικίλλει λόγω του ευρέως φάσματος των φορητών συσκευών, όπως τα κινητά τηλέφωνα, οι φορητοί υπολογιστές, οι σκληροί δίσκοι, τα tablet και οι έξυπνες συσκευές[1]. Προκειμένου να αποφευχθεί η πιθανότητα παραβίασης και να περιοριστεί η πρόσβαση, οι συσκευές δεσμεύονται και στην συνέχεια απομονώνονται[5].

Συλλογή: Το στάδιο της συλλογής δεδομένων περιλαμβάνει την κατάσχεση των συσκευών για την μετέπειτα εξαγωγή των αποδεικτικών στοιχείων με την ασφαλέστερη δυνατή διαδικασία και την χρήση κατάλληλων εργαλείων. Σε ορισμένες περιπτώσεις μπορεί να είναι απαραίτητη η ανάκτηση διαγραμμένων αρχείων ή η παραβίαση κωδικών πρόσβασης, για αυτό είναι απαραίτητη η δημιουργία αντιγράφων ασφαλείας, διασφαλίζοντας έτσι την ακεραιότητα των δεδομένων[3,6]. Με αυτόν τον τρόπο, τα αρχικά δεδομένα διατηρούνται αναλλοίωτα, και στη συνέχεια ανακτώνται μαζί με τα διαγραμμένα. Οι εγκληματολογικοί ερευνητές καθορίζουν τον τρόπο ανάκτησής τους με βάση την κατάσταση των μέσων αποθήκευσης στα οποία εμπεριέχονται. Μολονότι η ανάκτηση εγκληματολογικών δεδομένων μπορεί να είναι απλή, όπως στην περίπτωση της ανακατασκευής ενός κατεστραμμένου σκληρού δίσκου, αρκετές φορές απαιτείται η ανακάλυψη κρυφών δεδομένων χρησιμοποιώντας τεχνικές παράκαμψης συστημάτων ασφαλείας[6].

Εξαγωγή και Διατήρηση: Η μεταφορά δεδομένων από μια πηγή σε έναν καθορισμένο προορισμό, όπως μια ψηφιακή συσκευή αποθήκευσης, είναι ο στόχος της εξαγωγής δεδομένων. Τα δεδομένα που προκύπτουν μπορούν στη συνέχεια να αναλυθούν περαιτέρω μέσω διαφόρων τεχνικών και εργαλείων. Όσον αφορά τη διατήρηση αποδεικτικών στοιχείων, διασφαλίζεται η φύλαξη της εκάστοτε ψηφιακής συσκευής και αφαιρούμενου μέσου. Η διατήρηση συνεπάγεται την ταυτοποίηση, την τεκμηρίωση και την συλλογή των ψηφιακών αποδεικτικών στοιχείων μετά από ενδελεχή αναζήτηση. Η διατήρηση της αρχικής τους κατάστασης είναι ζωτικής σημασίας για να αποφευχθούν οι κίνδυνοι που εγκυμονούν σε μια έρευνα, οι οποίοι μπορεί να οδηγήσουν σε ανεπανόρθωτη απώλεια πολύτιμων για την υπόθεση πληροφοριών και δεδομένων[5,6].

Ανάλυση: Στόχος της ανάλυσης στην ψηφιακή εγκληματολογία είναι η διερεύνηση των ψηφιακών στοιχείων μιας έρευνας. Πιο συγκεκριμένα, αποσκοπεί στην αξιολόγηση της σημασίας και της αποδεικτικής αξίας των αποτελεσμάτων της. Οι ερευνητές σε αυτό το στάδιο εξετάζουν ευρήματα που σχετίζονται με διάφορους τύπους πληροφοριών, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία καταγραφής συνομιλιών, εικόνες, έγγραφα και ιστορικό διαδικτύου. Τα αποδεικτικά στοιχεία που συλλέγονται και αναλύονται στη συνέχεια χρησιμοποιούνται για την ανασύσταση γεγονότων και τη δημιουργία σχέσεων ανάμεσα σε άτομα, μέρη και αντικείμενα με σκοπό την εξαγωγή συμπερασμάτων.

Τεκμηρίωση: Μετά τη φάση της ανάλυσης, τα αποτελέσματα της έρευνας τεκμηριώνονται με κατάλληλο τρόπο ώστε να παρέχεται μια ολοκληρωμένη επισκόπηση της ερευνητικής διαδικασίας και των πορισμάτων της. Αυτή η τεκμηρίωση επιτρέπει την οπτικοποίηση ενός χρονοδιαγράμματος που αναπαριστά την ακολουθία γεγονότων, παρουσιάζοντας έτσι μια σαφή εικόνα των δραστηριοτήτων και των συνεπειών τους.

Αναφορά: Η φάση αναφοράς περιλαμβάνει μια λεπτομερή περιγραφή των βημάτων και των μεθοδολογιών που ακολουθήθηκαν σε όλη τη διαδικασία της έρευνας, των ψηφιακών αποδεικτικών στοιχείων που ανακαλύφθηκαν και των συμπερασμάτων που εξήχθησαν με βάση τα αποτελέσματα της εξέτασης[1,3]. Στόχος είναι η σύνταξη και παρουσίαση μιας ολοκληρωμένης αναφοράς η οποία προσφέρει μια συνοπτική αλλά περιεκτική περιγραφή των βημάτων της έρευνας. Επιπλέον, περιγράφει επακριβώς τα εργαλεία και τις τεχνικές που χρησιμοποιούνται για την απόκτηση, την διατήρηση και την ανάλυση των ψηφιακών αποδεικτικών στοιχείων, διασφαλίζοντας έτσι τη διαφάνεια σε όλη τη διαδικασία της έρευνας. Τέλος, η αναφορά παρέχει μια λεπτομερή λίστα με όλα τα στοιχεία που υποβλήθηκαν για εξέταση, διασφαλίζοντας σχολαστική και εμπεριστατωμένη τεκμηρίωση[4,6].

Παρουσίαση: Κατόπιν ολοκλήρωσης της έρευνας, τα πορίσματα παρέχονται σε αρμόδιες αρχές, οι οποίες είναι υπεύθυνες για τη λήψη αποφάσεων με βάση τα ευρήματα. Κατά τη φάση της παρουσίασης λοιπόν, οι ερευνητές ψηφιακής εγκληματολογίας ενεργούν συχνά ως πραγματογνώμονες[1,3,5]. Είναι ακριβείς στην παρουσίαση των αποδεικτικών στοιχείων που έχουν ανακαλυφθεί, διασφαλίζοντας ότι παρουσιάζονται με σαφήνεια και πληρότητα. Ο απώτερος σκοπός της παρουσίασης είναι να προσφέρει πειστικά επιχειρήματα βασισμένα σε ψηφιακά στοιχεία συμβάλλοντας στη διαμόρφωση μιας τεκμηριωμένης απόφασης ή κρίσης[6].

2.3 Τεχνικές και Εργαλεία

2.3.1 Εγκληματολογικές Τεχνικές

Οι εγκληματολόγοι χρησιμοποιούν διάφορες τεχνικές και εξειδικευμένα εργαλεία για την εξαγωγή και την ανάλυση των υπό διερεύνηση ψηφιακών στοιχείων. Οι τεχνικές αυτές διαδραματίζουν κρίσιμο ρόλο στις εγκληματολογικές έρευνες και επιτρέπουν στους ερευνητές να ανακαλύψουν πολύτιμες πληροφορίες. Ακολουθούν οι κύριες τεχνικές που χρησιμοποιούνται:

Ανάκτηση δεδομένων (Data Recovery): Αφορά την ανάκτηση δεδομένων από διάφορες συσκευές και αποτελεί θεμελιώδη πτυχή της εγκληματολογίας. Για την ανάκτηση δεδομένων χρησιμοποιείται μια ποικιλία εργαλείων λογισμικού, με δύο κύριες προσεγγίσεις: επιτόπου ανάκτηση και ανάκτηση μόνο για ανάγνωση[7]. Η επιτόπου ανάκτηση αφορά την αποκατάσταση δεδομένων που έχουν χαθεί ή αλλοιωθεί λόγω σφαλμάτων ή καταστροφής της μονάδας δίσκου. Στόχος είναι η ανάκτηση των δεδομένων και η επανατοποθέτησή τους. Αντιθέτως, η ανάκτηση μόνο για ανάγνωση αποσκοπεί στην αποκατάσταση των ανακτημένων αρχείων σε διαφορετική θέση του δίσκου[7].

Εγκληματολογική εξέταση πολλαπλών δίσκων (Cross-Drive): Η εγκληματολογική εξέταση πολλαπλών δίσκων (Cross-Drive Analysis) αφορά τη χρήση ειδικών εργαλείων για την συλλογή, την ανάλυση και τη σύγκριση πληροφοριών που προέρχονται από διαφορετικούς σκληρούς δίσκους[7]. Αυτή η τεχνική είναι υψίστης σημασίας στις διαδικασίες εντοπισμού και ανάλυσης ψηφιακών αποδεικτικών στοιχείων σε πολύπλοκες εγκληματολογικές έρευνες[3].

Ζωντανή εγκληματολογία (Live Forensics): Οι τεχνικές ζωντανής εγκληματολογίας χρησιμοποιούνται για την απόκτηση αποδεικτικών στοιχείων απευθείας από συνεχώς ενεργά συστήματα, εξετάζοντας τα δεδομένα που αποθηκεύονται στην μνήμη RAM[3]. Σκοπός αυτής της μεθόδου είναι να αποκτηθούν τα δεδομένα χωρίς να παραβιάζεται η ακεραιότητά τους κατά τη διαδικασία. Σε περιπτώσεις όπου η άμεση αντιμετώπιση ενεργών απειλών αποτελεί προτεραιότητα, είναι ζωτικής σημασίας να διεξάγεται η εγκληματολογική διαδικασία με ταχύτητα και αποτελεσματικότητα[7].

Ανάκτηση εγκληματολογικών δεδομένων: Αποτελεί μια μέθοδο που χρησιμοποιείται με σκοπό την ανάκτηση αρχείων που έχουν διαγραφεί από ένα υπολογιστικό σύστημα ή μνήμη. Αυτή, συνεπάγεται την αναζήτηση αρχείων που μπορεί να έχουν διαγραφεί μερικώς, αλλά εξακολουθούν να αφήνουν διάσπαρτα ίχνη στη συσκευή[1]. Με αυτόν τον τρόπο, οι ειδικοί μπορούν να αναγνωρίσουν και να ανακτήσουν αυτά τα κατακερματισμένα αρχεία, αναδημιουργώντας τα από τα υπολείμματα που βρίσκονται σε διάφορα μέρη του συστήματος[2].

Εγκληματολογία κωδικών πρόσβασης (Password Forensics): Η εγκληματολογία κωδικών πρόσβασης επιδιώκει την ανάλυση και ανάκτηση κωδικών που χρησιμοποιούνται για την εξασφάλιση της προστασίας ευαίσθητων δεδομένων σε υπολογιστές και συστήματα αρχείων. Μέσω διαφόρων τεχνικών ανάκτησης, όπως επιθέσεις ωμής βίας ή μείωση του αριθμού των πιθανών κωδικών, επιδιώκεται η πρόσβαση σε κρυπτογραφημένα αρχεία ή λογαριασμούς[7]. Η εν λόγω διαδικασία

αποτελεί κρίσιμο μέρος της διερεύνησης περιστατικών που αφορούν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή παραβιάσεις δεδομένων.

Εγκληματολογία ηλεκτρονικού ταχυδρομείου (Email Forensics): Χρησιμοποιώντας εγκληματολογικά εργαλεία ηλεκτρονικού ταχυδρομείου, οι ερευνητές μπορούν να αναλύσουν και να εξάγουν κρίσιμες πληροφορίες από τα μεταδεδομένα κεφαλίδας email. Αυτό περιλαμβάνει λεπτομέρειες όπως η διεύθυνση IP της πηγής, οι χρονικές σημάνσεις παράδοσης και το όνομα υπολογιστή[10]. Μέσω της διερεύνησης των μεταδεδομένων ενισχύεται η πλήρη κατανόηση της αλυσίδας γεγονότων που σχετίζονται με το συγκεκριμένο email και διαδραματίζει καθοριστικό ρόλο στη διαδικασία της ανάκτησης αποδεικτικών στοιχείων κατά τη διερεύνηση υποθέσεων που αφορούν ηλεκτρονικό έγκλημα [7].

Αντίστροφη Στεγανογραφία: Είναι ένα εξειδικευμένο πεδίο που ασχολείται με τον εντοπισμό κρυμμένων μηνυμάτων, τα οποία ενσωματώνονται σε υπάρχοντα δεδομένα χωρίς να γίνονται αντιληπτά.[8] Πρωταρχικός στόχος της είναι η ανίχνευση, η επιβεβαίωση και, εάν είναι εφικτό, η ανάκτηση αυτών των κρυφών πληροφοριών[9]. Η διαδικασία αυτή, παίζει καθοριστικό ρόλο για την αντιμετώπιση της στεγανογραφίας και την προστασία των ψηφιακών δεδομένων.

2.3.2 Εγκληματολογικά Εργαλεία

Τα σύγχρονα εγκληματολογικά εργαλεία παρέχουν ένα ευρύ φάσμα δυνατοτήτων που αποσκοπούν στον αποτελεσματικό εντοπισμό αρχείων, απλοποιώντας τη διαδικασία ανάλυσης στις ψηφιακές έρευνες.[13] Αυτά τα εργαλεία αυτοματοποιούν σημαντικές εργασίες, όπως η ανάκτηση μερικώς διαγραμμένων αρχείων και η ακριβής ανάλυσης του περιεχομένου τους. Επίσης, ανάμεσα στις προηγμένες δυνατότητες που παρέχουν, είναι οι σύνθετες αναζητήσεις και οι γραφικές αναπαραστάσεις των μονάδων δίσκου.[12] Χάρη σε αυτά τα χαρακτηριστικά, καθίσταται δυνατή η αποκατάσταση και η συλλογή ψηφιακών δεδομένων γεγονός που συμβάλλει στην συγκέντρωση στοιχείων που έχουν ζωτική σημασία για την έρευνα. Με αυτόν τον τρόπο, προωθείται η έγκυρη και συνεχής ενημέρωση των ερευνητών[11]. Τα εγκληματολογικα εργαλεία διακρίνονται για τον γρήγορο χρόνο απόκρισης τους και εκτελούν διάφορες βασικές λειτουργίες, όπως:

Λήψη: Η διαδικασία της λήψης περιλαμβάνει τη φυσική και λογική αντιγραφή δεδομένων και την επαλήθευσή τους κατόπιν απόκτησης τόσο από την ύποπτη μονάδα δίσκου όσο και απο και απο τη γραμμή εντολών ή GUI[7].

Επικύρωση: Η διαδικασία αυτή περιλαμβάνει τον κατακερματισμό, το φιλτράρισμα και την ανάλυση κεφαλίδων ώστε να διασφαλιστεί η ακεραιότητα και η αξιοπιστία των δεδομένων που αποκτήθηκαν[7].

Εξαγωγή: Η διαδικασια αυτή πραγματοποιείται με την αναζήτηση λέξεων-κλειδιών, την προβολή δεδομένων, την αποσυμπίεση αρχείων, την αποκρυπτογράφηση κρυπτογραφημένων δεδομένων και τη χάραξη αρχείων για την εξαγωγή σχετικών πληροφοριών από τα αποκτηθέντα δεδομένα[7].

Ανακατασκευή: Αυτή η διαδικασία εστιάζει στη δημιουργία αντιγράφων και περιλαμβάνει αντιγραφή περιεχομένου ενός φυσικού δίσκου σε ένα άλλο, αντιγραφή μιας ολόκληρης εικόνα δίσκου, που περιλαμβάνει όλα τα δεδομένα και τις κατατμήσεις, σε έναν φυσικό δίσκο, και τέλος, αντιγραφή του περιεχομένου ενός τμήματος ενός φυσικού δίσκου, σε ένα άλλο τμήμα[7].

Αναφορές: Δημιουργούνται αναφορές που τεκμηριώνουν ολόκληρη την εγκληματολογική διαδικασία, συμπεριλαμβανομένων των ενεργειών που ελήφθησαν, των ευρημάτων και της ανάλυσης τους[7].

Τα εγκληματολογικά εργαλεία διαδραματίζουν κρίσιμο ρόλο στις ψηφιακές έρευνες διευκολύνοντας τις διαδικασίες που προαναφέρθηκαν καθώς η ανάπτυξη και η χρήση τους διαρκώς εξελίσσεται, διασφαλίζοντας την αξιοπιστια και την αποτελεσματικότητά τους.

2.4 Κλάδοι Digital Forensics

2.4.1 Network Forensics

Η εγκληματολογία δικτύου είναι ένα εξειδικευμένο πεδίο της ψηφιακής εγκληματολογίας που εστιάζει στη διερεύνηση και ανάλυση της δραστηριότητας του δικτύου. Αφορά την εξέταση του δικτύου και της εσωτερικής κυκλοφορίας του, ιδιαίτερα σε περιπτώσεις όπου υπάρχουν ενδείξεις για κακόβουλες δραστηριότητες ή επιθέσεις στον κυβερνοχώρο. Καθώς το διαδίκτυο και οι σχετικές τεχνολογίες έχουν επεκταθεί, η ανάγκη για εγκληματολογικές αρχές δικτύου καθίσταται επιτακτική[14,15].

Ο πρωταρχικός στόχος της εγκληματολογίας δικτύου είναι η απόκτηση και η αναπαράσταση των δεδομένων που διαρρέουν εντός του δικτύου, συμπεριλαμβανομένων των μηνυμάτων, των αρχείων, των email και του ιστορικού περιήγησης στον ιστό. Αναλύοντας την κίνηση του δικτύου, δίνεται η δυνατότητα στους ερευνητές να αποκτήσουν σημαντικές πληροφορίες για τη φύση των υπό διερεύνηση δραστηριοτήτων[16].

Για τον εντοπισμό και την αποτελεσματική ανάλυση των ψηφιακών επιθέσεων, απαιτείται η κατανόηση των διαφόρων πρωτοκόλλων και εφαρμογών δικτύου, όπως πρωτόκολλα web, πρωτόκολλα email, πρωτόκολλα δικτύου και πρωτόκολλα μεταφοράς αρχείων. Η γνώση αυτών, επιτρέπει την έγκαιρη αναγνώριση ανωμαλιών ή υπόπτων συμπεριφορών δικτύου που μπορεί να υποδηλώνουν κακόβουλη πρόθεση[14].

Στην εγκληματολογία δικτύου, αναλύονται διάφορα πρωτόκολλα κυκλοφορίας και επίπεδα δικτύου για τη συλλογή στοιχείων και τη διερεύνηση των δραστηριοτήτων του. Ακολουθεί μια επισκόπηση ορισμένων πρωτοκόλλων και επιπέδων που εξετάζονται συνήθως:

Σύνδεσμος δεδομένων και φυσικό επίπεδο (Ethernet): Εργαλεία όπως το Wireshark και το Tcpdump χρησιμοποιούνται για τη λήψη δεδομένων κίνησης δικτύου παρακολουθώντας τη διεπαφή Ethernet. Αυτό το γεγονός, επιτρέπει στους ερευνητές να φιλτράρουν και να ανακατασκευάσουν τα στοιχεία που μεταδίδονται. Πρωτόκολλα όπως το Πρωτόκολλο Ανάλυσης Διεύθυνσης (ARP) και πρωτόκολλα υψηλότερου επιπέδου μπορούν επίσης να αναλυθούν, παρόλο που η κρυπτογράφηση τους δυσχεραίνει αυτήν τη διαδικασία. Ωστόσο, η ίδια η κρυπτογράφηση μπορεί να εγείρει υποψίες[15].

Επίπεδο μεταφοράς και δικτύου (TCP/IP): Οι εγκληματολογικές τεχνικές στο επίπεδο δικτύου παρέχουν πληροφορίες δρομολόγησης και στοιχεία καταγραφής ελέγχου ταυτότητας. Η διερεύνηση αυτών των πληροφοριών βοηθά στον εντοπισμό των παραβιασμένων πακέτων, στον εντοπισμό της πηγής τους και στην ανακατασκευή των διαδρομών δρομολόγησης. Τα αρχεία καταγραφής συσκευών δικτύου προσφέρουν λεπτομερείς πληροφορίες για τις δραστηριότητες δικτύου. Συσχετίζοντας αρχεία καταγραφής από διαφορετικές συσκευές δικτύου, οι ερευνητές μπορούν να συνθέσουν την ακολουθία των γεγονότων[15].

Χρήση εξέτασης κυκλοφορίας βάσει περιπτώσεων (Διαδίκτυο): Το Διαδίκτυο προσφέρει ένα ευρύ φάσμα υπηρεσιών, καθεμία από τις οποίες περιέχει πολύτιμα ψηφιακά στοιχεία. Οι ερευνητές επικεντρώνονται στον εντοπισμό αρχείων καταγραφής διακομιστή που σχετίζονται με αυτές τις

υπηρεσίες. Διακομιστές Ιστού, διακομιστές email και διακομιστές συνομιλίας αναμετάδοσης διαδικτύου (IRC) συλλέγουν πολύτιμες πληροφορίες καταγραφής, όπως ιστορικό περιήγησης, στοιχεία λογαριασμού email, πληροφορίες λογαριασμού χρήστη και άλλα[15].

Ασύρματα δίκτυα: Η εγκληματολογία δικτύου επεκτείνεται επίσης σε ασύρματα δίκτυα και συσκευές, όπως τα κινητά τηλέφωνα. Η κίνηση από ασύρματα δίκτυα συλλέγεται και αναλύεται, συμπεριλαμβανομένων των φωνητικών επικοινωνιών. Επιπλέον, μπορεί να προσδιοριστεί η θέση των κινητών συσκευών. Οι μέθοδοι ανάλυσης για την ασύρματη κίνηση είναι παρόμοιες με εκείνες που χρησιμοποιούνται για τα ενσύρματα δίκτυα, αλλά πρέπει να ληφθούν υπόψη συγκεκριμένα ζητήματα ασφάλειας που σχετίζονται με τα ασύρματα δίκτυα[15].

Προκλήσεις

Η εγκληματολογική ανάλυση δικτύου θέτει αρκετές προκλήσεις που πρέπει να αντιμετωπίσουν οι ερευνητές. Μια σημαντική πρόκληση περιλαμβάνει την ανίχνευση δεδομένων κίνησης, η οποία μπορεί να παρεμποδίζεται από ποικίλες διαμορφώσεις δικτύου και μέτρα ασφαλείας[17]. Για την αντιμετώπισή τους, θα πρέπει να αναπτυχθούν εργαλεία καταγραφής κίνησης (sniffers) σε πολλά σημεία του δικτύου χρησιμοποιώντας μια αποκλειστική θύρα που λαμβάνει ένα αντίγραφο της κίνησης δικτύου από τον μεταγωγέα(span)[18][93].

Η συσχέτιση δεδομένων αποτελεί ακόμη μια πολύπλοκη διαδικασία στην εγκληματολογία δικτύου, κατά την οποία είναι απαραίτητη η συσχέτιση δεδομένων με αιτιολογικά ή χρονικά κριτήρια συμπεριλαμβάνοντας τις ακριβείς χρονικές σφραγίδες στα αρχεία καταγραφής και στα δεδομένα που έχουν καταγραφεί[17,95].

Επιπλέον, χρησιμοποιούνται συχνά τεχνικές κρυπτογράφησης, όπως συνδέσεις SSL VPN, για την απόκρυψη των περιεχομένων επικοινωνίας. Αυτό καθιστά δύσκολη την ανάλυση των πραγματικών περιεχομένων, και για αυτόν τον λόγο, απαιτούνται πρόσθετες τεχνικές καταγραφής και διερεύνησης για την αποκάλυψη τους[17,94].

Επιπρόσθετα, ο προσδιορισμός της πραγματικής πηγής μιας επίθεσης αποτελεί μια ακόμη σημαντική πρόκληση. Με τη χρήση ενδιάμεσων κεντρικών υπολογιστών ή απομακρυσμένων διακομιστών μεσολάβησης, καθίσταται δύσκολος για τους ερευνητές ο εντοπισμός της αρχικής διεύθυνσης των υπόπτων[95].

Στην εγκληματολογία δικτύου, ο πρωταρχικός στόχος των ερευνητών είναι η ανάλυση των πακέτων δικτύου, που συνήθως αποθηκεύονται σε αρχεία PCAP. Για αυτόν τον λόγο, είναι απαραίτητη η εξέταση των δεδομένων που υπάρχουν εντός της κυκλοφορίας δικτύου, συμπεριλαμβανομένων πρωτοκόλλων, διευθύνσεων IP, αριθμών θυρών και χρονικών σημάνσεων. Η εξαγωγή και η ανάλυση αυτών των πληροφοριών από διαφορετικούς τύπους κίνησης δικτύου είναι ζωτικής σημασίας για την αποκάλυψη στοιχείων και την ανασύσταση των γεγονότων που σχετίζονται με την έρευνα[17,95].

2.4.2 Database Forensics

Η εγκληματολογία βάσεων δεδομένων είναι ένα εξειδικευμένο πεδίο της ψηφιακής εγκληματολογίας που εστιάζει στη διερεύνηση και ανάλυση βάσεων δεδομένων και των σχετικών μεταδεδομένων τους.

Ακολουθεί την καθιερωμένη διαδικασία εγκληματολογίας υπολογιστών που προαναφέρθηκε παραπάνω, ωστόσο εφαρμόζει ειδικές τεχνικές διερεύνησης για τα περιεχόμενα και τα μεταδεδομένα βάσης δεδομένων. Αυτός ο κλάδος, περιλαμβάνει επίσης την ανάλυση πληροφοριών που είναι αποθηκευμένες στη μνήμη RAM ενός διακομιστή, η οποία μπορεί να απαιτεί τεχνικές ζωντανής ανάλυσης[19,20].

Ο κύριος στόχος της εγκληματολογίας βάσεων δεδομένων είναι ο προσδιορισμός της πρόσβασης και των ενεργειών που πραγματοποιήθηκαν καθώς επίσης και τη χρονική στιγμή αυτών. Η εξέταση μιας βάσης δεδομένων σε ένα εγκληματολογικό πλαίσιο περιλαμβάνει την ανάλυση διαφόρων πτυχών, όπως οι χρονικές σημάνσεις των ενημερώσεων δεδομένων, τα αρχεία καταγραφής συναλλαγών και τα αρχεία καταγραφής ελέγχου. Αναλύοντας αυτά τα στοιχεία, οι ερευνητές μπορούν να ανασυνθέσουν γεγονότα, να εντοπίσουν ανωμαλίες ή μη εξουσιοδοτημένες δραστηριότητες[19,21].

Προκλήσεις και προβλήματα της Εγκληματολογικής Επιστήμης Βάσεων Δεδομένων

Ο τομέας της εγκληματολογίας Βάσεων Δεδομένων αντιμετωπίζει αρκετές προκλήσεις και ζητήματα, τα οποία απαιτούν περαιτέρω έρευνα και διερεύνηση. Οι κύριες προκλήσεις περιλαμβάνουν:

1. Ποικιλία υποδομών βάσεων δεδομένων: Διαφορετικά συστήματα βάσεων δεδομένων τα οποία έχουν τη δική τους μοναδική υποδομή και υπηρεσίες, όπως αρχεία δεδομένων, αρχεία καταγραφής και αρχεία ελέγχου. Αυτή η ποικιλομορφία περιπλέκει τη διαδικασία της εγκληματολογικής ανάλυσης. Επιπλέον, η ποικιλομορφία των τεχνουργημάτων της βάσης δεδομένων και των διαφορετικών λειτουργικών συστημάτων όπως τα WINDOWS, UNIX προσθέτουν περαιτέρω πολυπλοκότητα στη διαδικασία έρευνας[22,23].
2. Πολυδιάστατη φύση των συστημάτων βάσεων δεδομένων: Τα συστήματα βάσεων δεδομένων είναι εγγενώς πολυδιάστατα, αποτελούμενα από εσωτερικά, εννοιολογικά και εξωτερικά επίπεδα. Κάθε επίπεδο έχει τα δικά του χαρακτηριστικά και υποδομή, γεγονός που καθιστά δύσκολο για τους ερευνητές τον προσδιορισμό της έκτασης που έχει παραβιαστεί. Οι δυσκολίες στον εντοπισμό κατάλληλων δεδομένων μπορεί να οδηγήσουν σε περιορισμούς χρόνου και πόρων[22,23].
3. Έλλειψη διαχείρισης γνώσης: Η γνώση της εγκληματολογικής επιστήμης Βάσεων Δεδομένων είναι διάσπαρτη σε διάφορες πηγές, συμπεριλαμβανομένου του Διαδικτύου, των βιβλίων και των διατριβών, γεγονός που δυσχεραίνει τη διάδοση κρίσιμων πληροφοριών[22,23].

Για την αντιμετώπιση αυτών των προκλήσεων, έχουν αναπτυχθεί συγκεκριμένα μοντέλα διερεύνησης για διαφορετικά συστήματα βάσεων δεδομένων, όπως είναι η Oracle, ο MS SQL Server και η MySQL. Ωστόσο, αυτά τα μοντέλα συχνά έχουν αλληλοεπικαλυπτόμενες διαδικασίες και ορολογίες και οι βασικές εγκληματολογικές πρακτικές δεν είναι πάντα κατάλληλες για την έρευνα βάσεων δεδομένων λόγω των διακριτών χαρακτηριστικών τους. Αυτό έχει ως αποτέλεσμα την δυσκολία ανάλυσης μεγάλου όγκου δεδομένων που αποθηκεύονται σε διακομιστές. Για αυτόν τον λόγο, είναι απαραίτητη η προσοχή στην ανάλυση σχετικών αποδεικτικών στοιχείων που συλλέγονται από μια βάση, όπως τα αρχεία καταγραφής συναλλαγών, και ο έλεγχος τους με σκοπό την ανίχνευση ύποπτων συναλλαγών[23].

2.4.3 Cloud Forensics

Το Cloud Forensics είναι ένας τομέας εγκληματολογικής έρευνας που εστιάζει στη συλλογή και ανάλυση ψηφιακών δεδομένων από περιβάλλοντα cloud. Η εγκληματολογία του υπολογιστικού νέφους μπορεί επίσης να οριστεί ως η εφαρμογή επιστημονικών αρχών και τεχνολογικών πρακτικών με σκοπό την αναπαράσταση γεγονότων εντός του υπολογιστικού νέφους. Αυτή μπορεί να περιλαμβάνει τον εντοπισμό, τη συλλογή, τη διατήρηση, την εξέταση, την ερμηνεία και την αναφορά ψηφιακών στοιχείων[25].

Συχνά θεωρείται ένα υποσύνολο της εγκληματολογίας δικτύου, αξιοποιώντας τις αρχές της ψηφιακής εγκληματολογικής επιστήμης σε περιβάλλοντα cloud. Για την αποτελεσματική εφαρμογή τεχνικών ψηφιακής εγκληματολογίας στο πλαίσιο του cloud computing, είναι απαραίτητη η κατανόηση του τρόπου λειτουργίας του. Αυτό περιλαμβάνει τη γνώση μοντέλων υπολογιστικού νέφους, όπως η υποδομή ως υπηρεσία (IaaS), η πλατφόρμα ως υπηρεσία (PaaS) και το λογισμικό ως υπηρεσία (SaaS), καθώς και οι διάφορες εφαρμογές και τα ζητήματα ασφάλειας που σχετίζονται με περιβάλλοντα cloud[25].

Με την κατανόηση των εννοιών, των υπηρεσιών, των μοντέλων ανάπτυξης και των θεμάτων ασφάλειας του υπολογιστικού νέφους, μπορούν να εφαρμοστούν αποτελεσματικά οι εγκληματολογικές μεθοδολογίες οι οποίες είναι ζωτικής σημασίας για τη διεξαγωγή επιτυχημένων ερευνών με τον εντοπισμό αποδεικτικών στοιχείων και την πρόληψη και αντιμετώπιση των εγκλημάτων στο cloud.

Προκλήσεις Cloud Forensics

Είναι πολύ σημαντικό το cloud computing για τον τρόπο με τον οποίο αποθηκεύονται και επεξεργάζονται τα δεδομένα καθώς προσφέρει ευελιξία, επεκτασιμότητα και οικονομική απόδοση. Ωστόσο, η ευρεία υιοθέτηση των τεχνολογιών cloud έχει επίσης δημιουργήσει νέες προκλήσεις στον τομέα της ψηφιακής εγκληματολογίας[24]:

Προσβασιμότητα σε αποδεικτικά στοιχεία: Είναι σημαντική για τον εντοπισμό στοιχείων και κατ επέκταση, τη διεξαγωγή εγκληματολογικών ερευνών. Ωστόσο, η πρόσβαση σε αποδεικτικά στοιχεία που είναι αποθηκευμένα σε περιβάλλοντα cloud μπορεί να είναι δύσκολη εξαιτίας της ανάγκης για απόκτηση κατάλληλων αδειών, της αποκεντρωμένης αποθήκευσης δεδομένων και της άγνωστης φυσικής τοποθεσίας των συσκευών υλικού cloud. Σε αντίθεση με την παραδοσιακή ψηφιακή εγκληματολογία, η οποία επιτρέπει τη φυσική πρόσβαση στο υλικό, η εγκληματολογία του cloud αντιμετωπίζει περιορισμούς στη φυσική αλληλεπίδραση με αυτό[26].

Κατακερματισμός δεδομένων: Τα δεδομένα που βρίσκονται στο cloud, διανέμονται συχνά σε πολλούς διαφορετικούς διακομιστές και συσκευές, γεγονός που καθιστά δύσκολη τη συγκέντρωση των αποδεικτικών στοιχείων. Ο μεγάλος όγκος δεδομένων και τα τροποποιημένα ή διαγραμμένα δεδομένα περιπλέκουν περαιτέρω την εγκληματολογική διαδικασία[26].

Θέματα ασφαλείας: Τα συστήματα Cloud εφαρμόζουν ισχυρά μέτρα ασφαλείας για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Παρόλο που το γεγονός αυτό είναι σημαντικό για την προστασία των δεδομένων, μπορεί να δημιουργήσει δυσκολίες στην απόκτηση πρόσβασης στα δεδομένα κατα την έρευνα. Επιπλέον, ο εντοπισμός των αρχείων καταγραφής επηρεάζεται από τα διαφορετικά μοντέλα υπηρεσιών cloud. Στα μοντέλα Πλατφόρμα ως υπηρεσία (PaaS) και Λογισμικό ως υπηρεσία (SaaS), καθίσταται δύσκολη η αναγνώριση των αρχείων καταγραφής συστήματος και της

κατάστασής τους λόγω της περιορισμένης πρόσβασης, που συνήθως παρέχεται μέσω API ή προκαθορισμένων διεπαφών. Πολλοί πάροχοι υπηρεσιών Cloud επιβάλλουν περιορισμούς στις υπηρεσίες συλλογής αρχείων καταγραφής και σκόπιμα αποκρύπτουν ορισμένες λεπτομέρειες[26,24].

Νομικές επιπτώσεις: Η συλλογή και η εξέταση αποδεικτικών στοιχείων από ένα περιβάλλον cloud μπορεί να εγείρει νομικές προκλήσεις, ιδιαίτερα όταν τα δεδομένα αποθηκεύονται με διαφορετικές δικαιοδοσίες. Η παρουσία πολλαπλών δικαιοδοσιών και η πολλαπλή μίσθωση στο cloud computing παρουσιάζει σημαντικές προκλήσεις για τις εγκληματολογικές έρευνες καθώς προκαλούν διαφορετικές απαιτήσεις σχετικά με την πρόσβαση στα δεδομένα, και την εύρεση αποδεικτικών στοιχείων[26].

Τεχνολογικές προκλήσεις: Υπάρχει έλλειψη εξειδικευμένων εγκληματολογικών εργαλείων ειδικά σχεδιασμένων για περιβάλλοντα cloud. Ενώ τα υπάρχοντα εργαλεία που χρησιμοποιούνται στην ψηφιακή εγκληματολογία εφαρμόζονται σε έρευνες cloud, οι περιορισμοί τους στην αντιμετώπιση κατανεμημένων υποδομών και η έλλειψη φυσικής πρόσβασης εμποδίζουν την ολοκλήρωση των ερευνών. Η ανάπτυξη νέων εργαλείων για την απόκτηση, εξέταση και ανάλυση δεδομένων cloud είναι απαραίτητη. Επίσης, η κρυπτογράφηση δεδομένων από χρήστες cloud περιπλέκει περαιτέρω τις έρευνες, ειδικά εάν τα κλειδιά κρυπτογράφησης δεν είναι διαθέσιμα ή προσβάσιμα[26,24].

Είναι ζωτικής σημασίας να αντιμετωπιστούν αυτές οι προκλήσεις προκειμένου να διεξαχθούν επιτυχώς οι εγκληματολογικές έρευνες στο cloud. Απαιτείται έρευνα και ανάπτυξη εξειδικευμένων εγκληματολογικών εργαλείων και τεχνικών προσαρμοσμένων σε αυτά τα περιβάλλοντα.

2.4.4 IoT Forensics

Η εγκληματολογία του IoT είναι ένας αναδυόμενος τομέας που εστιάζει στη διερεύνηση εγκλημάτων και συμβάντων που αφορούν συσκευές IoT. Το Διαδίκτυο των Πραγμάτων (IoT) αναφέρεται στη διασύνδεση υπολογιστικών συσκευών με το Διαδίκτυο. Χαρακτηριστικά παραδείγματα τέτοιων συσκευών αποτελούν οι αισθητήρες, οι έξυπνες συσκευές της καθημερινότητας, ακόμα και εξειδικευμένες συσκευές που χρησιμοποιούνται σε βιομηχανίες, οι οποίες μπορούν να αλληλεπιδρούν μεταξύ τους, μειώνοντας την ανθρώπινη παρέμβαση στις εργασίες. Με την εκθετική ανάπτυξη και συνδεσιμότητα των συσκευών IoT, δημιουργείται ένας τεράστιος όγκος δεδομένων, καθιστώντας τες έναν στόχο επιθέσεων στον κυβερνοχώρο[27].

Η πολυπλοκότητα των συστημάτων IoT, που περιλαμβάνει διαφορετικές τεχνολογίες επικοινωνίας, συσκευές, πρωτόκολλα και πρότυπα, οδηγεί στην δημιουργία προκλήσεων που αφορούν τη διασφάλιση της ασφάλειας. Η προστασία των δεδομένων σε συσκευές IoT είναι ιδιαίτερα δύσκολη λόγω της ετερογενούς και δυναμικής φύσης τους. Ως αποτέλεσμα, η εγκληματολογία του IoT έχει αναδειχθεί ως μια εξειδικευμένη επέκταση της ψηφιακής εγκληματολογίας η οποία περιλαμβάνει την ανάλυση συσκευών IoT για τη συλλογή και τη διατήρηση της ασφάλειας δεδομένων[27,28,29].

Προκλήσεις IoT Forensics

Η εγκληματολογία του IoT αντιμετωπίζει πολλές προκλήσεις σε όλη τη διαδικασία διερεύνησης. Ξεκινώντας από τα γενικά ζητήματα, υπάρχει έλλειψη τυποποιημένης μεθοδολογίας και πλαισίου ειδικά προσαρμοσμένου για την εγκληματολογία του IoT. Το πεδίο βρίσκεται ακόμα στα αρχικά του

στάδια και συχνά βασίζεται στις μεθοδολογίες της απλής ψηφιακής εγκληματολογίας, οι οποίες μπορεί να μην ανταποκρίνονται πλήρως στις μοναδικές απαιτήσεις των ερευνών IoT[30].
Επιπλέον, υπάρχει έλλειψη κατάλληλων εργαλείων που έχουν σχεδιαστεί ειδικά για την εγκληματολογική έρευνα σε συσκευές και συστήματα IoT, καθώς τα υπάρχοντα εργαλεία είναι συχνά ανεπαρκή για τη διερεύνηση τους[27,31]. Η διαφορετική υπολογιστική ισχύς, η διάρκεια ζωής της μπαταρίας, τα λειτουργικά συστήματα, τα πρωτόκολλα δικτύου και η χωρητικότητα αποθήκευσης των συσκευών IoT απαιτούν εξειδικευμένα εργαλεία, ικανά να εξάγουν δεδομένα και στοιχεία από τη διευρυνόμενη σειρά συσκευών. Υπάρχει επιτακτική ανάγκη για αξιόπιστα και οικονομικά εργαλεία που μπορούν να αναλύσουν αποτελεσματικά τα ευρήματα ενισχύοντας την αξιοπιστία των αποδεικτικών στοιχείων[27,31].

Μία ακόμη βασική πρόκληση στην εγκληματολογία του IoT είναι ο εντοπισμός, η συλλογή και η διατήρηση των αποδεικτικών στοιχείων. Η ποικιλομορφία των συσκευών IoT, συμπεριλαμβανομένων των ποικίλων λειτουργικών συστημάτων τους, σε συνδυασμό με την απουσία τυποποιημένων πρακτικών, περιπλέκει περαιτέρω τη διαπίστωση της γνησιότητας και της αξιοπιστίας των εγκληματολογικών στοιχείων που λαμβάνονται από αυτές τις συσκευές. Συνεπώς, η καθιέρωση μιας τυποποιημένης προσέγγισης για τη συλλογή αποδεικτικών στοιχείων καθίσταται δύσκολη. Η εξαγωγή δεδομένων χωρίς την παραβίαση της συσκευής ή την αλλοίωση των αποδεικτικών στοιχείων καθίσταται αδύνατη[30].

Επιπρόσθετα, ο τεράστιος όγκος δεδομένων που προκύπτουν από συστήματα IoT αποτελεί σημαντική πρόκληση λόγω του πλήθους των ετερογενών πηγών δεδομένων και της έλλειψης συγχρονισμού μεταξύ των συσκευών. Το γεγονός αυτο, επιδεινώνεται περαιτέρω από την έλλειψη συνεκτικού χρονοδιαγράμματος, καθιστώντας ακόμη πιο δύσκολη την ενσωμάτωση δεδομένων από διαφορετικές πηγές και την εύρεση σημαντικών πληροφοριών.[30,27].

Επιπλέον, οι περιορισμένοι υπολογιστικοί πόροι και η μνήμη των συσκευών IoT συμβάλλουν στη σύντομη διάρκεια ζωής των δεδομένων και στον κίνδυνο απώλειάς τους. Ενώ η μεταφορά δεδομένων στο cloud μπορεί να μετριάσει τους περιορισμούς αποθήκευσης, εισάγει νέες προκλήσεις που σχετίζονται με τη διατήρηση της αλυσίδας αποδεικτικών στοιχείων και την διασφάλιση της ακεραιότητας των συλλεγόμενων δεδομένων[31,27].

Η διατήρηση της αλυσίδας επιμέλειας (chain of custody) είναι ακόμη μια πρόκληση, η οποία είναι σημαντική για τη διασφάλιση της εγκυρότητας των αποδεικτικών στοιχείων. Αυτή η διαδικασία περιλαμβάνει την τεκμηρίωση του χρονολογικού ιστορικού τους σε όλα τα στάδια της έρευνας. Συνεπώς, για να γίνουν αποδεκτά, η αλυσίδα επιμέλειας οφείλει να συμβάλλει στην ακεραιότητα των αποδεικτικών στοιχείων και τις σχετικές διαδικασίες ορθής διαχείρισης, συμπεριλαμβανομένων των μεθόδων που χρησιμοποιούνται για την εξέταση, την ανάλυση και την παρουσίαση των ευρημάτων. Επιπλέον, η αλυσίδα επιμέλειας είναι υπεύθυνη για τον καθορισμό, σε κάθε στάδιο της έρευνας, των συγκεκριμένων λεπτομερειών σχετικά με τον χώρο, τον χρόνο και τα πρόσωπα που εμπλέκονται με τα ψηφιακά αποδεικτικά στοιχεία[31,27].

Οι συσκευές IoT είναι επιρρεπείς σε διάφορα ζητήματα ασφάλειας που μπορεί να τις εκθέσουν σε πιθανές επιθέσεις, δυσχεραίνοντας τις ψηφιακές έρευνες. Ένα τέτοιο ζήτημα είναι η πλαστογράφηση ταυτότητας, την οποία χρησιμοποιούν οι κακόβουλοι χρήστες με σκοπό την μη εξουσιοδοτημένη πρόσβαση και τον έλεγχο της επικοινωνίας με τη συσκευή. Η παραποίηση δεδομένων είναι ένα ζήτημα που απορρέει από αυτό, όπου τα δεδομένα τροποποιούνται ή διαγράφονται, θέτοντας σε κίνδυνο την ακεραιότητα των αποδεικτικών στοιχείων[27,31].

Τέλος, τα ανεπαρκή μέτρα ασφαλείας μπορεί να θέσουν σε κίνδυνο την ακεραιότητα και την αξιοπιστία των δεδομένων που είναι αποθηκευμένα σε συσκευές IoT[27,31].

2.5 Digital Evidence

Τα ψηφιακά αποδεικτικά στοιχεία (Digital Evidence) της εγκληματολογικής επιστήμης αφορούν όλους τους κλάδους της εγκληματολογίας. Αναφέρονται σε οποιαδήποτε πληροφορία αποθηκεύεται ή μεταδίδεται σε ψηφιακή μορφή και μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο. Περιλαμβάνει ένα ευρύ φάσμα τύπων δεδομένων, όπως αρχεία ήχου, ηχογραφήσεις, λίστες επαφών, αντίγραφα ασφαλείας διαφόρων προγραμμάτων και συσκευών, ιστορικό προγράμματος περιήγησης, cookies, βάσεις δεδομένων και συμπιεσμένα αρχεία, συμπεριλαμβανομένων και των κρυπτογραφημένων. Αυτά τα αποδεικτικά στοιχεία είναι σημαντικά για την πορεία της έρευνας και μπορούν να παρέχουν πολύτιμες πληροφορίες για δραστηριότητες ή γεγονότα που σχετίζονται με μια υπόθεση[32,33].

Τύποι Digital Evidence

Τα ψηφιακά αποδεικτικά στοιχεία μπορούν να πάρουν διάφορες μορφές, καθεμία από τις οποίες απαιτεί συγκεκριμένες μεθόδους διαχείρισης για την διασφάλιση της αξιοπιστίας τους. Οι ιστοσελίδες, για παράδειγμα, δεν έχουν αποδεικτική αξία και μπορεί να αμφισβητηθούν εάν δεν αποδειχθεί η αυθεντικότητα και η ακεραιότητά τους. Μια προσέγγιση για την ασφάλεια των ιστοσελίδων είναι μέσω προσθηκών προγράμματος περιήγησης που αποθηκεύουν και κρυπτογραφούν το περιεχόμενο, μαζί με χρονικές σημάνσεις και πολλαπλά αντίγραφα ασφαλείας. Η εκτύπωση του προστατευμένου υλικού σε ασφαλή μορφή, όπως το PDF, μπορεί επίσης να βελτιώσει περαιτέρω την ακεραιότητά τους[34].

Ψηφιακά έγγραφα, όπως αρχεία XML ή Word, πρέπει επίσης να υποβάλλονται ως αποδεικτικά στοιχεία σε περιπτώσεις που είναι τα μόνα διαθέσιμα. Η μετατροπή τους σε ασφαλή μορφή, όπως το PDF, με πρόσθετες τροποποιήσεις, χρονικές σημάνσεις και άλλες σχετικές πληροφορίες μπορεί να βοηθήσει στην μετατροπή τους σε αξιόπιστα αποδεικτικά στοιχεία[34].

Τα email αποτελούν πολύτιμα στοιχεία για μια έρευνα, ωστόσο η αποδεικτική τους αξία μπορεί να περιοριστεί. Για να αποφευχθεί αυτό, χρησιμοποιούνται ορισμένα μοντέλα τα οποία δημιουργούν και εξάγουν αντίγραφα απεσταλμένων ή ληφθέντων μηνυμάτων ηλεκτρονικού ταχυδρομείου, διασφαλίζοντας την καταγραφή όλων των επικοινωνιών για αποδεικτικούς σκοπούς[34].

Τα αρχεία καταγραφής προσφέρουν μια πολύτιμη πηγή για την κατανόηση της αλληλουχίας των γεγονότων και των ενεργειών που πραγματοποιούνται σε ένα σύστημα ή μια συσκευή. Λειτουργούν ως ψηφιακό ίχνος, παρέχοντας κρίσιμες πληροφορίες για μη εξουσιοδοτημένες απόπειρες πρόσβασης, ευπάθειες συστήματος και ύποπτες δραστηριότητες. Αυτά τα αρχεία μπορούν να συμβάλουν στη δημιουργία αποδεικτικών στοιχείων με διάφορους τρόπους. Μια προσέγγιση είναι να παρουσιάζονται ως καταθέσεις, αντιμετωπίζοντάς τα ως τυπικά ψηφιακά έγγραφα. Ωστόσο, μια πιο ισχυρή μορφή αποδεικτικών στοιχείων μπορεί να επιτευχθεί με την ανάθεση τους σε ένα αξιόπιστο τρίτο μέρος (TTP) και επιτρέποντας του τη διαχείριση αυτών[34].

Καθώς οι ψηφιακές συναλλαγές και οι μέθοδοι ηλεκτρονικών πληρωμών συνεχίζουν να πολλαπλασιάζονται, καθίσταται κρίσιμο να καθοριστεί η αποδεικτική αξία τους. Η αυξανόμενη επικράτηση των ηλεκτρονικών καρτών και άλλων μηχανισμών ψηφιακών πληρωμών απαιτεί ιδιαίτερη

προσοχή στον τρόπο με τον οποίο μπορεί να ενισχυθεί η αποδεικτική τους σημασία. Η κατανόηση των πρωτοκόλλων ασφαλείας, των μεθόδων κρυπτογράφησης και των μηχανισμών ελέγχου ταυτότητας που χρησιμοποιούνται σε αυτά τα συστήματα είναι πρωταρχικής σημασίας για τη διαπίστωση της αυθεντικότητας των ψηφιακών αρχείων πληρωμών[34].

Μεθοδολογία Digital Evidence

Μια ψηφιακή εγκληματολογική έρευνα περιλαμβάνει συνήθως τρία κύρια στάδια τα οποία σχετίζονται άμεσα με τα ψηφιακά στοιχεία: απόκτηση ή απεικόνιση, ανάλυση και αναφορά. Με βάση αυτά τα τρία στάδια, παρουσιάζεται παρακάτω ένα πλαίσιο που αποτελείται από οκτώ φάσεις για τη συλλογή ψηφιακών στοιχείων.

1. Συλλογή: Το αρχικό βήμα αφορά την επιβεβαίωση της εμφάνισης ενός περιστατικού και περιλαμβάνει την αξιολόγηση της έκτασης του και των συνθηκών που προκύπτουν. Η κατανόηση της φύσης του, πιο συγκεκριμένα, του είδους του και των σχετικών λεπτομερειών είναι ζωτικής σημασίας σε αυτό το στάδιο. Αυτό το βήμα συμβάλλει στον προσδιορισμό των χαρακτηριστικών του και στην επιλογή των καταλληλότερων μεθόδων και εργαλείων για τον εντοπισμό, τη διατήρηση και τη συλλογή πληροφοριών[35].
2. Επεξήγηση συστήματος: Κατόπιν επιβεβαίωσης ενός περιστατικού, ακολουθεί η συλλογή συγκεκριμένων δεδομένων που σχετίζονται με αυτό. Σε αυτά περιλαμβάνονται οι σημειώσεις και μια ολοκληρωμένη περιγραφή του συστήματος που θα διερευνηθεί. Επιπλέον, είναι απαραίτητη η περιγραφή του λειτουργικού συστήματος και των τυπικών ρυθμίσεών του, όπως η μορφή της μονάδας δίσκου, η μνήμη RAM και η θέση δεδομένων. Αυτό το βήμα στοχεύει στη δημιουργία μιας σαφής εικόνας για το σύστημα και τη διαμόρφωση, ώστε να αναλυθεί περαιτέρω[35].
3. Απόκτηση αποδείξεων: Κατά τη διάρκεια αυτού του βήματος, είναι απαραίτητη η λήψη τόσο των πτητικών όσο και των μη πτητικών δεδομένων. Ο έλεγχος της ακεραιότητας των συλλεγόμενων πληροφοριών είναι ζωτικής σημασίας για την ασφάλειά τους, δεδομένου ότι τα πτητικά δεδομένα μπορούν να αλλάξουν με την πάροδο του χρόνου. Για αυτό το λόγο, έχει ιδιαίτερη σημασία η σειρά με την οποία θα συλλεχθούν. Αφού συγκεντρωθούν τα πτητικά δεδομένα, το επόμενο βήμα περιλαμβάνει τη συλλογή μη πτητικών δεδομένων, κυρίως από τον σκληρό δίσκο. Υπάρχουν συνήθως τρεις μέθοδοι που χρησιμοποιούνται για τη λήψη δεδομένων από τον σκληρό δίσκο:
    a. Η εκτέλεση εικόνας bitstream περιλαμβάνει τη δημιουργία ενός πλήρους και ακριβούς αντιγράφου του σκληρού δίσκου, με τη λήψη κάθε bit δεδομένων και τη διατήρηση της αρχικής δομής του[35].
    b. Η χρήση μιας συσκευής υλικού η οποία διασφαλίζει ότι το μηχάνημα είναι εκτός σύνδεσης και ο σκληρός δίσκος είναι αποσυνδεδεμένος και ασφαλής για την αποφυγή τυχόν τροποποιήσεων ή παραβίασης των αρχικών δεδομένων[35].
    c. Με τη χρήση μιας εγκληματολογικής εργαλειοθήκης επιτρέπεται η απόκτηση δεδομένων ενώ το μηχάνημα είναι ακόμα σε λειτουργία, με σκοπό την εξαγωγή σχετικών πληροφοριών με εξειδικευμένα εργαλεία και τεχνικές[35].

    Μετά την απόκτηση των δεδομένων, είναι σημαντική η διασφάλιση και η επαλήθευση της ακεραιότητά τους. Επιπλέον, θα πρέπει να παρέχεται μια σαφής περιγραφή του τρόπου με τον οποίο ανακαλύφθηκαν και διαχειρίστηκαν[35].

4. Αξιολόγηση χρονοδιαγράμματος: Μετά την απόκτηση αποδεικτικών στοιχείων, το επόμενο βήμα στην εγκληματολογική έρευνα περιλαμβάνει τη διεξαγωγή της ανάλυσης και της αξιολόγησης. Μια κρίσιμη πτυχή αυτού του σταδίου είναι η δημιουργία ενός αναλυτικού χρονοδιαγράμματος, το οποίο περιέχει πληροφορίες σχετικά με τις τροποποιήσεις και τη

δημιουργία εγγράφων. Για τη συλλογή αυτών των πληροφοριών, χρησιμοποιούνται διάφορα εργαλεία για την εξαγωγή μεταδεδομένων από το σύστημα. Η διαδικασία αυτή έχει ώς κύριο στόχο την δημιουργία μιας ολοκληρωμένης επισκόπησης των δραστηριοτήτων που πραγματοποιήθηκαν στη συσκευή[35].

5. Μέσα Μαζικής Ενημέρωσης και Αξιολόγηση Αντικειμένων: Για τον εξορθολογισμό του συνόλου δεδομένων, μια προσέγγιση είναι η κατηγοριοποίηση των αρχείων ως χρήσιμων και μη, κάτι που απαιτεί γνώση συστημάτων αρχείων και τεχνουργημάτων μητρώου. Αυτή η κατηγοριοποίηση συμβάλλει στη μείωση του όγκου των δεδομένων που πρέπει να εξεταστούν. Επιπλέον, είναι σημαντικό να εξεταστούν στοιχεία που σχετίζονται με τους λογαριασμούς χρηστών, τη χρήση του προγράμματος περιήγησης, τις λήψεις εγγράφων, τις δραστηριότητες αρχείων (άνοιγμα και δημιουργία) και τις εκτελέσεις προγραμμάτων.[35].
6. Αναζήτηση συμβολοσειράς ή Byte: Κατα τη διαδικασία αυτή, πραγματοποιείται η αναζήτηση εικόνων χαμηλής ανάλυσης. Αυτή η διαδικασία περιλαμβάνει τη χρήση εργαλείων και τεχνικών που μπορούν να αναζητήσουν συγκεκριμένες υπογραφές byte ή μοτίβα συμβολοσειρών[35].
7. Επαναφορά δεδομένων: Αυτό το βήμα περιλαμβάνει τη διαδικασία ανάκτησης δεδομένων από το σύστημα αρχείων με τη χρήση διαφόρων εργαλείων τα οποία χρησιμοποιούνται για την εξέταση των αρχείων όλων των δεδομένων. Μια άλλη τεχνική που χρησιμοποιείται είναι η χάραξη αρχείων, όπου τα αρχεία δεδομένων εξάγονται από ακατέργαστες εικόνες με βάση τις κεφαλίδες των αρχείων τους. Αυτή η προσέγγιση είναι κρίσιμη για την περαιτέρω συλλογή αποδεικτικών στοιχείων στην έρευνα[35].
8. Αναφορά αποτελεσμάτων: Το τελικό στάδιο αφορά την τεκμηρίωση και την παρουσίαση των ψηφιακών δεδομένων που εξετάστηκαν κατα την έρευνα. Αυτό περιλαμβάνει την περιγραφή των ενεργειών που πραγματοποιήθηκαν, τον εντοπισμό τυχόν περαιτέρω βημάτων που πρέπει να γίνουν και τη διατύπωση συστάσεων για βελτιώσεις στους κανονισμούς, στις οδηγίες, στις μεθόδους και στα εργαλεία.[35].

Κεφάλαιο 3ο: Εργαλεία της Ψηφιακής Εγκληματολογίας: Ανάλυση και Κατηγοριοποίηση ανά Κλάδους

Εργαλεία Network Forensics

Tcpdump

Το Tcpdump είναι ένα ευρέως χρησιμοποιούμενο εργαλείο γραμμής εντολών που επιτρέπει την καταγραφή και ανάλυση της κίνησης δικτύου, κυρίως σε συστήματα που βασίζονται σε Unix.[36] Προσφέρει τη δυνατότητα σύλληψης πακέτων και αποθήκευσης των αποτελεσμάτων σε μορφή αρχείου που μπορεί να εξεταστεί περαιτέρω χρησιμοποιώντας εργαλεία όπως το Wireshark[37]. Το Tcpdump είναι ευέλικτο, επιτρέποντας τη γρήγορη καταγραφή προβλημάτων και τη συνεχή λήψη μεγάλου όγκου επισκεψιμότητας για μελλοντική ανάλυση. Είναι σημαντικό να σημειωθεί ότι το tcpdump μπορεί να συλλάβει δεδομένα τόσο στο επίπεδο σύνδεσης δεδομένων (επίπεδο 2) όσο και στο επίπεδο δικτύου (επίπεδο 3). Ωστόσο, η καταγραφή δεδομένων στο επίπεδο δικτύου μπορεί να οδηγήσει σε μεγάλα αρχεία καταγραφής, προκαλώντας πιθανούς περιορισμούς αποθήκευσης[92]. Για να μετριαστεί αυτό, το tcpdump παρέχει επιλογές φιλτραρίσματος για την καταγραφή μόνο της επιθυμητής κίνησης, αποφεύγοντας τα περιττά δεδομένα. Γενικά συνιστάται η καταγραφή ενός μεγάλου εύρους επισκεψιμότητας και η εφαρμογή φίλτρων κατά τη φάση της ανάλυσης για να διασφαλιστεί η ολοκληρωμένη έρευνα.

NetworkMiner

Το NetworkMiner είναι ένα εργαλείο εγκληματολογικής ανάλυσης δικτύου που έχει σχεδιαστεί για το λειτουργικό σύστημα Windows, αλλά είναι συμβατό και με Linux, Mac OS X και FreeBSD. Αποτελεί ένα αξιοσημείωτο εργαλείο ανίχνευσης δικτύου και λήψης πακέτων, επιτρέποντας στους χρήστες να ανιχνεύουν διάφορα χαρακτηριστικά δικτύου, όπως λειτουργικά συστήματα, περιόδους σύνδεσης, ονόματα κεντρικών υπολογιστών και ανοιχτές θύρες. Το εργαλείο αυτό, ξεχωρίζει για την ικανότητά του να εκτελεί αυτές τις αναλύσεις χωρίς να δημιουργεί πρόσθετη κίνηση στο δίκτυο. Εκτός από την παρακολούθηση σε πραγματικό χρόνο, το NetworkMiner είναι σε θέση να αναλύει αρχεία καταγραφής πακέτων για ανάλυση εκτός σύνδεσης. Αυτή η λειτουργία επιτρέπει την ανακατασκευή και την εξαγωγή των μεταδιδόμενων αρχείων και πιστοποιητικών από την κυκλοφορία δικτύου που έχει καταγραφεί. Παρουσιάζοντας τα εξαγόμενα αντικείμενα σε μια φιλική προς τον χρήστη διεπαφή, το NetworkMiner απλοποιεί τη διαδικασία εκτέλεσης προηγμένης ανάλυσης επισκεψιμότητας δικτύου (NTA). Αυτό όχι μόνο ενισχύει τη διαδικασία ανάλυσης, αλλά εξοικονομεί επίσης πολύτιμο χρόνο για τους αναλυτές και τους εγκληματολόγους[91].

Wireshark

Το Wireshark είναι ένα εργαλείο ανάλυσης πρωτοκόλλου δικτύου που συλλαμβάνει πακέτα από μια σύνδεση δικτύου, όπως το Διαδίκτυο ή ένα τοπικό δίκτυο. Εκτελεί τρεις κύριες λειτουργίες: λήψη πακέτων, φιλτράρισμα και οπτικοποίηση[38].

Κατά τη λήψη πακέτων, το Wireshark εντοπίζει μια σύνδεση δικτύου σε πραγματικό χρόνο και καταγράφει τις ροές κίνησης που μπορεί να αποτελούνται από χιλιάδες πακέτα. Συλλέγει αυτά τα δεδομένα για περαιτέρω ανάλυση και εξέταση[38].

Επιπλέον, το Wireshark παρέχει ισχυρές δυνατότητες φιλτραρίσματος, επιτρέποντας στους χρήστες να διαιρούν όλα τα δεδομένα που έχουν συλληφθεί. Μπορούν να εφαρμοστούν φίλτρα για την εξαγωγή συγκεκριμένων πληροφοριών ενδιαφέροντος, επιτρέποντας τους να εστιάσουν στα δεδομένα που χρειάζονται ανάλυση[38].
Τέλος, όσον αφορά την οπτικοποίηση, το Wireshark επιτρέπει στους χρήστες να εμβαθύνουν στις λεπτομέρειες των μεμονωμένων πακέτων δικτύου. Παρέχει μια ολοκληρωμένη προβολή των συνομιλιών και των ροών δικτύου, επιτρέποντας στους χρήστες να κατανοήσουν τη ροή δεδομένων μεταξύ των κόμβων του δικτύου[38].

Η διαδικασία του sniffing πακέτων περιλαμβάνει τη χρήση του Wireshark ως εργαλείου για την εξερεύνηση και την αποκάλυψη ευρημάτων μέσα σε σήραγγες δικτύου και συνδέσεις. Οι χρήστες αξιοποιούν το Wireshark για να περιηγηθούν στον τεράστιο όγκο δεδομένων δικτύου και να ανακαλύψουν πολύτιμες πληροφορίες σχετικά με τη συμπεριφορά του, τα πρότυπα επικοινωνίας και τα πιθανά προβλήματα[38].

SNORT

Το SNORT είναι ένα ισχυρό εργαλείο ανοιχτού κώδικα που χρησιμεύει στον εντοπισμό και στην πρόληψη εισβολών σε δίκτυα υπολογιστών. Προσφέρει ανάλυση της κυκλοφορίας του δικτύου σε πραγματικό χρόνο και καταγραφή των πακέτων δεδομένων. Το SNORT χρησιμοποιεί μια γλώσσα βασισμένη σε κανόνες που συνδυάζει διάφορες μεθόδους επιθεώρησης για τον εντοπισμό δυνητικά επιβλαβών δραστηριοτήτων, συμπεριλαμβανομένων ανωμαλιών και παραβιάσεων πρωτοκόλλου. Με αυτό το εργαλείο, οι διαχειριστές δικτύου μπορούν να αναγνωρίσουν αποτελεσματικά τις επιθέσεις άρνησης υπηρεσίας (DoS), τις κατανεμημένες επιθέσεις DoS (DDoS), τις επιθέσεις CGI, τις υπερχειλίσεις buffer και τις σαρώσεις μυστικών θυρών. Καθορίζοντας κανόνες που καθορίζουν τη συμπεριφορά κακόβουλου δικτύου, το SNORT μπορεί να εντοπίσει κακόβουλα πακέτα και να δημιουργήσει ειδοποιήσεις για τους χρήστες. Μπορεί να χρησιμοποιηθεί ως ανιχνευτής ή σύστημα ανίχνευσης εισβολής δικτύου για την αποκάλυψη κακόβουλων πακέτων ή ως ολοκληρωμένη λύση δικτύου IPS που παρακολουθεί τη δραστηριότητα του δικτύου και αποκλείει προληπτικά πιθανούς φορείς επίθεσης[39].

SURICATA

Το Suricata είναι μια μηχανή ανίχνευσης απειλών ανοιχτού κώδικα που προσφέρει μια ολοκληρωμένη γκάμα δυνατοτήτων. Συνδυάζει τις λειτουργίες ενός συστήματος ανίχνευσης εισβολής (IDS), συστήματος πρόληψης εισβολής (IPS), συστήματος παρακολούθησης δικτύου (NMS) και εργαλείο ανάλυσης καταγραφής πακέτων ώστε να συμβάλλει στις εγκληματολογικές έρευνες με τον εντοπισμό, τη διερεύνηση και την άμυνα έναντι κακόβουλων επιθέσεων. Το Suricata είναι συμβατό με διάφορα λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows, Mac, Unix και Linux. Μπορεί να χρησιμοποιηθεί για δύο βασικούς σκοπούς: παρακολούθηση δικτύου σε πραγματικό χρόνο και ανάλυση μετά το συμβάν χρησιμοποιώντας αποθηκευμένες συλλήψεις πακέτων. Συχνά λειτουργεί παράλληλα με τα τείχη προστασίας, τους δρομολογητές ή άλλες συσκευές δικτύου που επεξεργάζονται την κυκλοφορία πριν την προωθήσουν στον επόμενο προορισμό δικτύου. Στη λειτουργία ανάλυσης μετά το συμβάν, το Suricata λειτουργεί ως μέρος ενός ευρύτερου συστήματος που συλλέγει και αναλύει τις συλλήψεις πακέτων, επιτρέποντας την εγκληματολογική εξέταση και την

αναδρομική ανάλυση. Η ευελιξία και η αποτελεσματικότητα του Suricata το καθιστούν ένα ανεκτίμητο εργαλείο για τους επαγγελματίες ασφάλειας δικτύων που επιδιώκουν να βελτιώσουν τις ικανότητές τους στον εντοπισμό απειλών και την απόκριση συμβάντων[40].

Εργαλεία Database Forensics

Στη συνέχεια παρουσιάζονται μερικά από τα κορυφαία εργαλεία λογισμικού για την εγκληματολογία βάσεων δεδομένων που συμβάλλουν στην ανάλυση και την ανάκτηση διαγραμμένων καταχωρίσεων βάσης δεδομένων προσφέροντας μια σειρά χαρακτηριστικών και δυνατοτήτων για τον συγκεκριμένο τομέα εγκληματολογίας, καλύπτοντας διαφορετικές ανάγκες και απαιτήσεις.

Database Forensic Analysis System:
Είναι ένα εμπορικό λογισμικό το οποίο υποστηρίζει διάφορες σχεσιακές και μη σχεσιακές βάσεις δεδομένων όπως Oracle, SQLite, MySQL, MongoDB, Redis και Cassandra. Βοηθά στην επίλυση ζητημάτων που σχετίζονται με διαγραμμένα, κατεστραμμένα ή κατακερματισμένα αρχεία βάσης δεδομένων και προσφέρει δυνατότητες όπως απεριόριστη προσβασιμότητα, εξαγωγή και ανάκτηση αντικειμένων και πολλαπλές λειτουργίες ανάλυσης[41].

Log Analyzer για SQL:
Είναι ακόμη ένα εμπορικό εργαλείο το οποίο έχει σχεδιαστεί ειδικά για την ανάλυση αρχείων καταγραφής των βάσεων δεδομένων του MySQL Server. Επιτρέπει την εγκληματολογική ανάλυση των συναλλαγών καταγραφής, τον εντοπισμό ανωμαλιών και την ανάκτηση των διαγραμμένων αρχείων καταγραφής συναλλαγών. Υποστηρίζει διάφορες μορφές καταγραφής και παρέχει φίλτρα και επιλογές αναφοράς[41].

SQLite Forensics Explorer:
Αυτό το εγκληματολογικό εργαλείο έχει σχεδιαστεί για την ανάκτηση χαμένων και διαγραμμένων βάσεων δεδομένων SQLite. Επισημαίνει τα διαγραμμένα ή ασφαλώς διαγραμμένα δεδομένα και επιτρέπει την εξαγωγή σε διαφορετικές μορφές[41].

SQLite Viewer:

Αυτό το εργαλείο ανοιχτού κώδικα επιτρέπει την επιθεώρηση των περιεχομένων της βάσης δεδομένων SQLite. Φορτώνει αυτόματα βάσεις δεδομένων από φακέλους και υποφακέλους και εξάγει και εμφανίζει εικόνες που είναι αποθηκευμένες σε αυτές. Παρέχει επίσης ένα πρόγραμμα προβολής hex για την εξέταση δυαδικών μεγάλων αντικειμένων (BLOBs) και την εξαγωγή τους για περαιτέρω ανάλυση[41].

Εργαλεία Cloud Forensics

UFED Cloud Analyzer: Το λογισμικό UFED Cloud Analyzer αποτελεί μια ισχυρή λύση ικανή να εξάγει, να αποθηκεύει και να αναλύει δεδομένα από ιδιωτικούς λογαριασμούς κοινωνικών μέσων, συμπεριλαμβανομένων δημοφιλών πλατφορμών όπως το Facebook, το Twitter, το Kik και το Instagram[90]. Το εργαλείο, είναι σχεδιασμένο για Windows και επιτρέπει την εισαγωγή

διαπιστευτηρίων λογαριασμού που είναι αποθηκευμένα στο cloud, χρησιμοποιώντας έναν αναλυτή UFED για εξαγωγή μέσω του συστήματος αρχείων ή φυσική εξαγωγή από τη μνήμη ενός smartphone. Εναλλακτικά, υπάρχει δυνατότητα χειροκίνητης εισαγωγής ονομάτων χρηστών και κωδικών πρόσβασης. Αξιοποιώντας τη διεπαφή προγραμματισμού εφαρμογών (API) που παρέχεται από τον πάροχο υπηρεσιών, το UFED Cloud Analyzer καταγράφει στιγμιότυπα ιδιωτικών στοιχείων. Εξειδικευμένα μέσα αποθήκευσης, συμπεριλαμβανομένων εσωτερικών δίσκων, εξωτερικών μονάδων δίσκου, μονάδων flash, εσωτερικών εγκληματολογικών δικτύων, υπολογιστών εγκληματολογίας ή κατατμήσεων, είναι απαραίτητα για την εξαγωγή εγκληματολογικών δεδομένων. Το UFED Cloud Analyzer χρησιμοποιεί μια ενοποιημένη μορφή για την παρουσίαση δεδομένων από διάφορες υπηρεσίες cloud, προσφέροντας οπτικές αναπαραστάσεις όπως χρονοδιαγράμματα, μικρογραφίες αρχείων, επαφές ή χάρτες, επιτρέποντας ολοκληρωμένη ανάλυση[90].

FROST: Το FROST είναι ένα εγκληματολογικό εργαλείο σχεδιασμένο για την πλατφόρμα υπολογιστικού νέφους OpenStack το οποίο χρησιμοποιείται ιδιαιτέρως σε ψηφιακές εγκληματολογικές έρευνες. Αυτό το εργαλείο συλλέγει δεδομένα από τα αρχεία καταγραφής API, τους εικονικούς δίσκους και τα αρχεία καταγραφής τειχών προστασίας επισκέπτη. Παρέχει δεδομένα καταγραφής με τη μορφή δέντρων κατακερματισμού τα οποία επιστρέφει σε κρυπτογραφική μορφή. Το FROST λειτουργεί στο επίπεδο διαχείρισης cloud και δεν απαιτεί αλληλεπίδραση με το λειτουργικό σύστημα σε εικονικές μηχανές φιλοξενουμένων[42].

Το FROST αποτελείται από τρία κύρια στοιχεία, το καθένα από τα οποία εξυπηρετεί μια συγκεκριμένη λειτουργία:

1. Απόκτηση εικόνας και επικύρωση ακεραιότητας: Αυτό το στοιχείο επιτρέπει στο FROST να ανακτήσει την εικόνα εικονικού δίσκου που σχετίζεται με κάθε χρήστη και στη συνέχεια να επαληθεύσει την ακεραιότητά του χρησιμοποιώντας κρυπτογραφικά αθροίσματα ελέγχου. Με τη λήψη αυτών των εικόνων, το FROST διασφαλίζει ότι τα δεδομένα παραμένουν άθικτα και αναλλοίωτα, παρέχοντας μια αξιόπιστη πηγή αποδεικτικών στοιχείων[42].
2. Πρόσβαση και επαλήθευση αρχείων καταγραφής ερωτημάτων API: Επιτρέπει στους χρήστες να έχουν πρόσβαση και να επικυρώνουν τα αρχεία καταγραφής που περιέχουν όλα τα ερωτήματα API που γίνονται στον πάροχο cloud χρησιμοποιώντας τα δικά τους διαπιστευτήρια. Αυτή η λειτουργία επιτρέπει στους χρήστες να επιβεβαιώνουν την αυθεντικότητα και την ακρίβεια των αλληλεπιδράσεών τους με την πλατφόρμα cloud[42].
3. Συλλογή και επαλήθευση αρχείων καταγραφής OpenStack Firewall: Με αυτό το εργαλείο, το FROST διευκολύνει τη συλλογή και την επαλήθευση των αρχείων καταγραφής τείχους προστασίας OpenStack για οποιαδήποτε εικονική μηχανή (VM) εντός του περιβάλλοντος cloud. Εξετάζοντας αυτά τα αρχεία καταγραφής, οι ερευνητές μπορούν να αποκτήσουν πληροφορίες για τις δραστηριότητες του δικτύου και τις πιθανές παραβιάσεις της ασφάλειας, βοηθώντας στον εντοπισμό και την ανάλυση των σχετικών στοιχείων[42].

Εργαλεία IoT Forensics

Οι εγκληματολογικές έρευνες IoT παρουσιάζουν ποικίλες προκλήσεις, συμπεριλαμβανομένης της ανάγκης για εκτεταμένη συλλογή δεδομένων και ανάλυση σε πραγματικό χρόνο. Ωστόσο, η χρήση των απαραίτητων και έγκυρων εγκληματολογικών εργαλείων συμβάλλει στην διευθέτησή τους. Για

την αποτελεσματική απόκτηση και ανάλυση εγκληματολογικών δεδομένων, απαιτείται ένας συνδυασμός εγκληματολογικών εργαλείων δικτύου και εργαλείων ηλεκτρονικών υπολογιστών.

Μερικά από τα εργαλεία που χρησιμοποιούνται συνήθως για τη συλλογή αποδεικτικών στοιχείων παρουσιάζονται παρακάτω.

NUIX: Το NUIX είναι ένα ψηφιακό εγκληματολογικό εργαλείο ανοιχτού κώδικα, γνωστό για τις εκτεταμένες δυνατότητες αναζήτησης σε διάφορες πηγές δεδομένων. Υπερέχει στην εξαγωγή πολύτιμων πληροφοριών που απαιτούνται για ολοκληρωμένη ανάλυση. Με το ευρύ φάσμα μεθόδων εξαγωγής δεδομένων, το NUIX είναι εξαιρετικά αποτελεσματικό στο χειρισμό πολύπλοκων ερευνών[43].

FTK: Το FTK (Forensic Toolkit) χρησιμεύει τόσο ως εργαλείο προεπισκόπησης όσο και ως εργαλείο απεικόνισης, επιτρέποντας στους ερευνητές να κάνουν προεπισκόπηση και να συλλέγουν δεδομένα από διαφορετικές πηγές, διατηρώντας παράλληλα την ακεραιότητα των αποδεικτικών στοιχείων. Είναι ευρέως αναγνωρισμένο για τις ολοκληρωμένες δυνατότητές του, συμπεριλαμβανομένης της ανάλυσης εικόνων και της ανάκτησης δεδομένων. Το FTK είναι ένα ανεκτίμητο εργαλείο στις εγκληματολογικές έρευνες[43].

SANS SIFT: Το SANS SIFT (SANS Investigative Forensic Toolkit) είναι μια εξειδικευμένη εργαλειοθήκη σχεδιασμένη για εγκληματολογικές έρευνες και αντιμετώπιση περιστατικών. Περιέχει ένα ολοκληρωμένο σύνολο εργαλείων που απαιτούνται για τη διεξαγωγή ενδελεχών εγκληματολογικών ερευνών. Περιλαμβάνει διάφορα εργαλεία ανοιχτού κώδικα, σενάρια και βοηθητικά προγράμματα που βοηθούν στην απόκτηση, τη διατήρηση, την ανάλυση και την αναφορά δεδομένων[43].

Συνδυάζοντας τη χρήση των προαναφερθέντων εργαλείων, οι ερευνητές μπορούν να αντιμετωπίσουν τις προκλήσεις που θέτει η εγκληματολογική ανάλυση του IoT. Η χρήση πολλαπλών εργαλείων όχι μόνο ενισχύει την αξιοπιστία των αποδεικτικών στοιχείων αλλά επιτρέπει επίσης τη διασταυρούμενη επαλήθευση των αποτελεσμάτων. Η ακρίβεια και η προσβασιμότητα είναι κρίσιμοι παράγοντες κατά την επιλογή των κατάλληλων εργαλείων για την απόκτηση δεδομένων και την εγκληματολογική ανάλυση[43].

Κεφάλαιο 4ο: Τεχνολογικό περιβάλλον ψηφιακής δικανικής για εργαλεία

4.1 Open Source περιβάλλον

Η ψηφιακή εγκληματολογία περιλαμβάνει την εφαρμογή εξειδικευμένων εργαλείων και μεθόδων για την εξαγωγή, την διατήρηση και την ανάλυση ψηφιακών δεδομένων από διάφορες ψηφιακές συσκευές και συστήματα. Αυτά τα στοιχεία διαδραματίζουν κρίσιμο ρόλο στην ανακάλυψη ψηφιακών δεδομένων και στον εντοπισμό των ψηφιακών εγκλημάτων στον κυβερνοχώρο.

Μια σημαντική εξέλιξη στον τομέα της ψηφιακής εγκληματολογίας ήταν η άνοδος των εργαλείων ανοιχτού κώδικα. Αυτά τα εργαλεία, που αναπτύχθηκαν και συντηρούνται από μια ομάδα εθελοντών, παρέχουν πολύτιμους πόρους σε εγκληματολογικούς ερευνητές και επαγγελματίες. Τα εργαλεία ανοιχτού κώδικα είναι διαθέσιμα δωρεάν στους χρήστες, επιτρέποντάς τους να τροποποιούν τον πηγαίο κώδικα, να αφαιρούν ή να προσθέτουν λειτουργίες, ακόμη και να διανέμουν το λογισμικό σύμφωνα με τις συγκεκριμένες ανάγκες τους.[45] Αυτή η συλλογική προσέγγιση προωθεί την καινοτομία, ενθαρρύνει την ανταλλαγή γνώσεων και εξουσιοδοτεί τους χρήστες να προσαρμόσουν τα εργαλεία στις μοναδικές προκλήσεις που τίθενται από τις ψηφιακές έρευνες.

4.2 Commercial και Open Source στην ψηφιακή εγκληματολογία: Πλεονεκτήματα και περιορισμοί

4.2.1 Οφέλη Commercial Software

Το εμπορικό λογισμικό προσφέρει συνήθως επαγγελματικές υπηρεσίες υποστήριξης, όπως τεχνική βοήθεια και εξυπηρέτηση πελατών. Οι χρήστες μπορούν να βασιστούν και να απευθυνθούν σε ομάδες υποστήριξης για την αντιμετώπιση τυχόν ζητημάτων που ενδέχεται να αντιμετωπίσουν, διασφαλίζοντας μια ομαλή εμπειρία για τον χρήστη. Για μεγάλους οργανισμούς με νομικές απαιτήσεις συμμόρφωσης και επεκτασιμότητας, συχνά προτιμώνται εμπορικές λύσεις[46].

Το εμπορικό λογισμικό συνοδεύεται από εκτενή τεκμηρίωση και οδηγούς χρήσης. Κατα συνέπεια, τα εμπορικά εργαλεία δίνουν προτεραιότητα στην εμπειρία του χρήστη προσφέροντας καλά σχεδιασμένες διεπαφές που είναι συνεπείς και εύχρηστες. Καταβάλλονται σημαντικές προσπάθειες για τη δημιουργία μιας ολοκληρωμένης τεκμηρίωσης και για εργαλεία υποστήριξης εντός του λογισμικού, διευκολύνοντας τους χρήστες να κατανοήσουν και να αξιοποιήσουν αποτελεσματικά τις δυνατότητες που παρέχονται[46].

Επιπλέον, το λογισμικό υποβάλλεται σε αυστηρές δοκιμές, συμπεριλαμβανομένων αξιολογήσεων ασφαλείας και δοκιμών για ευπάθειες. Δίνεται μεγάλη έμφαση στις συνεχείς ενημερώσεις ώστε να διασφαλιστεί ότι το λογισμικό παραμένει ενημερωμένο για ζητήματα ασφάλειας. Αυτή η έμφαση στην ασφάλεια συμβάλλει στον μετριασμό των κινδύνων και στην προστασία ευαίσθητων δεδομένων, παρέχοντας στους χρήστες μια πιο ασφαλή λύση λογισμικού[46].

Επιπρόσθετα, αναπτύσσεται συχνά με γνώμονα τη συμβατότητα με άλλες εφαρμογές λογισμικού και συσκευές. Αυτή η συμβατότητα επιτρέπει αποτελεσματικές ροές εργασίας και μειώνει τα προβλήματα που μπορεί να προκύψουν κατά τη χρήση διαφορετικών εργαλείων λογισμικού[46].

4.2.2 Μειονεκτήματα Commercial Software

Το κόστος είναι μια σημαντική ανησυχία με τις εμπορικές λύσεις, καθώς η δομή των τιμών είναι απρόβλεπτη. Πρόσθετες χρεώσεις, όπως χρεώσεις υποστήριξης ή ετήσιες πληρωμές, μπορούν να επιβαρύνουν επιπλέον τον χρήστη. Ορισμένα χαρακτηριστικά μπορεί επίσης να κλειδωθούν, με αποτέλεσμα απροσδόκητα έξοδα τα οποία το καθιστούν μια δυνητικά δαπανηρή επένδυση σε σύγκριση με εναλλακτικές λύσεις ανοιχτού κώδικα[46].

Επιπλέον, ο πηγαίος κώδικας δεν είναι ελεύθερα προσβάσιμος ή διαθέσιμος για έλεγχο. Σε αντίθεση με το λογισμικό ανοιχτού κώδικα, οι χρήστες δεν έχουν την ελευθερία να τροποποιήσουν ή να προσαρμόσουν τον υποκείμενο κώδικά του. Αυτή η έλλειψη επιλογών προσαρμογής μπορεί να περιορίσει την προσαρμοστικότητα του λογισμικού σε συγκεκριμένες ανάγκες και απαιτήσεις. Επίσης η έλλειψη διαφάνειας μπορεί να καταστήσει δύσκολη την αξιολόγηση της ασφάλειας, της ποιότητας ή ακόμα και των πιθανών τρωτών σημείων του λογισμικού[46].

Τέλος, μπορεί να σχεδιαστεί για να λειτουργεί βέλτιστα σε ένα συγκεκριμένο οικοσύστημα, γεγονός το οποίο μπορεί να περιορίσει την ευελιξία του σε σύγκριση με λογισμικό ανοιχτού κώδικα που μπορεί να προσαρμοστεί σε διάφορα περιβάλλοντα[46].

4.2.3 Οφέλη open source software

Το λογισμικό ανοιχτού κώδικα προσφέρει οικονομικά αποδοτικές λύσεις καθώς διατίθεται δωρεάν, εξαλείφοντας την ανάγκη για προκαταβολικά έξοδα ή τέλη αδειοδότησης. Αυτό σημαίνει ότι οποιοσδήποτε χρήστης μπορεί να αποκτήσει πρόσβαση σε αυτό χωρίς καμία οικονομική επιβάρυνση. Παρά το γεγονός ότι είναι δωρεάν, διατηρεί υψηλά πρότυπα ποιότητας και λειτουργικότητας διασφαλίζοντας ότι η αξιοπιστία και η απόδοσή του δεν διακυβεύονται[45,46,47,48].

Η αξιοπιστία του λογισμικού ανοιχτού κώδικα ενισχύεται από μια κοινότητα ειδικών προγραμματιστών που συμβάλλουν συνεχώς στη βελτίωσή του. Μέσω της συλλογικής αναθεώρησης κώδικα και του έγκαιρου εντοπισμού των ευπαθειών, τα τρωτά σημεία αναγνωρίζονται και αντιμετωπίζονται γρήγορα, ελαχιστοποιώντας τον κίνδυνο κρίσιμων ζητημάτων. Αυτό το περιβάλλον συνεργασίας προωθεί την καινοτομία, την ανταλλαγή γνώσεων, ενισχύοντας τη συνολική αξιοπιστία και λειτουργικότητα του λογισμικού[47].

Η ευελιξία είναι ακόμη ένα βασικό χαρακτηριστικό του λογισμικού ανοιχτού κώδικα, επιτρέποντάς του να εκτελείται σε διάφορες πλατφόρμες και συσκευές. Προσφέρει συμβατότητα σε διαφορετικά λειτουργικά συστήματα, επιτρέποντας στους χρήστες να αξιοποιήσουν το λογισμικό σε διαφορετικά περιβάλλοντα και συσκευές χωρίς σημαντικούς περιορισμούς. Σε αντίθεση με το ιδιόκτητο λογισμικό, οι χρήστες δεν περιορίζονται από περιορισμούς παρόχων λογισμικού, επιτρέποντας μεγαλύτερη ελευθερία. Αυτή η ευελιξία δίνει επίσης τη δυνατότητα στους οργανισμούς να προσαρμόσουν το λογισμικό στις μοναδικές τους ανάγκες, με αποτέλεσμα πιο εξατομικευμένες και αποτελεσματικές λύσεις[46,47].

Ίσως το πιο αξιοσημείωτο χαρακτηριστικό του λογισμικού ανοιχτού κώδικα είναι η διαφάνεια που προσφέρει τη δυνατότητα πρόσβασης και αναθεώρησης του πηγαίου κώδικα. Αυτή η διαφάνεια επιτρέπει στους χρήστες να αξιολογούν την αξιοπιστία του λογισμικού, να προτείνουν διορθώσεις και αλλαγές και να αντιμετωπίζουν άμεσα πιθανά σφάλματα[45].

Το λογισμικό ανοιχτού κώδικα είναι επίσης εξαιρετικά επεκτάσιμο καθώς προσαρμόζεται εύκολα στις μεταβαλλόμενες απαιτήσεις και στην κατανομή πόρων. Αυτή η ευελιξία επιτρέπει στις επιχειρήσεις να επεκτείνουν ή να μειώσουν τη χρήση τους όπως απαιτείται, διασφαλίζοντας ότι τα επιθυμητά αποτελέσματα μπορούν να επιτευχθούν χωρίς περιορισμούς[46].

Τέλος, η αδειοδότηση με λογισμικό ανοιχτού κώδικα είναι ευέλικτη, εξαλείφοντας την πολυπλοκότητα των συμφωνιών και της παρακολούθησης χρήσης. Μπορεί να εγκατασταθεί και να χρησιμοποιηθεί ελεύθερα από όλο τον κόσμο και συνήθως δεν υπάρχουν περιορισμοί στον αριθμό των εγκαταστάσεων[47].

4.2.4 Μειονεκτήματα open source software

Ενώ το λογισμικό ανοιχτού κώδικα επωφελείται από μια μεγάλη κοινότητα προγραμματιστών και χρηστών που συμβάλλουν στην ανάπτυξή του, το επίπεδο της διαθέσιμης επαγγελματικής υποστήριξης μπορεί να διαφέρει σε σύγκριση με το εμπορικό λογισμικό απαιτώντας απο τους χρήστες να καταφυγουν σε άλλους τρόπους βοήθειας, όπως τα forum[45,46].

Επίσης, η διαθεσιμότητα του πηγαίου κώδικα του λογισμικού στο ευρύ κοινό μπορεί να το κάνει πιο ευάλωτο σε θέματα ασφαλείας. Επιπλέον, η διαφάνεια που επιτρέπει τη συλλογική βελτίωση μπορεί κάλλιστα να αποκαλύψει αδυναμίες που μπορούν να εκμεταλλευτούν κακόβουλοι παράγοντες εάν δεν εφαρμοστούν τα κατάλληλα μέτρα ασφαλείας[45,46].

Επιπρόσθετα, η συνεργατική φύση της ανάπτυξης του ανοιχτού κώδικα μπορεί να έχει ως αποτέλεσμα περίπλοκες βάσεις κώδικα, έλλειψη συνέπειας και ενδελεχή σχολιασμό. Το ποικίλο φάσμα εταιρειών που εξυπηρετεί το λογισμικό ανοιχτού κώδικα μπορεί να συμβάλει περαιτέρω στην πολυπλοκότητά του και να εμποδίσει τη βελτιστοποίηση για συγκεκριμένες ανάγκες[45,46].

Τέλος, η διαθεσιμότητα και της τεκμηρίωσης και των οδηγών χρήσης για λογισμικό ανοιχτού κώδικα μπορεί να ποικίλει. Ορισμένα έργα μπορεί να έχουν περιορισμένους πόρους, γεγονός που καθιστά πιο δύσκολη την πρόσβαση των χρηστών σε σαφείς οδηγίες και καθοδήγηση[45,46].

4.3 Ασφάλεια Open Source εργαλείων

4.3.1 Κίνδυνοι ασφάλειας εργαλείων

Η ασφάλεια του λογισμικού ανοιχτού κώδικα προκαλεί σοβαρές ανησυχίες στους χρήστες κατά την ενσωμάτωση κώδικα third party στις εφαρμογές τους. Αναγνωρίζεται η ανάγκη για αποτελεσματικές διαδικασίες, μεθοδολογίες και εργαλεία για την αντιμετώπιση των σχετικών κινδύνων. Επιθέσεις που έχουν λάβει χώρα και αφορούν την εκμετάλλευση τρωτών σημείων στο λογισμικό και συνεπώς, στα εργαλεία ανοιχτού κώδικα έχουν φέρει στην επιφάνεια το σημαντικό αντίκτυπο και το κόστος που μπορεί να επιφέρουν. Αυτό ενισχύει τη σημασία που πρέπει να δοθεί στην προτεραιότητα της ασφάλειας αυτών των εργαλείων και της εφαρμογής ισχυρών μέτρων ασφαλείας για τον αποτελεσματικό μετριασμό των πιθανών κινδύνων[48,49].

Τα εργαλεία ανοιχτού κώδικα υιοθετούνται ευρέως όχι μόνο από απλούς χρήστες, αλλά και από οργανισμούς, καθιστώντας τα αναπόσπαστο κομμάτι σε διάφορους κλάδους. Ωστόσο, είναι σημαντικό να αναγνωριστούν οι εγγενείς κίνδυνοι που υφίστανται. Είναι υψίστης σημασίας όχι μόνο η αναγνώριση αυτών των κινδύνων, αλλά και η διάθεση πόρων για την ανάπτυξη και τη διατήρηση ενός

ολοκληρωμένου σχεδίου ασφαλείας ειδικά προσαρμοσμένου για εργαλεία ανοιχτού κώδικα. Λαμβάνοντας προληπτικά μέτρα για την αντιμετώπιση της ασφάλειάς τους, μπορούν να μετριαστούν πιθανές ευπάθειες και να προστατευτούν τα συστήματα και τα δεδομένα. Παρακάτω παρατίθενται τρεις από τους σημαντικότερους κινδύνους ασφάλειας:

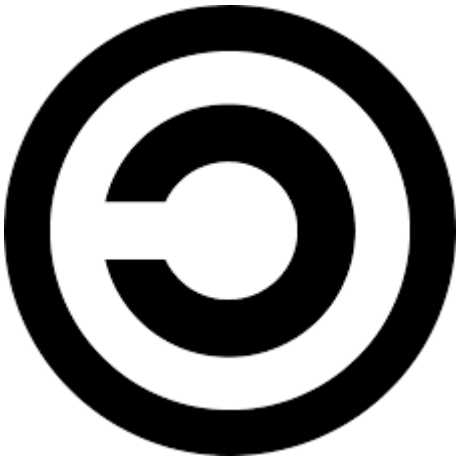
1. Το λογισμικό ανοιχτού κώδικα εγκυμονεί αρκετούς κινδύνους ασφάλειας λόγω τρωτών σημείων και ευπαθειών. Μπορεί να περιέχουν γνωστά και φανερά τρωτά σημεία, καθώς όμως και άγνωστα ή μη φανερά, καθιστώντας απαραίτητη τη συνεχή παρακολούθηση με σκοπό την έγκαιρη αντιμετώπιση και κατά συνέπεια την ελαχιστοποίηση των κινδύνων. Η χρήση εργαλείων και διαδικασιών που παρέχουν διαφάνεια μπορούν να βοηθήσουν στον εντοπισμό και τη διαχείριση πιθανών ζητημάτων ασφάλειας[48,49].
2. Η συμμόρφωση με την άδεια χρήσης αποτελεί επίσης κίνδυνο κατά τη χρήση λογισμικού ανοιχτού κώδικα, καθώς συνήθως υπόκειται σε συγκεκριμένες άδειες που υπαγορεύουν τη χρήση, την τροποποίηση και τη διανομή του. Τα εργαλεία ανοιχτού κώδικα διέπονται από συγκεκριμένες άδειες που περιγράφουν τους όρους και τις προϋποθέσεις για την χρήση, την τροποποίηση και την διανομή τους. Είναι σημαντική και απαραίτητη η σαφή και πλήρη κατανόηση των αδειών χρήσης καθως η μη συμμόρφωση με αυτές μπορεί να οδηγήσει σε νομικές συνέπειες[48,49].
3. Τα εργαλεία ανοιχτού κώδικα που δεν συντηρούνται κατάλληλα ενέχουν κινδύνους για την ασφάλεια, καθώς ενδέχεται να μην λαμβάνουν τακτικές ενημερώσεις και υποστήριξη. Καθώς οι έλεγχοι και η συντηρησή τους βασίζονται σε εθελοντές ή μικρές ομάδες, δεν λαμβάνεται η αμέριστη προσοχή. Το γεγονός αυτό έχει ως συνέπεια, την αύξηση της πιθανότητας εμφάνισης ευπαθειών και παραβάσεων ασφαλείας. Για να μετριαστούν αυτοί οι κίνδυνοι, θα πρέπει να αξιολογείται συχνά και σχολαστικά η κατάσταση συντήρησης των εργαλείων ανοιχτού κώδικα. Η διενέργεια τακτικών ελέγχων ασφαλείας και η έγκαιρη αξιολόγηση των ευπαθειών μπορούν επίσης να συμβάλλουν στον εντοπισμό πιθανών κινδύνων που σχετίζονται με μη συντηρημένο λογισμικό[48,49].

4.4 Άδειες χρήσης

Οι άδειες ανοιχτού κώδικα επιτρέπουν την ανάπτυξη ελεύθερου λογισμικού ανοιχτού κώδικα χρησιμοποιώντας τους υπάρχοντες νόμους περί πνευματικής ιδιοκτησίας με τρόπο που προάγει την κοινή χρήση και τη συνεργασία. Αυτές οι άδειες παρέχουν στους χρήστες δικαιώματα χρήσης, εξέτασης, τροποποίησης και διανομής του λογισμικού. Ισχύουν ιδιαίτερα για λογισμικό υπολογιστών, όπου η πρόσβαση στον πηγαίο κώδικα είναι σημαντική για την πραγματοποίηση τροποποιήσεων.

4.4.1 Τύποι αδειών

Οι άδειες ανοιχτού κώδικα μπορούν να ταξινομηθούν σε δύο κύριες κατηγορίες: copyleft και επιτρεπτές άδειες. Οι άδειες Copyleft, οι οποίες μπορούν να κατηγοριοποιηθούν περαιτέρω ως ισχυρές ή αδύναμες, απαιτούν τα παράγωγα έργα που βασίζονται στον αδειοδοτημένο κώδικα να διανέμονται με την ίδια άδεια copyleft, συμπεριλαμβανομένης της διαθεσιμότητας του πηγαίου κώδικα. Οι επιτρεπτές άδειες, από την άλλη πλευρά, δεν επιβάλλουν τέτοιες απαιτήσεις, επιτρέποντας τη χρήση του κώδικα εντός ιδιόκτητου λογισμικού χωρίς την ανάγκη κοινής χρήσης του πηγαίου κώδικα[50,51].



Σχημα 2 Λογότυπο Copyleft αδειών

Οι επιτρεπτές άδειες (permissive), που αναφέρονται επίσης ως ακαδημαϊκές άδειες, επιτρέπουν στους χρήστες να χρησιμοποιούν, να τροποποιούν και να διανέμουν ελεύθερα λογισμικό χωρίς την απαίτηση να αποκαλύπτουν τον πηγαίο κώδικα. Αυτές οι άδειες θεσπίστηκαν από ιδρύματα για να διευκολύνουν την κοινή χρήση των λογισμικών τους με το ευρύτερο κοινό. Επιβάλλουν ελάχιστους περιορισμούς στη χρήση, επιτρέποντας τη χρήση, την τροποποίηση και τη διανομή του πηγαίου κώδικα. Οι επιτρεπτές άδειες είναι συνήθως συνοπτικές και επιβάλλουν ελάχιστες υποχρεώσεις, που συχνά περιλαμβάνουν αποποίηση ευθύνης από την εγγύηση και την ανάγκη απόδοσης των αρχικών δημιουργών[50,51].

Οι άδειες Copyleft για τα εργαλεία ανοιχτού κώδικα είναι στρατηγικά διαμορφωμένες ώστε να διασφαλίζουν ότι ένα πρόγραμμα λογισμικού παραμένει ελεύθερο. Ωστόσο είναι απαραίτητο, οι τροποποιήσεις ή επεκτάσεις στο πρόγραμμα να εκδοθούν επίσης υπό τους ίδιους όρους. Όταν ένα έργο αδειοδοτείται με άδεια copyleft, οι προγραμματιστές έχουν τα δικαιώματα χρήσης, τροποποίησης και κοινής χρήσης του έργου, όμως, είναι επίσης υποχρεωμένοι να διανέμουν οποιοδήποτε παράγωγο ως ανοιχτού κώδικα. Αυτό σημαίνει ότι ακόμη και αν ένα μικρό τμήμα ενός προϊόντος λογισμικού βασίζεται σε άδεια copyleft ανοιχτού κώδικα, ολόκληρος ο πηγαίος κώδικας πρέπει να διατίθεται δωρεάν, μαζί με τα δικαιώματα τροποποίησης και διανομής του[50,51,52].

4.4.2 Κορυφαίες άδειες ανοιχτού κώδικα

GNU:Η Γενική Δημόσια Άδεια GNU (GPL) αποτελεί μια από τις πιο διαδεδομένες άδειες λογισμικού ανοιχτού κώδικα, που επινοήθηκε από το Ίδρυμα Ελεύθερου Λογισμικού (FSF) για να προστατεύσει το λογισμικό από τη μετατροπή του σε ιδιόκτητο. Η GPL, επιτρέπει την ελεύθερη διανομή του λογισμικού, είτε για εμπορικούς είτε για μη εμπορικούς σκοπούς, διασφαλίζοντας παράλληλα ότι ο πηγαίος κώδικας είναι προσβάσιμος σε όλους. Οι χρήστες έχουν την ελευθερία να τροποποιούν και να δημιουργούν παράγωγα έργα, αλλά πρέπει επίσης να μοιράζονται αυτές τις τροποποιήσεις. Η διάταξη copyleft της GPL επεκτείνει αυτές τις ελευθερίες σε μελλοντικές εκδόσεις, απαιτώντας τη συμμόρφωση για οποιαδήποτε τροποποιημένη ή παράγωγη έκδοση. Επιπλέον, η GPL είναι συμβατή με άλλες άδειες ελεύθερου λογισμικού, επιτρέποντας την ενσωμάτωση συμβατού με αυτήν κώδικα [51,52,53].

Σχήμα 3 GNU Licence

Apache License: Η Άδεια Apache, που δημιουργήθηκε από το Ίδρυμα Λογισμικού Apache (ASF), είναι μια επιτρεπτή άδεια ανοιχτού κώδικα που παρέχει στους χρήστες εκτεταμένη ελευθερία να χρησιμοποιούν, να τροποποιούν και να διανέμουν τροποποιημένες εκδόσεις του λογισμικού χωρίς ανησυχίες για δικαιώματα. Σε αντίθεση με τις άδειες copyleft, η άδεια χρήσης Apache δεν απαιτεί τη διανομή παράγωγων έργων ή τροποποιήσεων με την ίδια άδεια. Ωστόσο, απαιτείται να ισχύει για όλα τα μη τροποποιημένα μέρη του λογισμικού.Η Άδεια χρήσης Apache 2.0 ταξινομείται ως άδεια ελεύθερου λογισμικού και είναι συμβατή με τη Γενική Άδεια Δημόσιας Χρήσης GNU (GPL) έκδοση 3, επιτρέποντας τον συνδυασμό κώδικα και με τις δύο άδειες χρήσης στο λογισμικό που προκύπτει σύμφωνα με την GPLv3[54].

Σχήμα 4 Apache Licence

Microsoft Public Licenses (Ms-PL): Το Ms-PL είναι μια άδεια λογισμικού ελεύθερου και ανοιχτού κώδικα που εισήχθη από τη Microsoft. Σύμφωνα με αυτήν την άδεια, οι χρήστες έχουν την ελευθερία να αναπαράγουν και να διανέμουν πρωτότυπα ή παράγωγα έργα λογισμικού. Η Ms-PL προστατεύει τους δημιουργούς αποκηρύσσοντας τυχόν ρητές εγγυήσεις ή εγγυήσεις για τον κώδικα, διασφαλίζοντας ότι δεν φέρουν ευθύνη εάν αυτός δεν λειτουργεί όπως αναμένεται. Κατά τη διανομή λογισμικού σύμφωνα με το Ms-PL, δεν υπάρχει υποχρέωση κοινής χρήσης του πηγαίου κώδικα, αλλά η διατήρηση των πνευματικών δικαιωμάτων, ευρεσιτεχνιών, εμπορικών σημάτων και απόδοσης από το αρχικό λογισμικό είναι υποχρεωτική. Στην περίπτωση διανομής του λογισμικού στη μορφή του πηγαίου κώδικα, πρέπει να συμπεριληφθεί η πλήρης άδεια Ms-PL. Εναλλακτικά, η διανομή του λογισμικού σε μορφή μεταγλωττισμένου ή αντικειμενικού κώδικα απαιτεί συμμόρφωση με άλλη άδεια συμβατή με το Ms-PL[55].

Σχήμα 5 Microsoft Public Licenses (Ms-PL)

4.5 Open source εργαλεία

Τα εργαλεία ανοιχτού κώδικα είναι απαραίτητα για τους αναλυτές και τους ερευνητές κατά τις εγκληματολογικές έρευνες, καθώς διαδραματίζουν κρίσιμο ρόλο στην ενίσχυση της ανάλυσης και της ερμηνείας των συλλεγόμενων δεδομένων, επιτρέποντας τη μετατροπή τους σε τυποποιημένες μορφές. Το γεγονός αυτό συμβάλλει στην διεξαγωγή μιας ολοκληρωμένης και αποτελεσματικής εξέτασης, δίνοντας τη δυνατότητα στους ερευνητές να φιλτράρουν τον τεράστιο όγκο πληροφοριών με σκοπό την εξαγωγή αποδεικτικών στοιχείων ζωτικής σημασίας για την εξέλιξη των εγκληματολογικών ερευνών[56].

Sleuth Kit

Το Sleuth Kit (TSK) είναι μια ευέλικτη και ολοκληρωμένη συλλογή εργαλείων και βιβλιοθηκών command line ανοιχτού κώδικα που έχουν σχεδιαστεί για πλατφόρμες UNIX και Windows, εστιάζοντας στην εγκληματολογική ανάλυση συστημάτων αρχείων[59]. Επιτρέπει στους ερευνητές να εξετάζουν τα συστήματα αρχείων χωρίς να παρεμβαίνουν στα αρχικά δεδομένα, αποκαλύπτοντας τόσο διαγραμμένο όσο και κρυφό περιεχόμενο. Το TSK υποστηρίζει διάφορους τύπους συσκευών αποθήκευσης, όπως σκληροί δίσκοι (hard drives) ή δίσκοι(disks), συμπεριλαμβανομένων των DOS, BSD και Mac[57,58]. Χρησιμοποιώντας αυτά τα εργαλεία, οι ερευνητές μπορούν να εντοπίσουν και να εξάγουν τμήματα και πληροφορίες για περαιτέρω ανάλυση χρησιμοποιώντας εξειδικευμένα εργαλεία. Το λογισμικό είναι συμβατό με πολλά συστήματα αρχείων[56,57,58].

Ο σχεδιασμός του TSK ως μιας βιβλιοθήκης, του επιτρέπει να ενσωματωθεί σε μεγαλύτερα εργαλεία ψηφιακής εγκληματολογίας, ενώ τα εργαλεία γραμμής εντολών του προσφέρουν άμεση λειτουργικότητα για την ανακάλυψη και συλλογή αποδεικτικών στοιχείων. Επιτρέπει την ανάλυση εικόνων δίσκου που δημιουργούνται από εφαρμογές όπως το 'dd' ή παρόμοια εργαλεία που παράγουν ακατέργαστες εικόνες. Κάθε εργαλείο στο TSK εξυπηρετεί μια συγκεκριμένη εργασία χαμηλού επιπέδου και η συλλογική χρήση τους παρέχει μια ολοκληρωμένη ανάλυση του συστήματος που ερευνάται[58].

Επιπλέον, προσφέρει δυνατότητες δημιουργίας χρονικών γραμμών δραστηριότητας αρχείων, δημιουργίας κατακερματισμένων αρχείων και δεδομένων, οργάνωσης αρχείων με βάση τον τύπο και πραγματοποίησεις αναζητήσεων για συγκεκριμένα ονόματα αρχείων και καταχωρήσεις

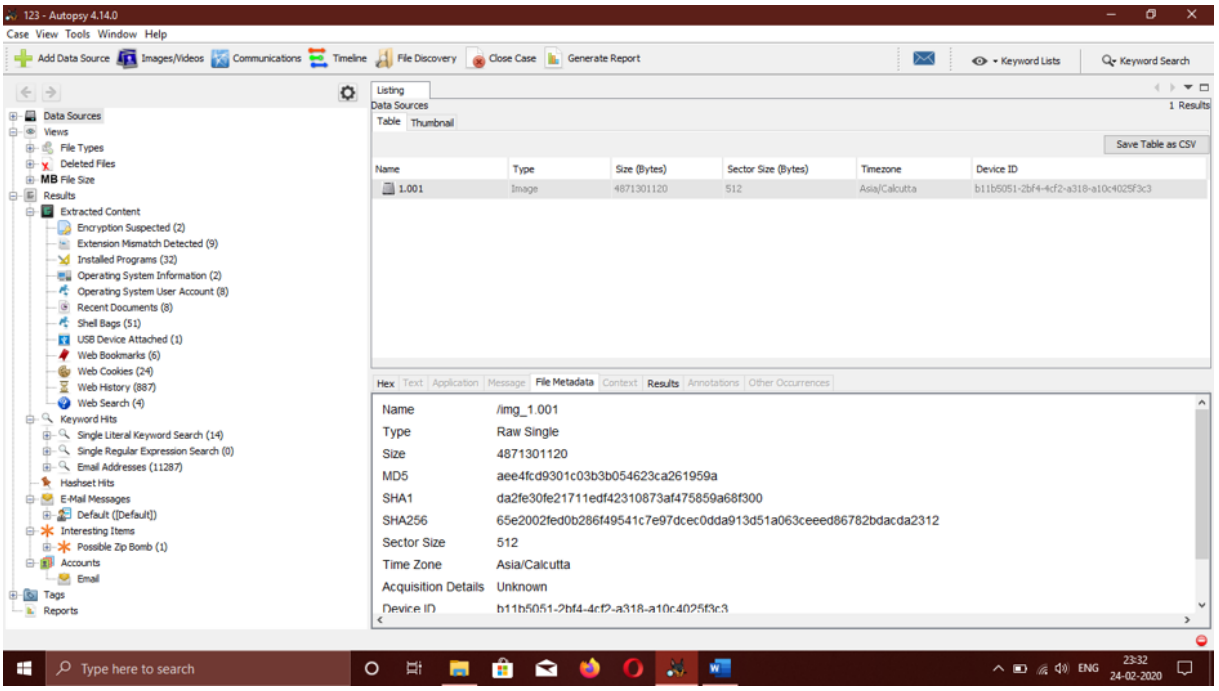
μεταδεδομένων. Το Sleuth Kit μπορεί επίσης να παράγει γραφικές αναφορές ενώ υποστηρίζει την ενοποίηση με βάσεις δεδομένων κατακερματισμού όπως το NIST NSRL και το Hash Keeper[58].

Autopsy

Το Autopsy είναι μια πλατφόρμα ψηφιακής εγκληματολογίας το οποίο χρησιμεύει ως πρόγραμμα περιήγησης γραφικής διεπαφής χρήστη (GUI) και λειτουργεί σε συνδυασμό με το The Sleuth Kit. Απλοποιεί την ανάπτυξη πολυάριθμων προγραμμάτων και προσθηκών ανοιχτού κώδικα από αυτό, παρέχοντας στους ερευνητές ένα φιλικό προς το χρήστη περιβάλλον για να προβάλλουν τα αποτελέσματα της εγκληματολογικής έρευνας[60]. Το Autopsy προσφέρει διάφορες δυνατότητες ανάλυσης αρχείων, όπως κατακερματισμό και αποσυμπίεση τυπικών αρχείων όπως ZIP και JAR, εξαγωγή τιμών EXIF, ανάλυση μεγάλων συστημάτων αρχείων και βασικών συστημάτων αρχείων για ανάλυση εξειδικευμένων μορφών, όπως μορφές email και αρχεία επαφών.[56, 61,62].

Το εργαλείο αυτό, διευκολύνει εργασίες όπως ανάλυση χρονοδιαγράμματος, αναζητήσεις λέξεων-κλειδιών, εξαγωγή τεχνουργημάτων Ιστού (web artifacts) και ανάλυση μητρώου. Το λογισμικό λειτουργεί αποτελεσματικά, χρησιμοποιώντας παράλληλη επεξεργασία και παρέχοντας άμεσα αποτελέσματα. Επιπλέον, το Autopsy αποδεικνύεται οικονομικά αποδοτικό ως εναλλακτική λύση στα εμπορικά εργαλεία ψηφιακής εγκληματολογίας, διατηρώντας παράλληλα βασικές λειτουργίες και παρέχοντας πρόσθετες λειτουργίες[60,61,62].

Η ευκολία χρήσης του, η επεκτασιμότητα και η σχέση κόστους-αποτελεσματικότητας το καθιστούν μια προτιμώμενη επιλογή για τους ερευνητές. Είναι μια ισχυρή και προσβάσιμη πλατφόρμα που συμβάλλει σε αποτελεσματικές και ενδελεχείς έρευνες. Υποστηρίζει πολλαπλά λειτουργικά συστήματα, προσφέρει επεκτασιμότητα μέσω μονάδων ενώ παρέχει βασικά χαρακτηριστικά που απαιτούνται για την παραγωγή και ανάλυση αποδεικτικών στοιχείων. Ωστόσο, είναι σημαντικό να σημειωθεί ότι δεν μπορεί να αναγνωρίσει κρυπτογραφημένα αρχεία[60,61,62].



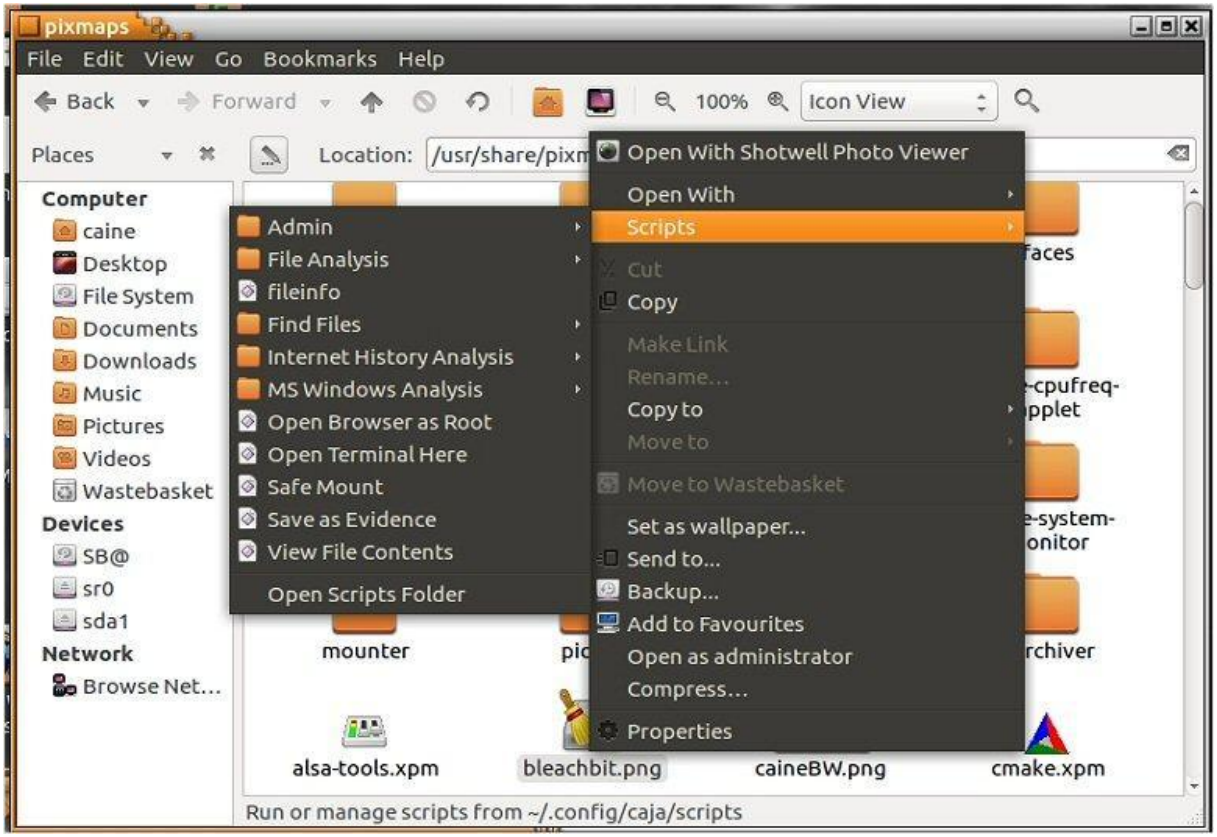
Σχήμα 6 Autopsy Tool

Caine

Το εργαλείο ανοιχτού κώδικα CAINE (Computer Aided Investigative Environment) αποτελεί μια ισχυρή και φιλική προς το χρήστη πλατφόρμα ψηφιακής εγκληματολογίας, προσφέροντας ένα λειτουργικό περιβάλλον για τους επαγγελματίες εγκληματολόγους. Με το ολοκληρωμένο σύνολο εργαλείων και τη διαλειτουργικότητά του, απλοποιεί τη διαδικασία έρευνας και διασφαλίζει την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων. Προσφέρει μια ασφαλή και οργανωμένη πλατφόρμα για τη διεξαγωγή ψηφιακών εγκληματολογικών ερευνών[63,64,65].

Πιο συγκεκριμένα, ο πρωταρχικός στόχος του CAINE είναι να παρέχει ένα πλήρες σύνολο εγκληματολογικών εργαλείων που απαιτούνται για τη διεξαγωγή ψηφιακών ερευνών, συμπεριλαμβανομένης της διατήρησης, της συλλογής, της εξέτασης και της ανάλυσης. Διαθέτει μια φιλική προς το χρήστη διεπαφή που απλοποιεί τη χρήση των εργαλείων και διευκολύνει την αποτελεσματική ανάλυση. Μπορεί να χρησιμοποιηθεί από αφαιρούμενα μέσα όπως μονάδες flash ή δίσκους και να εκτελείται στη μνήμη χωρίς να χρειάζεται η παρεμβολή του λειτουργικού συστήματος. Επιπλέον, είναι συμβατό τόσο με φυσικά συστήματα όσο και με εικονικά περιβάλλοντα όπως το VMware Workstation[64,65].

Τέλος, το CAINE βασίζεται στο Ubuntu 16.04 και υποστηρίζει την ανάλυση δεδομένων απο μια σειρά λειτουργικών συστημάτων, συμπεριλαμβανομένων των Microsoft Windows, Linux και ορισμένων συστημάτων Unix. Ρυθμίζει όλες τις συσκευές μπλοκ σε λειτουργία μόνο για ανάγνωση από προεπιλογή, διασφαλίζοντας την ακεραιότητα των δεδομένων. Οι απαιτήσεις συστήματος για την εκτέλεση του CAINE είναι παρόμοιες με το Ubuntu 16.04, συμπεριλαμβανομένου ενός επεξεργαστή διπλού πυρήνα 2 GHz και 2 GB μνήμης συστήματος[64].



Σχήμα 7 Caine Tool

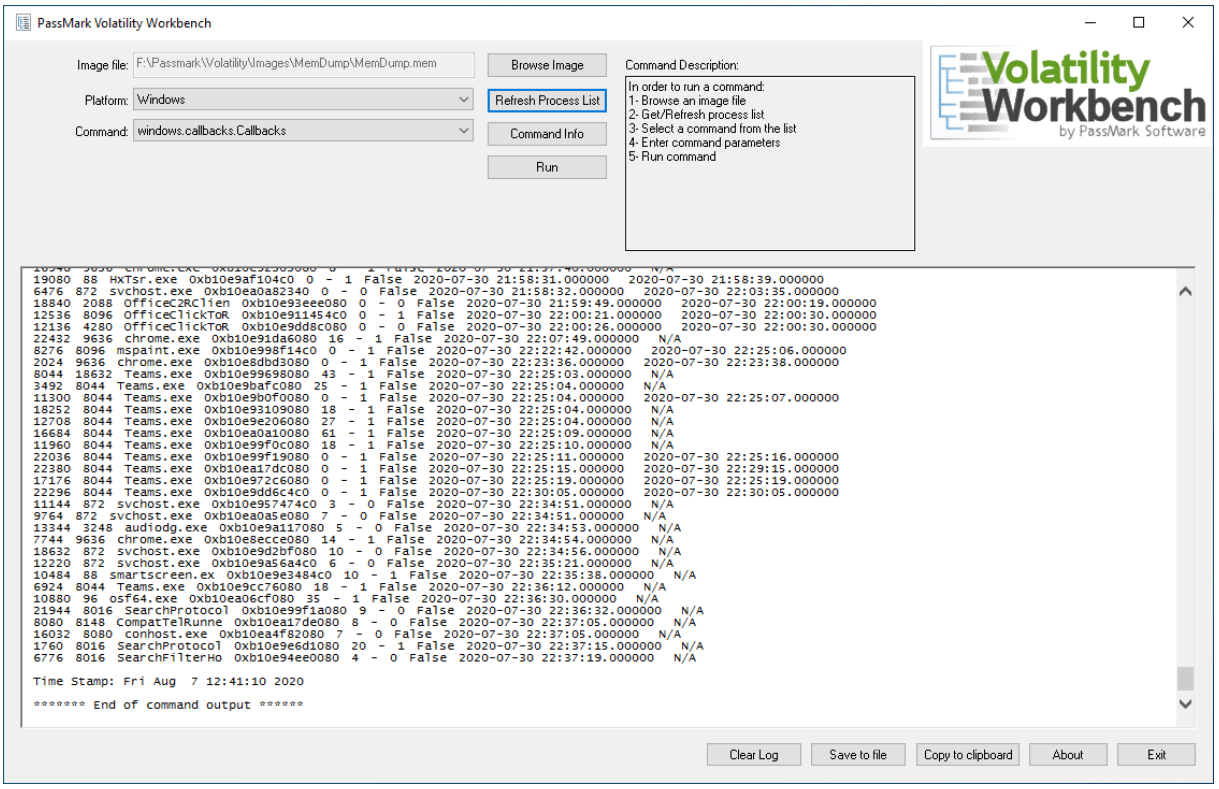
Volatility

Το Volatility είναι ένα εργαλείο ανοιχτού κώδικα που έχει σχεδιαστεί για την ανάλυση και εξαγωγή ψηφιακών στοιχείων από δείγματα μνήμης RAM. Υλοποιείται με Python και λειτουργεί υπό την άδεια GNU General Public 2. Παρέχει στους αναλυτές μια συλλογή εργαλείων που μπορούν να χρησιμοποιηθούν για την εξαγωγή πληροφοριών από τη μνήμη κατά τη διάρκεια ψηφιακών εγκληματολογικών ερευνών[56,66,67].

Ένα από τα βασικά πλεονεκτήματα του Volatility είναι ότι αποτελεί εργαλείο ανοιχτού κώδικα, που επιτρέποντας στους χρήστες να έχουν ελεύθερη πρόσβαση και να εξερευνούν τον πηγαίο κώδικα. Αυτό δίνει τη δυνατότητα στους αναλυτές να αποκτήσουν μια βαθύτερη κατανόηση του εργαλείου επεκτείνοντας τις δυνατότητές του και προσαρμόζοντας το σύμφωνα με τις συγκεκριμένες ανάγκες τους. Επιπλέον, υποστηρίζει ένα ευρύ φάσμα λειτουργικών συστημάτων, συμπεριλαμβανομένων των Windows, Mac, Linux και Android, καθιστώντας το ευέλικτο και προσαρμόσιμο[66,68].

Καθώς υποστηρίζει τόσο συστήματα 32-bit όσο και συστήματα 64-bit, καλύπτει μια σειρά λειτουργικών συστημάτων, καθιστώντας το μια ολοκληρωμένη λύση για την εγκληματολογία της μνήμης (Memory Forensics). Όντας γραμμένο σε Python, αξιοποιεί την ευελιξία και τις εκτεταμένες βιβλιοθήκες που είναι διαθέσιμες. Επιπλέον, η συμβατότητα του Volatility με πολλαπλά λειτουργικά συστήματα το κάνει να ξεχωρίζει από άλλα εργαλεία που περιορίζονται σε συγκεκριμένες πλατφόρμες[66,68].

Το Volatility αναγνωρίζεται και χρησιμοποιείται εκτενώς για την ανάλυση κακόβουλου λογισμικού. Παρέχει στους αναλυτές τη δυνατότητα να εντοπίζουν ενεργές συνδέσεις, να εξετάζουν πιθανά κακόβουλα προγράμματα, να καταγράφουν ανοιχτά αρχεία, να ανακτούν κωδικούς πρόσβασης και να εξάγουν το ιστορικό του προγράμματος περιήγησης και της γραμμής εντολών, μεταξύ άλλων λειτουργιών[66,68].



Σχήμα 8 Volatility Tool

FTK

Το FTK (Forensic Toolkit) είναι ένα εξαιρετικά αναγνωρισμένο λογισμικό εγκληματολογίας υπολογιστών το οποίο χρησιμοποιείται από επαγγελματίες της ψηφιακής εγκληματολογίας για την εκτεταμένη γκάμα χαρακτηριστικών και εργαλείων του. Το FTK έχει σχεδιαστεί ως μια ολοκληρωμένη λύση για την εγκληματολογία υπολογιστών, προσφέροντας ένα ολοκληρωμένο σύνολο εγκληματολογικών εργαλείων σε μια ενιαία πλατφόρμα[69,70].

Ένα χαρακτηριστικό στοιχείο του FTK είναι η εξαιρετική απόδοση του. Σε αντίθεση με άλλα λογισμικά, αξιοποιεί την κατανεμημένη επεξεργασία και χρησιμοποιεί επεξεργαστές πολλαπλών πυρήνων για παράλληλες ενέργειες. Αυτό έχει ως αποτέλεσμα σημαντικά ταχύτερους χρόνους διερεύνησης υποθέσεων, μειώνοντας πιθανώς τον απαιτούμενο χρόνο σε σύγκριση με εναλλακτικά εργαλεία[69,70].

Επιπλέον, το FTK χρησιμοποιεί μια ενιαία, κεντρική βάση δεδομένων για κάθε περίπτωση. Αυτό προάγει την αποτελεσματική συνεργασία μεταξύ ερευνητών, βελτιστοποιώντας τη χρήση των πόρων. Επίσης, η βάση δεδομένων παρέχει διατήρηση δεδομένων και προσβασιμότητα ακόμα και αν το πρόγραμμα κολλήσει[70].

Το λογισμικό δίνει επίσης έμφαση στις αποτελεσματικές δυνατότητες αναζήτησης. Με την εκ των προτέρων ευρετηρίαση αρχείων, το FTK μειώνει τους χρόνους αναζήτησης και δημιουργεί ένα κοινόχρηστο αρχείο ευρετηρίου. Αυτό εξαλείφει την ανάγκη για αντιγραφή αρχείων ή αναπαράσταση κατά τη διάρκεια των ερευνών, βελτιώνοντας περαιτέρω την αποτελεσματικότητα[70].

Μερικά από τα κύρια χαρακτηριστικά περιλαμβάνουν:

Ανάλυση email: Το FTK παρέχει μια διαισθητική διεπαφή για την ανάλυση email, συμπεριλαμβανομένης της ανάλυσης email για συγκεκριμένες λέξεις και τη διεξαγωγή ανάλυσης κεφαλίδων για διευθύνσεις IP πηγής.

Αποκρυπτογράφηση αρχείων: Η αποκρυπτογράφηση αρχείων είναι ένα σημαντικό χαρακτηριστικό του FTK, το οποίο επιτρέπει τη διάσπαση κωδικού πρόσβασης και την αποκρυπτογράφηση κρυπτογραφημένων αρχείων. Υποστηρίζει πάνω από 100 εφαρμογές, επιτρέποντας την ανάκτηση κωδικών πρόσβασης.

Data Carving: Ενσωματώνει μια ισχυρή μηχανή χάραξης δεδομένων, που δίνει τη δυνατότητα στους ερευνητές να αναζητούν αρχεία με βάση το μέγεθος, τον τύπο δεδομένων, ακόμη και το μέγεθος pixel.

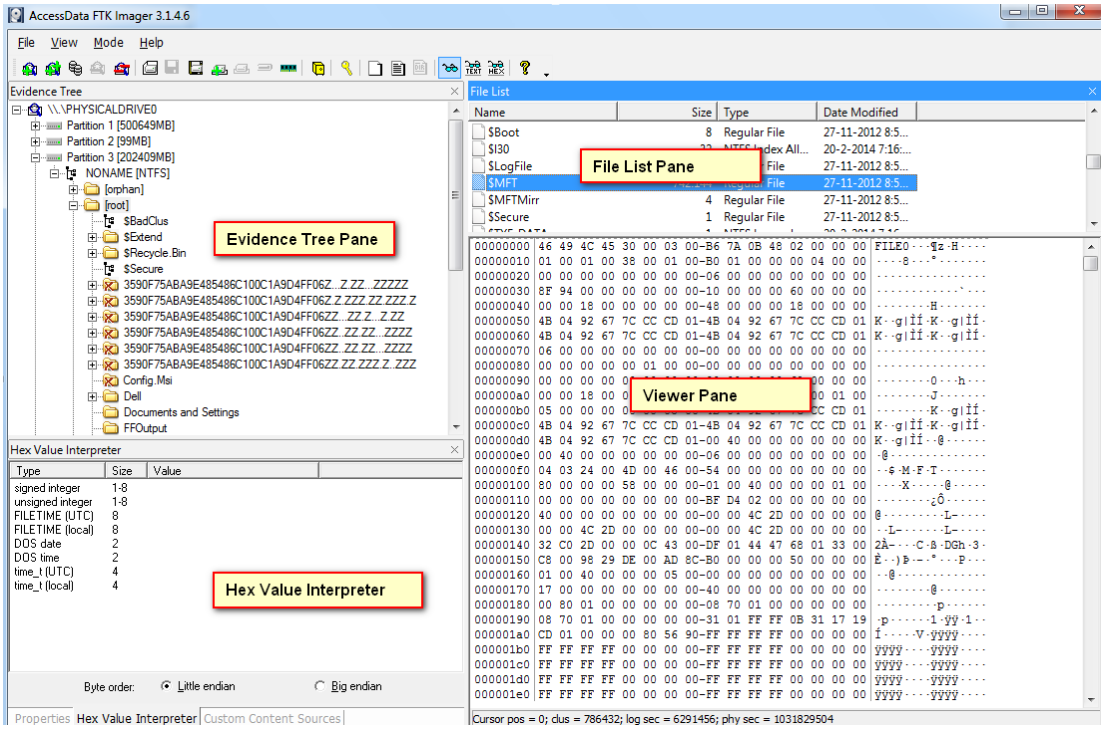
Οπτικοποίηση δεδομένων: Υποστηρίζει τεχνικές οπτικοποίησης αποδεικτικών στοιχείων, όπως κατασκευή χρονοδιαγράμματος, γραφήματα συμπλέγματος και γεωγραφική τοποθεσία. Αυτό δίνει τη δυνατότητα στους αναλυτές να δημιουργήσουν μια πιο διαισθητική και ολοκληρωμένη κατανόηση μιας υπόθεσης.

Web Viewer: Το FTK περιλαμβάνει το FTK Web Viewer, μια πρόσφατη προσθήκη που επιτρέπει την πρόσβαση σε πραγματικό χρόνο σε αρχεία υποθέσεων. Επιτρέπει επίσης την αναζήτηση πολλαπλών υποθέσεων, εξαλείφοντας την ανάγκη για χειροκίνητη διασταύρωση στοιχείων από διαφορετικές υποθέσεις.

Cerberus: Ενσωματώνει μια ισχυρή δυνατότητα αυτοματοποιημένης ανίχνευσης κακόβουλου λογισμικού που ονομάζεται Cerberus. Αυτό χρησιμοποιείται για τον εντοπισμό κακόβουλου λογισμικού σε έναν υπολογιστή και προτείνει κατάλληλες ενέργειες για τον μετριασμό του[70].

OCR (Optical Character Recognition): Η μηχανή OCR του FTK επιτρέπει τη γρήγορη μετατροπή εικόνων σε ευανάγνωστο κείμενο. Υποστηρίζει πολλές γλώσσες, ενισχύοντας τη χρηστικότητά του για διεθνείς υποθέσεις.

Το FTK Imager είναι ένα συμπληρωματικό εργαλείο του FTK το οποίο προσφέρει λειτουργικότητα για προεπισκόπηση και απεικόνιση δεδομένων. Επιτρέπει τη δημιουργία εγκληματολογικών εικόνων τοπικών σκληρών δίσκων, CD, DVD, συσκευών USB, φακέλων και μεμονωμένων αρχείων. Το FTK Imager διασφαλίζει τη διατήρηση της ακεραιότητας των δεδομένων δημιουργώντας πανομοιότυπες εγκληματολογικές εικόνες. Το εργαλείο επιτρέπει την τοποθέτηση εικόνων για προβολή μόνο για ανάγνωση, παρέχοντας πρόσβαση στο περιεχόμενο ακριβώς όπως ήταν στην αρχική μονάδα δίσκου. Επιπλέον, το FTK Imager επιτρέπει την εξαγωγή αρχείων και φακέλων από εγκληματολογικές εικόνες και διευκολύνει την ανάκτηση των διαγραμμένων αρχείων που δεν έχουν αντικατασταθεί στη μονάδα δίσκου[71, 72].



Σχήμα 9 FTK Tool

Wireshark

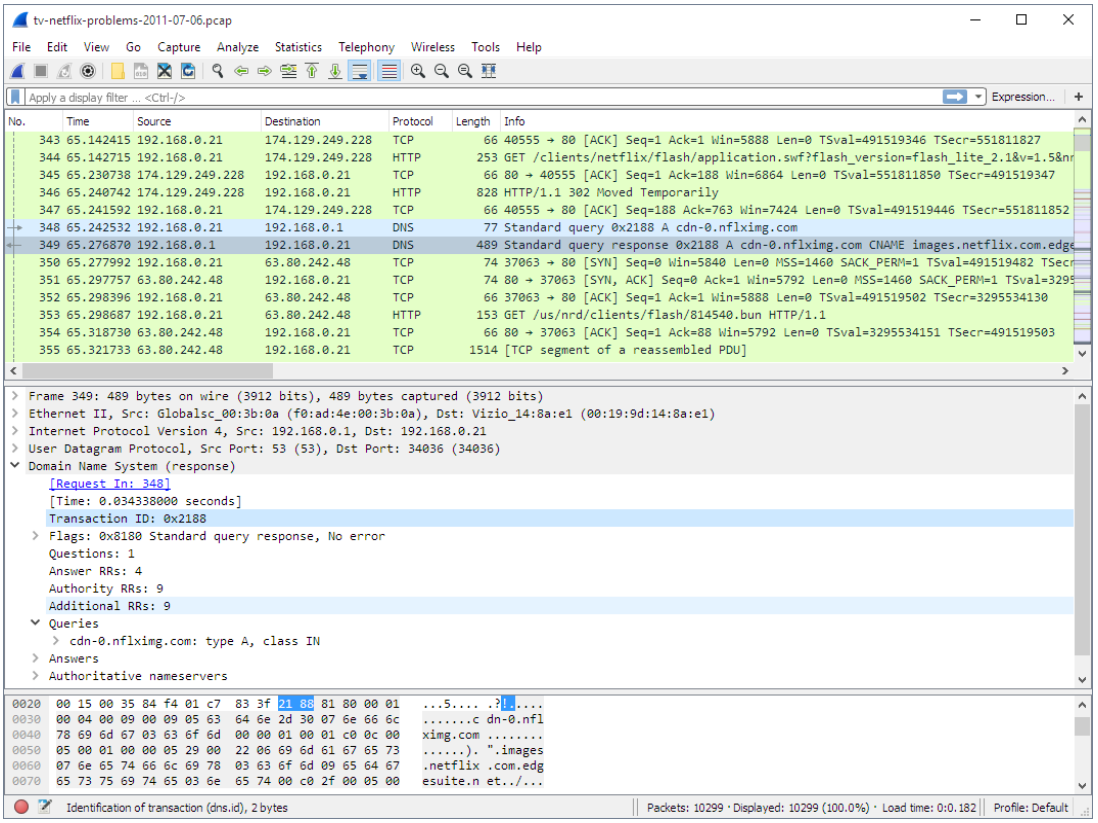
Το Wireshark είναι ένα ευρέως αναγνωρισμένο εργαλείο συλλογής και ανάλυσης πακέτων που χρησιμοποιείται στην εγκληματολογία δικτύου. Προσφέρει πολλά χαρακτηριστικά που διευκολύνουν τον εντοπισμό και την ανάλυση της κίνησης του δικτύου. Ένα αξιοσημείωτο χαρακτηριστικό είναι η ισχυρή ικανότητα φιλτραρίσματος, που επιτρέπει στους χρήστες να απομονώνουν συγκεκριμένα στοιχεία ή λέξεις-κλειδιά μέσα σε πακέτα για ανάλυση και ανίχνευση απειλών. Το Wireshark υποστηρίζει ζωντανή λήψη και ανάλυση εκτός σύνδεσης, επιτρέποντας την καταγραφή και την εξέταση δεδομένων σε οποιοδήποτε σημείο στο μέλλον. Είναι συμβατό με πολλές πλατφόρμες, συμπεριλαμβανομένων των Windows, Linux και macOS[73].

Το Wireshark μπορεί να διαβάζει διαφορετικά αρχεία καταγραφής, συμπεριλαμβανομένων αυτών που έχουν καταγραφεί από άλλο λογισμικό, όπως το tcpdump ή το Cisco Secure. Μπορεί να αποκρυπτογραφήσει κρυπτογραφημένα δεδομένα από πρωτόκολλα Διαδικτύου όπως HTTP και

FTP[74]. Η χρήση του Wireshark στην εγκληματολογία δικτύου περιλαμβάνει τη συλλογή διαφόρων τύπων πληροφοριών. Συμβάλλει στην κατανόηση της μεθοδολογίας επίθεσης, στον προσδιορισμό των παραβιασμένων πληροφοριών ή δεδομένων και στον εντοπισμό τυχόν κακόβουλων στοιχείων που άφησε πίσω ο εισβολέας, όπως δούρειοι ίπποι ή botware[74]. Το Wireshark βοηθά επίσης στην παρακολούθηση και ανάλυση συλλεγόμενων δεδομένων, διασφαλίζοντας επαρκείς πληροφορίες για ανάλυση δικτύου.

Η διεπαφή που βασίζεται σε GUI του Wireshark παρέχει πλεονεκτήματα έναντι των επιλογών της γραμμής εντολών, επιτρέποντας λεπτομερή επιθεώρηση της καταγραφόμενης κυκλοφορίας σε πραγματικό χρόνο. Μπορεί να εγκατασταθεί στο σύστημα ή να εκτελεστεί από μονάδα USB[75]. Όσον αφορά την ανάπτυξη, το Wireshark ενδέχεται να απαιτεί δικαιώματα εγκατάστασης και διαχείρισης, τα οποία μπορεί να επηρεάσουν την ταχεία ανάπτυξή του κατά τη διάρκεια συμβάντων.

Συνολικά, το Wireshark είναι ένα πολύτιμο εργαλείο ανοιχτού κώδικα για την ανάλυση πακέτων δικτύου στην ψηφιακή εγκληματολογία. Υποστηρίζει υποκλοπή δεδομένων σε πραγματικό χρόνο, αποκρυπτογράφηση και ανάλυση VoIP[76]. Με τα εκτεταμένα χαρακτηριστικά και τις δυνατότητές του, οι ερευνητές μπορούν να αποκτήσουν γνώσεις σχετικά με τις δραστηριότητες του δικτύου και να πραγματοποιήσουν λεπτομερείς εξετάσεις της κυκλοφορίας του δικτύου κατά τη διάρκεια ιατροδικαστικών ερευνών[75].



Σχήμα 10 Wireshark Tool

4.6 Συγκριτική Ανάλυση Εγκληματολογικών Εργαλείων Ανοικτού Κώδικα

Στον κόσμο της ψηφιακής έρευνας, η επιλογή του κατάλληλου εργαλείου είναι ζωτικής σημασίας για την επιτυχία και αποτελεσματικότητα της έρευνας. Κάθε εργαλείο διαθέτει τις δικές του εξειδικευμένες δυνατότητες και χαρακτηριστικά που το καθιστούν ιδανικό για συγκεκριμένους τύπους ερευνών.

1. Sleuth Kit:

Ιδανικό για εις βάθος διερεύνηση, το Sleuth Kit (TSK) είναι ένα εξαιρετικό εργαλείο για εγκληματολογική ανάλυση συστημάτων αρχείων, που επιτρέπει στους ερευνητές να εμβαθύνουν σε μέσα αποθήκευσης και συστήματα αρχείων. Προσφέρει μια ευέλικτη προσέγγιση για την ανάλυση συστημάτων αρχείων και την ανάκτηση διαγραμμένων και κρυπτογραφημένων δεδομένων. Επιτρέπει την εξερεύνηση διαφόρων τύπων συστημάτων αρχείων και συσκευών αποθήκευσης, αναζητώντας πολύτιμα ψηφιακά αποδεικτικά στοιχεία. Παρά την έλλειψη γραφικού περιβάλλοντος, το Sleuth Kit προσφέρει ευέλικτες λειτουργίες που απευθύνονται σε εξειδικευμένους χρήστες ψηφιακής εγκληματολογίας. Κατάλληλο για τη διατήρηση της ακεραιότητας των δεδομένων και την ανάλυση συστημάτων αρχείων, το Sleuth Kit υποστηρίζει ένα ευρύ φάσμα τύπων μέσων αποθήκευσης και συστήματα αρχείων.

2. Autopsy:

Το Autopsy, με τη φιλική προς το χρήστη διεπαφή GUI, ενισχύει τη λειτουργικότητα του Sleuth Kit απλοποιώντας την εξέταση ψηφιακών στοιχείων. Οι ερευνητές που δίνουν προτεραιότητα σε μια προσέγγιση που βασίζεται σε GUI και χρειάζονται γρήγορες αλλά ολοκληρωμένες αναλύσεις θα βρουν αυτό το εργαλείο ως την ιδανική επιλογή. Με τις πολύτιμες δυνατότητες του, όπως ο κατακερματισμός αρχείων, η τυπική αποσυμπίεση αρχείων, η εξαγωγή δεδομένων EXIF και η ανάλυση διαφορετικών συστημάτων αρχείων, το Autopsy είναι ιδιαίτερα συμφέρων σε σενάρια όπου οι ερευνητές πρέπει να επεξεργάζονται αποτελεσματικά στοιχεία χωρίς να αλλάζουν άμεσα τα αρχικά αρχεία.

3.Caine:

Το εργαλείο Caine συνδυάζει τις λειτουργίες του Sleuth Kit και του Autopsy, προσφέροντας μια προδιαμορφωμένη πλατφόρμα. Αναδεικνύεται ως μια ολοκληρωμένη και φιλική πλατφόρμα για επαγγελματίες εγκληματολόγους καθώς απλοποιεί τη διαδικασία έρευνας και διασφαλίζει την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων. Με ευέλικτες δυνατότητες ανάλυσης, το CAINE παρέχει μια ασφαλή και οργανωμένη πλατφόρμα για ψηφιακές εγκληματολογικές ερευνητικές εργασίες. Διατηρεί αυτόματα την ακεραιότητα των δεδομένων και απευθύνεται σε επαγγελματίες με διαφορετική τεχνογνωσία.

4.Volatility

Το Volatility αποτελεί μια εξειδικευμένη λύση για την ανάλυση μνήμης RAM. Κατάλληλο για περιπτώσεις που απαιτούν εξειδικευμένη ανάλυση μνήμης και εξαγωγή πληροφοριών, επιτρέπει τον εντοπισμό και την αντίδραση σε υποθέσεις κακόβουλου λογισμικού.

5.FTK (Forensics Toolkit):

Το FTK, ή Forensic Toolkit, υπερέχει στις δυνατότητες χειρισμού δεδομένων, ευρετηρίασης και αναζήτησης. Αυτό το εργαλείο συνιστάται για ερευνητές που εργάζονται με μεγάλους όγκους

αποδεικτικών στοιχείων, καθώς η ευρετηρίαση δεδομένων και οι γρήγορες αναζητήσεις του FTK αυξάνουν την αποτελεσματικότητα της έρευνας. Με ολοκληρωμένη λειτουργικότητα, υποστήριξη για πολλαπλές μορφές αρχείων και ενσωμάτωση με υπηρεσίες cloud, το FTK εξυπηρετεί τις αρχές επιβολής του νόμου και τους ερευνητές σε εταιρικά περιβάλλοντα.

6.Wireshark

Το Wireshark είναι κυρίως ένας αναλυτής πρωτοκόλλου δικτύου, γεγονός που τον καθιστά πολύτιμο για την εγκληματολογία δικτύου και την απόκριση συμβάντων. Η λήψη σε πραγματικό χρόνο και η ανάλυση σε επίπεδο πακέτων βοηθούν στον εντοπισμό ανωμαλιών δικτύου, μη εξουσιοδοτημένης πρόσβασης και δραστηριότητας κακόβουλου λογισμικού. Το Wireshark είναι το καλύτερο εργαλείο για ερευνητές που επικεντρώνονται στη συλλογή και ανάλυση αποδεικτικών στοιχείων που βασίζονται σε δίκτυο.

Συμπερασματικά, η επιλογή του καταλληλότερου εργαλείου εγκληματολογίας ανοιχτού κώδικα εξαρτάται από τις συγκεκριμένες απαιτήσεις της έρευνας. Οι επαγγελματίες ερευνητές πρέπει να επιλέξουν προσεκτικά το κατάλληλο εργαλείο που να ανταποκρίνεται στις ειδικές ανάγκες κάθε περίπτωσης. Η κατάλληλη επιλογή θα διασφαλίσει την αξιοπιστία και την αποτελεσματικότητα της ψηφιακής έρευνας και θα οδηγήσει σε επιτυχείς εκβάσεις των ερευνητικών εργασιών. Για ολοκληρωμένη ανάλυση συστήματος αρχείων και διατήρηση της ακεραιότητας των δεδομένων, το Sleuth Kit είναι η πρώτη επιλογή. Στη συνέχεια, το πιο αναγνωρισμένο ειναι το Autopsy το οποίο παρέχει ένα φιλικό προς τον χρήστη GUI για γρήγορη και ενδελεχή εξέταση των αποδεικτικών στοιχείων. Για τους ερευνητές που αναζητούν μια προδιαμορφωμενη λύση, το εργαλείο Caine μπορεί να παρέχει ένα ολοκληρωμένο περιβάλλον για αυτές τις περιπτώσεις. Επίσης, το Volatility είναι το πιο σημαντικό και ορθώς διαμορφωμένο για την ανάλυση της μνήμης RAM στην εγκληματολογία της μνήμης (Memory Forensics). Τέλος, το εργαλείο FTK είναι εξαιρετικό για γρήγορη επεξεργασία μεγάλων ποσοτήτων αποδεικτικών στοιχείων, ενώ το Wireshark διαπρέπει στη συλλογή αποδεικτικών στοιχείων βάσει κίνησης δικτύου. Ανάλογα με τη φύση της υπόθεσης και τις συγκεκριμένες ερευνητικές ανάγκες, οι ερευνητές μπορούν να χρησιμοποιήσουν αυτά τα εργαλεία ανοιχτού κώδικα για να εξασφαλίσουν μια ολοκληρωμένη και αποτελεσματική ψηφιακή ερευνητική διαδικασία.

Κεφάλαιο 5ο: Ψηφιακή Εγκληματολογία Φορητών Συσκευών: Μεθοδολογίες, Προκλήσεις και Εργαλεία Ανάλυσης

Η εγκληματολογία κινητών συσκευών, αποτελεί έναν κρίσιμο κλάδο της ψηφιακής εγκληματολογίας ο οποίος αναφέρεται στην διαδικασία εξαγωγής και ανάλυσης ψηφιακών δεδομένων από φορητές συσκευές, συμπεριλαμβανομένων των smartphone και των tablet, χρησιμοποιώντας καθιερωμένες μεθοδολογίες. Σε αντίθεση με την παραδοσιακή ψηφιακή εγκληματολογία, η οποία καλύπτει ένα ευρύ φάσμα υπολογιστικών συστημάτων, το Mobile Forensics επικεντρώνεται αποκλειστικά στην ανάκτηση και εξέταση δεδομένων από κινητές συσκευές, οι οποίες έχουν γίνει αναπόσπαστο μέρος της ζωής των ανθρώπων, αποθηκεύοντας μια τεράστια ποσότητα προσωπικών και ευαίσθητων πληροφοριών. Η εγκληματολογία κινητών συσκευών στοχεύει να αποκαλύψει πολύτιμα στοιχεία που περιέχονται σε αυτές τις συσκευές, που κυμαίνονται από μηνύματα κειμένου, αρχεία καταγραφής κλήσεων και email έως το ιστορικό περιήγησης στον ιστό, τη δραστηριότητα στα μέσα κοινωνικής δικτύωσης και δεδομένα τοποθεσίας GPS[77]. Αυτός ο κλάδος έχει αποκτήσει μεγάλη σημασία λόγω της αυξανόμενης ζήτησης για υπηρεσίες κινητής τηλεφωνίας, του αυξανόμενου αριθμού χρηστών και των ραγδαίων εξελίξεων στις κινητές τεχνολογίες όπως η διάχυτη συνδεσιμότητα και το Διαδίκτυο των Πραγμάτων (IoT).

5.1 Βασικά Βήματα της Ψηφιακής Εγκληματολογίας Φορητών συσκευών

Η διαδικασία της εγκληματολογίας φορητών συσκευών περιλαμβάνει συγκεκριμένα βασικά βήματα για τη διασφάλιση του κατάλληλου χειρισμού, απόκτησης, ανάλυσης και τεκμηρίωσης ψηφιακών αποδεικτικών στοιχείων. Αυτά τα βήματα είναι απαραίτητα για τη διατήρηση της ακεραιότητας των αποδεικτικών στοιχείων και τη διασφάλιση του παραδεκτού τους σε δικαστικές διαδικασίες. Ακολουθεί παρακάτω μια εκτεταμένη ανάλυση της διαδικασίας:

Κατάσχεση: Το πρώτο βήμα είναι η κατάσχεση της κινητής συσκευής. Είναι σημαντική η υλοποίηση αυτού του βήματος λαμβάνοντας υπόψη τα νομικά πλαίσια και τους δικαστικούς περιορισμούς που πρεπει να τηρηθουν. Οι συσκευές αυτές, κατάσχονται ενω ειναι ενεργοποιημένες ώστε να αποφευχθεί οποιαδήποτε αλλοίωση των ψηφιακών στοιχείων. Συνήθως τοποθετούνται σε ειδικές τσάντες (Faraday) κατασκευασμένες από πολλαπλές στρώσεις διαφόρων μεταλλικών στρωμάτων, ώστε να εμποδίζουν και να απομακρύνουν τα ηλεκτρομαγνητικά κύματα από τη συσκευή, για να αποτραπεί η συνδεσιμότητα δικτύου[80]. Επιπλέον, ενεργοποιείται η λειτουργία πτήσης για να διατηρηθεί η ακεραιότητα των αποδεικτικών στοιχείων[78,79].

Σχήμα 11 Τσάντες Faraday

Απόκτηση: Η φάση απόκτησης περιλαμβάνει τον εντοπισμό και την εξαγωγή δεδομένων από την κατασχεθείσα συσκευή. Ένα αντίγραφο του αρχείου πολυμέσων της συσκευής δημιουργείται χρησιμοποιώντας εργαλεία απεικόνισης λογισμικού. Αυτό το αντίγραφο αποθηκεύεται προσεκτικά για να αποφευχθεί η παραβίαση. Για να διασφαλιστεί η ακεραιότητα των δεδομένων, το διπλότυπο αρχείο επαληθεύεται μέσω κατακερματισμού, το οποίο επιβεβαιώνει ότι όλα τα δεδομένα παραμένουν στην αρχική τους κατάσταση[78,79].

Ανάλυση: Μόλις αποκτηθεί το αρχείο πολυμέσων, υποβάλλεται σε ανάλυση χρησιμοποιώντας διάφορες τεχνικές και εργαλεία. Η εγκληματολογία κινητών συσκευών χρησιμοποιεί μια σειρά διαφόρων προσεγγίσεων για την εξαγωγή σχετικών δεδομένων από το αρχείο πολυμέσων. Λόγω του ευρέος φάσματος των διαθέσιμων κινητών συσκευών, ενδέχεται να απαιτούνται διαφορετικές προσεγγίσεις για την αποτελεσματική εξαγωγή δεδομένων[78,79].

Εξέταση: Η φάση εξέτασης της εγκληματολογίας κινητών περιλαμβάνει σχολαστική τεκμηρίωση και ασφαλή αποθήκευση σημαντικών αποδεικτικών στοιχείων. Ακολουθώντας τις κατάλληλες διαδικασίες και διατηρώντας λεπτομερή αρχεία, οι ερευνητές μπορούν να διασφαλίσουν την ακεραιότητα και το παραδεκτό των αποδεικτικών στοιχείων, διευκολύνοντας τη χρήση τους στην εγκληματολογική εξέταση και τις νομικές διαδικασίες[78,79].

5.2 Μέθοδοι απόκτησης δεδομένων

Η απόκτηση δεδομένων στην εγκληματολογία κινητών συσκευών μπορεί να κατηγοριοποιηθεί σε διαφορετικούς τύπους, ο καθένας με διαφορετικά επίπεδα τεχνικής πολυπλοκότητας και εγκληματολογικής αξιοπιστίας.

Χειροκίνητη απόκτηση: Αυτή η μέθοδος περιλαμβάνει τη χρήση της διεπαφής χρήστη της συσκευής με σκοπό τη διερεύνηση της μνήμη της. "Απεικονίζεται" το περιεχόμενο κάθε συσκευής και το λειτουργικό σύστημα συμβάλλει στη μετατροπή των ακατέργαστων δεδομένων σε αναγνώσιμες από τον άνθρωπο πληροφορίες. Αυτή η προσέγγιση χρησιμοποιείται συνήθως για κινητά τηλέφωνα, PDA

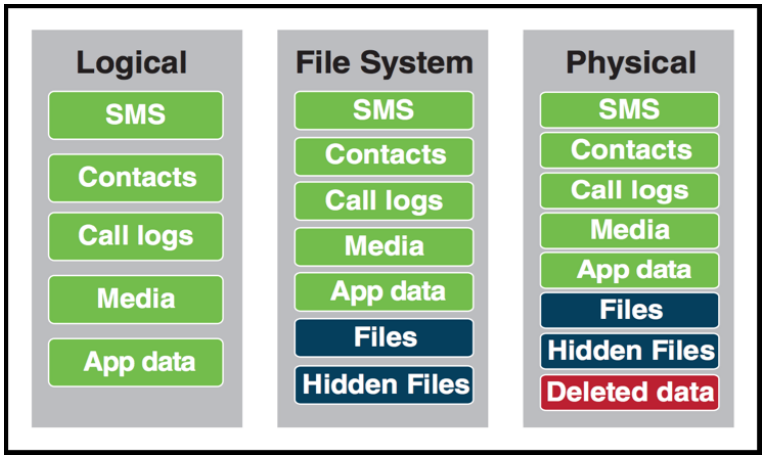
και συστήματα πλοήγησης. Ωστόσο, υπάρχουν περιορισμοί, όπως η ανάκτηση δεδομένων που είναι ορατά μόνο στο λειτουργικό σύστημα, η λήψη δεδομένων μόνο σε μορφή εικόνας και η χρονοβόρα διαδικασία[78].

Λογική απόκτηση: Σε αυτήν τη μέθοδο, δημιουργείται ένα αντίγραφο bit-by-bit αντικειμένων λογικής αποθήκευσης (π.χ. καταλόγων και αρχείων) που βρίσκονται στο λογικό χώρο αποθήκευσης της συσκευής, όπως ένα σύστημα αρχείων. Η λογική εξαγωγή επιτρέπει στα εργαλεία να εξάγουν και να οργανώνουν εύκολα δομές δεδομένων συστήματος. Διευκολύνεται μέσω της διεπαφής προγραμματισμού εφαρμογής του κατασκευαστή και του πρωτότυπου εξοπλισμού της συσκευής για συγχρονισμό με τον υπολογιστή. Μολονότι η λογική εξαγωγή δεδομένων είναι πιο διαχειρίσιμη οι ειδικευμένοι ερευνητές μπορούν συχνά να ανακτήσουν περισσότερες πληροφορίες μέσω φυσικής εξαγωγής[78].

Λήψη συστήματος αρχείων: Η λογική εξαγωγή ενδέχεται να μην ανακτήσει τις διαγραμμένες πληροφορίες από το σύστημα αρχείων της συσκευής. Ωστόσο, σε ορισμένες περιπτώσεις, οι συσκευές διατηρούν ένα αρχείο βάσης δεδομένων με διαγραμμένα δεδομένα που επισημαίνονται για μεταγενέστερη αντικατάσταση (π.χ. πλατφόρμες που είναι κατασκευασμένες σε SQLite, όπως iOS και Android). Εάν η πρόσβαση στο σύστημα αρχείων είναι δυνατή μέσω διεπαφών συγχρονισμού, οι διαγραμμένες πληροφορίες μπορούν να ανακτηθούν. Η εξαγωγή συστήματος αρχείων είναι πολύτιμη για την κατανόηση των δομών αρχείων, του ιστορικού περιήγησης στον ιστό, της χρήσης εφαρμογών και επιτρέπει την ανάλυση με παραδοσιακά εγκληματολογικά εργαλεία υπολογιστών[78].

Φυσική απόκτηση: Αυτή η μέθοδος περιλαμβάνει τη δημιουργία ενός αντιγράφου bit-by-bit ολόκληρου του φυσικού χώρου αποθήκευσης, όπως η μνήμη flash, παρόμοια με την εξέταση ενός προσωπικού υπολογιστή. Η φυσική απόκτηση επιτρέπει την εξέταση διαγραμμένων αρχείων και υπολειμμάτων δεδομένων. Η επίτευξη φυσικής εξαγωγής δεδομένων ενδέχεται να είναι πιο δύσκολη λόγω των μέτρων ασφαλείας που εφαρμόζουν οι κατασκευαστές των συσκευών για την πρόληψη της αυθαίρετης ανάγνωσης μνήμης. Τα εγκληματολογικά εργαλεία ενδέχεται να χρησιμοποιούν προσαρμοσμένους φορτωτές εκκίνησης για να παρακάμψουν την ασφάλεια και να έχουν πρόσβαση στη μνήμη[78].

Απόκτηση ωμής βίας: Η απόκτηση ωμής βίας αφορά τη χρήση ειδικών εργαλείων από τρίτα πρόσωπα για να προσπαθήσουν να εισέλθουν σε συσκευές ή κινητές συσκευές, χωρίς να έχουν την απαιτούμενη άδεια ή κωδικό πρόσβασης. Αυτή η πρακτική συνήθως θεωρείται χρονοβόρα και υποχρεωτικά δαπανηρή. Ωστόσο, η ωμή επιβολή κρίνεται αποτελεσματική όταν άλλες μέθοδοι αποτυγχάνουν να ανακτήσουν τον κωδικό πρόσβασης από τη συσκευή[78].



Σχήμα 12 Μέθοδοι απόκτησης δεδομένων

5.3 Προβληματισμοί κατα την εξαγωγή δεδομένων από φορητές συσκευές για εγκληματολογική έρευνα

Κατά την εξαγωγή δεδομένων από φορητές συσκευές, οι ερευνητές χρησιμοποιούν διάφορες τεχνικές που ενδέχεται να αφήσουν ψηφιακά ίχνη, όπως η εγκατάσταση ενός bootloader ή ενός προγράμματος πελάτη, η απόκτηση πρόσβασης "root" ή η σύνδεση σε ασύρματα δίκτυα[77][81]. Γι' αυτό, είναι απαραίτητη η σχολαστική τεκμηρίωση της εφαρμογής αυτών των μεθόδων προκειμένου να διασφαλιστεί η διαφάνεια και η αξιοπιστία κατα τη διαδικασία διερεύνησης.

Δεδομένου ότι ένα μεμονωμένο εργαλείο μπορεί να μην καταγράφει πλήρως όλα τα δεδομένα από μια φορητή συσκευή, μπορεί να κριθεί απαραίτητη η διεξαγωγή χειροκίνητης ανασκόπησης ή η χρήση πρόσθετων εγκληματολογικών εργαλείων για την επαλήθευση των ευρημάτων ή την ανάκτηση τυχόν δεδομένων που ενδέχεται να παραληφθούν[83].

Επιπλέον, λόγω της δυναμικής φύσης των μέσων αποθήκευσης σε αυτές τις συσκευές, οι τιμές κατακερματισμού που λαμβάνονται από πολλαπλές εξαγωγές της ίδιας συσκευής ενδέχεται να μην ταιριάζουν[83].

Σε περιπτώσεις που αφορούν αφαιρούμενα μέσα σε φορητές συσκευές, θα πρέπει να λαμβάνεται υπόψη η κατάσταση ισχύος της συσκευής κατά τη διαδικασία εξαγωγής. Εάν η συσκευή είναι ενεργοποιημένη, το αφαιρούμενο μέσο θα πρέπει να παραμείνει στη θέση του κατά την απόκτηση. Αντίθετα, εάν η συσκευή είναι απενεργοποιημένη, τα αφαιρούμενα μέσα θα πρέπει να εξαχθούν από τη συσκευή. Σε περιπτώσεις όπου η ζωντανή πρόσβαση στη συσκευή είναι απαραίτητη για την ερμηνεία δεδομένων στα αφαιρούμενα μέσα, μπορεί να πραγματοποιηθεί ξεχωριστή απόκτηση μόλις επιστραφεί το μέσο στη συσκευή[83].

Επιπρόσθετα, σε περιπτώσεις όπου οι συσκευές απαιτούν UICC/SIM, οι ερευνητές πρέπει να αποκτήσουν και να αναλύσουν τόσο τη συσκευή όσο και τις UICC/SIM. Εάν η συσκευή είναι απενεργοποιημένη, η UICC/SIM θα πρέπει να είναι η κύρια εστίαση για την επεξεργασία πριν από την ενεργοποίηση της συσκευής ή την εξαγωγή του αποθηκευτικού χώρου της. Αντίθετα, εάν η συσκευή είναι ενεργοποιημένη, θα πρέπει να πραγματοποιηθεί ταυτόχρονη εξαγωγή δεδομένων τόσο της συσκευής όσο και της UICC/SIM πριν από την αφαίρεση της. Επιπλέον, η άμεση εξαγωγή τους μπορεί να είναι αναγκαία για την ανάκτηση διαγραμμένων μηνυμάτων που δεν είναι προσβάσιμα μέσω της συσκευής[82,83].

5.4 Προκλήσεις και απειλές Mobile Forensics

Η εγκληματολογία φορητών συσκευών αντιμετωπίζει σημαντικές προκλήσεις λόγω της δυναμικής φύσης των κινητών συσκευών, όπου τα δεδομένα μπορούν να αποθηκευτούν και να συγχρονιστούν σε πολλές συσκευές. Αυτό δημιουργεί δυσκολίες στη διατήρηση και την ασφάλεια των δεδομένων, καθώς είναι πτητικά και επιρρεπή σε παραποίηση ή απομακρυσμένη διαγραφή[77]. Σε αντίθεση με την εγκληματολογία υπολογιστών, η εγκληματολογία κινητών συσκευών είναι μοναδικά πολύπλοκη λόγω της μεγάλης ποικιλίας μοντέλων κινητών τηλεφώνων με ποικίλες δυνατότητες και λειτουργικά συστήματα που διατίθενται στην αγορά. Η συχνή εισαγωγή νέων μοντέλων απαιτεί συνεχή

προσαρμογή από τους ερευνητές για να αντιμετωπίσουν τις αναδυόμενες προκλήσεις και να συμβαδίσουν με το διαρκώς εξελισσόμενο φάσμα των φορητών συσκευών[84].

Η διατήρηση της ακεραιότητας των δεδομένων είναι κρίσιμη, καθώς απαιτεί προσεκτικό χειρισμό των κινητών συσκευών για την αποφυγή τυχαίας διαγραφής ή επαναφοράς δεδομένων. Οι εγκληματολογικοί ερευνητές πρέπει να έχουν πρόσβαση σε μια σειρά εργαλείων και εξοπλισμού για την υποστήριξη διαφόρων φορητών συσκευών και εφαρμογών που συναντώνται κατά τη διάρκεια των ερευνών. Η χρήση τεχνικών κατά της εγκληματολογίας από προγραμματιστές εφαρμογών και εγκληματίες έχει ως στόχο την απόκρυψη δεδομένων και την παράκαμψη της εξέτασης, συμπεριλαμβανομένης της συσκότισης δεδομένων, της πλαστογραφίας και του secure wiping, καθιστώντας τις ιατροδικαστικές έρευνες για κινητές συσκευές πιο περίπλοκες[85,77].

Επιπλέον, διαδραματίζει κρίσιμο ρόλο στην ανάκτηση ευαίσθητων δεδομένων που μπορεί να είναι πολύτιμα ως αποδεικτικά στοιχεία σε νομικές διαδικασίες. Ωστόσο, είναι σημαντικό να αναγνωριστεί ότι η χρήση τέτοιων δεδομένων διέπεται από διάφορους νόμους, ιδίως αυτούς που διασφαλίζουν το απόρρητο των χρηστών[81]. Η τήρηση αυτών των νομικών πλαισίων είναι υψίστης σημασίας για τη διασφάλιση του νόμιμου χειρισμού και του παραδεκτού των αποδεικτικών στοιχείων κινητής συσκευής σε δικαστικές υποθέσεις.

Για την αντιμετώπιση αυτών των προκλήσεων, έχουν αναπτυχθεί εξειδικευμένα εργαλεία, που επιτρέπουν στους εξεταστές να παρακάμπτουν το λειτουργικό σύστημα και να έχουν πρόσβαση σε ακατέργαστα δεδομένα από συσκευές, συμπεριλαμβανομένων των προστατευμένων και διαγραμμένων δεδομένων. Τα δημοφιλή λειτουργικά συστήματα για κινητά, όπως το Android και το Apple iOS, διευκολύνουν τη λειτουργία της συσκευής και την αποθήκευση δεδομένων. Ωστόσο, ορισμένες περιπτώσεις αφορούν τηλέφωνα με δυνατότητες και ιδιόκτητα λειτουργικά συστήματα, που απαιτούν εξειδικευμένες ιατροδικαστικές τεχνικές.

5.4.1 Απειλές

Οι πρωταρχικοί κίνδυνοι στην εγκληματολογία κινητής τηλεφωνίας προκύπτουν από απώλεια ή κλοπή φυσικής συσκευής, όπου η φορητότητα των κινητών συσκευών τις καθιστά επιρρεπείς σε λάθος τοποθέτηση, εκθέτοντας δυνητικά ευαίσθητα δεδομένα σε μη εξουσιοδοτημένα άτομα[81].

Επιπλέον, οι κινητές συσκευές είναι ευάλωτες σε κακόβουλο λογισμικό και διάφορες επιθέσεις στον κυβερνοχώρο, ιδιαίτερα όταν συνδέονται σε δημόσια Wi-Fi ή μη προστατευμένα δίκτυα. Το ανθρώπινο σφάλμα παραμένει ένας σημαντικός παράγοντας, καθώς τα άτομα μπορούν ακούσια να κάνουν κλικ σε κακόβουλους συνδέσμους ή να πέσουν θύματα σε απόπειρες phishing, παρέχοντας στους εγκληματίες του κυβερνοχώρου μη εξουσιοδοτημένη πρόσβαση σε κινητές συσκευές[81].

Η αντιμετώπιση αυτών των προκλήσεων απαιτεί ισχυρά μέτρα για την προστασία των δεδομένων, την ενίσχυση της ασφάλειας των συσκευών και την εκπαίδευση των χρηστών σχετικά με τις βέλτιστες πρακτικές στον τομέα της ασφάλειας στον κυβερνοχώρο κινητής τηλεφωνίας[81].

5.5 Θεμελιώδη κριτήρια αξιολόγησης εργαλείων

Ο προσδιορισμός της μάρκας και του μοντέλου της κινητής συσκευής είναι ζωτικής σημασίας και μόλις ολοκληρωθεί, είναι απαραίτητος ο έλεγχος των διαθέσιμων εγχειριδίων, τα οποία βρίσκονται συχνά στον ιστότοπο του κατασκευαστή[82]. Η επιλογή των εγκληματολογικών εργαλείων εξαρτάται

από τα χαρακτηριστικά της υπό διερεύνηση συσκευής. Ως εκ τούτου, συγκεκριμένα θεμελιώδη κριτήρια θα πρέπει να λαμβάνονται σχολαστικά υπόψη όταν αποφασίζονται τα κατάλληλα εργαλεία.

Τα επιλεγμένα εργαλεία θα πρέπει να δίνουν προτεραιότητα στη χρηστικότητα, παρουσιάζοντας αποτελεσματικά τα δεδομένα με τρόπο συνεκτικό για τους ερευνητές. Μια κρίσιμη πτυχή είναι η ύπαρξη εργαλείων που επιτρέπουν την παρουσίαση όλων των δεδομένων για τον εντοπισμό τόσο δυνητικά ενοχοποιητικών όσο και αθωωτικών στοιχείων[82]. Η πτυχή της ακρίβειας είναι πρωταρχικής σημασίας, καθιστώντας απαραίτητη την αυστηρή επαλήθευση της ποιότητας και της αξιοπιστίας των αποτελεσμάτων των εργαλείων.

Η απαίτηση για επαλήθευση των δεδομένων είναι σημαντική για να διασφαλιστεί η ακρίβεια του τελικού αποτελέσματος. Επίσης, η διεξοδική έρευνα είναι απαραίτητη για να διαπιστωθεί ότι τα δεδομένα στην εσωτερική μνήμη της κινητής συσκευής παραμένουν αναλλοίωτα[82]. Για την εξοικείωση με τις δυνατότητες των εργαλείων και την κατάλληλη προετοιμασία για πραγματικές εφαρμογές, συνιστάται ιδιαίτερα ο πειραματισμός με διάφορα εργαλεία.

5.6 Εξαγωγή κρίσιμων αποδεικτικών στοιχείων από σύγχρονες φορητές συσκευές

Καθώς η τεχνολογία των κινητών συσκευών εξελίσσεται ραγδαία, ο όγκος και η ποικιλομορφία των δεδομένων που μπορούν να βρεθούν διαφέρουν ανά συσκευές. Τα κινητά τηλέφωνα ενδέχεται να περιέχουν πολύτιμα στοιχεία από διάφορες πηγές, όπως κάρτες SIM και εξωτερικές κάρτες μνήμης, όπως κάρτες SD.

Η παραδοσιακή εγκληματολογία φορητών συσκευών και πιο συγκεκριμένα κινητών τηλεφώνων επικεντρώθηκε κυρίως στην ανάκτηση SMS, MMS, αρχείων καταγραφής κλήσεων, λιστών επαφών του τηλεφώνου[86]. Ωστόσο, τα σύγχρονα smartphone προσφέρουν ένα ευρύτερο φάσμα πληροφοριών, όπως δεδομένα περιήγησης ιστού, ρυθμίσεις ασύρματου δικτύου, πληροφορίες γεωγραφικής τοποθεσίας (συμπεριλαμβανομένων γεωγραφικών ετικετών στα μεταδεδομένα εικόνας), email και άλλα πλούσια μέσα στο διαδίκτυο, όπως αναρτήσεις υπηρεσιών κοινωνικής δικτύωσης και επαφές που είναι αποθηκευμένες σε εφαρμογές smartphone.

Παρόλο που τα αρχεία κλήσεων και τα μηνύματα κειμένου δεν θεωρούνται επίσημα μέρος της εγκληματολογίας κινητών συσκευών, μπορούν να χρησιμεύσουν ως εφεδρικά αποδεικτικά στοιχεία μετά την κατάσχεση ενός κινητού τηλεφώνου. Αυτές οι εγγραφές αποκτούν ιδιαίτερη αξία σε περιπτώσεις όπου το ιστορικό κλήσεων ή τα μηνύματα κειμένου έχουν διαγραφεί από το τηλέφωνο ή όταν οι υπηρεσίες που βασίζονται στην τοποθεσία δεν είναι ενεργοποιημένες[86]. Αναλύοντας τα σήματα που αναπηδούν από διάφορους πύργους, τα αρχεία λεπτομερειών κλήσεων μπορούν να παρέχουν πληροφορίες για την τοποθεσία του κατόχου του τηλεφώνου.

Το GPS είναι ένα ουσιαστικό εργαλείο για τον ακριβή προσδιορισμό της θέσης ενός υπόπτου κατά τη διάρκεια εγκληματικών δραστηριοτήτων. Το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS) παρέχει ανεκτίμητα εμπειρικά στοιχεία βοηθώντας στην παρακολούθηση των κινήσεων ενός υπόπτου. Με 27 επιχειρησιακούς δορυφόρους, το σύστημα GPS επιτρέπει ακριβείς δυνατότητες παρακολούθησης και επιτήρησης, καθιστώντας το απαραίτητο πόρο όταν ένας ύποπτος έχει μια ενεργή κινητή συσκευή στον τόπο του εγκλήματος[86].

Τα δεδομένα εφαρμογών είναι ακόμη μια σημαντική πτυχή της εγκληματολογίας για φορητές συσκευές, καθώς πολλές εφαρμογές έχουν πρόσβαση και αποθηκεύουν εν αγνοία των χρηστών δεδομένα. Κατά την εγκατάσταση της εφαρμογής, πολλές εφαρμογές ζητούν άδεια πρόσβασης σε

ευαίσθητες πληροφορίες όπως αρχεία πολυμέσων, κάμερα και GPS για πλοήγηση[86]. Αυτά τα δεδομένα χρησιμεύουν ως πρωταρχικά στοιχεία σε νομικές διαδικασίες, προσφέροντας ζωτικής σημασίας πληροφορίες για τις δραστηριότητες, τα πρότυπα επικοινωνίας και τις γεωγραφικές κινήσεις ενός υπόπτου.

Τα γραπτά μηνύματα έχουν γίνει ένας δημοφιλής τρόπος επικοινωνίας, αφήνοντας ηλεκτρονικά αρχεία διαλόγου που έχουν ουσιαστική αξία ως αποδεικτικά στοιχεία. Αυτές οι εγγραφές περιλαμβάνουν βασικές λεπτομέρειες, όπως χρονικές σημάνσεις μηνυμάτων, καθώς και τους αριθμούς τηλεφώνου τόσο των αποστολέων όσο και των παραληπτών. Τέτοια αρχεία διαδραματίζουν κρίσιμο ρόλο στον καθορισμό των χρονοδιαγραμμάτων[86].

Τέλος, οι φωτογραφίες και τα βίντεο είναι σημαντικά αποδεικτικά στοιχεία, των οποίων η συνάφεια και η αυθεντικότητα είναι κρίσιμες στις ποινικές έρευνες[86]. Με τον κατάλληλο χειρισμό και την επικύρωση, τα αρχεία πολυμέσων μπορούν να παρέχουν πολύτιμες πληροφορίες σε μια έρευνα, βοηθώντας στη διερεύνηση και την επίλυση νομικών υποθέσεων.

5.7 Αναδυόμενες τάσεις στην τεχνολογία κινητών τηλεφώνων και ο αντίκτυπός τους στην εγκληματολογία φορητών συσκευών

Ο τομέας της τεχνολογίας κινητών συσκευών πρόκειται να γνωρίσει σημαντικές προόδους σε τρεις κρίσιμους τομείς: ταχύτητα επεξεργαστή, τύποι και τεχνολογίες μπαταριών και χωρητικότητα μνήμης και αποθήκευσης. Αυτές οι τεχνολογικές εξελίξεις αναμένεται να έχουν εκτεταμένο αντίκτυπο στην εγκληματολογία κινητών συσκευών.

Στοιχεία επεξεργαστή και ταχύτητα: Εταιρείες όπως η Intel έχουν ήδη παρουσιάσει επεξεργαστές 1 GHz σχεδιασμένους για κινητές συσκευές και υπάρχει μια αυξανόμενη υιοθέτηση της τεχνολογίας System on Chip (SoC) στα έξυπνα κινητά τηλέφωνα. Το SoC διευκολύνει την ενσωμάτωση πολλαπλών λειτουργιών σε ένα μόνο πακέτο, μειώνοντας τον αριθμό των τσιπ που απαιτούνται και ενσωματώνοντας περισσότερη ενσωματωμένη μνήμη[87]. Ωστόσο, αυτή η εξελισσόμενη αρχιτεκτονική επεξεργαστή μπορεί να παρουσιάζει προκλήσεις στην ιατροδικαστική κινητής τηλεφωνίας.

Διάρκεια ζωής μπαταρίας: Τα κινητά τηλέφωνα βασίζονται συνήθως σε μπαταρίες NiMH, Li-ion ή Li-polymer. Οι επερχόμενες εξελίξεις, όπως η τεχνολογία μπαταριών ιόντων λιθίου της Toshiba, υπόσχονται γρήγορους χρόνους επαναφόρτισης[87]. Η ενσωμάτωση επιλογών ασύρματης επικοινωνίας όπως το Wi-Fi, το Wi-Max και το Bluetooth μπορεί να οδηγήσει σε ταχύτερη εξάντληση της μπαταρίας, θέτοντας προκλήσεις για τους κατασκευαστές μπαταριών. Η διάρκεια ζωής της μπαταρίας είναι κρίσιμη στις εγκληματολογικές έρευνες για κινητά, καθώς μια εξαντλημένη μπαταρία μπορεί να οδηγήσει σε απώλεια ασταθών δεδομένων.

Μνήμη και αποθήκευση: Λόγω του μικρού μεγέθους τους, οι φορητές συσκευές αποθηκεύουν το λειτουργικό σύστημα και τις εφαρμογές τους σε RAM, ROM ή μνήμη flash. Τα κινητά τηλέφωνα υψηλής τεχνολογίας διαθέτουν ήδη σημαντικές χωρητικότητες μνήμης και αυτή η τάση αναμένεται να συνεχιστεί, διευκολύνοντας τη βελτιωμένη πρόσβαση στα δεδομένα και τους ρυθμούς μεταφοράς[87]. Ωστόσο, οι αυξημένες δυνατότητες αποθήκευσης καθιστούν αυτές τις συσκευές πιο επιρρεπείς σε απόκρυψη ή παραποίηση από κακόβουλους παράγοντες. Επιπλέον, ορισμένα κινητά τηλέφωνα υποστηρίζουν την ανταλλαγή εξωτερικής μνήμης αποθήκευσης, κάτι που απαιτεί προσεκτικό έλεγχο κινητών σε επίπεδο λειτουργικού συστήματος.

Οι αυξανόμενες επιλογές συνδεσιμότητας, η υψηλότερη χωρητικότητα αποθήκευσης και η επεξεργαστική ισχύς στα κινητά τηλέφωνα θα μπορούσαν να κλιμακώσουν τον κίνδυνο κατάχρησης και των ψηφιακών εγκλημάτων[87]. Καθώς τα κινητά τηλέφωνα ξεπερνούν τους προσωπικούς υπολογιστές σε πωλήσεις, μπορεί να γίνουν πρωταρχικός στόχος για ψηφιακές εγκληματικές δραστηριότητες. Η αύξηση των ιών και του κακόβουλου λογισμικού, ιδιαίτερα σε ευρέως χρησιμοποιούμενα λειτουργικά συστήματα, δημιουργεί σημαντική ανησυχία. Για να συμβαδίσει με την ταχεία εξέλιξη της κινητής τεχνολογίας, υπάρχει επιτακτική ανάγκη για ένα ολοκληρωμένο πλαίσιο για την αξιολόγηση των εγκληματολογικών εργαλείων. Η διασφάλιση της έγκαιρης πρόσβασης σε κατάλληλα εργαλεία και τεχνικές για διαφορετικούς τύπους τηλεφώνων είναι ζωτικής σημασίας και οι συνεχείς προσπάθειες είναι καθοριστικές για την αντιμετώπιση αυτών των προκλήσεων.

5.8 Open source εργαλεία για Mobile συσκευές

XRY:

Το XRY είναι ένα ευρέως χρησιμοποιούμενο εργαλείο ψηφιακής εγκληματολογίας, το οποίο επιτρέπει την ανάλυση και την ανάκτηση δεδομένων από διάφορες συσκευές, όπως κινητά τηλέφωνα, εργαλεία πλοήγησης GPS και tablet[88]. Χρησιμοποιεί στοιχεία τόσο υλικού όσο και λογισμικού, επιτρέποντας στους χρήστες να συνδέουν τις συσκευές σε έναν υπολογιστή και να εξάγουν δεδομένα με εγκληματολογικές τεχνικές, με γνώμονα την αξιοπιστία των δεδομένων.

Οι έρευνες και αναλύσεις κινητών συσκευών ενέχουν μεγαλύτερες προκλήσεις σε σύγκριση με την παραδοσιακή εγκληματολογία υπολογιστών, καθώς τα ιδιόκτητα λειτουργικά συστήματα πολλών φορητών συσκευών κάνουν την αντίστροφη μηχανική περίπλοκη. Ωστόσο, το XRY διευκολύνει τόσο την λογική εξαγωγή, που περιλαμβάνει άμεση επικοινωνία με το λειτουργικό σύστημα της συσκευής, όσο και την φυσική εξαγωγή δεδομένων, κατα την οποία παρακάμπτεται το λειτουργικό σύστημα και αποκτάται πρόσβαση στη διαθέσιμη μνήμη[88]. Η φυσική εξαγωγή προσφέρει το πλεονέκτημα της ανάκτησης περισσότερων διαγραμμένων και κρυφών πληροφοριών, όπως μηνύματα κειμένου SMS, εικόνες και αρχεία κλήσεων.

Το XRY παρέχει υποστήριξη για ανάκτηση δεδομένων από δημοφιλείς μάρκες smartphone, όπως Android, iPhone και Blackberry[88].Ωστόσο, λόγω της πολυπλοκότητάς του, συνιστάται η εξειδίκευση και η εκπαίδευση για τη σωστή χρήση του λογισμικού.

Oxygen Forensics:

Το Oxygen Forensics παρέχει μια πλατφόρμα που επιτρέπει την ανάκτηση, την αποκρυπτογράφηση και την ανάλυση ψηφιακών εικόνων από κινητές συσκευές, μέσω μιας φιλικής προς το χρήστη διεπαφής που επιτρέπει γρήγορη και αποτελεσματική ανάλυση για τους ερευνητές. Το λογισμικό είναι ευέλικτο και επιτρέπει τη διερεύνηση πολλαπλών εξαγωγών μέσα από την ίδια διεπαφή, παρέχοντας μια ολοκληρωμένη θέαση όλων των αποκτηθέντων δεδομένων[89].

Τα βασικά χαρακτηριστικά του Oxygen Forensics Suite περιλαμβάνουν την ανάκτηση αρχείων συστήματος για τις περισσότερες κινητές συσκευές, τη δυνατότητα εγκληματολογίας σε drones, την παράκαμψη κλειδώματος οθόνης σε δημοφιλείς συσκευές Android, την εξαγωγή αρχείων cloud για

απόκτηση δεδομένων από υπηρεσίες cloud και την αποθήκευση και υποστήριξη εισαγωγής αρχείων δεδομένων κλήσεων[89].

Το Oxygen Forensics Suite διαδραματίζει κρίσιμο ρόλο στην ανάκτηση δεδομένων από διάφορες φορητές συσκευές, όπως αντίγραφα ασφαλείας, εικόνες, δεδομένα κάρτας SIM, αρχεία καταγραφής μηνυμάτων και αποθήκευση cloud.

Το λογισμικό επιτρέπει την ανακάλυψη βασικών πληροφοριών από διάφορες πηγές, όπως έξυπνα ρολόγια, δεδομένα συσκευών IoT (όπως το Amazon, Alexa), καθώς και δεδομένα από πάνω από 60 υπηρεσίες αποθήκευσης cloud, όπως το Huawei, το ICloud, το MI cloud storage, το Microsoft, το Samsung και το Amazon Drive[89].

Η φιλική προς το χρήστη διεπαφή του Oxygen Forensics Suite περιλαμβάνει βασικά αναλυτικά εργαλεία, όπως χρονοδιαγράμματα και γραφήματα. Οι προηγμένες τεχνικές αναζήτησης όπως λέξεις-κλειδιά, κατακερματισμός και κανονικές εκφράσεις, επιτρέπουν στους ερευνητές να ανακαλύπτουν γρήγορα κρίσιμες πληροφορίες. Το λογισμικό υποστηρίζει την εξαγωγή δεδομένων σε διάφορες μορφές, όπως PDF, RTF και XLS, γεγονός που διευκολύνει την παρουσίαση των ευρημάτων[89].

Το Oxygen Forensics Suite είναι συμβατό με συστήματα Windows 7, Windows 8 και Windows 10 και υποστηρίζει σύνδεση μέσω καλωδίου USB και Bluetooth. Μπορεί να ανακτά και να αναλύει δεδομένα από διάφορα αντίγραφα ασφαλείας συσκευών και λειτουργικά συστήματα, όπως Apple iOS, Windows OS, Android OS, Nokia και BlackBerry[89].

UFED:

Το Cellebrite Universal Forensic Extraction Device (UFED) είναι ένα φορητό εργαλείο εγκληματολογίας που μπορεί να θεωρηθεί και ως λογισμικό εργαλείο. Παρέχει τη δυνατότητα εξαγωγής φυσικών και λογικών δεδομένων από διάφορες κινητές συσκευές, συμπεριλαμβανομένων κινητών τηλεφώνων και φορητών συσκευών[82].

Ως λογισμικό εργαλείο, το UFED προσφέρει μια εύχρηστη διεπαφή και ποικίλες δυνατότητες που επιτρέπουν στους ερευνητές να εξάγουν, να αποκωδικοποιούν και να αναλύουν δεδομένα από κινητές συσκευές. Αναλαμβάνει την ανάκτηση διαγραμμένων δεδομένων, την αποκρυπτογράφηση κρυπτογραφημένων πληροφοριών, καθώς και την παροχή ανάλυσης δεδομένων.

Μεταξύ των βασικών χαρακτηριστικών του UFED περιλαμβάνονται[82]:

1. Εξαγωγή διαφόρων τύπων δεδομένων από κινητές συσκευές, όπως επαφές, πολυμέσα, μηνύματα SMS και MMS, αρχεία καταγραφής κλήσεων, και πληροφορίες SIM.
2. Υποστήριξη πολλών πρωτοκόλλων κινητής τηλεφωνίας, συμπεριλαμβανομένων των CDMA, GSM, IDEN και TDMA.

3. Ανάκτηση δεδομένων από μη πτητική μνήμη και πτητική αποθήκευση.
4. Φυσική εξαγωγή για ανάκτηση διαγραμμένων πληροφοριών και αποκρυπτογράφηση κρυπτογραφημένων δεδομένων.
5. Υποστήριξη για πολλά λειτουργικά συστήματα και μοντέλα κινητών συσκευών.

Επιπλέον, το UFED δίνει έμφαση στην διατήρηση της ακεραιότητας των ψηφιακών αποδεικτικών στοιχείων και εφαρμόζει μέτρα ασφαλείας, όπως υποδοχές καλωδίων αποκλεισμού εγγραφής και θωρακισμένες τσάντες Faraday, για να διασφαλίσει την ασφάλεια της διαδικασίας εξαγωγής δεδομένων[82].

Magnet Acquire:

Το εργαλείο ανοιχτού κώδικα Magnet Acquire αποτελεί μια κορυφαία λύση για την απόκτηση και απεικόνιση ψηφιακών δεδομένων από συσκευές Android και IOS, αφαιρούμενα μέσα και σκληρούς δίσκους. Πρόκειται για ένα εξειδικευμένο εργαλείο το οποίο προσφέρει στους ερευνητές ευέλικτες λειτουργίες για την συλλογή δεδομένων εξασφαλίζοντας την αξιοπιστία και την ασφάλεια τους κατά τις ψηφιακές έρευνες ενώ παράλληλα διατηρεί αναλλοίωτα τα πρωτότυπα δεδομένα. Συνδυάζει μια διαισθητική διεπαφή χρήστη με συνοπτικές διαδικασίες εξαγωγής τα οποία επιτρέπουν την εύκολη αλληλεπίδραση των χρηστών με το σύστημα ή την συσκευή. Επιπρόσθετα, επιτρέπει την ανάκτηση διαγραμμένων ή κρυπτογραφημένων δεδομένων υποστηρίζοντας διάφορα λειτουργικά συστήματα όπως Windows, Mac, Linux.

5.9 Συγκριτική ανάλυση open source εργαλείων για Mobile συσκευές

Αυτή η ανάλυση συγκριτικής αξιολόγησης στοχεύει στην εκτενή αξιολόγηση των τεσσάρων δημοφιλέστερων εργαλείων εγκληματολογίας για φορητές συσκευές, το UFED,το XRY, το Oxygen Forensics, το Autopsy και το Magnet Acquire. Στην ουσία, μέσω μιας ολοκληρωμένης αξιολόγησης των βασικών χαρακτηριστικών τους συγκρίνει και αντιπαραβάλλει τις ικανότητες και τις δυνατότητες των πέντε εργαλείων, προσφέροντας μια ολοκληρωμένη εικόνα για κάθε ένα από αυτά. Με την κατανόηση των διαφορετικών πτυχών και δυνατοτήτων κάθε εργαλείου, οι επαγγελματίες εγκληματολόγοι μπορούν να επιλέξουν αυτό που καλύπτει καλύτερα τις ανάγκες και τους στόχους των ερευνών τους.

1. Εξόρυξη δεδομένων:

Τα εργαλεία αυτά είναι ευρέως διαδεδομένα για την αξιοσημείωτη ικανότητά τους τόσο στην φυσική όσο και λογική εξαγωγή δεδομένων από διάφορες κινητές συσκευές. Το UFED, όπως προαναφέρθηκε, ξεχωρίζει για την ικανότητα ανάκτησης διαγραμμένων και κρυπτογραφημένων δεδομένων, ενώ το XRY αποτελεί μια εξέχουσα και ισχυρή λύση για την ανάκτηση πολλών τύπων δεδομένων, όπως μηνύματα κειμένου, εικόνες και κλήσεις. Το Oxygen Forensics είναι επαρκώς εξοπλισμένο all-in-one εργαλείο, που παρέχει ολοκληρωμένες δυνατότητες εξαγωγής δεδομένων για την επιτάχυνση της αποτελεσματικής ανάλυσης των δεδομένων που αποκτήθηκαν. Το εργαλείο Magnet Acquire

συνδυάζει όλα τα παραπάνω χαρακτηριστικά.

2. Συμβατότητα:

Η ευρεία συμβατότητα του UFED αντικατοπτρίζεται στην υποστήριξή του για πολλαπλά πρωτόκολλα κινητής τηλεφωνίας και λειτουργικά συστήματα, συμπεριλαμβανομένων των CDMA, GSM, IDEN, TDMA. Ομοίως, το XRY και το Magnet Acquire συνδέονται απρόσκοπτα με μια ποικιλία λειτουργικών συστημάτων, συμπεριλαμβανομένων των iOS, Android OS, BlackBerry, Symbian, Windows Mobile και παλαιού τύπου/χαρακτηριστικών τηλεφώνων. Το Oxygen Forensics υποστηρίζει περισσότερα από 25.000 μοντέλα φορητών συσκευών με διαφορετικά λειτουργικά συστήματα, διασφαλίζοντας ένα ευρύ φάσμα συμβατότητας.

3. Εγκληματολογικά χαρακτηριστικά:

Όλα τα εργαλεία διαθέτουν πληθώρα προηγμένων δυνατοτήτων ανάλυσης που κυμαίνονται από εξαγωγή και ανάλυση επαφών τηλεφωνικού καταλόγου, περιεχομένου πολυμέσων, μηνυμάτων SMS και MMS έως IMEI, πληροφορίες τοποθεσίας SIM και κρυπτογραφημένες εφαρμογές για κινητά. Το UFED και το XRY συγκεκριμένα, παρουσιάζουν αξιοσημείωτη ευελιξία για την κάλυψη διαφορετικών αναγκών έρευνας ενώ το Oxygen Forensics και το Magnet Acquire παρέχουν μια φιλική προς το χρήστη ενότητα ανάλυσης γεμάτη οπτικοποιήσεις βασικών στοιχείων, διευκολύνοντας έτσι την αποτελεσματική και συστηματική ανάλυση δεδομένων.

4. Διεπαφή χρήστη:

Οι διεπαφές χρήστη των εργαλείων UFED, Magnet Acquire και Oxygen Forensics έχουν σχεδιαστεί προσεκτικά για να εξυπηρετούν χρήστες διαφορετικών επιπέδων τεχνογνωσίας, εξασφαλίζοντας ευκολία λειτουργίας. Αντιθέτως, το XRY συνίσταται για χρήστες με πιο εξειδικευμένες γνώσεις. Πιο συγκεκρυμένα, το UFED απλοποιεί τη διαδικασία εξαγωγής δεδομένων απευθείας σε κάρτα SD ή μονάδα flash USB ενώ το Oxygen Forensics είναι σε θέση να εξάγει απρόσκοπτα δεδομένα σε διάφορες μορφές, όπως PDF, RTF και XLS, διευκολύνοντας έτσι μια βελτιστοποιημένη και ολοκληρωμένη διαδικασία αναφοράς δεδομένων. Επιπλέον, το Magnet Acquire έχει σχεδιαστεί με έμφαση στην ευκολία για την αλληλεπίδραση των χρηστών με τις συσκευές ανεξαρτήτως επιπέδου γνώσης.

5. Μέτρα για την διατήρηση ακεραιότητας των δεδομένων:

Το UFED παρέχει φορητότητα και εξειδίκευση για την εξαγωγή φυσικών και λογικών δεδομένων από διάφορες συσκευές. Χρησιμοποιώντας πιστοποιημένα καλώδια και τσάντες Faraday, το UFED διασφαλίζει την ακεραιότητα των δεδομένων και την ασφάλεια της διαδικασίας εξαγωγής. Επιπλέον, προσφέρει τη δυνατότητα ανάκτησης διαγραμμένων πληροφοριών και αποκρυπτογράφησης κρυπτογραφημένων δεδομένων.

Το XRY χρησιμοποιεί εγκληματολογικές τεχνικές για να επικοινωνεί άμεσα με το λειτουργικό σύστημα των συσκευών και να εξάγει δεδομένα με αξιοπιστία. Οι μηχανισμοί κατακερματισμού παρέχουν επιπλέον επίπεδο ασφαλείας και ακεραιότητας κατά την εξαγωγή και την ανάλυση

δεδομένων.

Το Oxygen Forensics προσφέρει μια φιλική προς το χρήστη πλατφόρμα που επιτρέπει γρήγορη και αποτελεσματική ανάλυση για τους ερευνητές. Η δυνατότητα εξαγωγής δεδομένων σε διάφορες μορφές και η υποστήριξη πολλών λειτουργικών συστημάτων και μοντέλων κινητών συσκευών παρέχουν ευελιξία στην ανάκτηση και ανάλυση δεδομένων.

Το Magnet Acquire παρέχει την ιδανική ισορροπία μεταξύ φορητότητας και εξειδίκευσης για την φυσική και λογική ανάκτηση δεδομένων από διάφορες συσκευές εξασφαλίζοντας την ακεραιότητα και την ασφάλεια κατά τη διαδικασία εξαγωγής τους. Επιπλέον, προσφέρει τη δυνατότητα ανάκτησης διαγραμμένων πληροφοριών και αποκρυπτογράφησης δεδομένων.

Συνοψίζοντας, το UFED, το XRY, το Magnet Acquire και το Oxygen Forensics αναδεικνύονται ως ισχυρά και απαραίτητα εργαλεία ψηφιακής εγκληματολογίας, το καθένα προσφέροντας μοναδικά πλεονεκτήματα και δυνατότητες. Το UFED ξεχωρίζει για την επιδεξιότητά του να ανακτά διαγραμμένα και κρυπτογραφημένα δεδομένα, ενώ το XRY είναι κατάλληλο για διαφορετικά σενάρια διερεύνησης. Από την άλλη πλευρά, το Oxygen Forensics και το Magnet Acquire διακρίνονται για την ολοκληρωμένη πλατφόρμα τους και την ευρεία υποστήριξη συσκευών. Είναι ζωτικής σημασίας για τους ερευνητές και τους επαγγελματίες να αξιολογούν προσεκτικά τις συγκεκριμένες απαιτήσεις της διερεύνησής τους, τη συμβατότητα των συσκευών και τις ανάγκες ανάλυσης δεδομένων προκειμένου να επιλέξουν το καταλληλότερο εργαλείο για μια επιτυχημένη και ακριβή ψηφιακή εγκληματολογική έρευνα. Αυτά τα εργαλεία παρέχουν την τεχνολογική και μεθοδολογική υποστήριξη που απαιτείται για την αξιόπιστη ανάλυση και ανάκτηση στοιχείων από φορητές συσκευές, επιτρέποντας στους ερευνητές να ερευνούν κρίσιμες πληροφορίες και να παρουσιάζουν αξιόπιστα αποδεικτικά στοιχεία σε δικαστικές διαδικασίες.

Πολλά από τα εργαλεία ανοικτού κώδικα που αναφέρθηκαν στην ενότητα 4.5 είναι συμβατά με κινητές συσκευές στα πλαίσια της εγκληματολογίας. Συγκεκριμένα, το εργαλείο Autopsy έχει γνωρίσει μεγάλη δημοτικότητα τα τελευταία χρόνια και χρησιμοποιείται εκτενώς σε υποθέσεις εγκληματολογίας σε κινητές συσκευές.

Παρακάτω παρουσιάζεται ένας πίνακας σύγκρισης των χαρακτηριστικών των εργαλείων εγκληματολογίας κινητών συσκευών που προαναφέρθηκαν και αναλύθηκαν.

Χαρακτηριστικά	UFED	XRY	Oxygen Forensics	Autopsy	Magnet Acquire
Εξόρυξη Δεδομένων	Φυσική και Λογική ανάκτηση δεδομένων	Φυσική και Λογική ανάκτηση δεδομένων	Φυσική και Λογική ανάκτηση δεδομένων	Λογική ανάκτηση δεδομένων	Φυσική και Λογική ανάκτηση δεδομένων
Συμβατότητα	Διάφορα πρωτόκολλα κινητής τηλεφωνίας	Πολλά λειτουργικά συστήματα	25,000+ μοντέλα φορητών συσκευών	Κινητά, Υπολογιστές και Άλλες Συσκευές	Πολλά λειτουργικά συστήματα και συσκευές
Εγκληματολογικά Χαρακτηριστικά	Πολλές δυνατότητες ανάκτησης δεδομένων και ανάλυσης	Εξειδικευμένες αναλύσεις, κρυπτογραφημένων δεδομένων	Πολλές προηγμένες δυνατότητες ανάλυσης δεδομένων και εξαγωγή δεδομένων	Εξειδικευμένες δυνατότητες ανάλυσης δεδομένων και εξαγωγή δεδομένων	Πολλές προηγμένες δυνατότητες ανάλυσης δεδομένων και εξαγωγή δεδομένων
Διεπαφή Χρήστη	Συνοπτική και ευέλικτη διεπαφή	Συνοπτική διεπαφή	Φιλική προς το χρήστη, με οπτικοποιήσεις	Φιλική προς το χρήστη, με οπτικοποιήσεις	Φιλική προς το χρήστη, με οπτικοποιήσεις
Ακεραιότητα Δεδομένων	Ασφαλής διαδικασία εξαγωγής και ανάλυσης	Μηχανισμοί κατακερματισμού	Εξασφάλιση δεδομένων με κατακερματισμο	Εξασφάλιση δεδομένων με κατακερματισμο	Εξασφάλιση δεδομένων με κατακερματισμο
Επεκτασιμότητα	Οχι	Οχι	Ναι	Ναι	Ναι
Κόστος	Υψηλό	Υψηλό	Υψηλό	Δωρεάν	Δωρεάν

Πίνακας 1: Συγκριτική ανάλυση εργαλείων Mobile Forensics

Κεφάλαιο 6ο: Μελέτη περίπτωσης

Η εγκληματολογική ανάλυση φορητών συσκευών αποτελεί μια σύνθετη διαδικασία, η οποία περιλαμβάνει την εξαγωγή, την διατήρηση και, κατ' επέκταση την ανάλυση των ψηφιακών δεδομένων που βρίσκονται σε μια συσκευή. Η παρούσα μελέτη περίπτωσης εμβαθύνει σε αυτή τη διαδικασία στις κινητές συσκευές που χρησιμοποιούν λειτουργικό Android, εξερευνώντας τις δυνατότητες ανάλυσης δεδομένων με τη χρήση των εργαλείων ανοιχτού κώδικα, Autopsy και Magnet Acquire. Από την εξαγωγή και εώς και την ανάλυση σημαντικών δεδομένων, αυτή η μελέτη αναδεικνύει τη σημασία των προαναφερθέντων εργαλείων στο πλαίσιο της ψηφιακής έρευνας και της επιτυχούς ανίχνευσης ποικίλων τύπων δεδομένων από τις συσκευές. Στόχος αυτής της μελέτης περίπτωσης είναι η ανάδειξη της αξιοπιστίας και αποτελεσματικοτητας των εργαλείων για τον εντοπισμό και την εξαγωγή κρίσιμων πληροφοριών.

Το Autopsy, όπως προαναφέρθηκε, αποτελεί ένα προηγμένο εργαλείο ανοιχτού κώδικα το οποίο προσφέρει ένα ολοκληρωμένο περιβάλλον για εκτενή και πολύπλευρη ανάλυση ψηφιακών δεδομένων. Η επιλογή για τη χρήση αυτού του εργαλείου στο πλαίσιο της μελέτης προκύπτει από την ευελιξία του και τη δυνατότητα ανάλυσης ενός συνόλου πληροφοριών από διάφορες πηγές. Γεωγραφικά δεδομένα, μεταδεδομένα εφαρμογών, ανάλυση φωτογραφιών και ανάκτηση διαγραμμένων δεδομένων είναι μερικά από τα στοιχεία που θα διερευνηθούν για να αποτυπωθεί περιεκτικά το φάσμα των λειτουργιών του. Επίσης, παρέχει εξελιγμένες δυνατότητες αναφοράς και γραφικής αναπαράστασης των ευρημάτων, αποτελώντας ένα πολυδιάστατο εργαλείο για την εξαγωγή πορισμάτων.

Το Magnet Acquire αποτελεί ένα εργαλείο ανάκτησης και ανάλυσης πληροφοριών από διάφορες συσκευές Android. Με τις προηγμένες λειτουργίες του, διευκολύνει την απεικόνιση του χώρου αποθήκευσης της συσκευής, ανακτώντας δεδομένα όπως εφαρμογές και αρχεία συστήματος. Στο πλαίσιο της μελέτης, το εργαλείο αυτό επιλέχθηκε λόγω της ικανότητάς του να προσφέρει ευέλικτες λύσεις για την εξαγωγή δεδομένων, διασφαλίζοντας παράλληλα την ακεραιότητα και την ασφάλειά τους.

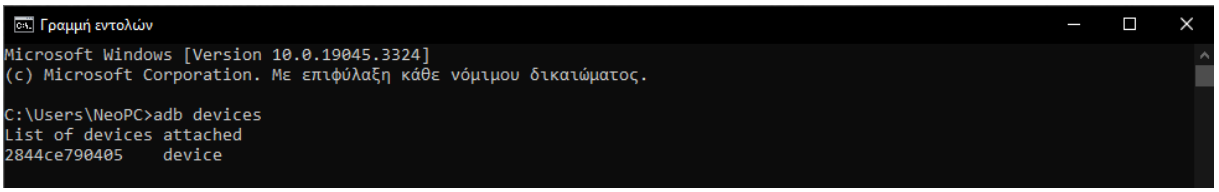
Φάση κατάσχεσης

Το πρώτο βήμα της εγκληματολογικής μελέτης κινητών συσκευών αφορά την ασφαλή κατάσχεση της υπό διερεύνηση συσκευης. Η συσκευή που επιλέχθηκε, η οποία αναφέρεται παρακάτω, κατασχέθηκε όντας ενεργοποιημένη ώστε να αποφευχθεί οποιαδήποτε αλλοίωση ψηφιακών δεδομένων.

Για την πραγματοποίηση της μελέτης, επιλέχθηκε η κινητή συσκευή Redmi Note 9, της εταιρείας Xiaomi με λειτουργικό Android. Η επιλογή αυτή βασίστηκε στην χρόνια κατοχή της συσκευής και στην ευελιξία του λειτουργικού συστήματος Android για την πρόσβαση στα δεδομένα. Η συσκευή παρέχει προηγμένες δυνατότητες καταγραφής γεωγραφικών δεδομένων και εξαγωγής δεδομένων εφαρμογών, τα οποία αποδείχθηκαν ζωτικής σημασίας για την επίτευξη των στόχων της μελέτης. Το μοντέλο Redmi Note 9 διαθέτει ενσωματωμένες λειτουργίες ασφαλείας, γεγονός που διασφαλίζει την ακεραιότητα και την ασφάλεια των δεδομένων κατά τη διαδικασίας της εξαγωγης. Επίσης διαθέτει μνήμη RAM 4,00 GB και λειτουργικό σύστημα Android έκδοσης 10.

Φάση Απόκτησης

Για την επικοινωνία με τον υπολογιστή απαιτείται η ανίχνευση της Android συσκευής μέσω γραμμής εντολών (command line) και κατ' επέκταση η εγκατάσταση του εργαλείου Android Debug Bridge. Το εργαλείο αυτό διασφαλίζει την ασφαλή και κρυπτογραφημένη σύνδεση της συσκευής μέσω καλωδίου USB, καθώς επίσης και την προστασία των δεδομένων κατα τη μεταφορά τους με την εντολή που φαίνεται παρακάτω.

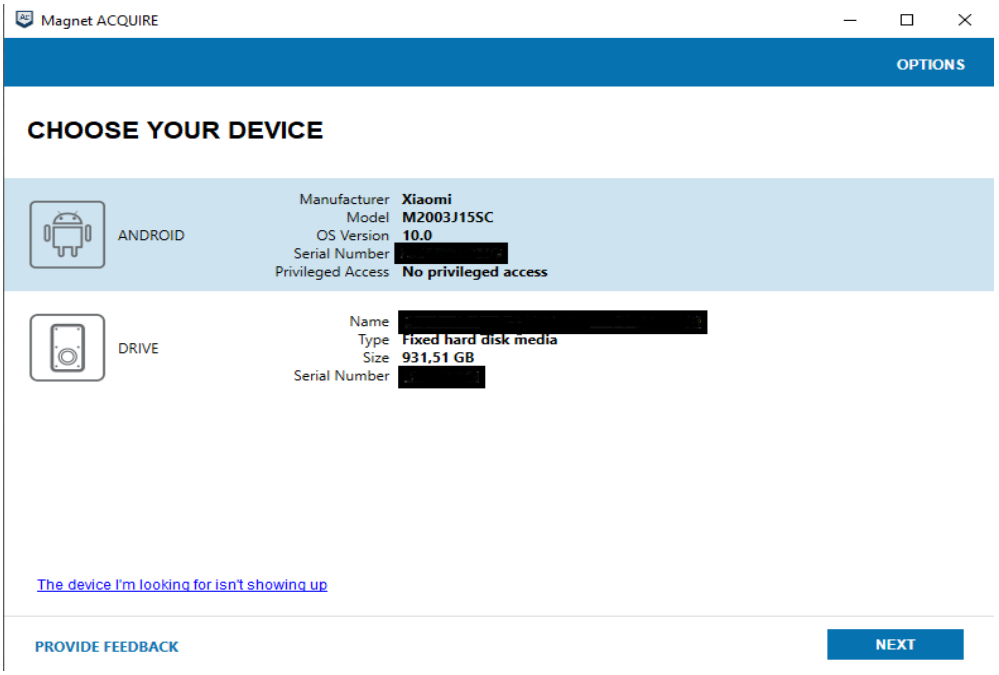


Σχήμα 13 Σύνδεση συσκευής με ADB

Για την εξαγωγή των αντιγράφων ασφαλείας των δεδομένων από τη συσκευή στον υπολογιστή με σκοπό την περαιτέρω ανάλυση τους με το εργαλείο Magnet Acquire, απαιτείται η χρήση της εντολή adb pull.

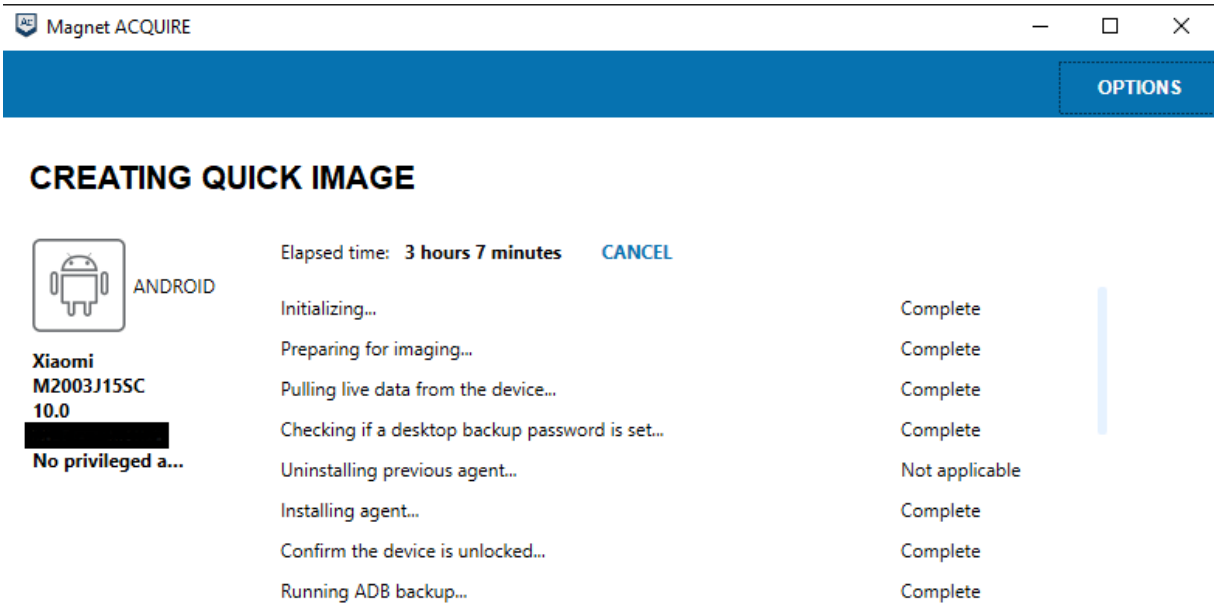
Σχήμα 14 Εντολή για εξαγωγή αντιγράφων

Κατόπιν εγκατάστασης του Magnet Acquire για την απόκτηση όλων των δεδομένων, ήταν απαραίτητη η ενεργοποίηση των ρυθμίσεων για προγραμματιστές στη συσκευή, η οποία πραγματοποιήθηκε μεταβαίνοντας στις ρυθμίσεις του κινητού και πατώντας την έκδοση λογισμικού 7 φορές, ώστε να ενεργοποιηθεί ο εντοπισμός σφαλμάτων USB (USB Debugging). Η διαδικασία αυτή είναι απαραίτητη για την πρόσβαση και τον έλεγχο του εσωτερικού της συσκευής γεγονός που επιτρέπει την ασφαλή αλληλεπίδραση της με τον υπολογιστή μέσω της σύνδεσης με το καλώδιο USB. Ανοίγοντας το εργαλείο, εμφανίζονται οι συνδεδεμένες συσκευές από τις οποίες επιλέχθηκε η συσκευή Android όπως διακρίνεται στην παρακάτω φωτογραφία.



Σχήμα 15 Επιλογή συσκευής στο Magnet Acquire

Έπειτα, ξεκίνησε η διαδικασία απεικόνισης και εξαγωγής των αρχείων συστήματος.



Σχήμα 16 Διαδικασία imaging και εξαγωγής αρχείων

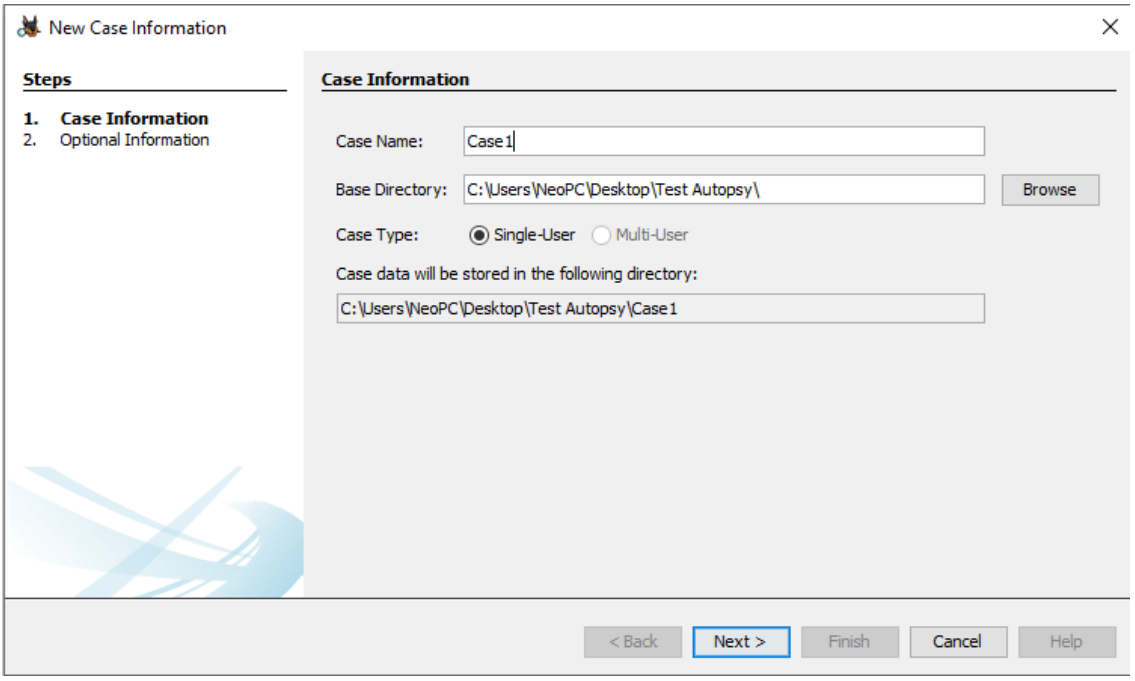
Ολοκληρώνοντας αυτήν την διαδικασία, αφού δημιουργήθηκε η απεικόνιση του συστήματος και το αντίγραφο όλων των δεδομένων μεταφέρθηκε στον υπολογιστή, σειρά έχει η ανάλυσή τους με τη βοήθεια του εργαλείου Autopsy.

Φάση ανάλυσης

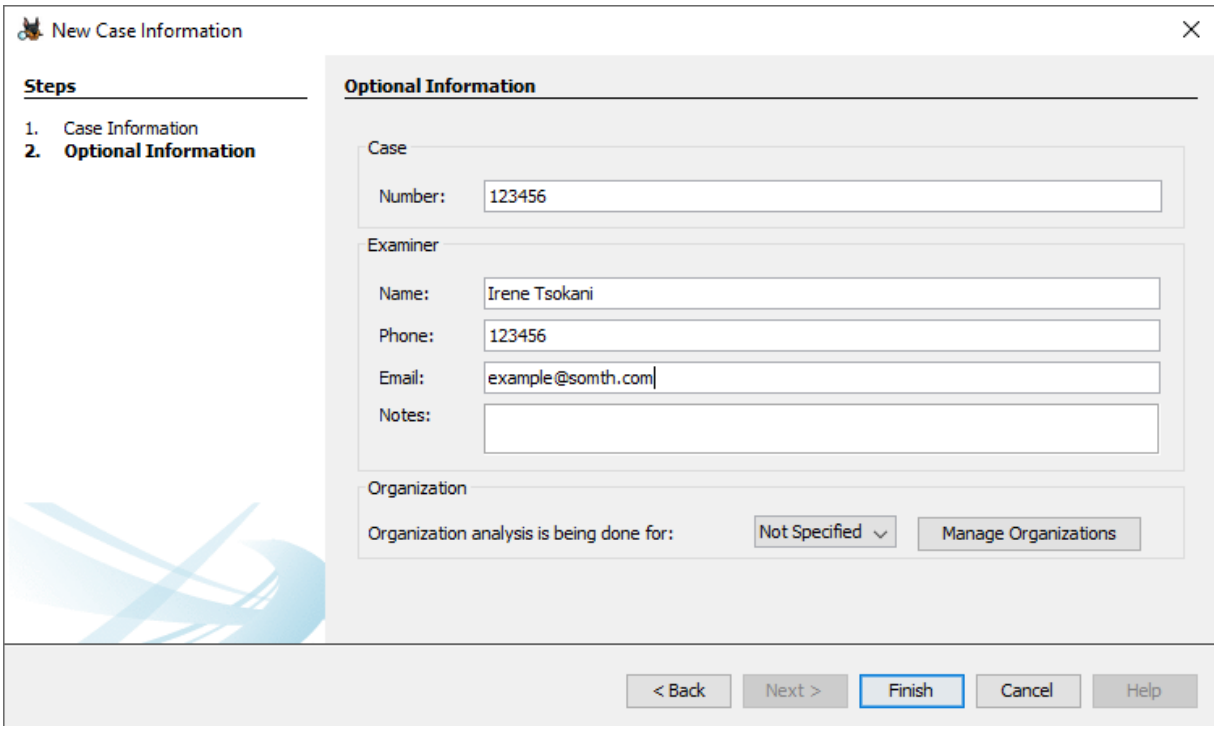
Η διαδικασία της ανάλυσης των δεδομένων που αποκτήθηκαν από τη συσκευή ξεκινά με τη δημιουργία μιας νέας υπόθεσης(case).

Σχήμα 17 Αρχική εργαλείου Autopsy

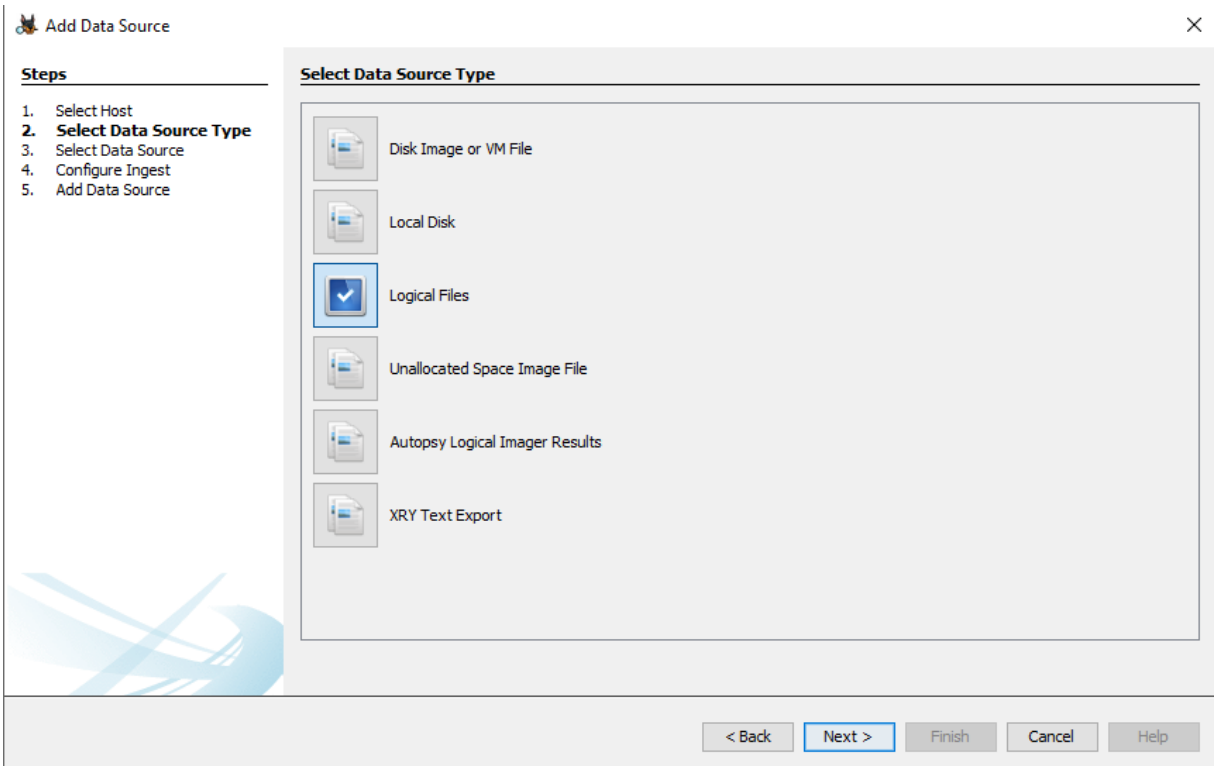
Στη συνέχεια προσδιορίστηκε το όνομα της υπόθεσης και τα στοιχεία του εξεταστή, καθώς επίσης και τα δεδομένα που αποκτήθηκαν από το εργαλείο Magnet Acquire. Επιλέχθηκε ο τύπος τους και καθορίστηκε η τοποθεσία τους στον υπολογιστή.



Σχήμα 18 Δημιουργία καινούργιου case



Σχήμα 19 Στοιχεία ερευνητή

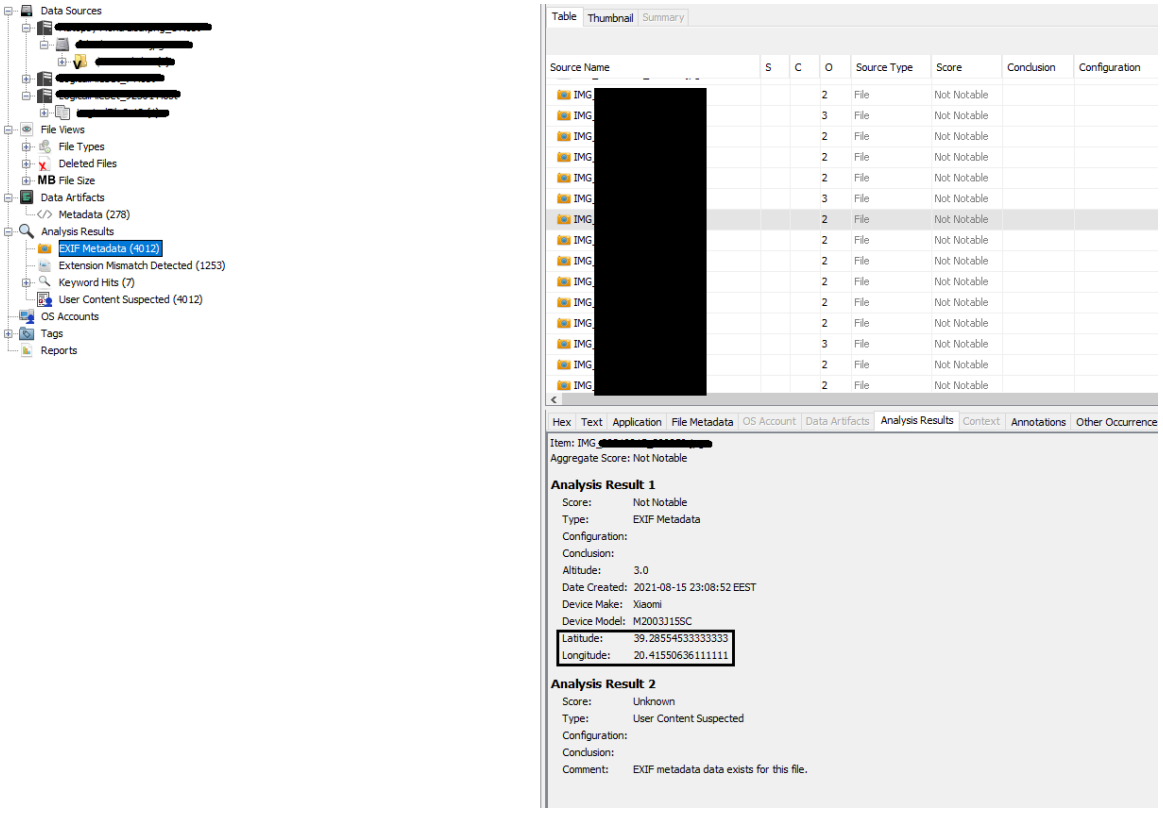


Σχήμα 20 Επιλογή τύπου πηγής

Αμέσως δημιουργήθηκε μια βάση δεδομένων με κάθε λογής πληροφορία που υπάρχει μέσα στην κινητή συσκευή, για παραδειγμα αρχεία εφαρμογών, διαγραμμένες και μη εικόνες, βίντεο, αρχεία

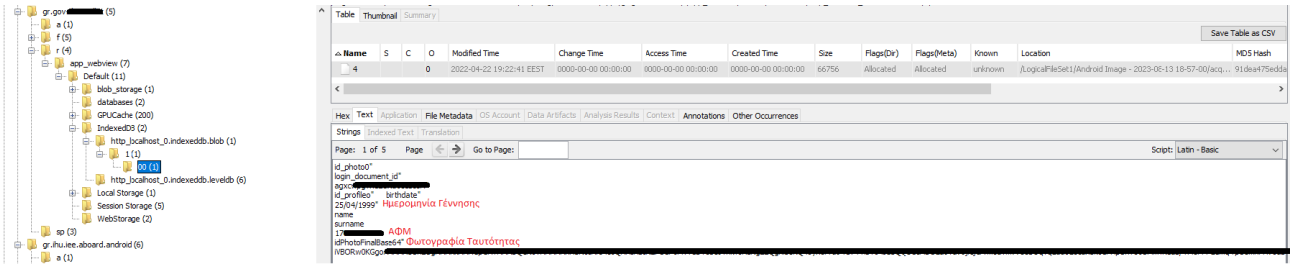
κειμένου και άλλα δεδομένα με σκοπό την περαιτέρω ανάλυση αξιοποιώντας τις δυνατότητες που προσφέρονται από το εργαλείο.

Με τη χρήση του εργαλείου Autopsy, πραγματοποιήθηκε μια εμπεριστατωμένη ανάλυση μιας εικόνας. Στόχος ήταν η ανίχνευση κρυφών δεδομένων και πληροφοριών σχετικά με την γεωγραφική τοποθεσία, την ακριβή ώρα και την ημέρα λήψης της, γεγονός που επιτεύχθηκε με τον φάκελο EXIF Metadata, ο οποίος περιείχε τις πληροφορίες που αφορούσαν τις συνθήκες λήψης της. Η εξαγωγή των μεταδεδομένων της εικόνας, περιλαμβανομένων των γεωγραφικών συντεταγμένων (GPS) και της χρονικής σφραγίδας αποδείχθηκε κρίσιμη για την εκτίμηση του χρονικού και γεωγραφικού πλαισίου στο οποίο διαδραματίστηκε μια πιθανή περίπτωση ψηφιακού εγκλήματος, και αποτέλεσε σημαντικό πεδίο ανάλυσης για την πορεία των ψηφιακών ερευνών. Εξήχθησαν σημαντικές πληροφορίες για το πλαίσιο και τις πιθανές συνθήκες που σχετίζονται με την φωτογραφία, συμβάλλοντας στην διερεύνηση και ίσως αποκάλυψη εγκληματικών δραστηριοτήτων.



Σχήμα 21 Γεωγραφικές συντεταγμένες λήψης

Στη συνέχεια, στο πλαίσιο της ανάλυσης αρχείων εφαρμογών, ανακαλύφθηκε μια σημαντική ένδειξη που αφορά τον εντοπισμό του Αριθμού Φορολογικού Μητρώου (ΑΦΜ) στις πληροφορίες που εξήχθησαν. Αυτός ο προσωπικός αριθμός, αποτελεί ζωτικής σημασίας πληροφορία για την ταυτοποίηση ενός προσώπου και εντοπίστηκε μέσα στα αρχεία των εφαρμογών. Το γεγονός αυτό επιφέρει διάφορα ερωτήματα σχετικά με τον τρόπο και τους λόγους που στοιχεία σαν το ΑΦΜ καταγράφονται και αποθηκεύονται σε εφαρμογές όπως αυτή.



Σχήμα 22 Ευρήματα αρχείων εφαρμογών

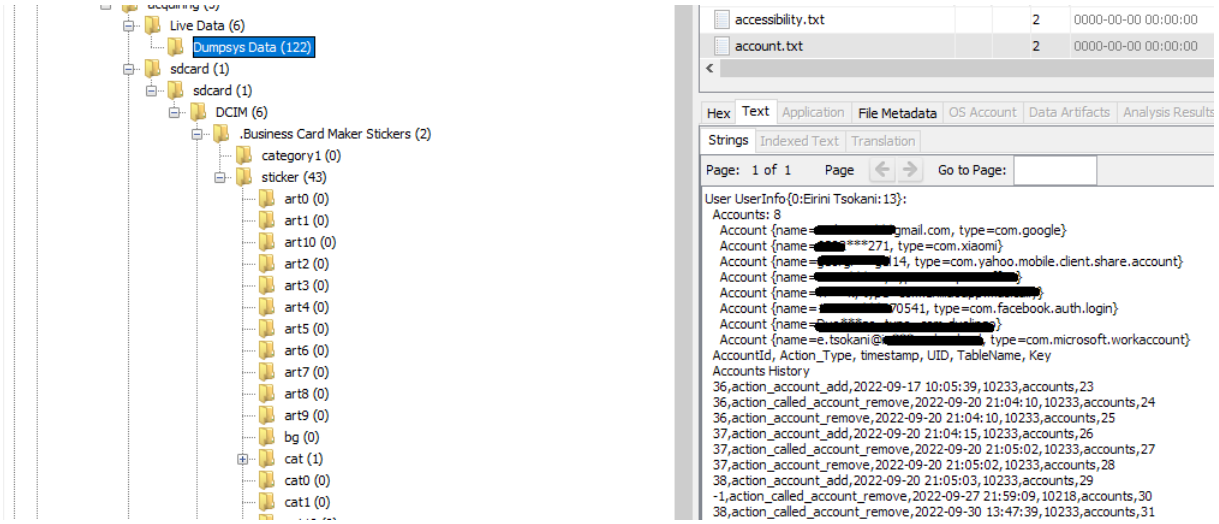
Με την ανακάλυψη αυτού του ευρήματος τίθενται πολλά ζητήματα για την ασφάλεια των προσωπικών δεδομένων. Είναι απαραίτητη η αξιολόγηση των πρακτικών που εφαρμόζονται σε εφαρμογές όπως και αυτή, που περιλαμβάνουν τέτοια ευαίσθητα δεδομένα. Επιπλέον, πρέπει να διερευνηθεί ο τρόπος διαχείρισης αυτης της πληροφορίας, καθώς επίσης και το ενδεχόμενο μη συγκατάθεσης για τη συλλογή και την αποθήκευσή της.

Αυτή η ενδιαφέρουσα πληροφορία που βρέθηκε υπογραμμίζει τη σημασία της ανάλυσης των αρχείων εφαρμογών μέσω εργαλείων ψηφιακής εγκληματολογίας όπως το Autopsy, καθώς μπορεί να φέρει στην επιφάνεια τέτοια ζητήματα που αφορούν την ιδιωτικότητα και την ασφάλεια των προσωπικών πληροφοριών των χρηστών.

Επίσης, δύο ακόμα σημαντικά ευρήματα που διακρίνονται στο απόκομμα, είναι η ημερομηνία γέννησης και η ύπαρξη ενός κρυπτογραφημένου κωδικού Base64. Κατόπιν αποκωδικοποίησης του κωδικού αυτού, αποκαλύπτεται η φωτογραφία της ταυτότητας που είχε εισαχθεί στην εφαρμογή. Η παρουσία αυτού του στοιχείου προδίδει την χρήση μιας μορφής κρυπτογράφησης από την εφαρμογη, που αποσκοπεί στην ασφαλή αποθήκευση των ευαίσθητων πληροφοριών.

Με την περαιτέρω διερεύνηση της λειτουργίας της εφαρμογής και του τρόπου που χρησιμοποιείται ο κωδικός base64, μπορούν να αναδειχθούν τα κίνητρα πίσω από αυτήν την επιλογή κρυπτογράφησης. Είναι επίσης δυνατόν να αναλυθεί η αλληλεπίδραση αυτού του ευρήματος με τις διαδικασίες προστασίας δεδομένων και ιδιωτικότητας που εφαρμόζει η εφαρμογή.

Συνεχίζοντας με την διαδικασία ανάλυσης των αρχείων της συσκευής με το εργαλείο Autopsy, ανακαλύφθηκε ένα αρχείο με την ονομασία "account.txt," το οποίο φαίνεται να περιέχει πληροφορίες σχετικά με τους λογαριασμούς email που έχουν προστεθεί στη συσκευή καθώς επίσης και ονόματα χρηστών. Παρόλο που η ακριβής φύση του αρχείου και η προέλευσή του δεν είναι γνωστή, αυτό το εύρημα μπορεί να διαδραματίσει σημαντικό ρόλο στην πορεία της ανάλυσης καθώς οι εγγραφές που περιλαμβάνονται φαίνεται να περιγράφουν δραστηριότητες που σχετίζονται με αυτούς τους λογαριασμούς. Ενδεχομένως, αυτό το αρχείο να αποτελεί μέρος μιας εφαρμογής επικοινωνίας, ή να είναι συνδεδεμένο με μια εφαρμογή που αποθηκεύει αυτές τις πληροφορίες για λόγους διαχείρισης και συγχρονισμού.



Σχήμα 23 Δεδομένα κράτησης, προσθήκης και αφαίρεσης λογαριασμών email

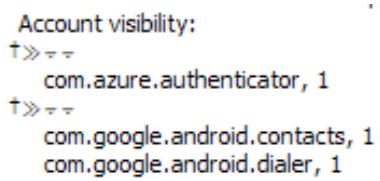
Σύμφωνα με τις πληροφορίες που παρέχονται στις εγγραφές, παρακάτω φαίνεται να έχουν καταγραφεί οι προσθήκες νέων λογαριασμών καθώς επίσης και ενέργειες που σχετίζονται με την κλήση για την αφαίρεση λογαριασμών. Τα αριθμητικά δεδομένα μετά τις ημερομηνίες φαίνονται να αναπαριστούν κωδικούς ή παραμέτρους σχετικά με τη διαχείριση των λογαριασμών.

Εξετάζοντας περαιτέρω το ίδιο αρχείο, εντοπίστηκαν παρακάτω κάποιες παράμετροι σχετικές με τις εφαρμογές και τους λογαριασμούς που έχουν εντοπιστεί στη συσκευή. Η παράμετρος που απεικονίζεται, δηλώνει την ύπαρξη υπηρεσιών που έχουν καταγραφεί, οι οποίες μπορεί να αναφέρονται σε διάφορες εφαρμογές και υπηρεσίες που έχουν εγκατασταθεί στο σύστημα. Η επιμέρους εξέταση αυτών των υπηρεσιών μπορεί να αποκαλύψει τη λειτουργία και τις πιθανές διασυνδέσεις τους με άλλες εφαρμογές και λειτουργίες της συσκευής.

```
-1,action_called_account_remove,2023-04-16 05:35:16,10218,accounts,18
4,action_called_account_remove,2023-04-20 11:24:14,10236,accounts,19
4,action_account_remove,2023-04-20 11:24:14,1000,accounts,20
49,action_authenticator_remove,2023-04-30 23:50:18,1000,accounts,21
-1,action_called_account_remove,2023-06-09 21:36:37,10218,accounts,22
Active Sessions: 0
RegisteredServicesCache: 15 services
  ServiceInfo: AuthenticatorDescription {type=com.google.android.gm.pop3}, ComponentInfo{com.google.android.gm/com.android.email.service.Pop3AuthenticatorService}, uid 10190
  ServiceInfo: AuthenticatorDescription {type=com.duolingo}, ComponentInfo{com.duolingo/com.duolingo.core.account.AccountService}, uid 10211
  ServiceInfo: AuthenticatorDescription {type=com.google}, ComponentInfo{com.google.android.gms/com.google.android.gms.auth.account.authenticator.GoogleAccountAuthenticatorService}, uid 10183
```

Σχήμα 24 Παράμετρος 1, καταγραφή υπηρεσιών

Η παρακάτω παράμετρος, αναφέρεται στην ορατότητα των λογαριασμών που ανακαλύφθηκαν από ορισμένες εφαρμογές με σκοπό την αυθεντικοποίηση κατά τη σύνδεσή τους.



Σχήμα 25 Παράμετρος 2, ορατότητα λογαριασμών

Φάση Εξέτασης

Κατά την ανάλυση της συσκευής με το εργαλείο Autopsy, ανακαλύφθηκαν σημαντικές πληροφορίες που διαδραμάτισαν καθοριστικό ρόλο για την πορεία της έρευνας και συνέβαλαν στην βαθύτερη κατανόηση της ψηφιακής δραστηριότητας.
Αρχικά, εντοπίστηκε μια φωτογραφία με ενσωματωμένα δεδομένα στον φάκελο μεταδεδομένων Exif, τα οποία παρέχουν πληροφορίες σχετικά με τη γεωγραφική τοποθεσία λήψης της φωτογραφίας. Οι αναλυτικές πληροφορίες για την ώρα, την ημερομηνία και τις γεωγραφικές συντεταγμένες της φωτογραφίας μπορούν να προσφέρουν σημαντικές ενδείξεις για το περιβάλλον της λήψης.
Στη συνέχεια, κατά την ανάλυση των αρχείων εφαρμογών, ανακαλύφθηκε μια εφαρμογή η οποία διαθέτει τον ΑΦΜ, την ημερομηνία γέννησης και μια κωδικοποιημένη φωτογραφία ταυτότητας. Η αποθήκευση της φωτογραφίας με χρήση κωδικοποίησης Base64 εγείρει ζητήματα ασφάλειας και απορρήτου. Η προσέγγιση αυτή μπορεί να επηρεάσει τον τρόπο με τον οποίο προστατεύονται τα προσωπικά δεδομένα των χρηστών και την ευαισθησία που δείχνει η εφαρμογή απέναντι σε αυτά.
Τέλος, ανακαλύφθηκε ένα αρχείο με την ονομασία 'account.txt', το οποίο περιείχε εγγραφές σχετικές με λογαριασμούς email και ονόματα χρηστών που έχουν προστεθεί σε εφαρμογές και υπηρεσίες. Οι εγγραφές αυτές περιλάμβαναν τις χρονοσφραγίδες (timestamps) των ενεργειών προσθήκης και αφαίρεσης λογαριασμών, καθώς και μοναδικά αναγνωριστικά. Κατα συνέπεια, αποκαλύπτουν πληροφορίες σχετικά με τις δραστηριότητες και τον τρόπο διαχείρισης των λογαριασμών.

Τα παραπάνω στοιχεία που ανακαλύφθηκαν κατά την ανάλυση είναι ζωτικής σημασίας για το ερευνητικό πλαίσιο και τον στόχο της παρούσας εργασίας. Η ανάλυση των δεδομένων από τη συσκευή και τις εφαρμογές της, παρείχε εμπεριστατωμένες πληροφορίες για την ψηφιακή δραστηριότητα και τα προσωπικά δεδομένα που περιέχονται στην συσκευή. Τα ευρήματα αυτά μπορούν να συμβάλουν στην κατανόηση του τρόπου διαχείρισης των προσωπικών δεδομένων απο τις ψηφιακές συσκευές και των μέτρων ασφαλείας που υιοθετούνται για την προστασία τους.

Ωστόσο, υπάρχουν σημαντικές επιπτώσεις τόσο για την ανάλυση της συγκεκριμένης συσκευής όσο και για την ευρύτερη κατανόηση της ψηφιακής ασφάλειας και των προκλήσεων που αντιμετωπίζονται σε αυτές. Η ανάλυση του εγγράφου που αφορά τη διαχείριση λογαριασμών αποκαλύπτει τις πρακτικές που ακολουθεί η συσκευή για τη διαχείριση προσωπικών πληροφοριών των χρηστών της. Η αποκάλυψη αυτών των δεδομένων παροτρύνει την περαιτέρω εξέταση των πρακτικών προστασίας της ιδιωτικότητας και της ασφάλειας των λογαριασμών.
Επιπλέον, η ανάλυση των μεταδεδομένων των εικόνων αναδεικνύει τη σημασία της γεωγραφικής τοποθεσίας και της χρονοσφραγίδας στην κατανόηση των δραστηριοτήτων των χρηστών. Αυτές οι πληροφορίες διευρύνουν το πλαίσιο της ανάλυσης και παρέχουν μια συσχέτιση των ψηφιακών δραστηριοτήτων με το περιβάλλον.
Συμπερασματικά, όλα αυτά τα ευρήματα αναδεικνύουν την σημαντικότητα της αντίληψης για τις διαδικασίες διαχείρισης προσωπικών δεδομένων. Η ανάλυση αυτή αποκαλύπτει την ανάγκη για βέλτιστες πρακτικές ασφάλειας και προστασίας των προσωπικών δεδομένων, καθώς και τη συνεχή εκπαίδευση για τους κινδύνους που απορρέουν από τη μη συμμόρφωση με αυτές.

Κεφάλαιο 7ο: Συμπεράσματα ή/και προτάσεις βελτίωσης

Η παρούσα πτυχιακή εργασία επικεντρώνεται στον πολυδιάστατο τομέα της ψηφιακής εγκληματολογίας. Η εκτεταμένη ψηφιακή δραστηριότητα και η εξέλιξη της τεχνολογίας έχουν φέρει στο προσκήνιο νέες προκλήσεις και απειλές για τον τομέα της κυβερνοασφάλειας, καθιστώντας αναγκαία την ανίχνευση και άμεση αντιμετώπιση των ψηφιακών εγκλημάτων. Στο πλαίσιο αυτό, καθίσταται επιτακτική η χρήση των εγκληματολογικών εργαλείων. Τα εργαλεία ανοιχτού κώδικα, έχουν αναδειχθεί ώς πολύτιμοι πόροι που προσφέρουν σύγχρονες πρακτικές διερεύνησης και ανάλυσης για τους ερευνητές της εγκληματολογίας, διασφαλίζοντας την ακεραιότητα και την ασφάλεια των ψηφιακών δεδομένων.
Η εργασία αναλύει εκτενώς τον ρόλο αυτών των εργαλείων και των τεχνικών ανίχνευσης και ανάλυσης των ψηφιακών αποδεικτικών στοιχείων. Από την εισαγωγή του ορισμού και της διαδικασίας ανάλυσης έως την ανάλυση των διαφόρων κλάδων της ψηφιακής εγκληματολογίας, προσφέρει μια σφαιρική επισκόπηση του πεδίου. Με αυτόν τον τρόπο, αναδεικνύονται οι ποικίλες προκλήσεις που αντιμετωπίζει κάθε κλάδος, και οι εξειδικευμένες μεθοδολογίες που αναπτύσσονται για την αντιμετώπισή τους. Επιπλεον, η ανάλυση των πλεονεκτημάτων και των περιορισμών των εργαλείων εμπορικού και ανοικτού κώδικα συμπληρώνεται από την διερεύνηση της ασφάλειας τους και των διαφόρων τύπων αδειών χρήσης.
Τέλος, ένα από τα σημαντικότερα κεφάλαια της εργασίας είναι η μελέτη περίπτωσης που αναδεικνύει τη συνολική διαδικασία ανάλυσης ψηφιακών δεδομένων κινητής συσκευής σε πραγματικό περιβάλλον. Μέσα από την περιγραφή της διαδικασίας, των εργαλείων και των αποτελεσμάτων, αναδεικνύεται πώς η φύση τους και η εφαρμογή της κατάλληλης μεθοδολογίας μπορούν να συντελέσουν στην επιτυχή αντιμετώπιση των προκλήσεων της ψηφιακής εγκληματολογίας.

Αναφορικά με τις προτάσεις βελτίωσης της εργασίας, προτείνονται προσεγγίσεις για την αξιοποίηση της τεχνητής νοημοσύνης με σκοπό την αποτελεσματικότερη αντιμετώπιση των ψηφιακών εγκλημάτων. Με την ενίσχυση των υπαρχόντων εγκληματολογικών και τεχνολογικών υποδομών και την υιοθέτηση των προηγμένων εργαλείων τεχνητής νοημοσύνης καθίσταται δυνατή η αυτοματοποίηση και επίσπευση της ανίχνευσης εγκληματικών δραστηριοτήτων.
Μια σημαντική πρόταση, αφορά τη διερεύνηση του τρόπου με τον οποίο η τεχνητή νοημοσύνη μπορεί να συνδυαστεί με την ανάλυση δεδομένων μεγάλου όγκου για την ανίχνευση πιθανών κυβερνοεπιθέσεων. Το γεγονός αυτό, θα μπορούσε συμβάλλει στην πρόληψη πιθανών απειλών και στην ανάπτυξη στρατηγικών για την αντιμετώπισή τους.
Μια ακόμα πρόταση που μπορεί να ενσωματωθεί στα πλαίσια της εργασίας αφορά την ανάλυση της ασφάλειας και της ιδιωτικότητας κατά τη διαδικασία ανίχνευσης προσώπων στις εγκληματολογικές έρευνες. Αυτά τα χαρακτηριστικά μπορούν να ενισχύσουν την αξιοπιστία της τεχνολογίας ενώ παράλληλα εξασφαλίζουν την προστασία των ατόμων. Παρόλο που η ανίχνευση προσώπων μέσω τεχνητής νοημοσύνης αποτελεί ισχυρό εργαλείο για την αντιμετώπιση εγκλημάτων, είναι σημαντικό να δοθεί προσοχή στα ζητήματα ασφάλειας και ιδιωτικότητας των δεδομένων. Πιο συγκεκριμένα, μια προσέγγιση που μπορεί να εξεταστεί είναι η εφαρμογή τεχνικών κρυπτογράφησης στα δεδομένα προσώπων πριν από την επεξεργασία τους. Η κρυπτογράφηση μπορεί να εξασφαλίσει ότι τα δεδομένα

παραμένουν ασφαλή κατά τη διάρκεια της μεταφοράς και της αποθήκευσης τους.
Τέλος, μια ενδιαφέρουσα πρόταση για περαιτέρω έρευνα με την τεχνητή νοημοσύνη είναι η διερεύνηση του τρόπου με τον οποίο μπορεί να εφαρμοστεί σε περιπτώσεις αυτοματοποιημένου εντοπισμού προσώπων με τη χρήση συγκεκριμένων παραμέτρων, όπως η ηλικία και το φύλο. Μια τέτοια προσέγγιση θα μπορούσε να προσφέρει εξειδίκευση στη διαδικασία ανίχνευσης προσώπων, προσαρμόζοντας την αναγνώριση στις απαιτήσεις διαφόρων περιβαλλόντων και εφαρμογών.

Η τεχνητή νοημοσύνη (AI) διαδραματίζει κρίσιμο ρόλο στον τομέα της ψηφιακής εγκληματολογίας ενισχύοντας την αποτελεσματικότητα των εγκληματολογικών μεθόδων ενώ παράλληλα βελτιστοποιεί τις πρακτικές ασφάλειας και προστατεύει την ακεραιότητα των ψηφιακών δεδομένων κατα τη διάρκεια των εγκληματολογικών ερευνών. Με τον αυξανόμενο όγκο και την πολυπλοκότητα των ψηφιακών δεδομένων, η ενσωμάτωση της στην ψηφιακή εγκληματολογία έχει καταστεί απαραίτητη. Στο πλαίσιο αυτό, προσφέρει μια γκάμα από εξειδικευμένα εργαλεία και τεχνικές που μπορούν να συμβάλλουν σημαντικά στον τρόπο με τον οποίο οι ερευνητές διαχειρίζονται τα ψηφιακά δεδομένα κατά τη συλλογή και ανάλυση τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

[7][95] Ευρωπαϊκή Επιτροπή (Erasmus+), ec.europa.eu,“FORC BOOK 5”, Επίσκεψη 20/05/2023

[24]Ευρωπαϊκή Επιτροπή (Erasmus+), ec.europa.eu, ”Emerging Trends and Special Topics in Digital Forensics” FORC BOOK 8, Επισκεψη 20/05/2023

[11]Nihad Ahmad Hassan, Rami Hijazi, “Data Hiding Techniques in Windows OS”, Chapter 7 - Antiforensic Techniques, 2017, Επίσκεψη 16/06/2023

[12]Leighton R. Johnson III, “Computer Incident Response and Forensics Team Management”, Section 14 - Forensics Tools, 2014, Επίσκεψη 4/06/2023

[13]James O. Holley, Paul H. Luehr, Jessica Reust Smith, Joseph J. Schwerha IV, “Handbook of Digital Forensics and Investigation, Chapter 3 - Electronic Discovery, 2010,Επίσκεψη 7/06/2023

[27]Ammar Alazab, Ansam Khraisat and Sarabjot Singh,”A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools | IntechOpen, February, 2023,Επίσκεψη 14/06/2023

[30]Sasa Mrdovic, “Security of Ubiquitous Computing Systems”, 2021,Επίσκεψη 28/06/2023

[46]Aishwarya Mahale, “Digital Forensics with Open Source Tools”,Επίσκεψη 7/07/2023

Internet Site

[1] Blue Voyant, “Understanding Digital Forensics: Process, Techniques, and Tools”, Available: https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools ,Επίσκεψη 17/05/2023

[2]Altlaw,“How does forensic data collection work?”, March 2023.[Online]. Available:https://www.altlaw.co.uk/blog/how-does-forensic-data-collection-work,Επίσκεψη 1705/2023

[3] Tech Target, “What is Computer Forensics (Cyber Forensics)?”, Ben Lutkevich, May 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/computer-forensics, Επίσκεψη 17/05/2023

[4]Recfaces,”What Is Digital Forensics: Process, Tools, and Types | Computer ForensicsOverview”, January 2021.[Online]. Available:https://recfaces.com/articles/digital-forensics, Επίσκεψη 17/05/2023

[5]ERMProtect, “What Are the 5 Stages of a Digital Forensics Investigation? - Cybersecurity | Digital Forensics | Crypto Investigations”, August 2022. [Online]. Available:https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/, Επίσκεψη 22/05/2023

[9]tutorialspoint, ”What are the techniques of Steganalysis”, Ginni, March 2022. [Online] Available:https://www.tutorialspoint.com/what-are-the-techniques-of-steganalysis, Επίσκεψη 23/07/2023

[18]Niagara Networks, “ Explain Network TAP Vs. SPAN Port”, Available:https://www.niagaranetworks.com/solutions/tap-versus-span, Επίσκεψη 17/07/2023

[21]Idera, “Database Forensics”, Available:https://www.idera.com/glossary/database-forensics/, Επίσκεψη 3/06/2023

[32]Digital Evidence - ANZPAA Website, Available:https://www.anzpaa.org.au/forensic-science-2/forensic-sciences/forensic-science-disciplines/digital-evidence, Επίσκεψη 14/07/2023

[36]O’Reilly, Samir Datt, “Collecting network traffic using tcpdump”, Available:https://www.oreilly.com/library/view/learning-network-forensics/9781782174905/ch02s03.html, Επίσκεψη 16/07/2023

[37]”Collecting network traffic using tcpdump”, Available:https://subscription.packtpub.com/book/security/9781782174905/2/ch02lvl1sec20/collecting-network-traffic-using-tcpdump, Επίσκεψη 11/06/2023

[91]SecurityOnion,“NetworkMiner”, Available:https://docs.securityonion.net/en/2.3/networkminer.html, Επίσκεψη 29/07/2023

[92]Ricardo Gerardi, opensource.com, “An introduction to using tcpdump at the Linux command line”, September 1, 2020. Available:https://opensource.com/article/18/10/introduction-tcpdump, Επίσκεψη 29/07/2023

[38]CompTIA, “What Is Wireshark and How Is It Used?”, Available:https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it, Επίσκεψη 5/07/2023

[39]FORTINET, “SNORT—Network Intrusion Detection and Prevention System”, Available:https://www.fortinet.com/resources/cyberglossary/snort, Επίσκεψη 7/07/2023

[40]QA Cafe, “New ways to analyze network traffic with Suricata”, Available:https://www.qacafe.com/resources/new-ways-to-analyze-network-traffic-with-suricata/, Επίσκεψη 11/07/2023

[44]Mishal Roomi May 12, 2021, “6 Advantages and Disadvantages of Open Source Software | Drawbacks & Benefits of Open Source Software”, Available:https://www.hitechwhizz.com/2021/05/6-advantages-and-disadvantages-drawbacks-benefits-of-open-source-software.html, Επίσκεψη 29/05/2023

[47]Mishal Roomi May 12, 2021, “6 Advantages and Disadvantages of Open Source Software | Drawbacks & Benefits of Open Source Software”, Available:https://www.hitechwhizz.com/2021/05/6-advantages-and-disadvantages-drawbacks-benefits-of-open-source-software.html, Επίσκεψη 27/06/2023

[48]Snyk, ”Open Source Security Explained”, Available:https://snyk.io/series/open-source-security/, Επίσκεψη 13/07/2023

[49]Snyk, “5 potential risks of open source software” Available:https://snyk.io/learn/risks-of-open-source-software/, Επίσκεψη 6/06/2023

[51]ADAM MURRAY,mend.io, JANUARY 19, 2023, “Top Open Source Licenses Explained” Available:https://www.mend.io/blog/top-open-source-licenses-explained/, Επίσκεψη 23/07/2023

[52]ADAM MURRAY,mend.io OCTOBER 24, 2020, “Open Source Copyleft Licenses: All You Need to Know”, Available:https://www.mend.io/blog/open-source-copyleft-licenses/, Επίσκεψη 2/07/2023

[53]ADAM MURRAY,mend.io JUNE 8, 2023, “The Top 10 Questions about the GPL License – Answered!”, Available:https://www.mend.io/blog/top-10-gpl-license-questions-answered/ , Επίσκεψη 2/07/2023

[55]RAMI SASS,mend.io, SEPTEMBER 3, 2020, “Top 10 Microsoft Public License (Ms-PL) Questions Answered”, Available:https://www.mend.io/blog/top-10-microsoft-public-license-ms-pl-questions-answered/, Επίσκεψη 2/07/2023

[56]Blue Voyant, “Digital Forensics: Get Started with These 9 Open Source Tools”, Available:https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools ,Επίσκεψη 16/06/2023

[57] sleuthkit | Kali Linux Tools, Available:https://www.kali.org/tools/sleuthkit/, Επίσκεψη 27/06/2023

[59]Brian Carrier, ”The Sleuth Kit: File and Volume System Analysis”, Available:http://www.sleuthkit.org/sleuthkit/desc.php, Επίσκεψη 27/06/2023

[61]”Introduction To Autopsy | An Open-Source Digital Forensics Tool - CYBERVIE”, Availabl:https://www.cybervie.com/blog/introduction-to-autopsy-an-open-source-digital-forensics-tool./ Επίσκεψη23/07/2023

[62] ”Autopsy”, Available:http://sleuthkit.org/ , Επίσκεψη 2/06/2023

[63]”CAINE Live USB/DVD - computer forensics digital forensics”, Available:https://www.caine-live.net/, Επίσκεψη 2/06/2023

[66]”Volatility | Popular and Open Source Memory Forensics Tool”, Available:https://products.containerize.com/digital-forensic-software/volatility/, Επίσκεψη 2/06/2023

[72] forensiccomputers, “FTK Imager”, Available: https://www.forensiccomputers.com/ftk-imager ,Επίσκεψη 2/06/2023

[73]subscription.packtpub, Digital Forensics and Incident Response - Second Edition, ”Wireshark”, Available:https://subscription.packtpub.com/book/security/9781838649005/6/ch06lvl1sec32/wireshark , Επίσκεψη 2/06/2023

[74]https://forensicyard.com/wireshark-in-forensics/ , Επίσκεψη 2/06/2023

[75]Top 20 Computer (Digital) Forensics Tools - Startup Stash, October 3, 2022, Available:https://startupstash.com/computer-digital-forensics-tools/ ,Επίσκεψη 10/06/2023

[77]”Mobile Forensics and Its Challanges”, Available:https://hub.packtpub.com/mobile-forensics-and-its-challanges/, Επίσκεψη 11/06/2023

[83]Scientific Working Group on Digital Evidence,”Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition”, September 2020. Available: https://drive.google.com/file/d/1sVko_Uo7o6iootWwn9IoLJ3mrMVXqTDg/view, Επίσκεψη 12/07/2023

[85]James Eichbaum, September, 2019, “Five continual challenges with smartphone forensics” Available:https://www.msab.com/blog/five-continual-challenges-with-smartphone-forensics/, Επίσκεψη 25/07/2023

Paper in Conference Proceedings

[93]J. Buric; D. Delija, “Challenges in network forensics” IEEE 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015, Επίσκεψη 13/08/2023

[94] Ahmad Almulhem,” Network Forensics: Notions and Challenges”, Signal Processing and Information Technology (ISSPIT), 2009 IEEE, Επίσκεψη 13/08/2023

[8] H. A. Nimr, “Defuzzification of the outputs of fuzzy controllers,” presented at 5th International Conference on Fuzzy Systems, Cairo, Egypt, 2006., Επίσκεψη 29/05/2023

[23]Arafat Mohammed Rashad Al- Dhaqm,Siti Hajar Othman,Shukor Abd Razak,Asri Ngadi, “Towards adapting metamodelling technique for database forensics investigation domain”, 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Επίσκεψη 11/06/2023

[25] Syed Ahmed Ali,Shahzad Memon,Farhan Sahito”Challenges and Solutions in Cloud Forensics”, 2018 2nd International Conference, Επίσκεψη 1/07/2023

[31]Ahmed Alenezi,Hany F. Atlam,Reem Alsagri,Madini O. Alassafi, “IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions”, May 2019, The 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), Επίσκεψη 13/07/2023

[42]Josiah Dykstra and Alan Sherman, “Design and Implementation of FROST - Digital Forensic

Tools for the OpenStack Cloud Computing Platform”, The Digital Forensic Research Conference

DFRWS 2013 USA, Επίσκεψη 19/07/2023

Posts

[6]Ramya Mohanakrishnan,”Digital Forensics Meaning and Importance”,Spiceworks, July 2022. Available:https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-digital-forensics/ ,Επίσκεψη 17/05/2023

[10]SalvationData, “Email Forensics - Definition and Guideline” September 2022. Available:https://www.salvationdata.com/knowledge/email-forensics-definition-and-guideline/ ,Επίσκεψη 22/05/2023

[14]”What is Network Forensics?”, March 2022. Available : https://www.geeksforgeeks.org/what-is-network-forensics/ ,Επίσκεψη 29/05/2023

[17]Vehere, “Network Forensics: Concepts and Challenges”, August 2021. Available:https://vehereinteractivepvtltd.medium.com/network-forensics-concepts-and-challenges-7be2a3eb4f3d ,Επίσκεψη 29/05/2023

[19]SalvationData, “What is Database Forensics?”, May 2022. Available:https://www.salvationdata.com/knowledge/what-is-database-forensics/ ,Επίσκεψη 19/06/2023

[26]0xffccdd, Medium, “Cloud Forensics Tools” December 2022, Available:https://medium.com/@cloud_tips/cloud-forensics-tools-4beed278ea5e, Επίσκεψη 27/06/2023

[29]Praveen, “Understanding the Meaning and Purpose of IoT Forensics”, June 2022, Available:https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/understanding-meaning-purpose-iot-forensics/, Επίσκεψη 27/06/2023

[33]rashi_garg, “Recovering Deleted Digital Evidence”, August 2022. Available:https://www.geeksforgeeks.org/recovering-deleted-digital-evidence/, Επίσκεψη 6/07/2023

[41]”7 Best Database Forensics Software Tools [Recover Deleted] – TickTechTold”, May 2023, Available:https://www.ticktechtold.com/best-database-forensics-tool/, Επίσκεψη 4/07/2023

[45]Satyabrata_Jena, “Difference between Open source Software and Commercial Software”, March 2023.
Available:https://www.geeksforgeeks.org/difference-between-open-source-software-and-commercial-software/, Επίσκεψη 10/07/2023

[58]Brian Carrier, “The Sleuth Kit – analyze disk images and recover files”, Last Updated on July 13, 2021, Available:https://www.linuxlinks.com/thesleuthkit/, Επίσκεψη 16/07/2023

[64]rashi_garg,”CAINE Forensic Environment”, Last Updated : 02 Jun, 2020, Available:https://www.geeksforgeeks.org/caine-forensic-environment/, Επίσκεψη 28/07/2023

[67]Neil Fox, April 12, 2022, “How to Use Volatility for Memory Forensics and Analysis”, Available:https://www.varonis.com/blog/how-to-use-volatility, Επίσκεψη 25/07/2023

[68]Yumna Fatima, October 21, 2022, “Volatility Tool – Working & Usage”, Available:https://www.onworks.net/blog/volatility-tool-working-usage/, Επίσκεψη 27/07/2023

[70]Claudio Dodt, July 7, 2019,” Computer forensics: FTK forensic toolkit overview [updated 2019]” Available:
https://resources.infosecinstitute.com/topic/computer-forensics-ftk-forensic-toolkit-overview/
,Επίσκεψη 2/06/2023

[71]zhohadamani, Last Updated : 05 Sep, 2022, “How to Create a Forensic Image with FTK Imager?”, Available:https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/, Επίσκεψη 3/8/2023

[76]”The Top 20 Open Source Digital Forensic Tools for 2023”, December 2022, Available:https://www.salvationdata.com/work-tips/the-top-20-open-source-digital-forensic-tools-for-2023/, Επίσκεψη 3/08/2023

[80]Dimitar Kostadinov, July 2019, “The mobile forensics process: steps and types”, Available:https://resources.infosecinstitute.com/topics/digital-forensics/mobile-forensics-process-steps-types/, Επίσκεψη 1/08/2023

[81]”Mobile Device Forensics: Challenges, Threats, & Solutions”, November 2022, Available:https://securityscorecard.com/blog/mobile-device-forensics/, Επίσκεψη 1/08/2023

[86]Fakhar Imam, July 7, 2019, “Common mobile forensics tools and techniques”, Available:https://resources.infosecinstitute.com/topics/digital-forensics/common-mobile-forensics-tools-techniques/, Επίσκεψη 6/08/2023

[89]Usama Azad, 2020, “Oxygen Forensic Suite in-depth tutorial”, Available:https://linuxhint.com/oxygen_forensics_suite_guideline/, Επίσκεψη 6/08/2023

Επιστημονικά Άρθρα

[16]Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi “A Generic Framework for Network Forensics”, 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 11, Επίσκεψη 11/06/2023

[22]Arafat Al-Dhaqm,, Shukor Abd Razak, Siti Hajar Othman, Asri Nagdi, Abdulalem Ali, “A GENERIC DATABASE FORENSIC INVESTIGATION PROCESS MODEL”Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Επίσκεψη 25/06/2023

[28]Hany F. Atlam , Ezz El-Din Hemdan , Ahmed Alenezi , Madini O. Alassafi , Gary B. Wills, “Internet of Things”Volume 11, September 2020, Επίσκεψη 22/06/2023

[34] Nicklas Lundblad,”Digital Evidence”, Επίσκεψη 4/07/2023

[35]Nik Khidzir, “Towards Fact-Based Digital Forensic Evidence Collection Methodology”, 2019, International Journal for Information Security Research, Επίσκεψη 4/07/2023

[90]Sandesh Achar, “CLOUD COMPUTING FORENSICS”, September 2022INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY, Επίσκεψη 22/07/2023

[43]Asia ALJAHDALI, Hanan ALDISSI, Shoroq BANAFEE, Sundos SOBAHI, Wafaa NAGRO, “IoT Forensic models analysis” , Romanian Journal of Information Technology and Automatic Control, Vol. 31, No. 2, 21-34, 2021, Επίσκεψη 5/07/2023

[60]Brandon Alexander, “Evaluation of Open-Source & Proprietary Forensic Software Tools”,December 2022, Επίσκεψη 22/06/2023

[79]G Maria Jones and S Godfrey Winster, “Forensics Analysis On Smart Phones Using Mobile

Forensics Tools”, International Journal of Computational Intelligence Research

ISSN 0973-1873 Volume 13, Number 8 (2017), pp. 1859-1869, Επίσκεψη 13/07/2023

[82]Konstantinos Georgokitsos, “Mobile Device Forensics: Guidelines, Analysis and Tools”, Επίσκεψη 25/06/2023

[84]Bhoopesh Kumar Sharma, Vipin Yadav, Mandeep Kaur Purba, Yogesh Sharma, “Challenges, Tools, and Future of Mobile Phone Forensics”, May 2022, Επίσκεψη 25/06/2023

[87]Rizwan Ahmed and Rajiv V. Dharaskar, “Mobile Forensics: an Overview, Tools, Future trends

and Challenges from Law Enforcement perspective”, Επίσκεψη4/07/2023

Εκπαιδευτικές Σελίδες

[20]Wikipedia, “Database forensics”, December 2022. Available:https://en.wikipedia.org/wiki/Database_forensics., Επίσκεψη 14/06/2023

[8]Wikipedia,”Steganalysis”, February 2023.Available:https://en.wikipedia.org/wiki/Steganalysis ,Επίσκεψη 04/07/2023

[15]Wikipedia,“Network forensics”,September 2022. Available:https://en.wikipedia.org/wiki/Network_forensics ,Επίσκεψη 22/05/2023

[50]Wikipedia, “Open-source license”,last edited July 2023, Available:https://en.wikipedia.org/wiki/Open-source_license,Επίσκεψη 5/08/2023

[54]Wikipedia, “Apache License”, last edited Agust 2023, Available:https://en.wikipedia.org/wiki/Apache_License,Επίσκεψη 5/08/2023

[65]Wikipedia, “CAINE Linux”, last edited on 21 July 2023,Available:https://en.wikipedia.org/wiki/CAINE_Linux,Επίσκεψη 5/08/2023

[69]Wikipedia, “Forensic Toolkit”, last edited on 21 July 2023, Available:https://en.wikipedia.org/wiki/Forensic_Toolkit, Επίσκεψη 5/08/2023

[78]Wikipedia,”Mobile device forensics”, last edited on 3 May 2023, Available:https://en.wikipedia.org/wiki/Mobile_device_forensics, Επίσκεψη 5/06/2023

[88] Wikipedia: “XRY (software)”, last edited on 14 May 2023, Available:https://en.wikipedia.org/wiki/XRY_(software), Επίσκεψη 12/06/2023

Εικόνες

Σχήμα 1: Digital Forensics https://www.linkedin.com/pulse/how-properly-investigate-digital-devices-jaevon-george, Επίσκεψη 18/08/2023

Σχήμα 2:Λογότυπο Copyleft αδειών https://en.wikipedia.org/wiki/Copyleft, Επίσκεψη 18/08/2023

Σχήμα 3 GNU License https://ipkitten.blogspot.com/2019/01/gpl-cooperation-commitment-promise-of.html, Επίσκεψη 18/08/2023

Σχήμα 4: Apache License https://en.wikipedia.org/wiki/Apache_License, Επίσκεψη 18/08/2023

Σχήμα 5: Microsoft Public Licenses (Ms-PL) https://firebearstudio.com/blog/open-source-license-guide.html, Επίσκεψη 18/08/2023

Σχήμα 6: Autopsy Tool https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d, Επίσκεψη 18/08/2023

Σχήμα 7: Caine Tool https://nannib.wordpress.com/caine-forensic-live-distro/, Επίσκεψη 18/08/2023

Σχήμα 8: Volatility Tool https://www.osforensics.com/tools/volatility-workbench.html, Επίσκεψη 18/08/2023

Σχήμα 9: FTK Tool https://eforensicsmag.com/how-to-investigate-files-with-ftk-imager/, Επίσκεψη 18/08/2023

Σχήμα 10: Wireshark Tool https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html, Επίσκεψη 18/08/2023

Σχήμα 11 Τσάντες Faraday https://faradaybag.com/, Επίσκεψη 18/08/2023

Σχήμα 12 Μέθοδοι απόκτησης δεδομένων https://privacyinternational.org/long-read/3256/technical-look-phone-extraction , Επίσκεψη 18/08/2023