



ΔΗΜΟΚΡΙΤΕΙΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΘΡΑΚΗΣ

DEMOCRITUS  
UNIVERSITY  
OF THRACE

**Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας**  
**Κατεύθυνση Τεχνολογία και Συστήματα Πληροφοριών**  
**Εργαστήριο Ηλεκτρονικής Εγκληματολογίας και Διαχείρισης**  
**Ψηφιακών Δεδομένων**

**Ιχνηλάτηση δραστηριοτήτων χρήστη χρησιμοποιώντας το μητρώο των windows**

**(Tracking user activities using the windows registry)**

**Υπεύθυνος διδάσκων: Δρ. Μαρδύρης Βασίλειος**

**Γεώργιος Καλπακίδης**

**[geklpa@mst.ihu.gr](mailto:geklpa@mst.ihu.gr)**

**Καβάλα 2024**

## ΠΕΡΙΛΗΨΗ

Το Microsoft Windows εδώ και πολλά χρόνια πρόκειται για το πιο διαδεδομένο και χρησιμοποιούμενο λειτουργικό σύστημα. Το εύχρηστο και όμορφο περιβάλλον, το σχετικά χαμηλό κόστος, οι δυνατότητες παραμετροποίησης καθώς και το γεγονός ότι έρχεται προ εγκατεστημένο σε αρκετά συστήματα, αποτελούν καθοριστικοί παράγοντες για τους χρήστες που επιλέγουν το συγκεκριμένο λειτουργικό. Η αυξημένη χρήση των windows όμως αποτελεί πρόβλημα για τους ειδικούς της κυβερνοασφάλειας και της ψηφιακής εγκληματολογίας. Εφόσον οι περισσότεροι χρήστες χρησιμοποιούν τα windows, είναι αναμενόμενο ένας μεγάλος αριθμός εγκλημάτων να σχετίζεται με το συγκεκριμένο λειτουργικό. Με αφορμή τον αυξημένο αριθμό ψηφιακών εγκλημάτων, από και προς το windows OS, σκοπός της συγκεκριμένης εργασίας είναι η περιγραφή της διαδικασίας ιχνηλάτησης δραστηριοτήτων σε ένα σύστημα windows χρησιμοποιώντας το windows registry. Πιο συγκεκριμένα, θα πραγματοποιηθεί λεπτομερής ανάλυση του windows registry forensics, θα μελετηθεί η σχετική βιβλιογραφία και τέλος θα εφαρμοστεί μια μεθοδολογία από αυτές που μελετήθηκαν στην σχετική βιβλιογραφία.

## Λέξεις κλειδιά

Ψηφιακή εγκληματολογία, Μητρώο windows, Ιχνηλάτηση δραστηριοτήτων, Λογισμικά εργαλεία

## **ABSTRACT**

For many years, Microsoft Windows has been the most widespread and widely used operating system. Its user-friendly and aesthetically pleasing environment, relatively low cost, customization capabilities, and the fact that it comes pre-installed on many systems are some factors for which users choose this particular operating system. However, the increased use of Windows poses a problem for experts in cybersecurity and digital forensics. Since most users use Windows, it is expected that a large number of crimes will be related to this operating system. Given the increased number of digital crimes involving the Windows OS, the purpose of this work is to describe the process of tracking activities on a Windows system using the Windows Registry. More specifically, a detailed analysis of Windows Registry forensics will be conducted, relevant literature review will be studied, and a methodology will be proposed.

## **Keywords**

Digital forensics, Windows registry, Activity tracking, Software tools

## Περιεχόμενα

Περίληψη	2
Abstract	3
Κατάλογος Συντομογραφιών	5
Κατάλογος Εικόνων	6
1. Εισαγωγή	7
2. Ιστορικό (Background)	8
2.1 Registry Forensics	8
2.2 Πρόσβαση στο registry και διαθέσιμα εργαλεία	11
2.3 Δυσκολίες έρευνας στο registry	12
3. Επισκόπηση Βιβλιογραφίας (Literature Review)	14
4. Ανάπτυξη Συγκεκριμένου Πεδίου	17
5. Μελέτη Περίπτωσης (Use Case)	18
6. Συμπεράσματα	22
Προτάσεις για περαιτέρω έρευνα (Future Work)	22
Βιβλιογραφία	23

## **ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ**

OS – Operating System

SAM – Security Accounts Manager

ASEPs – Auto Start Extension Points

CPU – Central Processing Unit

HDFS – Hadoop Distributed File System

USB – Universal Serial Bus

SID – Security Identifier

RegEx – Regular Expression

VM – Virtual Machine

GUI – Graphical User Interface

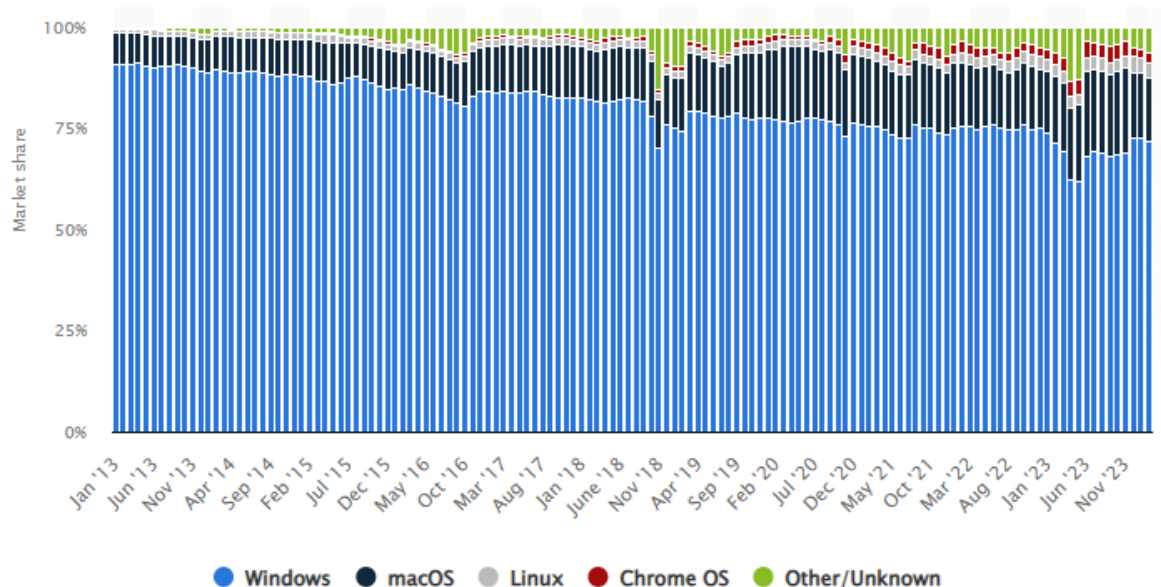
## ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Μερίδιο αγοράς λειτουργικών συστημάτων υπολογιστών	7
Εικόνα 2: Αναπαράσταση του registry	8
Εικόνα 3: Snapshot πριν την εγκατάσταση της εφαρμογής	18
Εικόνα 4: Snapshot μετά την εγκατάσταση της εφαρμογής	19
Εικόνα 5: Σύγκριση των δυο snapshot	19
Εικόνα 6: Περιεχόμενο του .txt αρχείου μετά την εγκατάσταση	20
Εικόνα 7: Περιεχόμενο του .txt αρχείου μετά την απεγκατάσταση	21

## 1 - ΕΙΣΑΓΩΓΗ

Έπειτα από έρευνα που πραγματοποίησε η Statista, το κυρίαρχο λειτουργικό σύστημα υπολογιστών είναι το Microsoft Windows με μερίδιο αγοράς 72% τον Φεβρουάριο του 2024. Αμέσως μετά ακολουθεί το λειτουργικό macOS της Apple με 15% ενώ στην τρίτη θέση βρίσκεται το Linux με 4% [1]. Όπως γίνεται κατανοητό, οι περισσότεροι χρήστες χρησιμοποιούν windows με αποτέλεσμα τα περισσότερα ψηφιακά εγκλήματα να σχετίζονται με το συγκεκριμένο λειτουργικό. Ο αυξημένος αριθμός χρηστών σε συνδυασμό με την συνεχή ανάπτυξη των windows αποτελεί σημαντικό πρόβλημα για τους ειδικούς της κυβερνοασφάλειας και της ψηφιακής εγκληματολογίας, με αποτέλεσμα αυτοί να χρήζουν συνεχή ενημέρωση και κατάλληλη εκπαίδευση. Σκοπός της συγκεκριμένης εργασίας είναι η περιγραφή της διαδικασίας ιχνηλάτησης δραστηριοτήτων του χρήστη σε ένα σύστημα windows χρησιμοποιώντας το windows registry. Πιο συγκεκριμένα, στο κεφάλαιο 2 θα πραγματοποιηθεί λεπτομερής ανάλυση του υποκλάδου registry forensics και θα μελετηθεί το windows registry, τα διαθέσιμα λογισμικά εργαλεία και το μείζων πρόβλημα που επικρατεί κατά την διάρκεια μιας ψηφιακής εγκληματολογικής έρευνας αυτού του υποκλάδου. Στο κεφάλαιο 3 θα μελετηθεί η σχετική βιβλιογραφία ενώ στο κεφάλαιο 4 θα μελετηθεί λεπτομερέστερα μια από τις εργασίες της σχετικής βιβλιογραφίας. Τέλος, στο πέμπτο κεφάλαιο θα προταθεί μια μεθοδολογία η οποία σχετίζεται με αυτή που αναλύθηκε στο κεφάλαιο 4.

Εικόνα 1: Μερίδιο αγοράς λειτουργικών συστημάτων υπολογιστών



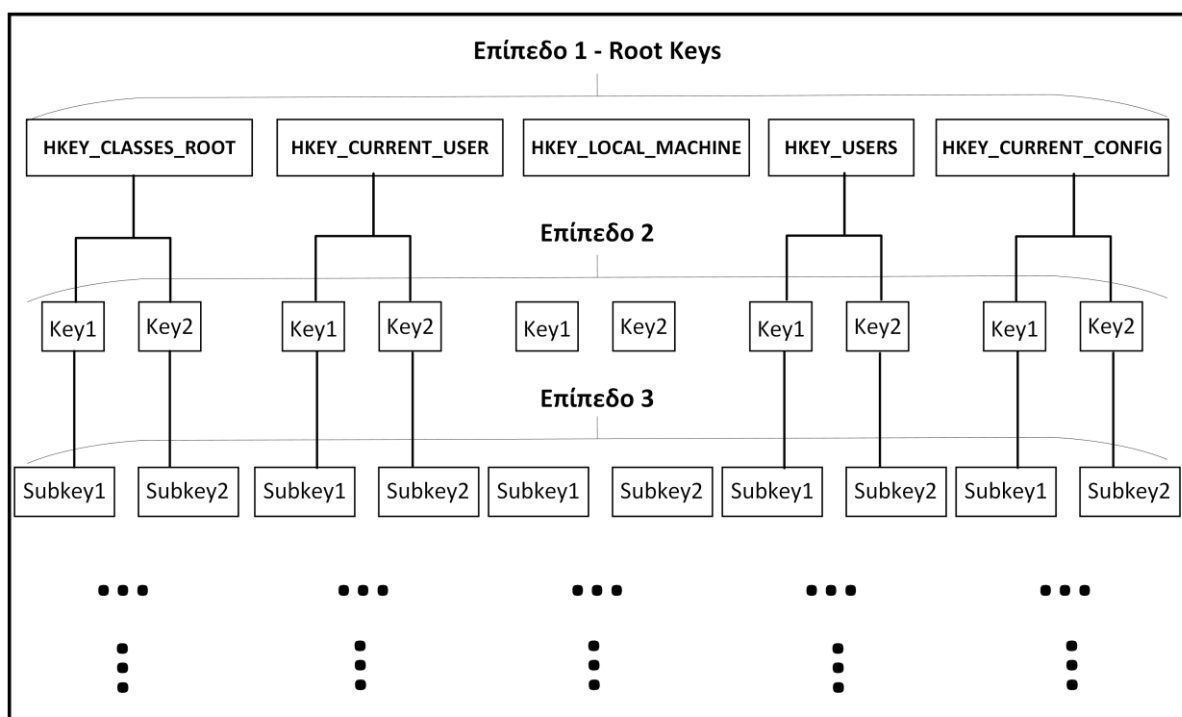
## 2 - ΙΣΤΟΡΙΚΟ (BACKGROUND)

### 2.1 Registry Forensics

Σύμφωνα με το computer dictionary της Microsoft, το windows registry πρόκειται για μια κεντρική ιεραρχική βάση δεδομένων, η οποία χρησιμοποιείται στα λειτουργικά συστήματα της για την αποθήκευση πληροφορίας, η οποία είναι απαραίτητη για την διαμόρφωση του συστήματος. Λεπτομερέστερα, στο registry εμπεριέχονται πληροφορίες σχετικά με το υλικό (hardware) στο οποίο βασίζεται το σύστημα, τις θύρες που χρησιμοποιούνται, τα προφίλ των χρηστών, τις εγκατεστημένες εφαρμογές και γενικά όλες τις ρυθμίσεις του συστήματος. Κατά την διάρκεια λειτουργίας, το λειτουργικό σύστημα συμβουλεύεται συνεχώς το registry για την ομαλή λειτουργία του συστήματος [2, 3]. Όπως γίνεται κατανοητό, το registry αποτελεί μια εξαιρετική πηγή αποδεικτικών στοιχείων με αποτέλεσμα ο υποκλάδος registry forensics να είναι πολύ σημαντικός.

Η δομή του windows registry είναι δενδροειδής (tree structured). Υπάρχουν δηλαδή πολλά επίπεδα και το πρώτο επίπεδο αποτελείται από πέντε βασικές εγγραφές, οι οποίες αποτελούν τα root keys [2, 3]. Μια πρόχειρη αναπαράσταση του registry, με τα πέντε root keys και τα υπόλοιπα επίπεδα παρουσιάζεται στο σχήμα 1.

Εικόνα 2: Αναπαράσταση του registry



Τα root keys αποτελούν κυψέλες (hives) του registry και αποκαλούνται έτσι γιατί μέσα σε αυτά εμπεριέχονται άλλα κλειδιά (keys), υποκλειδιά (subkeys) και τιμές (values).



Ένα κλειδί που αποτελεί hive, στην αρχή του ονόματος του υπάρχει το “HKEY” και το συνολικό μήκος του ονόματος μπορεί να είναι ως 255 χαρακτήρες. [2, 3]. Όσον αφορά το μήκος του ονόματος μιας τιμής (value name) και το βάθος του registry (registry tree depth) αυτά είναι 16.383 χαρακτήρες και 512 επίπεδα, αντίστοιχα [2, 4]. Παρακάτω πραγματοποιείται ανάλυση του κάθε hive.

## **HKEY\_CURRENT\_USER**

Η συντομογραφία του συγκεκριμένου key είναι HKCU και σε αυτό περιέχονται πληροφορίες διαμόρφωσης του τρέχοντος συνδεδεμένου χρήστη, όπως για παράδειγμα οι φάκελοι, τα χρώματα οθόνης, η ταπετσαρία (wallpaper) της επιφάνειας εργασίας, οι ρυθμίσεις οθόνης και οι ρυθμίσεις του πίνακα ελέγχου. Το HKCU αποτελεί subkey του HKU [2]. Από την στιγμή που το συγκεκριμένο hive διατηρεί πληροφορίες ενός συγκεκριμένου χρήστη και οι οποίες διαφέρουν ανάλογα τον χρήστη, το HKCU αποτελεί ένα τοπικό (local) key. Αντιθέτως, τα υπόλοιπα hive αποτελούν καθολικά (public) keys καθώς οι πληροφορίες παραμένουν ίδιες ανεξαρτήτως χρήστη [3].

## **HKEY\_USERS**

Η συντομογραφία του συγκεκριμένου key είναι HKU και σε αυτό περιέχονται πληροφορίες σχετικά με τα ενεργά προφίλ των χρηστών του συστήματος. Το HKU αποτελεί κλειδί του HKCU [2]. Κάθε κλειδί μέσα σε αυτό το hive αντιστοιχεί σε έναν χρήστη και είναι ονομασμένο με το αντίστοιχο SID. Τα πρώτα τέσσερα κλειδιά αναφέρονται στους λογαριασμούς συστήματος και συνήθως υπάρχουν σε κάθε σύστημα. Πιο συγκεκριμένα το HKU\DEFAULT περιέχει καθολικές πληροφορίες του χρήστη, το HKU\S-1-5-18 αναφέρεται στον τοπικό λογαριασμό του συστήματος, το HKU\S-1-5-19 χρησιμοποιείται για την εκτέλεση τοπικών υπηρεσιών και το HKU\S-1-5-20 αναφέρεται στον δικτυακό λογαριασμό του συστήματος, το οποίο χρησιμοποιείται για την εκτέλεση υπηρεσιών δικτύου. Στο hive του HKEY\_USERS μπορούν να βρεθούν πολύ σημαντικές πληροφορίες για τον χρήστη, όπως για παράδειγμα το όνομα, ο αριθμός μαζί με την ημερομηνία και ώρα σύνδεσης του χρήστη στο σύστημα, η ημερομηνία και ώρα της τελευταίας αλλαγής κωδικού πρόσβασης, ο αριθμός των αποτυχημένων συνδέσεων και ούτω καθεξής [3].

## **HKEY\_LOCAL\_MACHINE**

Η συντομογραφία του συγκεκριμένου key είναι HKLM και σε αυτό περιέχονται πληροφορίες διαμόρφωσης που σχετίζονται με το σύστημα - μηχανήμα [2]. Σύμφωνα με [3] στο συγκεκριμένο hive εμπεριέχονται πληροφορίες διαμόρφωσης για τα εγκατεστημένα λογισμικά και το λειτουργικό σύστημα. Επίσης εμπεριέχονται πληροφορίες για το εντοπισμένο υλικό (hardware) που χρησιμοποιείται. Τα πέντε βασικά keys αυτού του hive είναι το HARDWARE, το SYSTEM, το SOFTWARE, το SAM και το SECURITY. Αναλυτικότερα, στα κλειδιά HARDWARE και SYSTEM υπάρχουν πληροφορίες που σχετίζονται με το hardware του μηχανήματος και τις ρυθμίσεις του συστήματος. Στο SOFTWARE υπάρχουν πληροφορίες σχετικά με τις εγκατεστημένες εφαρμογές, τις παραμέτρους για την απόδοση των windows αλλά και τις προκαθορισμένες (default) ρυθμίσεις. Τέλος, στο SAM και στο SECURITY υπάρχουν πληροφορίες σχετικά με την υπηρεσία Security Accounts Manager, η οποία

διαχειρίζεται του λογαριασμούς και γενικές πληροφορίες που αφορούν την ασφάλεια. Πρέπει να σημειωθεί πως οι τιμές των SAM και SECURITY δεν είναι readable ή modifiable χρησιμοποιώντας το regedit καθώς απαιτούνται ειδικά δικαιώματα [5].

## HKEY\_CLASSES\_ROOT

Η συντομογραφία του συγκεκριμένου key είναι HKCR και σε αυτό περιέχονται πληροφορίες, οι οποίες είναι υπεύθυνες για την εκτέλεση της σωστής εφαρμογής ή αρχείου, όταν ζητηθεί από τον χρήστη. Το HKCR αποτελεί subkey του HKEY\_LOCAL\_MACHINE\Software [2]. Η λίστα με όλα τα κλειδιά αυτού του hive είναι πολύ μεγάλη αλλά μερικοί τύποι αρχείων που υπάρχουν σε αυτό το hive είναι το .avi, το .bmp, το .exe, το .html, το .pdf και το .dll. Κάθε κλειδί περιέχει πληροφορίες σχετικά με το ποια ενέργεια πρέπει να πραγματοποιηθεί, όταν ο χρήστης εκτελέσει ένα αρχείο με κάποια από τις προηγουμένως αναφερθείσες επεκτάσεις [3].

## HKEY\_CURRENT\_CONFIG

Η συντομογραφία του συγκεκριμένου key είναι HKCC και σε αυτό περιέχονται πληροφορίες που σχετίζονται με το προφίλ του υλικού (hardware) που χρησιμοποιείται από το σύστημα κατά την εκκίνηση [2]. Στην ουσία το HKCC είναι απλά ένας δείκτης (pointer) στο HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\HardwareProfiles\Currentregistry το οποίο με την σειρά του αποτελεί δείκτης στο HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\HardwareProfiles. Λόγος ύπαρξης του HKCC αποτελεί η εύκολη προβολή και επεξεργασία των δεδομένων, ενέργειες οι οποίες μπορούν να πραγματοποιηθούν και στα άλλα δυο κλειδιά [3].

Στο registry των windows υπάρχουν δεδομένα συγκεκριμένου τύπου. Στον παρακάτω πίνακα αναφέρονται όλοι οι διαθέσιμοι τύποι δεδομένων του registry [2].

Πίνακας 1: Τύποι δεδομένων του registry

Είδος Τιμής	Τύπος	Περιγραφή
Δυαδική Τιμή	REG_BINARY	Ακατέργαστα (raw) δεδομένα, δηλαδή δεδομένα που δεν έχουν υποστεί κάποια τροποποίηση όπως για παράδειγμα συμπίεση (compression), σε δυαδική μορφή. Με την συγκεκριμένη μορφή αποθηκεύονται οι περισσότερες πληροφορίες που σχετίζονται με το υλικό του συστήματος.
Τιμή DWORD	REG_DWORD	Δεδομένα που αναπαρίστανται με έναν ακέραιο αριθμό 4 byte (32 bit). Με την συγκεκριμένη μορφή αποθηκεύονται παράμετροι για τους οδηγούς (drivers) της συσκευής και των υπηρεσιών.

Επεκτάσιμη Τιμή String	REG_EXPAND_SZ	Μεταβλητού μήκους δεδομένα string. Περιέχονται οι μεταβλητές που χρησιμοποιούνται από κάποιο πρόγραμμα.
Multi-String Τιμή	REG_MULTI_SZ	Δεδομένα πολλαπλών string. Τιμές που περιέχουν λίστες και χωρίζονται με κόμμα, κενά ή άλλα διαχωριστικά.
Τιμή String	REG_SZ	Σταθερού μήκους string κειμένου
Διαδική Τιμή	REG_RESOURCE_LIST	Σειρά ένθετων λιστών που έχουν σχεδιαστεί για την αποθήκευση πόρων και χρησιμοποιείται από έναν οδηγό υλικού (hardware driver).
Διαδική Τιμή	REG_RESOURCE_REQUIREMENTS_LIST	Παρόμοιο με το παραπάνω
Διαδική Τιμή	REG_FULL_RESOURCE_DESCRIPTOR	Παρόμοιο με το παραπάνω
None	REG_NONE	Δεδομένα απροσδιόριστου τύπου
Σύνδεσμος (Link)	REG_LINK	Σύνδεσμος σε μορφή string με κωδικοποίηση Unicode
Τιμή QWORD	REG_QWORD	Δεδομένα που αναπαρίστανται με έναν ακέραιο αριθμό 8 byte (64 bit).

Το windows registry χωρίζεται σε δυο διακριτά πεδία, σύστημα και χρήστη. Οι κυψέλες συστήματος συνήθως βρίσκονται αποθηκευμένες στο %SystemRoot%\System32\Config ενώ οι κυψέλες χρήστη, στο %USERPROFILE%. Είναι σημαντικό να σημειωθεί πως στο %USERPROFILE% βρίσκεται αποθηκευμένο το αρχείο NTUSER.DAT, το οποίο περιέχει σημαντικές πληροφορίες για τον χρήστη του συστήματος και είναι χρήσιμο για αυτή την εργασία. Κάθε φορά που δημιουργείται ένας νέος χρήστης στο σύστημα, ταυτόχρονα δημιουργείται και ένα αρχείο NTUSER.DAT. Το συγκεκριμένο αρχείο βρίσκεται στο path: C:\Users\<όνομα χρήστη>\NTUSER.DAT [6].

## 2.2 Πρόσβαση στο registry και διαθέσιμα εργαλεία

Η πρόσβαση στο windows registry πραγματοποιείται με το Regedit, το οποίο πρόκειται για έναν ενσωματωμένο επεξεργαστή registry και υπάρχει σε όλες τις εκδόσεις των windows. Ο επεξεργαστής αυτός παρέχει ένα φιλικό προς τον χρήστη περιβάλλον, εμφανίζοντας όλα τα περιεχόμενα του registry με μια ιεραρχική σειρά. Μέσω του regedit μπορεί να πραγματοποιηθεί εύρεση συγκεκριμένων πληροφοριών, τροποποίηση κλειδιών και τιμών, εξαγωγή όλων των πληροφοριών σε ένα αρχείο και εισαγωγή αρχείου που ενδεχομένως να περιέχει διαφορετικά κλειδιά και τιμές [2, 7]. Εκτός από το regedit υπάρχουν διάφορα εργαλεία για την εξαγωγή και ανάλυση του registry. Μερικά από αυτά παρουσιάζονται παρακάτω.

### RegRipper

Πρόκειται για ένα διαδεδομένο εργαλείο ανάλυσης του registry, το οποίο υποστηρίζει εξαγωγή και ανάλυση πληροφορίας από αρχεία του hive. Η πλούσια συλλογή πρόσθετων

που προσφέρει, χρησιμοποιείται για την ανάλυση ποικίλων δεδομένων του registry. Είναι δωρεάν και ανοιχτού κώδικα.

## **Registry Explorer**

Το συγκεκριμένο εργαλείο έχει αναπτυχθεί από τον Eric Zimmerman και παρέχεται δωρεάν. Προσφέρει χρήσιμες εντολές για την πλοήγηση, αναζήτηση και εξαγωγή δεδομένων του registry. Η offline χρήση του, η υποστήριξη πολλών hive και η διαχείριση κλειδωμένων αρχείων, αποτελούν πλεονεκτήματα του συγκεκριμένου εργαλείου.

## **Registry Viewer**

Το registry viewer έχει αναπτυχθεί από την Exterro (παλιά AccessData), μια εταιρία αρκετά γνωστή που παρέχει πληθώρα εργαλείων για ψηφιακή εγκληματολογική έρευνα. Το συγκεκριμένο εργαλείο προσφέρεται δωρεάν από την εταιρία και χρησιμοποιείται για την εύρεση και ανάλυση κλειδιών, τιμών και δεδομένων του registry. Πλεονέκτημα του registry viewer αποτελεί η χρήση ελάχιστων πόρων του συστήματος (lightweight) και η απλή διεπαφή που προσφέρει.

## **Regshot**

Το regshot πρόκειται για ένα απλό εργαλείο το οποίο λαμβάνει στιγμιότυπα του registry, πριν και μετά τις αλλαγές στο σύστημα, με σκοπό την σύγκριση τους και εξαγωγή των απαραίτητων αποτελεσμάτων. Προσφέρεται δωρεάν, είναι ανοιχτού κώδικα και χρήσιμο για την ιχνηλάτηση τροποποιήσεων στο σύστημα έπειτα από εκτέλεση μιας ενέργειας, όπως για παράδειγμα η εγκατάσταση μιας εφαρμογής. Χρησιμοποιείται συχνά για malware forensics αλλά η χρήση του δεν περιορίζεται μόνο σε αυτό.

## **RegScanner**

Το regscanner προσφέρεται δωρεάν από την NirSoft και πρόκειται για ένα lightweight εργαλείο το οποίο χρησιμοποιείται για την αναζήτηση συγκεκριμένων κλειδιών και τιμών στο registry. Πλεονέκτημα του αποτελεί η ευέλικτη αναζήτηση που υποστηρίζει regex για τους προχωρημένους χρήστες.

## **2.3 Δυσκολίες έρευνας στο registry**

Όπως και στους υπόλοιπους υποκλάδους του digital forensics, ένα από τα σημαντικότερα προβλήματα του registry forensics αποτελεί το anti-forensics. Το anti-forensics πρόκειται για την σκόπιμη τροποποίηση, ενημέρωση και διαγραφή των δεδομένων και πιθανών ψηφιακών αποδεικτικών στοιχείων. Συνήθως πραγματοποιείται από τον ένοχο, ο οποίος μπορεί επίσης να προκαλέσει ζημιά ή ακόμα και να καταστρέψει την συσκευή, με σκοπό την αντίκρουση της έρευνας και αποφυγή οποιασδήποτε κατηγορίας [8, 9]. Ορισμένα παραδείγματα anti-forensics αποτελούν η κρυπτογράφηση (encryption), η θόλωση ή συσκοτίση δεδομένων (obfuscation), η στεγανογραφία (steganography), οι κρυφές επικοινωνίες (tunneling – onion routing) και οι εικονικές μηχανές (virtual machines – docker containers) [10]. Στην περίπτωση του registry forensics, παράδειγμα anti-forensics αποτελεί η τροποποίηση του registry, δηλαδή η επεξεργασία ή διαγραφή κλειδιών και τιμών [11].

Σημαντικό πρόβλημα αποτελεί επίσης η αύξηση των προκαθορισμένων (default) κλειδιών και τιμών του registry, λόγω νέων εκδόσεων του λειτουργικού και προσθήκη νέων χαρακτηριστικών σε αυτό. Μια νέα έκδοση του λογισμικού (π.χ. windows 11) έχει νέες δυνατότητες και περισσότερα χαρακτηριστικά, με αποτέλεσμα να υπάρχουν περισσότερες προκαθορισμένες εγγραφές στο registry. Στην εργασία [12], οι συγγραφείς καταγράψανε το registry των windows 7 και των windows 10 και παρατηρήσανε πως υπήρξε σημαντική διαφορά. Στον παρακάτω πίνακα μπορούμε να παρατηρήσουμε τις διαφορές μεταξύ των δυο εκδόσεων (windows 7 & 10) ανά hive.

Hive	Windows 7		Windows 10		% Διαφοράς	
	Keys	Values	Keys	Values	Keys	Values
<b>HKLM</b>	354.553	217.193	568.162	343.200	+160%	+158%
<b>HKCR</b>	113.642	94.597	187.458	161.053	+165%	+170%
<b>HKU</b>	7.182	2.554	29.505	13.806	+411%	+540%
<b>HKCU</b>	4.486	1.906	10.563	5.237	+235%	+275%

Όπως μπορούμε να διακρίνουμε, το ποσοστό διαφοράς μεταξύ των δυο εκδόσεων είναι όντως σημαντικό. Παρόλο που υπάρχουν αρκετά λογισμικά εργαλεία τα οποία απαλλάσσουν τους ερευνητές από την χειροκίνητη αναζήτηση και αλληλεπίδραση με το registry και που αυξάνουν την αποδοτικότητα, η αυξητική τάση των προκαθορισμένων keys και values, σίγουρα δυσκολεύει την ψηφιακή έρευνα στο registry.

### 3 - ΕΠΙΣΚΟΠΗΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑΣ (LITERATURE REVIEW)

Έπειτα από μελέτη σχετικών εργασιών, προκύπτει πως το windows registry χρησιμοποιείται σε αρκετές εργασίες, μερικές από τις οποίες θα περιγραφούν στο σημείο αυτό. Στο [3] πραγματοποιήθηκε έρευνα στην δομή του windows 7 registry για την αναγνώριση χρήσιμων πληροφοριών από τα κλειδιά του registry. Πιο συγκεκριμένα προτάθηκε ένα εργαλείο το οποίο τροφοδοτείται με δεδομένα του registry και έπειτα τα επεξεργάζεται με σκοπό τον εντοπισμό αποδεικτικών στοιχείων. Τα αποδεικτικά στοιχεία που μπορεί να εντοπίσει το συγκεκριμένο εργαλείο είναι το όνομα του συστήματος, ο τελευταίος τερματισμός λειτουργίας της συσκευής, τα ασύρματα δίκτυα στα οποία έχει συνδεθεί ο υπολογιστής, τα πρόσφατα χρησιμοποιούμενα αρχεία και εφαρμογές καθώς και άλλα χρήσιμα στοιχεία. Σκοπός του εργαλείου είναι η μείωση του χρόνου έρευνας και αύξηση της αποδοτικότητας εξαγωγής αποδεικτικών στοιχείων καθώς η χειρωνακτική εξαγωγή και ανάλυση του registry πρόκειται για μια πολύ κουραστική διαδικασία.

Στο [6] μελετήθηκαν τα ASEP, τα οποία επιτρέπουν την εκτέλεση συγκεκριμένου προγράμματος στο σύστημα αυτόματα, χωρίς την αλληλεπίδραση του χρήστη. Επίσης αναπτύχθηκε ένα πρόσθετο για το Volatility framework, ονομαζόμενο “winesap”. Το συγκεκριμένο πρόσθετο αναλύει ένα αποτύπωμα μνήμης και εντοπίζει ASEPs των windows που βασίζονται στο registry και θεωρούνται ύποπτα. Το εργαλείο εφαρμόστηκε σε ένα εικονικό περιβάλλον με νέα εγκατάσταση των windows 7, ανέκτησε με επιτυχία όλα τα ASEP τα οποία βασίζονταν στο registry και από αυτά εντόπισε τα ύποπτα.

Στο [7] προτάθηκε μια μεθοδολογία για ψηφιακή εγκληματολογική έρευνα μεγάλης κλίμακας, χρησιμοποιώντας το λογισμικό Apache Spark. Πιο συγκεκριμένα πραγματοποιήθηκε συλλογή μεγάλου όγκου δεδομένων από registry πολλών συστημάτων, τα οποία μετασχηματίστηκαν και φορτώθηκαν σε ένα κατανεμημένο σύστημα Hadoop, για αναγνώριση κακόβουλων εγγράφων στο registry. Επίσης προτάθηκαν αλγόριθμοι οι οποίοι υποστήριζαν την κατανεμημένη και παράλληλη επεξεργασία των δεδομένων αποδοτικά. Η παραπάνω μεθοδολογία εφαρμόστηκε σε δεδομένα του registry τα οποία συλλέχθηκαν από τέσσερις υπολογιστές και είχαν συνολικό μέγεθος 1.52GB. Η μεθοδολογία απέδειξε πως είναι αρκετά αποδοτική, μειώνοντας τον χρόνο επεξεργασίας κατά 3.3 φορές. Αυτό ήταν εφικτό αυξάνοντας τον αριθμό των CPU και των λειτουργικών κόμβων (nodes) του HDFS, από 1 σε 8 καθώς επίσης και με την βοήθεια των προτεινόμενων αλγορίθμων.

Στο [11] παρουσιάζεται το UserAssist key του windows 10 registry και συγκρίνεται με αυτό του windows XP. Το UserAssist key αποτελεί μέρος του windows registry και καταγράφει πληροφορίες σχετικά με τα προγράμματα που τρέχει ο χρήστης. Έπειτα από κάποιες δοκιμές που πραγματοποίησαν οι συγγραφείς παρατηρήθηκε ότι όταν διαγράφονταν εφαρμογές, ορισμένα δεδομένα παρέμεναν στο σύστημα. Αυτό αποτελεί μια εξαιρετική πηγή απόκτησης αποδεικτικών στοιχείων σε μια ψηφιακή έρευνα.

Στο [13] αναπτύχθηκε μια μεθοδολογία για την απόκτηση και ανάλυση στοιχείων του windows 10 registry, τα οποία σχετίζονται με το πρόγραμμα περιήγησης Tor. Η μεθοδολογία εφαρμόστηκε σε μια νέα εγκατάσταση windows 10, πραγματοποιήθηκε επίσκεψη σε ιστοσελίδες του dark web (hidden wiki, secmail, keybase και άλλα) αλλά και σε κανονικές

(gmail, outlook, mega storage) και χρησιμοποιήθηκε το Regshot για την λήψη στιγμιότυπων (snapshots) του registry. Μετά από ανάλυση των στιγμιότυπων του windows registry, προέκυψε πως υπήρχαν πληροφορίες σχετικά με τις ενέργειες του χρήστη. Όπως αποδεικνύεται, το Tor τελικά δεν προσφέρει πλήρη ιδιωτικότητα και ανωνυμία.

Ακόμη μια εργασία που σχετίζεται με το πρόγραμμα περιήγησης Tor, είναι η [14]. Οι συγγραφείς του συγκεκριμένου paper δημιούργησαν ένα πλαίσιο εργασίας (framework) για το dark web forensics αναλύοντας εγγραφές του registry. Όπως και στην παραπάνω έρευνα, έτσι και εδώ, προετοιμάζεται ένα σύστημα windows 10 στο οποίο εγκαθίσταται το εργαλείο Regshot, καταγράφονται στιγμιότυπα και αναλύονται για την εξαγωγή συμπερασμάτων. Παρομοίως, χρησιμοποιώντας το registry μπορούν να αποκτηθούν πληροφορίες σχετικά με την έκδοση του Tor, την τοποθεσία και ώρα εγκατάστασης του.

Στο [15] αναλύεται το windows registry για την αναγνώριση των χαρακτηριστικών μια συσκευής USB, όπως είναι το id του προϊόντος, το όνομα του προμηθευτή, οι σειριακοί αριθμοί και η έκδοση του λειτουργικού συστήματος, τα οποία μπορούν να αποτελέσουν σημαντικά στοιχεία σε μια έρευνα. Οι πληροφορίες αυτές εντοπίστηκαν στα εξής hive: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USB*, *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR* και *HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices*.

Στο [16] παρουσιάζεται ένα εργαλείο το οποίο εξάγει και επεξεργάζεται δεδομένα από το windows registry για την δημιουργία μιας χρονοσειράς (timeline). Στο registry υπάρχουν κλειδιά τα οποία τροποποιούνται με τις ενέργειες του χρήστη και κάθε κλειδί περιέχει μια τιμή Lastwrite, η οποία δείχνει την χρονική στιγμή της τελευταίας εγγραφής. Από αυτές τις τιμές μπορεί να δημιουργηθεί μια χρονοσειρά με τις ενέργειες του χρήστη. Σύγκριση μεταξύ του προτεινόμενου εργαλείου και του FTK έδειξε πως και τα δυο εργαλεία εντόπισαν αρκετές πληροφορίες για την δημιουργία της χρονοσειράς με μοναδικό μειονέκτημα την αργή αναγνώριση αρχείων από την μεριά του FTK. Το προτεινόμενο εργαλείο εφαρμόζεται μόνο σε παλιά συστήματα με λειτουργικό σύστημα Microsoft XP και Microsoft Vista.

Στο [17] σκοπός της εργασίας είναι η χρήση του registry για την αναγνώριση και εξαγωγή στοιχείων που σχετίζονται με το iDrive. Το iDrive πρόκειται για μια υπηρεσία αποθήκευσης δεδομένων στο cloud. Στην μεθοδολογία για ακόμη μια φορά χρησιμοποιήθηκαν εικονικές μηχανές με λειτουργικό windows 10 και το εργαλείο SysTracer, για τον εντοπισμό στοιχείων που σχετίζονται με την συγκεκριμένη υπηρεσία. Το λογισμικό, κατά την διάρκεια της εγκατάστασης, σύνδεσης, αλληλεπίδρασης και απεγκατάστασης της εφαρμογής, ήταν ικανό να εντοπίσει στοιχεία στο registry. Εφόσον τα συγκεκριμένα στοιχεία σχετίζονται με μια εφαρμογή και τις ρυθμίσεις του χρήστη, ήταν αναμενόμενο να βρεθούν στο *HKEY\_LOCAL\_MACHINE\Software\xxx* και στο *HKEY\_CURRENT\_USER\SOFTWARE\xxx*.

Παρόμοια με την παραπάνω εργασία αποτελεί το [18] όπου πραγματοποιείται έρευνα στο registry των windows 10 για στοιχεία που σχετίζονται με το Dropbox. Το Dropbox πρόκειται για άλλη μια εφαρμογή αποθήκευσης δεδομένων στο cloud. Η μεθοδολογία είναι παρόμοια χρησιμοποιώντας εικονικές μηχανές και λογισμικά εργαλεία, κατάλληλα για κάθε

στάδιο της έρευνας. Δεδομένα όπως η έκδοση της εφαρμογής, η τοποθεσία εγκατάστασης, η ώρα εγκατάστασης και τα κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, εντοπίστηκαν στα hive: *HKEY\_LOCAL\_MACHINE*, *HKEY\_CLASSES\_ROOT*, *HKEY\_CURRENT\_USER* και *HKEY\_USERS*.

Οι συγγραφείς στο [19] πραγματοποίησαν έρευνα για πιθανά στοιχεία στο registry, μετά την εγκατάσταση και απεγκατάσταση δυο διαδεδομένων εφαρμογών άμεσων μηνυμάτων, αυτών του Viber και του Telegram. Για ακόμη μια φορά γίνεται χρήση εικονικών μηχανών λόγω της δυνατότητας επιστροφής σε προηγούμενη κατάσταση, σε περίπτωση που κάτι πάει στραβά. Για την εξαγωγή των αρχείων registry χρησιμοποιήθηκε το Regshot Portable ενώ για την αναγνώριση δραστηριοτήτων χρήστη χρησιμοποιήθηκε το RegRipper. Τα αποτελέσματα δείχνουν πως αν και το Telegram θεωρείται μια από της πιο ασφαλής εφαρμογές άμεσων μηνυμάτων, μετά την απεγκατάσταση της εφαρμογής, στο registry συνεχίζουν να υπάρχουν σημαντικές και χρήσιμες πληροφορίες. Πληροφορίες συνεχίζουν να υπάρχουν και στην περίπτωση του Viber.

Οι συγγραφείς της εργασίας [20] ανέπτυξαν ένα εργαλείο το οποίο ονομάζεται AXREL και χρησιμοποιείται για εξαγωγή event logs και αρχείων από το registry. Το εργαλείο έχει αναπτυχθεί σε python3, προσφέρει GUI και δημιουργήθηκε για να διευκολύνει τους ερευνητές που εξαγάγουν αρχεία χειροκίνητα. Έπειτα από δοκιμή του λογισμικού, τα εξαχθέν αρχεία συγκρίθηκαν χρησιμοποιώντας το Registry Explorer και επιβεβαιώθηκε πως αυτά ήταν σωστά.



#### 4. ΑΝΑΠΤΥΞΗ ΣΥΓΚΕΚΡΙΜΕΝΟΥ ΠΕΔΙΟΥ

Στο παρόν κεφάλαιο θα πραγματοποιηθεί λεπτομερής ανάλυση μιας εργασίας που μελετήθηκε στο κεφάλαιο 3. Πιο συγκεκριμένα θα πραγματοποιηθεί ανάλυση της εργασίας [13] η οποία σχετίζεται με το πρόγραμμα περιήγησης Tor, το οποίο χρησιμοποιείται για την πρόσβαση στο dark web. Στην συγκεκριμένη εργασία δημιουργήθηκε ένα σενάριο, στο οποίο ο χρήστης φαίνεται να απέκτησε πολύ σημαντικές πληροφορίες για την κυβέρνηση μέσω του dark web και εφαρμόστηκε μια μεθοδολογία, με σκοπό την συλλογή δεδομένων που σχετίζονται με το tor καθώς και απόκτηση των απαραίτητων πληροφοριών. Οι συγγραφείς προσομοίωσαν κάθε πιθανή ενέργεια του χρήστη, πραγματοποιώντας εγκατάσταση, εκτέλεση, απεγκατάσταση του tor καθώς επίσης επίσκεψη κανονικών σελίδων αλλά και σελίδων του dark web. Κανονικές σελίδες αποτέλεσαν το gmail - google drive, το outlook – skype και το MEGA ενώ onion websites αποτέλεσαν το hidden wiki, τρεις μηχανές αναζήτησης (Ahmia, DuckDuckGo & Excavator), το secmail, το galaxy3 και άλλες. Η μεθοδολογία εφαρμόστηκε σε ένα νέο (Fresh Install – New VM) εικονικό σύστημα με windows 10, χρησιμοποιώντας εικονική μηχανή αλλά και σε κινητά τηλέφωνα με android 10. Οι εικονικές μηχανές χρησιμοποιήθηκαν καθώς παρέχουν την δυνατότητα καταγραφής στιγμιotypών της τρέχουσας κατάστασης του συστήματος και την δυνατότητα επαναφοράς μιας προηγούμενης κατάστασης, όταν το επιθυμεί ο χρήστης. Και στις δυο συσκευές αναλύθηκε ο αποθηκευτικός χώρος και η μνήμη, με μόνη ιδιαιτερότητα την ανάλυση του registry στο σύστημα με windows 10. Εφόσον στην συγκεκριμένη εργασία μελετάτε το registry των windows, έμφαση θα δοθεί στις ενέργειες και τα αποτελέσματα που σχετίζονται με το registry. Έτσι λοιπόν οι συγγραφείς χρησιμοποίησαν το λογισμικό εργαλείο snapshot για την καταγραφή στιγμιotypών (snapshots), πριν και μετά την εγκατάσταση, την χρήση και την απεγκατάσταση του tor. Αναλύοντας τα στιγμιότυπα, οι συγγραφείς εντόπισαν πως κατά την εγκατάσταση προστέθηκαν 8 registry keys και 3 που σχετίζονταν με το tor. Τα κλειδιά αυτά περιέχουν τιμές οι οποίες διατηρούν πληροφορίες σχετικά με την εκτέλεση και το κλείσιμο της εφαρμογής. Οι πληροφορίες αυτές είναι πολύ σημαντικές για τους ερευνητές καθώς μπορούν να δημιουργήσουν μια χρονοσειρά (timeline). Δυστυχώς βέβαια, στις τιμές αυτές δεν περιέχονται πληροφορίες σχετικά με την περιήγηση του χρήστη στο tor. Τέλος, αυτό που παρατηρήθηκε είναι πως τα κλειδιά συνεχίζουν να παραμένουν στο registry ακόμη και μετά την απεγκατάσταση του tor.

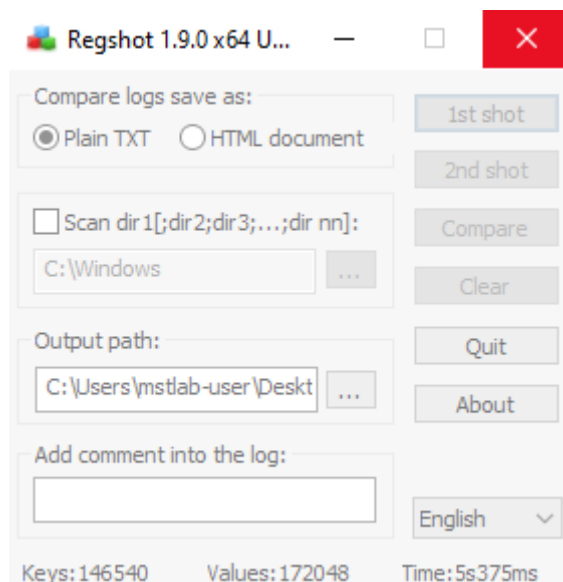
## 5. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ (USE CASE)

Σε αυτό το κεφάλαιο θα εφαρμοστεί η μεθοδολογία που εφάρμοσαν οι συγγραφείς της εργασίας [13]. Λεπτομερέστερα θα χρησιμοποιηθεί το λογισμικό regshot, με το οποίο θα αποκτήσουμε και θα συγκρίνουμε στιγμιότυπα κατά την εγκατάσταση και απεγκατάσταση μιας δημοφιλής εφαρμογής κοινωνικής δικτύωσης (social media), το Instagram.

### Εγκατάσταση του Instagram

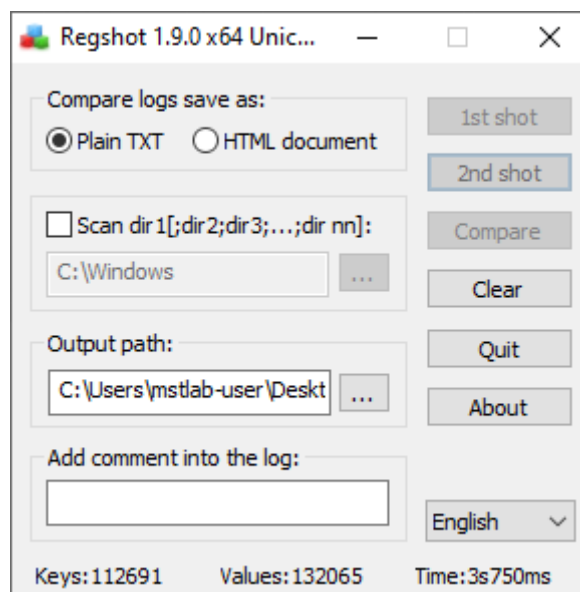
Πρώτο βήμα αποτελεί η εκτέλεση της εφαρμογής και η καταγραφή του πρώτου στιγμιότυπου. Στο πρώτο στιγμιότυπο καταγράφεται το registry πριν την εγκατάσταση της εφαρμογής.

Εικόνα 3: Snapshot πριν την εγκατάσταση της εφαρμογής



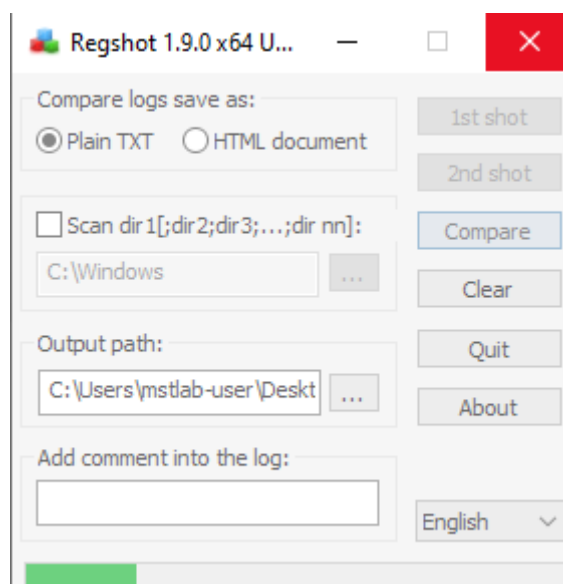
Εφόσον ολοκληρώθηκε το πρώτο snapshot, εγκαταστάθηκε το Instagram και ξεκίνησε το δεύτερο snapshot.

Εικόνα 4: Snapshot μετά την εγκατάσταση της εφαρμογής



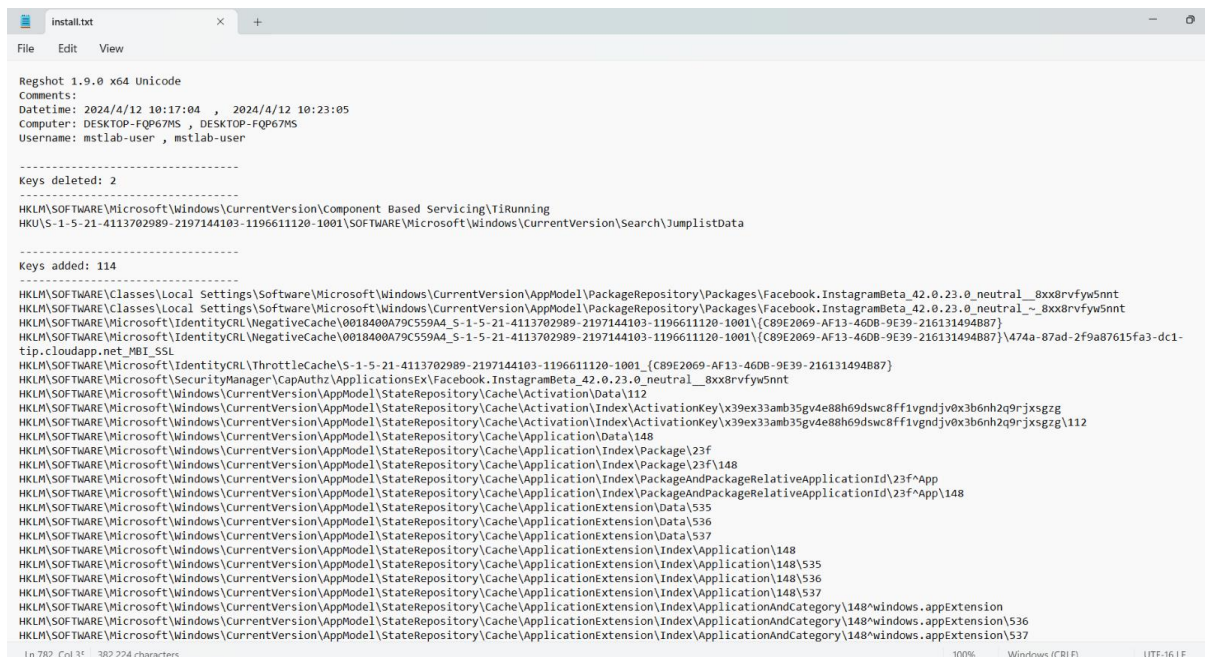
Με την επιτυχή ολοκλήρωση του δεύτερου snapshot, επόμενο βήμα αποτέλεσε η σύγκριση των δυο snapshot.

Εικόνα 5: Σύγκριση των δυο snapshot



Έπειτα από ολοκλήρωση της σύγκρισης, το regshot εξήγαγε ένα αρχείο .txt το οποίο περιείχε όλες τις τροποποιήσεις στο registry μετά από την εγκατάσταση της εφαρμογής. Το μέγεθος του αρχείου ήταν 748 KB και περιείχε 382.224 χαρακτήρες.

Εικόνα 6: Περιεχόμενο του .txt αρχείου μετά την εγκατάσταση



```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/4/12 10:17:04 , 2024/4/12 10:23:05
Computer: DESKTOP-FQP67MS , DESKTOP-FQP67MS
Username: mstlab-user , mstlab-user

-----
Keys deleted: 2
-----
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\TiRunning
HKU\S-1-5-21-4113702989-2197144103-1196611120-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData

-----
Keys added: 114
-----
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Facebook.InstagramBeta_42.0.23.0_neutral_8xx8rvfyw5nnt
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Facebook.InstagramBeta_42.0.23.0_neutral_8xx8rvfyw5nnt
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0018400A79C559A4_S-1-5-21-4113702989-2197144103-1196611120-1001\{C89E2069-AF13-460B-9E39-216131494887}
HKLM\SOFTWARE\Microsoft\IdentityCRL\NegativeCache\0018400A79C559A4_S-1-5-21-4113702989-2197144103-1196611120-1001\{C89E2069-AF13-460B-9E39-216131494887}\474a-87ad-2f9a87615fa3-dc1-tip.cloudapp.net_001_SSL
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-4113702989-2197144103-1196611120-1001_{C89E2069-AF13-460B-9E39-216131494887}
HKLM\SOFTWARE\Microsoft\SecurityManager\CapAuthz\ApplicationsEX\Facebook.InstagramBeta_42.0.23.0_neutral_8xx8rvfyw5nnt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Activation\Data\112
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Activation\Index\ActivationKey\X39ex33amb35gv4e88h69dswc8ff1vgndjv0x3b6nh2q9rjxsgzg
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Activation\Index\ActivationKey\X39ex33amb35gv4e88h69dswc8ff1vgndjv0x3b6nh2q9rjxsgzg\112
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Data\148
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\Package\23f
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\Package\23f\148
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackageRelativeApplicationId\23f^App
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\Application\Index\PackageAndPackageRelativeApplicationId\23f^App\148
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Data\535
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Data\536
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Data\537
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Application\148
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Application\148\535
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Application\148\536
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\Application\148\537
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\ApplicationAndCategory\148^windows.appExtension
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\ApplicationAndCategory\148^windows.appExtension\536
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationExtension\Index\ApplicationAndCategory\148^windows.appExtension\537
```

Από την εικόνα 6 παρατηρήσαμε πως διαγράφηκαν δυο κλειδιά. Αναλυτικότερα, το πρώτο key σχετίζεται με το HKEY\_LOCAL\_MACHINE\SOFTWARE hive, ενώ το δεύτερο σχετίζεται με το HKEY\_USERS το οποίο αφορά τον χρήστη του συστήματος (S-1-5-21). Συνεχίζοντας παρατηρήσαμε ότι προστέθηκαν 114 keys. Στα πρώτα δυο keys φαίνεται ξεκάθαρα το όνομα της εφαρμογής καθώς και η έκδοση της (InstagramBeta\_42.0.23.0). Εφόσον πρόκειται για εφαρμογή, το hive που τροποποιήθηκε ήταν το HKEY\_LOCAL\_MACHINE\SOFTWARE. Φτάνοντας στο τέλος του αρχείου, παρατηρήθηκε πως συνολικά πραγματοποιήθηκαν 398 τροποποιήσεις.

## Απεγκατάσταση του Instagram

Για την ανάλυση του registry μετά την απεγκατάσταση του Instagram εφαρμοστήκαν τα ίδια βήματα όπως και παραπάνω. Αρχικά καταγράφηκε ένα snapshot πριν την απεγκατάσταση και έπειτα καταγράφηκε δεύτερο snapshot μετά την απεγκατάσταση. Συγκρίνοντας τα δυο snapshot, το regshot εξήγαγε ένα αρχείο 393 KB με 201.146 χαρακτήρες.



αποτέλεσμα να προστεθούν άσχετα keys. Παρόλο αυτά από την δική μας πλευρά, κατά την διάρκεια λήψης των στιγμιotypων δεν εκτελούσαμε άλλες (διαφορετικές) διεργασίες. Έτσι λοιπόν, οι επιπλέον προσθήκες πρέπει να πραγματοποιήθηκαν αυτόματα από το σύστημα. Πρέπει επίσης να σημειωθεί ότι οι προσθήκες αυτές δεν σχετίζονται με το regshot καθώς αυτό πρόκειται για ένα standalone εργαλείο το οποίο δεν χρειάζεται εγκατάσταση ή σύνδεση στο δίκτυο. Το γεγονός αυτό επιβεβαιώνεται και από την επισκόπηση της βιβλιογραφίας, στην οποία οι συγγραφείς δεν αναφέρονε την προσθήκη κλειδιών από την χρήση του λογισμικού εργαλείου.

## **6. ΣΥΜΠΕΡΑΣΜΑΤΑ**

Στη συγκεκριμένη εργασία μελετήθηκε το windows registry forensics, το οποίο πρόκειται για έναν υποκλάδο της ψηφιακής εγκληματολογίας. Αρχικά παρουσιάστηκε το background του κλάδου στο οποίο πραγματοποιήθηκε ανάλυση της δομής του registry, περιγραφή διαθέσιμων εργαλείων για την έρευνα στο registry και αναφορά στις κυριότερες δυσκολίες που αντιμετωπίζουν οι ερευνητές κατά την διάρκεια μιας έρευνας που σχετίζεται με το registry. Στην συνέχεια πραγματοποιήθηκε βιβλιογραφική επισκόπηση και μελετήθηκαν εργασίες άλλων συγγραφέων έτσι ώστε να συγκεντρωθούν πληροφορίες που σχετίζονται με τον κλάδο του windows registry forensics. Επιλέγοντας μια από αυτές τις εργασίες, πιο συγκεκριμένα της εργασίας [13], πραγματοποιήθηκε λεπτομερής ανάλυση έτσι ώστε να γίνει κατανοητή η εργασία και η μεθοδολογία που εφαρμόστηκε σε αυτή. Έπειτα από ανάλυση της παραπάνω εργασίας, εφαρμόστηκε μια μελέτη περίπτωσης όπου χρησιμοποιήθηκε το λογισμικό εργαλείο regshot, για την καταγραφή και σύγκριση στιγμιotypων της εφαρμογής κοινωνικής δικτύωσης Instagram. Στην συγκεκριμένη μελέτη περίπτωσης καταγράφηκαν στιγμιότυπα πριν και μετά την εγκατάσταση καθώς και πριν και μετά την απεγκατάσταση της εφαρμογής. Αναλύοντας τα στιγμιότυπα, προέκυψε πως μετά την απεγκατάσταση του Instagram δεν αφαιρέθηκαν όλα τα keys που προστέθηκαν μετά την εγκατάσταση. Αυτό οφείλετε στο γεγονός ότι κατά την διάρκεια καταγραφής του στιγμιotypου εκτελούνταν διεργασίες από το σύστημα και προστέθηκαν keys που δεν σχετίζονταν με το Instagram.

## **ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ (FUTURE WORK)**

Future work αποτελεί η χρήση εικονικών μηχανών με freshly installed windows, όπου σε κάθε μηχανήμα θα εγκαθίσταται μια εφαρμογή κοινωνικής δικτύωσης την φορά και θα καταγράφονται τα νέα keys. Σκοπός, η συλλογή όλων των νέων κλειδιών - τιμών κάθε εφαρμογής και σύγκριση αυτών όταν είναι απαραίτητο. Παράδειγμα θα μπορούσε να αποτελεί ένα μηχανήμα στο οποίο είχε εγκατασταθεί το Facebook και μετά απεγκαταστάθηκε. Εάν στο μηχανήμα αυτό υπάρχουν leftover keys μπορούμε να τα ελέγξουμε και αν αυτά διασταυρώνονται με τα κλειδιά που υπάρχουν στην συλλογή, τότε είναι σίγουρο πως η εφαρμογή είχε εγκατασταθεί κάποια στιγμή στο παρελθόν.

## BIBΛΙΟΓΡΑΦΙΑ

- [1] Statista, [“Global market share held by operating systems for desktop PCs, from January 2013 to February 2024”](#)
- [2] Microsoft, [Windows registry information for advanced users](#), 2023
- [3] Abhijeet Ramani, Somesh Kumar Dewangan, “Digital Forensics Identification, Collection, Examination and Decoding of Windows Registry Keys for Discovering User Activities Patterns”, International Journal of Computer Trends and Technology (IJCTT) - Vol. 17 No. 2 – November 2014
- [4] Jungjeum Park, “TREDE and VMPOP: Cultivating multi-purpose datasets for digital forensics – A Windows registry corpus as an example”, Digital Investigation 26 (2018) 3 – 18
- [5] W. De A. Chirath, L. Rupasinghe, “Comprehensive Forensic Data Extraction and Representation System for Windows Registry”, International Conference on Advancements in Computing (ICAC), December 5-6 2019, Malabe Sri Lanka
- [6] Daniel Uroz, Ricardo J. Rodriguez, “Characteristics and detectability of Windows auto-start extensibility points in memory forensics”, Digital Investigation 28 (2019) S95 – S104
- [7] Jun-Ha-Lee, Hyuk-Yoon Kwon, “Large-scale digital forensic investigation for Windows registry on Apache Spark”, Plos ONE 17 (12): e0267411 (2022)
- [8] Heloise Pieterse, Martin Olivier and Renier van Heerden, “Evaluation Framework for Detecting Manipulated Smartphone Data”, South African Institute of Electrical Engineers Vol. 110 (2), June 2019
- [9] Justin Grover, “Android Forensics: Automated data collection and reporting from a mobile device”, Digital Investigation 10 (2013) S12 - S20
- [10] Fran Casino, Thomas K. Dasaklis, Georgios P. Spathoulas et al., “Research Trends, Challenges and Emerging Topics in Digital Forensics: A Review of Reviews”, IEEE Vol. 10 (2022)
- [11] Bhupendra Singh, Upasna Singh, “Program Execution Analysis using UserAssist Key in Modern Windows”, 14<sup>th</sup> International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Vol. 4: SECRIPT pages 420-429
- [12] A. Amin, F. Shabbir, S. Saleem et al., “Microsoft Word Forensic Artifacts in Windows 10 Registry”, IEEE (ISBN:978-1-7281-2353-0/19)
- [13] Muhammad Raheel Arshad, Mehdi Hussain, Hasan Tahir, et al., “Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems”, IEEE Vol. 9 (2021)
- [14] Leng Tao, Yu Aimin, “A Framework of Darknet Forensics”, 3<sup>rd</sup> International Conference on Advanced Information Science and System (AISS 2021)



- [15] Ashar Neyaz, Narasimha Shashidhar, "USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs", Electronics 2019 Vol. 8 1322
- [16] Anthony Keane, Stephen O' Shaughnessy, "Tracking User Activity on Personal Computers", October 2011
- [17] Adesoji A. Adesina, Ayodele Ariyo Adebiyi, Charles K. Ayo, "Identification of forensics artifacts from the registry of windows 10 device in relation to idrive cloud storage usage", Bulletin of Electrical Engineering and Informatics Vol. 11, No. 1, pp. 521-529 February 2022
- [18] Walter Buyu, Elisha Odira Abade, "Forensic Analysis of Dropbox Data Remnants on Windows 10", International Journal of Computer Applications (0975-8887) Vol. 176 No. 41, July 2020
- [19] Alexander I. Borodin, Roman R. Veynberg et al., "Simulation of artefact detection in Viber and Telegram instant messengers in Windows operating systems", Business Informatics Vol. 13 No. 4 2019
- [20] V. Visoottiviseth, A. Noonkhan et al., "AXREL: Automated Extracting Registry and Event Logs for Windows Forensics", 27<sup>th</sup> International Computer Science and Engineering Conference (ICSEC) 2023