Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ιδιωτική περιήγηση: τι αφήνει στον υπολογιστή ;** **Incognito mode: what's left behind**
Ονοματεπώνυμο Φοιτητή	**Αλέξανδρος Νικόλαος Αγγελής**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΣΠ/ 15002**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2018**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής	Ευθύμιος Αλέπης Επίκουρος Καθηγητής	Γεώργιος Τσιχριτζής Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη – Abstract

Η παρούσα πτυχιακή διατριβή υποβάλλεται στο πλαίσιο του μεταπτυχιακού προγράμματος πληροφορικής <<Προηγμένα Συστήματα Πληροφορικής>> του Πανεπιστημίου Πειραιώς. Σκοπός της διατριβής είναι να εντοπίσουμε πιθανά ευρήματα της δραστηριότητας του χρήστη μετά τη χρήση ενός φυλλομετρητή σε κατάσταση ιδιωτικής περιήγησης. Αυτό επιτυγχάνεται διενεργώντας ανάλυση ψηφιακών πειστηρίων σε λειτουργικά συστήματα Windows και Linux στα οποία έχουμε εγκαταστήσει τους ποιο διαδεδομένους φυλλομετρητές (Internet Explorer, Firefox, Google Chrome, Opera) στις τελευταίες εκδόσεις τους, αφού πρώτα έχουμε επισκεφτεί διαδικτυακές σελίδες σε κατάσταση ιδιωτικής περιήγησης. Η έρευνα έγινε στους δίσκους και τη μνήμη των συστημάτων οι οποίοι εξήχθησαν με τη βοήθεια λογισμικού ψηφιακής σήμανσης.

This dissertation is submitted to the University of Piraeus in partial fulfillment of the requirements for the Master's degree in Advanced Informatics Systems. The aim of this dissertation is to identify possible findings of the user's activity after using a browser in private browsing mode. This was achieved by conducting digital forensics in two different operational systems, Windows and Linux while using the most popular browsers(Internet Explorer, Firefox, Google Chrome, Opera) in private mode. The investigation was performed on the disk and memory, both of which were captured with the help of forensic software.

1. ΕΙΣΑΓΩΓΗ

1.1 ΕΙΣΑΓΩΓΗ

Στις μέρες οι κακόβουλοι χρήστες προσπαθούν συνεχώς να κλέψουν τα δεδομένα ανυποψίαστων χρηστών με όποιον τρόπο μπορούν. Δεδομένα όπως αριθμοί πιστωτικών καρτών, κωδικοί τραπεζικών λογαριασμών, αριθμοί κοινωνικής ασφάλισης, διευθύνσεις ηλεκτρονικού ταχυδρομείου και άλλα πολλά τα οποία μπορούν να χρησιμοποιηθούν άμεσα ή έμμεσα για κάποιο κακόβουλο σκοπό. Για παράδειγμά κλέβοντας τον τραπεζικό κωδικό για το e-banking θα μπορούσε κάποιος να αφαιρέσει χρήματα από το λογαριασμό σας ή να κάνει ηλεκτρονικές αγορές. Σε άλλο επίπεδο όμως γνωρίζοντας τις προτιμήσεις σας όσον αφορά τη διαδικτυακή περιήγηση σας με τον φυλλομετρητή, θα μπορούσε με τη χρήση social engineering να σας αποσπάσει περισσότερες πληροφορίες. Επίσης στις μέρες παρατηρούμε ότι σε πολλές εφαρμογές δίνετε βαρύτητα στη client side λειτουργικότητα,η οποία είναι και πιο επιρρεπής αφού η ασφάλεια των δεδομένων επαφίεται στον πελάτη-χρήστη, και φυσικά οι φυλλομετρητές(browsers) δεν αποτελούν εξαίρεση. Επομένως είναι πολύ σημαντικό να διασφαλίσουμε την ιδιοτικότητα των πληροφοριών στο διαδίκτυο. Σε επίπεδο δικτύου πολλές σελίδες χρησιμοποιούν κρυπτογράφηση (SSL, TLS κ.α) για τη μεταφορά δεδομένων ιδίως ηλεκτρονικά καταστήματα ή τράπεζες. Από τι πλευρά του χρήστη όμως που χρησιμοποιεί τις υπηρεσίες αυτές μέσω ενός φυλλομετρητή τι γίνεται ; Εδώ έρχονται οι εταιρίες που παρέχουν τους browsers τους οποίους εμπλουτίζουν με λειτουργίες όπως την ιδιωτική περιήγηση (Private Browsing Mode) η οποία είναι και το αντικείμενο έρευνας της παρούσας διπλωματικής εργασίας.

1.2 Ιστορία των φυλλομετρητών και ασφάλεια αυτών

Προκάτοχοι των φυλλομετρητών εμφανίστηκαν με τη μορφή hyperlinked εφαρμογών κατά τα τέλη της δεκαετίας του 80. Στη συνέχεια ο Tim Berners-Lee ανέπτυξε τον πρώτο web server και web browser γνωστό και ως WorldWideWeb που αργότερα μετονομάστηκε σε Nexus. Πολλοί ακολούθησαν όπως ο Mosaic του Marc Andreessen το 1993 ο οποίος ήταν αρκετά εύκολος στη χρήση και την εγκατάσταση. Μάλιστα συχνά του πιστώνουν καταλυτικό ρόλο στην έκρηξη του διαδικτύου τη δεκαετία του 1990. Ο Mosaic ήταν ο πρώτος γραφικός φυλλομετρητής που έτρεχε σε μια πλειάδα δημοφιλών υπολογιστών. Ήταν ο πρώτος φυλλομετρητής που σκόπευε να φέρει πολυμεσικό περιεχόμενο σε απλούς χρήστες και επομένως να εμφανίζει περιεχόμενο που περιελάμβανε εικόνα και κείμενο στην ίδια σελίδα αντίθετα με προηγούμενους φυλλομετρητές. Στη συνέχεια η ομάδα στη συνέχεια δημιούργησε τον Netscape Navigator και αργότερα το 2002 τον Mozilla 1 που αργότερα μετονομάστηκε σε Firefox. Γρήγορα ακολούθησε και η Microsoft το 1995 με τον Internet Explorer. Το 2003 η Apple έβγαλε τον δικό της φυλλομετρητή τον Safari. Το 2008 η Google δημιούργησε τον δικό της Google Chrome. Σήμερα οι πιο διαδεδομένοι φυλλομετρητές είναι οι Chrome, Firefox, Safari, Internet Explorer και Edge.

Στις μέρες ο browser είναι αναπόσπαστο κομμάτι της περιήγησης μας στο διαδίκτυο αφού είναι η διεπαφή που μας επιτρέπει να κάνουμε τα πάντα σ αυτό. Επομένως είναι και επιτακτική ανάγκη να επικεντρωθούμε στην ασφάλεια για να διασφαλίσουμε ότι δε θα έχουμε διαρροή των προσωπικών δεδομένων μας σε τρίτους μέσω του φυλλομετρητή μας. Αν και στην αρχή οι εταιρίες που δούλευαν πάνω στους φυλλομετρητές δεν εστίαζαν καθόλου στην ασφάλεια και τους ενδιέφερε περισσότερο το γραφικό περιβάλλον και η αλληλεπίδραση με το χρήστη, σιγά σιγά η αύξηση χρήσης και η εισαγωγή καινούργιων εφαρμογών τους ανάγκασε να επικεντρωθούν σ αυτή. Ας δούμε όμως μια χρονική σειρά γεγονότων που μας διαφωτίζουν γύρω από την ασφάλεια των φυλλομετρητών.

Στις 14 Νοεμβρίου 1993 έχουμε την εμφάνιση του Common Gateway Interface που επιτρέπει στους διακομιστές να τρέχουν σε πραγματικό χρόνο scripts ώστε οι ιστότοποι να ανταποκρίνονται πιο γρήγορα στις αιτήσεις των χρηστών. Αυτό όμως είχε ως αποτέλεσμα και κάποιους κινδύνους όπως ότι έκανε τους διακομιστές πιο επιρρεπείς σε επιθέσεις από hackers. Στις 15 Δεκεμβρίου 1994 έχουμε τι πρώτη έκδοση του Netscape Navigator στον οποίο τον Μάρτιο του 1995 εισάγετε το SSL 2 (Secure Sockets Layer) και έτσι έχουμε τον πρώτο browser που προσφέρει HTTPS σύνδεση με σελίδες. Πρώτη

Σεπτεμβρίου 1995 δυο φοιτητές από το πανεπιστήμιο της Καλιφόρνια στο Berkeley ανακάλυψαν ένα ελάττωμα στην κρυπτογράφηση που χρησιμοποιούταν για τις πληρωμές μέσω διαδικτύου. Το paper δημοσιεύθηκε το 1996 αλλά η αδυναμία είχε αποκαλυφθεί το 1995. Δεκαεφτά μέρες μετά κάνει τη πρώτη της εμφάνιση η JavaScript στον NETSCAPE 2.0 και μαζί φέρνει πολλά προβλήματα ασφαλείας. Επίσης εισάγει τη λειτουργία same-origin policy για να προστατέψει από τυχόν πρόσβαση κακόβουλου χρήστη στο Document Object Model(DOM) πλεον όμως έχει διευρυνθεί η χρήση του για να προστατεύσει ευαίσθητα στοιχεία του JavaScript αντικοιμένου. Δέκα Οκτωβρίου τον ίδιο χρόνο η Netscape παρουσιάζει το πρόγραμμα “Bugs Bounty” που ανταμείβει με χρήματα όσους βρίσκουν ελαττώματα στο λογισμικό του φυλλομετρητή της. Δυο δεκαετίες μετά η δουλειά αυτή θα γνωρίσει μεγάλη άνθιση. Το 2000 η Microsoft εισάγει ένα νέο όρο το XSS (cross site scripting) μετά από πολλές αναφορές αδυναμιών και έρευνα. Επτά χρόνια αργότερα η Symantec θα υπολογίσει ότι τα XSS exploits, μια μεγάλη κατηγορία επιθέσεων είναι υπεύθυνα για το 84 τις εκατό όλων τον επιθέσεων. Σήμερα οι φυλλομετρητές έχουν φίλτρα για να εμποδίζουν αρκετά είδη αυτών τον επιθέσεων όχι όμως και όλα.

Το 2000 άρχισε ο μακρύς δρόμος της αλλαγής για το HTTPS απο SSL σε TLS λόγω όμως των δυσκολιών που έχουν οι αλλαγές σε θέματα ασφαλείας μόλις το 2014 μετά την ανακάλυψη του Poodle vulnerability οι πιο γνωστοί browsers σταμάτησαν να υποστηρίζουν το παλιό πρωτόκολλο. Τον Αύγουστο του 2001 η Microsoft βγάζει τον Internet Explorer 6 ο οποίος θα φτάσει να χρησιμοποιείτε από το 95% των χρηστών (φυσικά των Windows) και θα μείνει έτσι για μια δεκαετία. Το Μάιο του 2002 hackers αποκάλυψαν ότι μπορούν να κλέψουν το ιστορικό περιήγησης σου. Η διαρροή πληροφοριών είναι ένα πρόβλημα που αντιμετωπίζουμε ακόμα και σήμερα. Η συγκεκριμένη αδυναμία αντιμετωπίστηκε το 2014! Το 2004 και συγκεκριμένα την 25η Ιουνίου η Microsoft αρχίζει να παίρνει πιο σοβαρά την ασφάλεια του IE 6 όταν κυκλοφόρησε το Windows XP Service Pack 2, βελτιώνοντας έτσι τον browser με αναβαθμίσεις όπως τον pop up blocker. Το Νοέμβριο του 2004 έχουμε την εμφάνιση του Firefox, ο μόνος φυλλομετρητής που κατάφερε διψήφιο αριθμό χρήσης του πριν κάνει την εμφάνιση του ο Chrome της Google. Ο Firefox κατάφερε να ανεβάσει τη δημοτικότητα του εν μέρει λόγο των προβλημάτων ασφαλείας του IE 6 αλλά και ότι οι δημιουργοί του άνοιξαν ένα bug bounty για εύρεση αδυναμιών του φυλλομετρητή τους. Το Μάιο του 2005 το NoScript 1.0 κάνει την εμφάνιση του στο διαδίκτυο ως ένα αποκλειστικά Firefox πρόσθετο το οποίο μπλοκάρει διαδικτυακό περιεχόμενο απο το να εμφανίζει JavaScript, όπως και plug-ins Flash και Java. Το εν λόγο πρόσθετο είναι δημοφιλές ακόμα και σήμερα. Τον Αύγουστο του 2005 η Microsoft θα ενσωματώσει στον Internet Explorer 7 μια antiphishing list. Έτσι θα καταφέρει να κάνει πιο δύσκολο την εξαπάτηση πολλών ανθρώπων να και οι πρώτες εφαρμογές της λίστας έκαναν και πιο εύκολο να κατασκοπεύσεις τη διαδικτυακή κίνηση των χρηστών του IE. Το Adblock Plus εμφανίζεται στον Firefox τον Ιούνιο του 2006, η χρησιμότητα του είναι να σταματάει διαφημίσεις που εμφανίζονται σε διάφορους ιστοτόπους. Αν και αργότερα θα θεωρηθεί αμφιλεγόμενο πρόσθετο λόγο της εξαίρεσής κάποιον διαφημίσεων από το μπλοκάρισμα. Το Νοέμβριο του 2006 το ηλεκτρονικό ψάρεμα (phishig) μετρά 9200 phising sites και σχεδόν 100 πρόσθετα που αντιμετωπίζουν αυτό το είδος επίθεσης. Ακόμα και σήμερα το ηλεκτρονικό ψάρεμα μαστίζει το διαδίκτυο μαζί με τον πιο εστιασμένο spear phishing. Την 1η Ιουνίου 2008 ένας νέος όρος γεννιέται από τους ερευνητές. Ο όρος clickjacking περιγράφει όταν ένας κακόβουλος χρήστης κρύβει κακόβουλο κώδικα πίσω από ένα φαινομενικά έγκυρο περιεχόμενο. Την 1η Σεπτεμβρίου του ιδίου χρόνου η Google βγάζει τον δικό της φυλλομετρητή, τον Chrome ο οποίος έχει το πρώτο sandbox ασφαλείας σε επίπεδο διεργασίας. Τελικά όλοι οι μεγάλοι browser υιοθετούν την ίδια τεχνική σε διάφορες μορφές. Είναι το κλειδί για τη τελευταία λέξη στην ασφάλεια των φυλλομετρητών. Τον Μάρτιο του 2009 ένα αμφιλεγόμενο πρόσθετο, το Do Not Track προσπαθεί απεγνωσμένα για αποδοχή και τελικά αποτυγχάνει να ενδυναμώσει την ιδιοτικότητα των χρηστών κυρίως λόγο των ισχυρών διαφημιστικών εταιριών. Τον Ιούνιο του 2009 ο Mozilla παρουσιάζει στους προγραμματιστές ένα τρόπο να ορίζουν λίστες με αξιόπιστους ιστοτόπους με αποτέλεσμα να μειωθούν οι XSS(cross side script) απειλές. Έτσι γεννήθηκε και η ιδέα, των οδηγούμενων απο τους προγραμματιστές,μετριασμών των απειλών στον φυλλομετρητή. Τον Ιανουάριο του 2010 η Google ανοίγει το δικό της bug bounty για τον Chrome μαζί με ένα κύκλο ενημερώσεων 6 εβδομάδων του browser. Μαζί με την αυτόματη ενημέρωση αυτά βεβαιώνουν ότι όλο και περισσότεροι χρήστες θα έχουν τις πιο πρόσφατες ενημερώσεις ασφαλείας. Ο Firefox ακολουθεί κι αυτός το 2011.

Τον Ιούνιο του 2011 η Google οδηγούμενη από τις εξελίξεις στα χαρακτηριστικά των φυλλομετρητών και την ανάπτυξη στη δημιουργία των ιστοτόπων, βγάζει το δικό της laptop που χρησιμοποιεί τον Chrome ως λειτουργικό σύστημα που είναι πολυδιαφημισμένο για την αυστηρή ασφάλεια του. Τον ίδιο χρόνο τον Ιούλιο έχουμε την έκδοση των απαραίτητων προϋποθέσεων για την καθιέρωση κοινής προτυποποίησης για τα πιστοποιητικά ασφαλείας των ιστοτόπων. Μετά από αρκετά χρόνια ανάπτυξης, τον Οκτώβριο του 2012, το HTTP Strict Transport Security (HSTS) γίνεται δεκτό ως πρότυπο για τους browsers. Δουλειά του να προστατεύει ιστοτόπους από επιθέσεις που τους αναγκάζουν να αλλάξουν από HTTPS σε HTTP πρωτόκολλο. Η Google, μετά από αρκετά περιστατικά διανομής κακών πιστοποιητικών google.com, προτείνει ως άμυνα το καρφίτσωμα του δημοσίου κλειδιού. Η Google μειώνει το Σεπτέμβριο του 2016 τα NPAPI binary plug-ins, στα πρόσθετα αυτά συγκαταλέγονται το Flash Player, QuickTime και Java, τα οποία είναι γνωστά για τα συνεχή προβλήματα ασφαλείας τους. Οι υπόλοιπες εταιρίες ακολουθούν.

Την πρώτη Απριλίου του 2014 ένα σοβαρό ελάττωμα ασφαλείας στην κρυπτογραφική βιβλιοθήκη του OpenSSL αφήνει εκτεθειμένο περίπου το 66 τοις εκατό στους hackers. Αν και πολλοί ιστότοποι διευθέτησαν την αδυναμία, το Heartbleed κατάφερε να συνταράξει το διαδίκτυο. Νοέμβριος 2014 ανακοινώνετε μια πρωτοβουλία τεχνολογικών εταιριών και οργανισμών ψηφιακών δικαιωμάτων, το Let's Encrypt. Σκοπός του να διανείμει δωρεάν πιστοποιητικά στους web servers. Μέχρι τον Ιούνιο του 2016 πάνω από 7 εκατομμύρια μοναδικά domain ήταν προστατευμένα. Το 2016 ακόμα το 0.26 τοις εκατό των χρηστών του διαδικτύου χρησιμοποιούν τον Internet Explorer 6 αν και η Microsoft πλέον υποστηρίζει μόνο τον IE 11 και τον καινούργιο φυλλομετρητήτης EDGE. Τον Ιούλιο του 2016 ο Chrome και ο Firefox μειώνουν ακόμα περισσότερο την υποστήριξη τους για τον Flash λόγω των πολλών προβλημάτων ασφαλείας που συνεχίζει να έχει. Τον Αύγουστο του 2016 ο Mozilla ανακοινώνει ότι ο Firefox θα αποκτήσει sandboxed browser διεργασίες.

1.3 Αντικείμενο της Ερευνας

'Όπως βλέπουμε και από το ιστορικό της ασφάλειας των φυλλομετρητών, η ιδιωτικότητα ήταν πάντα ένα πρόβλημα για τους φυλλομετρητές. Ο στόχος αυτής της διατριβής είναι να διερευνήσουμε κατά πόσο η λειτουργία ιδιωτικής περιήγησης παρέχει και διασφαλίζει την ιδιωτικότητα του χρήστη. Χρησιμοποιώντας τα εργαλεία της ψηφιακής ανάλυσης πειστηρίων αλλά και την κατάλληλη μεθοδολογία θα εξακριβώσουμε κατά πόσο οι φυλλομετρητές διασφαλίζουν την ιδιωτικότητα μας.

'Όλοι οι μεγάλοι browsers στους ιστότοπους τους έχουν άρθρα για το πως να ενεργοποιήσεις την ιδιωτική περιήγηση αλλά και πως λειτουργεί. Όλοι οι φυλλομετρητές υποστηρίζουν πως αφού κλείσεις την εφαρμογή περιήγησης αυτή δε κρατά αποθηκευμένα το ιστορικό(browsing history), τα cookies, την cache, και πληροφορίες που έχουν πληκτρολογηθεί σε φόρμες όπως κωδικοί, ονόματα χρήστη και άλλα. Ποιο συγκεκριμένα ο κάθε browser αναφέρει τα εξής στον ιστότοπο του:

Chrome: Δεν αποθηκεύει browsing history, cookies, site data ή πληροφορίες που εισάγουμε σε φόρμες. Διευκρινίζεται ότι οι πληροφορίες των ιστοτόπων και τα cookies όσο χρησιμοποιείτε η ιδιωτική περιήγηση υπάρχουν στον φυλλομετρητή, μετά το κλείσιμο του Incognito όμως αυτά διαγράφονται.

Firefox:: Δεν αποθηκεύει σελίδες που επισκεφθήκαμε, φόρμες και τις αναζητήσεις μας, κωδικούς, λίστα με τα download, cookies, cache web περιεχόμενο και offline web περιεχόμενο ή δεδομένα χρηστών.

Opera: Αφού κλείσουμε την εφαρμογή δεν αποθηκεύετε το ιστορικό, η cache, cookies, και logins.

Internet Explorer: Αντίστοιχα και εδώ δεν αποθηκεύεται το ιστορικό, προσωρινά αρχεία Internet, δεδομένα φορμών, cookies, κωδικοί και ονόματα χρηστών.

Να σημειώσουμε εδώ ότι τα αρχεία που μπορεί να έχουμε μεταφορτώσει ή πιθανά αγαπημένα που δημιουργήσαμε κατά τη διάρκεια της ιδιωτικής περιήγησης θα παραμείνουν και δε θα σβηστούν μετά το κλείσιμο του φυλλομετρητή.

Σχετική έρευνα όσον αφορά την ιδιωτική περιήγηση έχει γίνει με διαφορετικές προσεγγίσεις. Αρκετές επικεντρώθηκαν στην ανάλυση μνήμης και δίσκου από την οποία βρήκαν ίχνη της ιδιωτικής περιήγησης αναλύοντας τα ίδια αρχεία στο δίσκο που αναλύσαμε σ αυτή την διατριβή. Στο δίσκο πιο συγκεκριμένα βρήκαν στοιχεία από το pagefile και από διάφορα log αρχεία[27][28]. 'Άλλη έρευνα

επικεντρώθηκε στα extensions, plugins, certificates αλλά και σε site-specific preferences απο τα οποία μπορούσαν να βρουν στοιχεία για την ιδιωτική περιήγηση [29]. Τέλος έχουν γίνει και κάποιες ώστε να γίνει γνωστό κατά πόσο οι χρήστες κατανοούν την έννοια της ιδιωτικής περιήγησης. Από τα αποτελέσματα των ερευνών αυτών αντιλαμβανόμαστε μια γενική παρανόηση σχετικά με το τη προστατεύει και τι όχι η επιλογή της ιδιωτικής περιήγησης. Συγκεκριμένα υπάρχουν αρκετοί που πιστεύουν ότι είναι “αόρατοι”, δεν μπορούν να πέσουν θύμα κακόβουλης ενέργειας(hacking), ότι μπλοκάρετε το tracking των ιστοτόπων και η διαφημίσεις[26][31][33].

2. Digital Forensics – Ψηφιακή σήμανση - Ανάλυση

2.1 Ορισμοί

Ανάλυση:Ως ανάλυση ορίζουμε τη διαδικασία της συλλογής δεδομένων, τη συσχέτιση τους και τελικά την ερμηνεία τους

Για τη ψηφιακή σήμανση έχουμε δυο ορισμούς οι οποίοι είναι οι εξής:

1. Ψηφιακή σήμανση είναι ένας κλάδος της σήμανσης που περιλαμβάνει την ανάκτηση και την έρευνα του ψηφιακού υλικού (που βρίσκεται σε ψηφιακές συσκευές), που έχει σχέση με το έγκλημα πληροφορικής(κυβερνοέγκλημα).
2. Ψηφιακή σήμανση (Digital Forensics) είναι η αποδεδειγμένη επιστημονική διεργασία με την οποία συλλέγουμε, αναλύουμε και παρουσιάζουμε αποδεικτικά στοιχεία στο δικαστήριο.

2.2 Πρακτική μεθοδολογία

Για να έχουμε το καλύτερο δυνατό αποτέλεσμα όπως και αποδεκτά από το δικαστήριο στοιχεία ακολουθούμε μια τυποποιημένη πρακτική μεθοδολογία η οποία αποτελείτε από 8 απλά βήματα.

1. Επιβεβαίωση συμβάντος (Verification)
2. Περιγραφή συστήματος (System description)
3. Συλλογή δεδομένων (Evidence Acquisition)
4. Χρονική ανάλυση δεδομένων (Timeline Analysis)
5. Ανάλυση συσκευών αποθήκευσης (Media analysis)
6. String or Byte αναζήτηση (search)
7. Αποκατάσταση δεδομένων (Data Recovery)
8. Αναφορά (Reporting)

Με λίγα λόγια στη πράξη ανακτούμε, διατηρούμε (προσοχή να τηρούμε τη σωστή διαδικασία φύλαξης-επιμέλειας chain of custody) και εξετάζουμε τα δεδομένα μας. Στη συνέχεια αναλύουμε τη μνήμη, τη registry(ανάλογα το λειτουργικό σύστημα) και το σκληρό δίσκο. Ακολουθεί ο εντοπισμός και η ανάλυση αγνώστων αρχείων και τελειώνοντας αναλύουμε δυναμικά και στατικά το πιθανό ιομορφικό λογισμικό.

Τελικά ακολουθώντας τα παραπάνω βήματα όπως προαναφέρθηκαν θα έχουμε ένα σωστό αποτέλεσμα. Πρέπει να δώσουμε ιδιαίτερη προσοχή στη διαδικασία φύλαξης-επιμέλειας ώστε να μην αλλοιώσουμε τα δεδομένα μας. Να λαμβάνουμε σημειώσεις για κάθε βήμα που κάνουμε, να ελέγχουμε τα εργαλεία που χρησιμοποιούμε (πχ αν επιφέρουν κάποιες σημαντικές αλλαγές στα δεδομένα μας που θα μας δημιουργήσουν πρόβλημα στην ανάλυση άρα και σε εσφαλμένα αποτελέσματα). Να επιβεβαιώνουμε τη μεθοδολογία συνεχώς ότι την ακολουθούμε σωστά και τέλος να επιβεβαιώνουμε τα αποτελέσματα που βγάζουμε.

Σε γενικές γραμμές μπορούμε να επιτύχουμε τα εξής:

1. Αποκατάσταση διαγραφέντων δεδομένων

2. Αποκάλυψη πότε τα αρχεία τροποποιήθηκαν, δημιουργήθηκαν, διαγράφτηκαν
3. Μπορούμε να καθορίσουμε ποιες συσκευές τοποθετήθηκαν σε συγκεκριμένο υπολογιστή
4. Ποιες εφαρμογές εγκαταστάθηκαν και από ποιον χρήστη
5. Ποιες ιστοσελίδες επισκέφτηκε ο χρήστης του υπολογιστή

Παρόλα αυτά όσον αφορά την αποκατάσταση δεδομένων δε μπορεί να γίνει αν το αποθηκευτικό μέσο έχει καταστραφεί. Επίσης είναι πολύ δύσκολο έως αδύνατο να γίνει αποκατάσταση δεδομένων σε κάποιο αποθηκευτικό μέσο το οποίο έχει διαγραφεί με ασφαλή τρόπο.

2.3 Ψηφιακή ανάλυση φυλλομετρητή (Browser forensics)

Με την ανάλυση του φυλλομετρητή μπορούμε να εντοπίσουμε αρκετά πράγματα όσον αφορά τη συμπεριφορά του χρήστη στο διαδίκτυο.

- Ποιες ιστοσελίδες επισκέφτηκε ο χρήστης(history, cache, cookies, recovery folders)
- Πόσες φορές επισκέφτηκε μια ιστοσελίδα(history)
- Πότε επισκέφτηκε μια ιστοσελίδα(history,cache,cookies)
- Τι ιστοσελίδες αποθήκευσε ο χρήστης(bookmarks)
- Αρχεία που τυχόν κατέβασε ο χρήστης(download folder, cache)
- Εντοπισμός ονομάτων χρηστών(cache, cookies, recovery folders, autocomplete)
- Εντοπισμός αναζητήσεων χρήστη(cache, autocomplete)

Ποιο συγκεκριμένα σε κάθε browser που αναλύουμε μπορούμε να βρούμε τα αρχεία στις εξής τοποθεσίες.

Google Chrome:

Ο Chrome χρησιμοποιεί για τα περισσότερα αρχεία του το SQLite database format όπως για το ιστορικό, τα cookies, τη δραστηριότητα των πρόσθετων. Επίσης χρησιμοποιεί αρκετές cache(Disk_cache(backing storage),Memory_Cache(δεδομένα που αποθηκεύονται μόνο στη μνήμη),Media_Cache(χρησιμοποιείτε για το χειρισμό των media αρχείων),APP_Cache(backing store για AppCache),Shader_Cache(backing store για την GL shader cache και PNACL_CACHE(ως backing store για την PnaCL translation cache).

Η τοποθεσία σε Linux λειτουργικό για cache, history, downloads και cookies είναι:

/home/$USER/.config/google-chrome/$PROFILE/(και εδώ θα βρούμε history,cookies και download σε SQLite database μορφή, όπως και τις υπόλοιπες cache)

/home/$USER/.cache/google-chrome/$PROFILE/Cache/

/home/$USER/.config/google-chrome/$PROFILE/Cache/

Η τοποθεσία σε Windows VISTA και στις επόμενες εκδόσεις είναι:

C:\Users\%USERNAME%\APPData\Local\Google\Chrome\User Data\%PROFILE%\ (Αντίστοιχα και εδώ θα βρούμε ιστορικό κτλ)

C:\Users\%USERNAME%\APPData\Local\Google\Chrome\User Data\%PROFILE%\Cache\

C:\Users\%USERNAME%\APPData\Local\Google\Chrome\User Data\%PROFILE%\Application Cache\Cache

C:\Users\%USERNAME%\APPData\Local\Google\Chrome\User Data\%PROFILE%\Media Cache\

C:\Users\%USERNAME%\APPData\Local\Google\Chrome\User Data\%PROFILE%\GPUCache\

Firefox::

Και ο Firefox χρησιμοποιεί SQLite database για το ιστορικό τα cookies και τα downloads, η τοποθεσία είναι:

Linux:

/home/$USER/.mozilla/firefox/{profile folder}/(places.sqlite για το ιστορικό, cookies.sqlite για τα cookies, downloads)

/home/$USER/.mozilla/firefox/{profile folder}/Cache (cache v1)

/home/$USER/.cache/mozilla/firefox/{profile folder}/cache2 (cache v2 Firefox 32 και μετά)

Windows Vista/7/8:

C:\User\{user}\AppData\Roaming\Mozilla\Firefox\{profiles folder}\

C:\Users\{user}\AppData\Local\Mozilla\Firefox\Profiles\{profile folder}\Cache (cache v1)

C:\Users\{user}\AppData\Local\Mozilla\Firefox\Profiles\{profile folder}\cache2 (cache v2)

Opera:

Linux:

/home/$USER/.opera/ (εδώ βρίσκονται όλα τα δεδομένα του χρήστη)

/home/$USER/.opera/cache/

Windows:

C:\Users\%USERNAME%\AppData\Roaming\Opera\Opera\(για τα δεδομένα του χρήστη)

C:\Users\%USERNAME%\AppData\Local\Opera\Opera\cache\

Τρία σημαντικά αρχεία είναι το global_history.dat ένα αρχείο κειμένου με τρία πεδία (Title, URL,data and time), search_field_history.dat ένα XML αρχείο που περιέχει τις αναζητήσεις του χρήστη και typed_history.xml που περιέχει τα URL που πληκτρολόγησε ο χρήστης στη μπάρα διευθύνσεων.

Microsoft Edge:

Windows 8-10

Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\xxxxx\DBStore\spartan.edb

Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\

Users*user_name*\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\

Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Η Microsoft κάνει κι αυτή πλέον χρήση των βάσεων δεδομένων και όλες τις cache/history πληροφορίες τις αποθηκεύει σε μια μοναδική Jet Blue database, γνωστή και ως ESE (Extensible Storage Engine) με κατάληξη .edb. Το όνομα του αρχείου είναι WebCacheV*.dat και βρίσκεται στον WebCache φάκελο.

3. ΑΝΑΛΥΣΗ ΤΩΝ BROWSER

3.1 Περιγραφή διαδικασίας

Η ανάλυση της ιδιωτικής περιήγησης έγινε σε λειτουργικό σύστημα Windows 8.1 και Ubuntu Linux 16.04 LTS σε εικονικό περιβάλλον. Οι φυλλομετρητές που χρησιμοποιήθηκαν ήταν οι Microsoft Edge, Google Chrome, Firefox, Opera για το Windows λειτουργικό και Chrome, Firefox, Opera για το Linux. Το μέγεθος των σκληρών δίσκων ήταν 10 και 20 GB για Windows και Linux και οι μνήμες στα 1 και 2GB αντίστοιχα για τα δυο συστήματα. Στους φυλλομετρητές δεν είχαμε εγκαταστήσει κανένα πρόσθετο εκτός τα προεπιλεγμένα που είναι μαζί με την εγκατάσταση.

Σε κάθε σύστημα η διαδικασία ήταν να ανοίξουμε ένα παράθυρο ιδιωτικής περιήγησης να επισκεφθούμε έναν ιστότοπο με κάθε έναν browser. Αφού κλείσουμε τους φυλλομετρητές με κατάλληλα εργαλεία πήραμε τον δίσκο και τη μνήμη των λειτουργικών για να διεξάγουμε την ανάλυση τους. Επίσης συγκρίναμε και τις μνήμες μετά από sleep/hibernation. Οι ιστότοποι που επισκεφτήκαμε ήταν οι εξής:

Windows:

- Microsoft Edge: www.facebook.com
- Firefox : www.protagon.gr
- Chrome : www.gmail.com
- Opera : www.unipi.gr

Linux:

- Firefox : www.protagon.gr
- Chrome : www.gmail.com
- Opera : www.facebook.com

Τα εργαλεία που χρησιμοποιήσαμε για τη δημιουργία image του δίσκου και της μνήμης ήταν:

Για το Windows λειτουργικό:

- LiveResponseCollection-Allosaurus συλλογή script που εξάγουν μνήμη δίσκο αλλά και διάφορες άλλες πληροφορίες.

Για το Linux λειτουργικό:

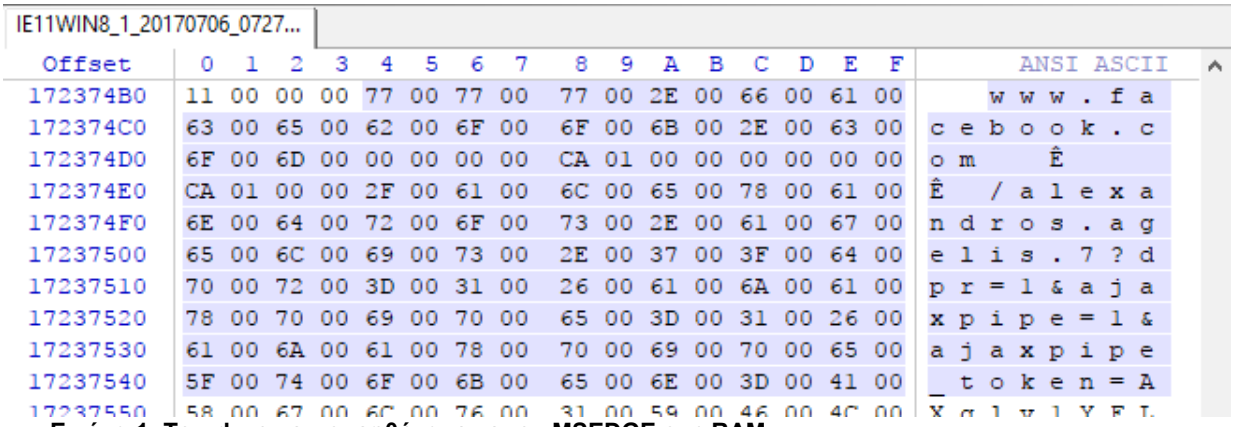
- dcfldd εργαλείο για να πάρουμε το δίσκο
- LiME-master εργαλείο για την μνήμη

Οι αναλύσεις έγιναν με το εργαλείο Autopsy για τους δίσκους και για τις μνήμες χρησιμοποιήσαμε το winhex.. Επίσης χρησιμοποιήσαμε και το SQLite Forensic Explorer και το ESEDatabaseview για τον έλεγχο των βάσεων δεδομένων. Στη συνέχεια παραθέτουμε τα αποτελέσματα της ανάλυσης των δεδομένων μας για τα 2 λειτουργικά και για κάθε φυλλομετρητή συγκεκριμένα.

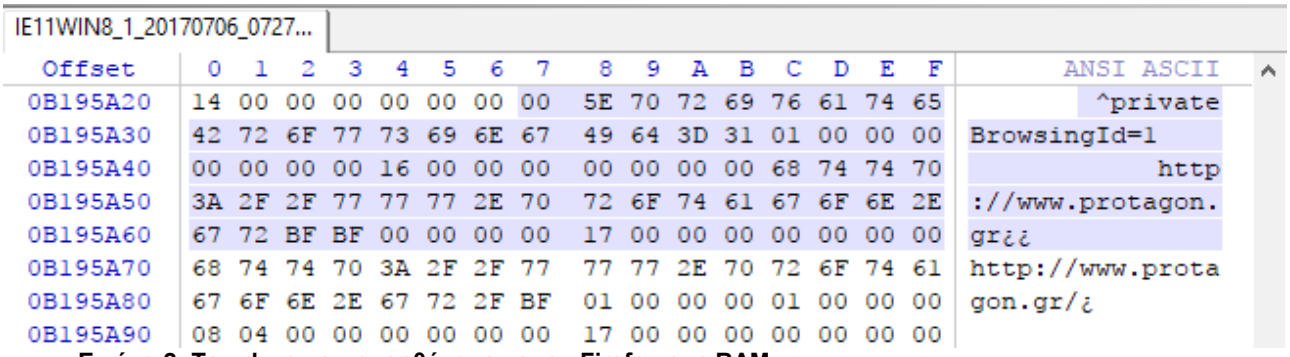
3.2 Αποτελέσματα ανάλυσης μνήμης Windows και Linux

Από την ανάλυση της μνήμης με τη βοήθεια του winhex μπορέσαμε να δούμε όλους τους ιστοτόπους που επισκεφθήκαμε σε ιδιωτική περιήγηση και στη περίπτωση των Unix βρήκαμε και τους κωδικούς του ηλεκτρονικού ταχυδρομείου και του facebook. Μάλιστα σε μερικά απ αυτά βλέπαμε και το αναγνωριστικό της ιδιωτικής περιήγησης.

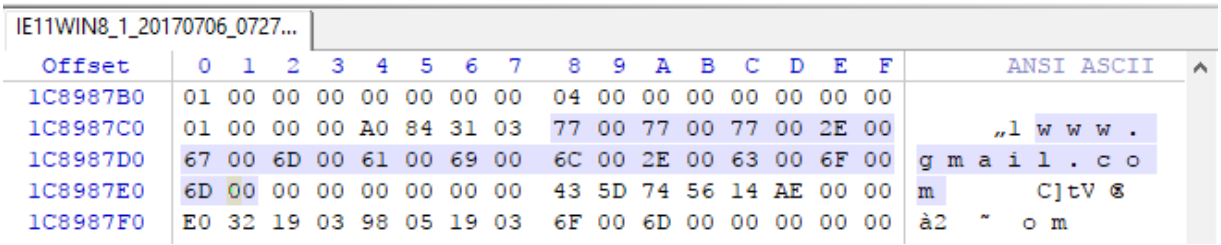
Εικόνες από την ανάλυση της μνήμης των Windows:



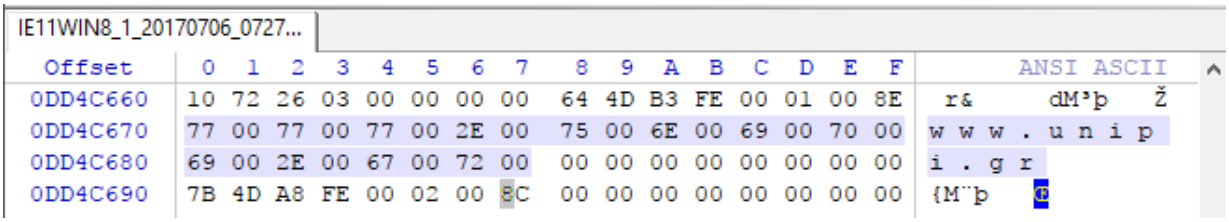
Εικόνα 1: Το url που επισκεφθήκαμε με τον MSEDGE στη RAM



Εικόνα 2: Το url που επισκεφθήκαμε με τον Firefox στη RAM



Εικόνα 3: Το url που επισκεφθήκαμε με τον Chrome στη RAM

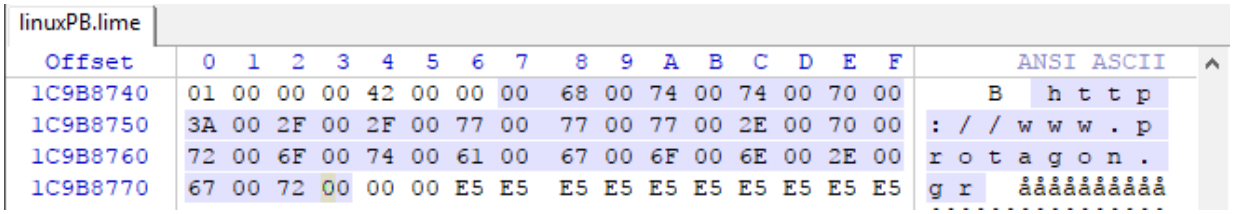


IE11WIN8_1_20170706_0727...

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0DD4C660	10	72	26	03	00	00	00	00	64	4D	B3	FE	00	01	00	8E	r& dM³þ Ž
0DD4C670	77	00	77	00	77	00	2E	00	75	00	6E	00	69	00	70	00	w w w . u n i p
0DD4C680	69	00	2E	00	67	00	72	00	00	00	00	00	00	00	00	00	i . g r
0DD4C690	7B	4D	A8	FE	00	02	00	8C	00	00	00	00	00	00	00	00	{M¨þ Œ

Εικόνα 4: Το url που επισκεφθήκαμε με τον Opera στη RAM

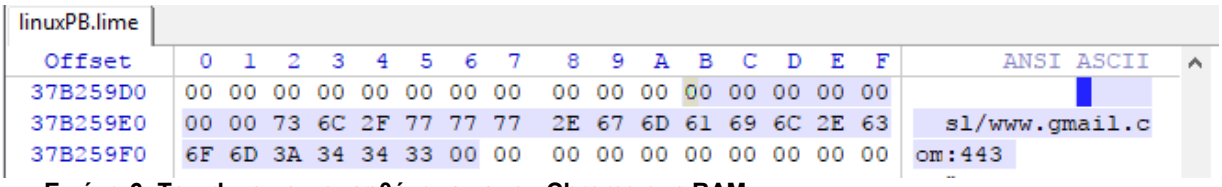
Εικόνες από την ανάλυση μνήμης των Linux:



linuxPB.lime

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1C9B8740	01	00	00	00	42	00	00	00	68	00	74	00	74	00	70	00	B h t t p
1C9B8750	3A	00	2F	00	2F	00	77	00	77	00	77	00	2E	00	70	00	: / / w w w . p
1C9B8760	72	00	6F	00	74	00	61	00	67	00	6F	00	6E	00	2E	00	r o t a g o n .
1C9B8770	67	00	72	00	00	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	g r åååååååååå

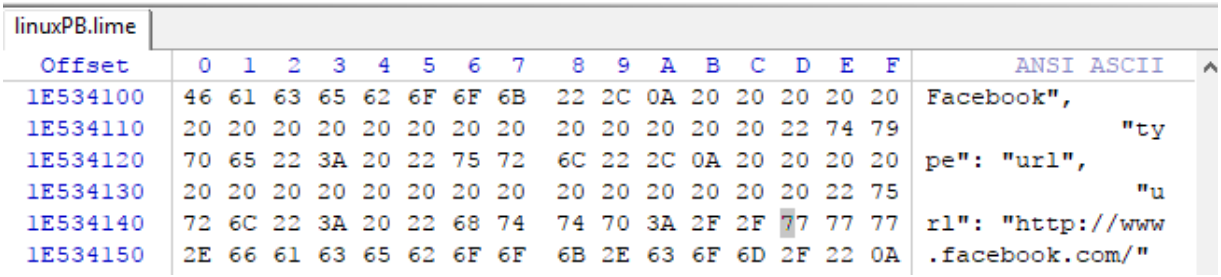
Εικόνα 5: Το url που επισκεφθήκαμε με τον Firefox στη RAM



linuxPB.lime

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
37B259D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
37B259E0	00	00	73	6C	2F	77	77	77	2E	67	6D	61	69	6C	2E	63	sl/www.gmail.c
37B259F0	6F	6D	3A	34	34	33	00	00	00	00	00	00	00	00	00	00	om:443

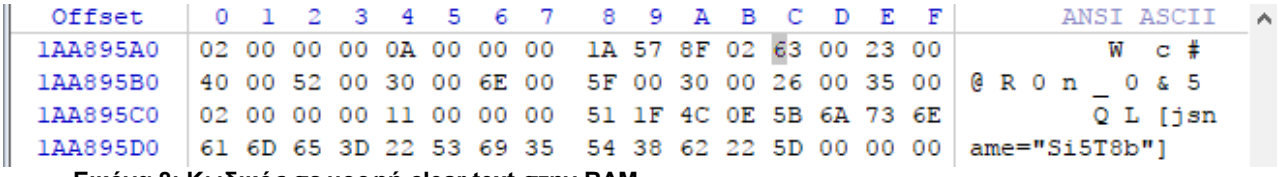
Εικόνα 6: Το url που επισκεφθήκαμε με τον Chrome στη RAM



linuxPB.lime

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1E534100	46	61	63	65	62	6F	6F	6B	22	2C	0A	20	20	20	20	20	Facebook",
1E534110	20	20	20	20	20	20	20	20	20	20	20	20	20	22	74	79	"ty
1E534120	70	65	22	3A	20	22	75	72	6C	22	2C	0A	20	20	20	20	pe": "url",
1E534130	20	20	20	20	20	20	20	20	20	20	20	20	20	20	22	75	"u
1E534140	72	6C	22	3A	20	22	68	74	74	70	3A	2F	2F	77	77	77	rl": "http://www
1E534150	2E	66	61	63	65	62	6F	6F	6B	2E	63	6F	6D	2F	22	0A	.facebook.com/"

Εικόνα 7: Το url που επισκεφθήκαμε με τον Opera στη RAM



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1AA895A0	02	00	00	00	0A	00	00	00	1A	57	8F	02	63	00	23	00	W c #
1AA895B0	40	00	52	00	30	00	6E	00	5F	00	30	00	26	00	35	00	@ R 0 n _ 0 & 5
1AA895C0	02	00	00	00	11	00	00	00	51	1F	4C	0E	5B	6A	73	6E	Q L [jsn
1AA895D0	61	6D	65	3D	22	53	69	35	54	38	62	22	5D	00	00	00	ame="Si5T8b"]

Εικόνα 8: Κωδικός σε μορφή clear text στην RAM

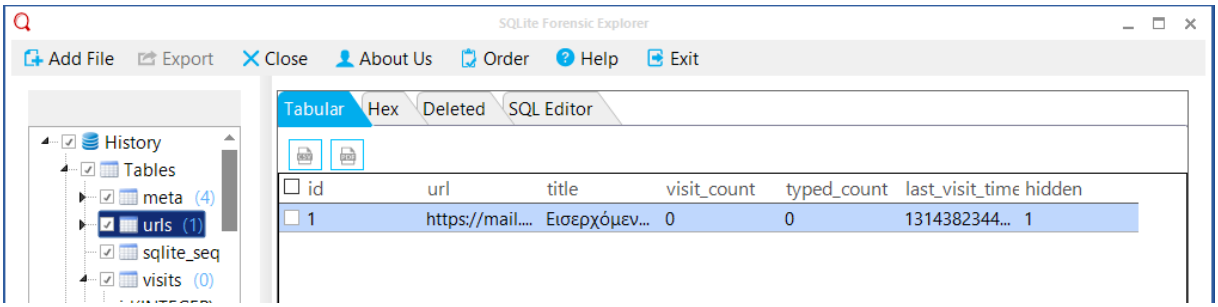
3.3 Αποτελέσματα ανάλυσης δίσκου Windows και Linux

Αν και γενικά στα Windows τα στοιχεία είχαν διαγραφεί και τα μόνα που ήταν ορατά ήταν τα αγαπημένα μπορέσαμε να βρούμε στοιχεία για τη περιήγηση μας με τον MSEdge συγκεκριμένα από διαγραμμένα αρχεία και το αρχείο pagefile.sys(εικονική μνήμη). Οι υπόλοιποι browsers είχαν στοιχεία αρκετά μόνο στο pagefile.sys.

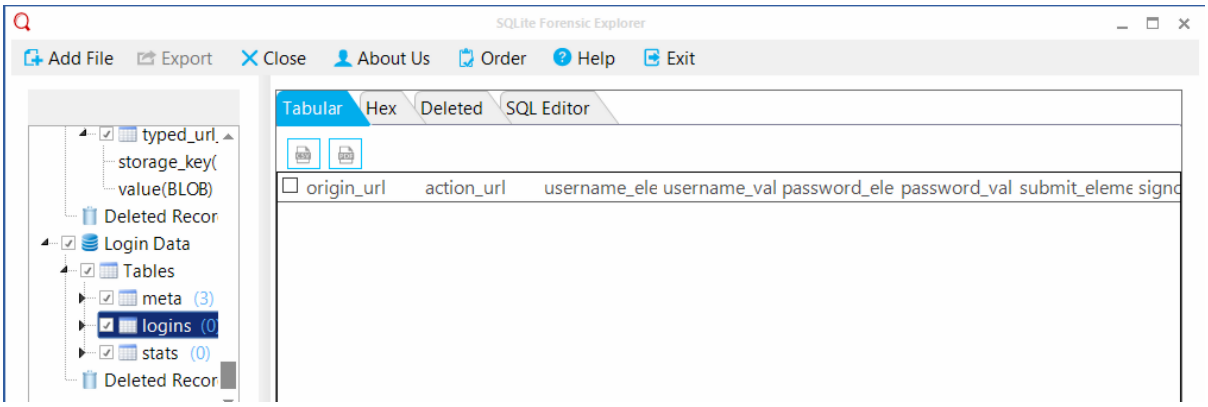
Αποτελέσματα ανάλυσης δίσκου Windows:

Chrome:

Ο chrome σβήνει όλα τα δεδομένα από τις sqlite βάσεις του κρατάει το bookmark που βάλαμε (gmail.com για το ηλεκτρονικό ταχυδρομείο) , μάλιστα στη βάση του history και datalogin δεν υπήρχαν δεδομένα αφού υπήρχε μόνο unallocate και χώρος που χρησιμοποιείτε.



Εικόνα 9: History database στον Chrome



Εικόνα 10: Login database στον Chrome

Πέρα από τις βάσεις ελέγξαμε και το αρχείο pagefile.sys στο οποίο βρήκαμε όπως και στη μνήμη προηγουμένως πληροφορίες της περιήγησης μας(url, κωδικούς κτλ)

114-pagefile.sys

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
6AD6A0B0	30	41	39	44	00	EC	00	A1	F2	83	37	A1	92	68	61	C6	0A9D ì ¡òƒ7¡'haÆ
6AD6A0C0	4A	8B	D5	2C	45	91	04	88	68	74	74	70	73	3A	2F	2F	J‹Õ,E' ˆhttps://
6AD6A0D0	6D	61	69	6C	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2F	mail.google.com/
6AD6A0E0	6D	61	69	6C	2F	75	2F	30	2F	00	00	00	0F	00	00	00	mail/u/0/
6AD6A0F0	98	02	80	08	08	8F	04	08	4D	8B	CE	2C	9B	92	04	8C	˜€ M‹Î,›' Œ
6AD6A100	C8	EB	D3	0B	68	03	D4	0B	C8	EB	D3	0B	01	00	90	08	ÈëÓ h Ô ÈëÓ
6AD6A110	50	55	42	53	10	ED	D3	0B	00	00	00	00	FF	FF	FF	FF	PUBS íÓ ÿÿÿÿ

Εικόνα 11: Σύνδεση στο gmail

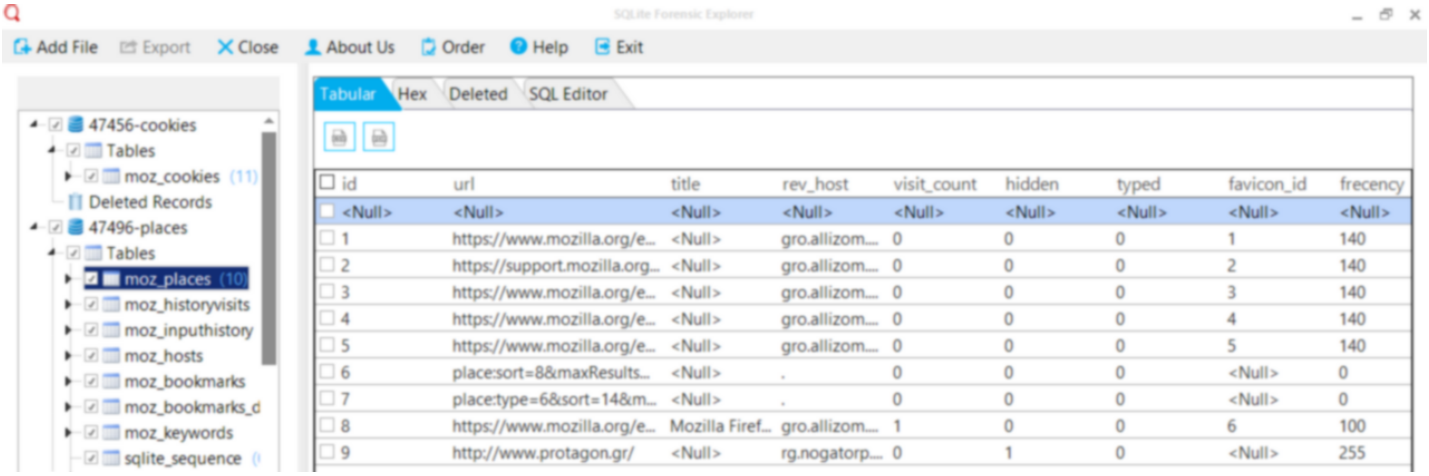
114-pagefile.sys

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
C782F010	5C	C6	B1	C5	3C	B2	2E	00	72	03	00	00	48	54	54	50	\Æ±Å<². r HTTP
C782F020	2F	31	2E	31	20	33	30	32	00	73	74	61	74	75	73	3A	/1.1 302 status:
C782F030	33	30	32	00	63	6F	6E	74	65	6E	74	2D	74	79	70	65	302 content-type
C782F040	3A	61	70	70	6C	69	63	61	74	69	6F	6E	2F	62	69	6E	:application/bin
C782F050	61	72	79	00	6C	6F	63	61	74	69	6F	6E	3A	68	74	74	ary location:htt
C782F060	70	73	3A	2F	2F	61	63	63	6F	75	6E	74	73	2E	67	6F	ps://accounts.go
C782F070	6F	67	6C	65	2E	63	6F	6D	2F	53	65	72	76	69	63	65	ogle.com/Service
C782F080	4C	6F	67	69	6E	3F	70	61	73	73	69	76	65	3D	31	32	Login?passive=12
C782F090	30	39	36	30	30	26	6F	73	69	64	3D	31	26	63	6F	6E	09600&osid=1&con

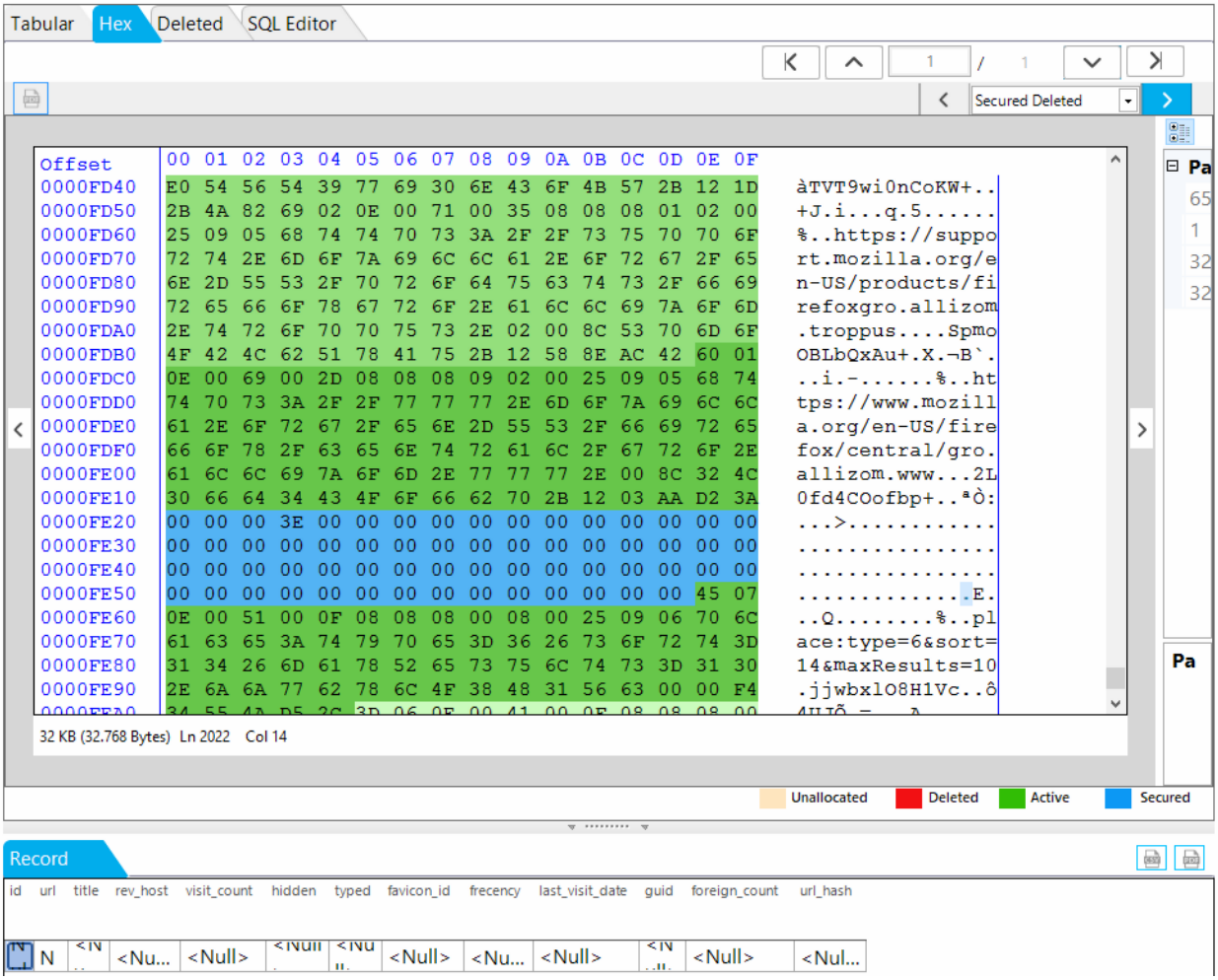
Εικόνα 12: Login σελίδα του gmail

Firefox::

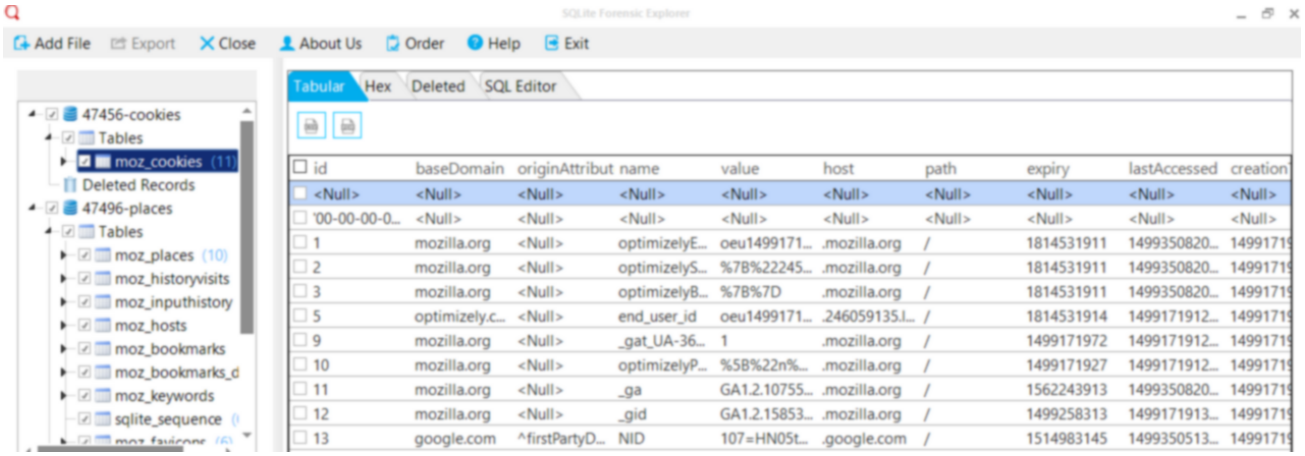
Και εδώ οι βάσεις ήταν άδειες από στοιχεία που είχαν σχέση με την ιδιωτική περιήγηση εκτός του bookmark και μάλιστα διαπιστώσαμε ασφαλή διαγραφή των περιεχομένων.



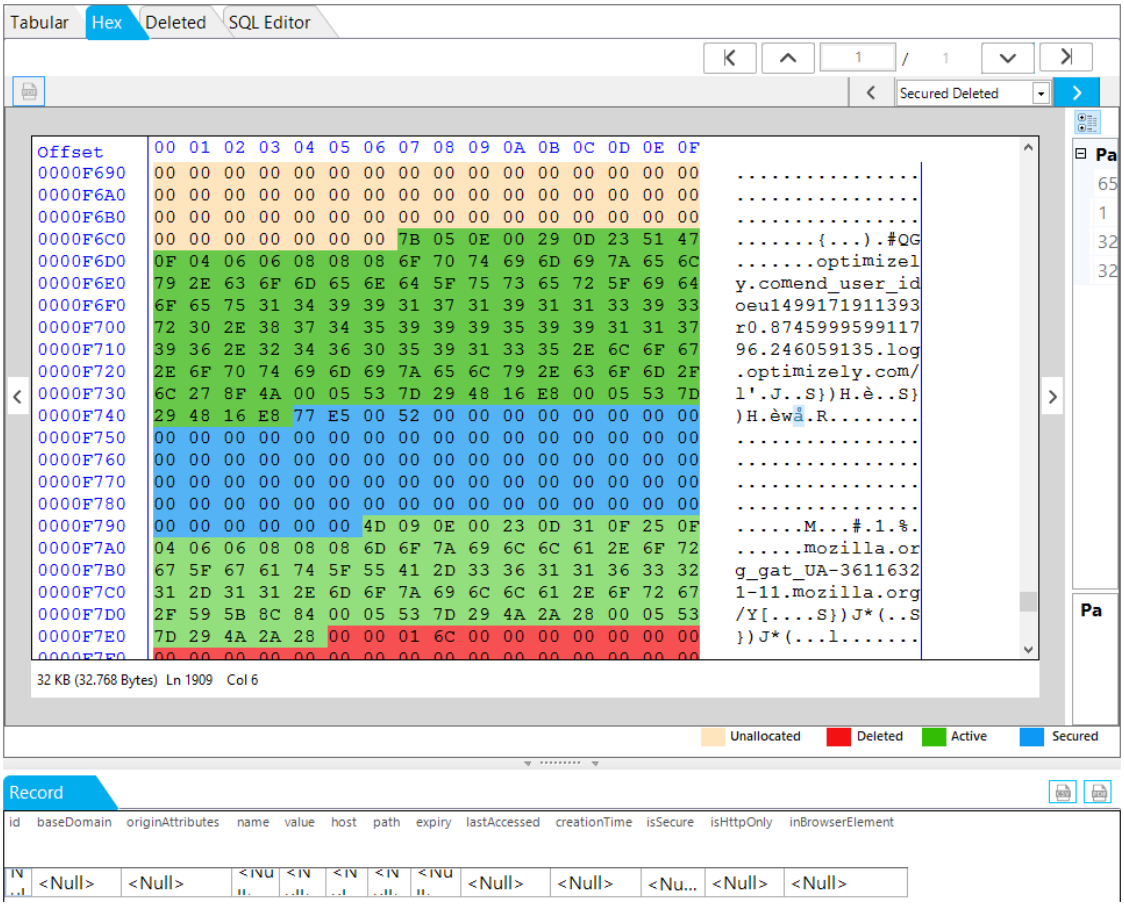
Εικόνα 13: Firefox places.sqlite



Εικόνα 14: Firefox places.sqlite secure data (μπλε χρώμα)

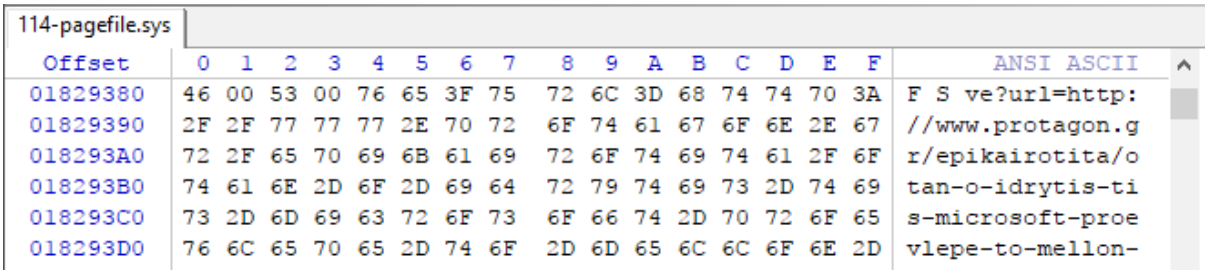


Εικόνα 15: Firefox cookie.sqlite



Εικόνα 16: Firefox cookie.sqlite secure delete (μπλε χρώμα)

Επίσης και στον firefox βρήκαμε δεδομένα από τη περιήγηση στο αρχείο pagefile.sys.



Εικόνα 17: Το url που επισκεφθήκαμε στο pagefile.sys

Opera:

Και στον Opera οι βάσεις ήταν άδεις από δεδομένα, μόνο το αγαπημένο που εισάγαμε εμείς(www.unipi.gr) υπάρχει από την συνεδρία μας και κάποιες φωτογραφίες που αντιστοιχούν σ αυτό.

Γενικά φαίνεται ότι δεν γράφει κάτι όταν περιηγούμαστε σε κατάσταση ιδιωτικής περιήγησης. Στο pagefile.sys και εδώ θα βρούμε τον ιστότοπο όπως και στους άλλους φυλλομετρητές.

114-pagefile.sys

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
D904A970	69	00	64	00	65	00	76	00	69	00	6E	00	65	00	43	00	i d e v i n e C
D904A980	64	00	6D	00	00	00	68	74	74	70	3A	2F	2F	77	77	77	d m http://www
D904A990	2E	75	6E	69	70	69	2E	67	72	2F	75	6E	69	70	69	2F	.unipi.gr/unipi/
D904A9A0	65	6C	2F	00	00	00	10	00	00	00	00	00	00	00	08	00	el/
D904A9B0	00	00	00	00	00	00	48	00	00	00	40	00	00	00	68	74	H @ ht
D904A9C0	74	70	3A	2F	2F	77	77	77	2E	75	6E	69	70	69	2E	67	tp://www.unipi.g
D904A9D0	72	2F	75	6E	69	70	69	2F	65	6C	2F	63	6F	6D	70	6F	r/unipi/el/compo
D904A9E0	6E	65	6E	74	2F	73	65	61	72	63	68	2F	3F	66	6F	72	nent/search/?for
D904A9F0	6D	61	74	3D	6F	70	65	6E	73	65	05	00	00	00	90	09	mat=opense

Εικόνα 18: Η διεύθυνση που επισκεφθήκαμε με τον Opera

id	url	title	visit_count	typed_count	last_visit_time	hidden
1	https://www.mozilla...	Firefox — 54.0.1 ...	1	0	1314364528304...	0
2	https://www.mozilla...		0	0	1314364528034...	1
3	https://www.mozilla...	Download Firefo...	1	0	1314364532212...	0
4	https://www.mozilla...	Desktop comput...	1	0	1314364530829...	0
5	https://www.mozilla...		0	0	1314364528035...	1
6	https://stubdownloa...		0	0	1314364532212...	1
7	http://app.prntscr.co...	Lightshot — scre...	1	0	1314382168248...	0
8	https://app.prntscr.c...	Lightshot — scre...	1	0	1314382168248...	0
9	https://app.prntscr.c...	Lightshot — scre...	1	0	1314382168248...	0

Εικόνα 19: Αποθηκευμένες διευθύνσεις του Opera – το unipi.gr δεν υπάρχει πουθενά

MSEdge:

Ο MS EDGE κι αυτός διαγράφει το ιστορικό και τα υπόλοιπα στοιχεία παρ όλα αυτά καταφέραμε να εντοπίσουμε διαγραμμένα αρχεία από την περιήγηση μας. Επιπλέον βρήκαμε και το url στην εικονική μνήμη και εδώ.

114-pagefile.sys

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
03B27420	00	00	00	00	68	00	74	00	74	00	70	00	73	00	3A	00	h t t p s :
03B27430	2F	00	2F	00	77	00	77	00	77	00	2E	00	66	00	61	00	/ / w w w . f a
03B27440	63	00	65	00	62	00	6F	00	6F	00	6B	00	2E	00	63	00	c e b o o k . c
03B27450	6F	00	6D	00	2F	00	00	00	00	00	00	00	00	00	04	00	o m /

Εικόνα 20: Διεύθυνση που επισκεφτήκαμε με τον MSEdge – facebook

Σε δυο διαδρομές βρήκαμε διαγραμμένα αρχεία (εικόνες, .js, .css, video κ.α.) τα οποία ήταν απο τη περιήγηση μας στο facebook. Οι διαδρομές αυτές είναι:

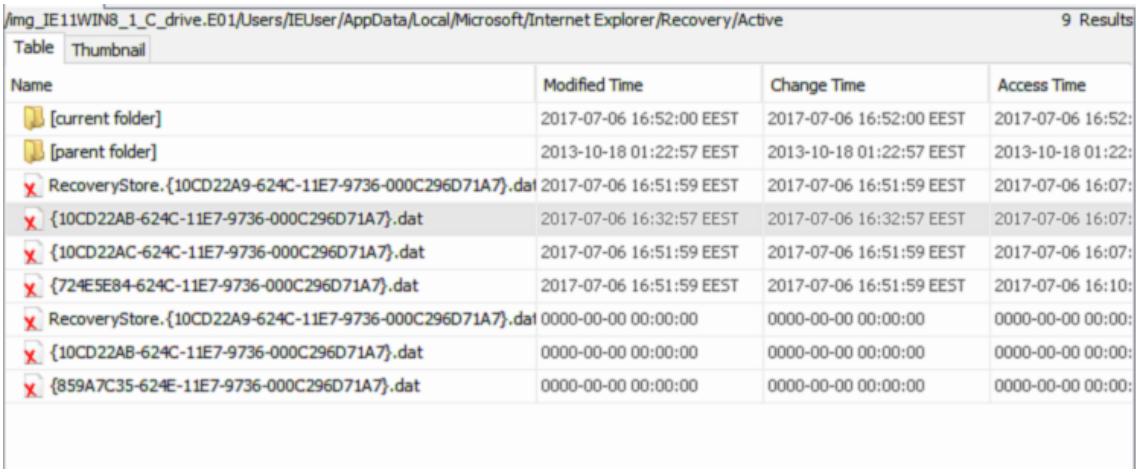
> Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\#!001\MicrosoftEdge\Cache\

Ολοι οι φάκελοι στη παραπάνω διαδρομή περιείχαν διαγραμμένα στοιχεία από τη περιήγηση μας.

Users*user_name*\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\Active\

Εδώ πιάσαμε διαγραμμένα αρχεία που περιείχαν στοιχεία για την περιήγηση μας πάλι και αποθηκευόντουσαν ώστε σε περίπτωση διακοπής λειτουργίας του φυλλομετρητή να επανέλθει στην προηγούμενη κατάσταση !!!!!

Το αρχείο WebCacheV01.dat δεν είχε κανένα ίχνος από τη διεύθυνση του facebook μετά από έλεγχο.



/img_IE11WIN8_1_C_drive.E01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/Active — 9 Results

Table | Thumbnail

Name	Modified Time	Change Time	Access Time
[current folder]	2017-07-06 16:52:00 EEST	2017-07-06 16:52:00 EEST	2017-07-06 16:52:
[parent folder]	2013-10-18 01:22:57 EEST	2013-10-18 01:22:57 EEST	2013-10-18 01:22:
RecoveryStore.{10CD22A9-624C-11E7-9736-000C296D71A7}.dat	2017-07-06 16:51:59 EEST	2017-07-06 16:51:59 EEST	2017-07-06 16:07:
{10CD22AB-624C-11E7-9736-000C296D71A7}.dat	2017-07-06 16:32:57 EEST	2017-07-06 16:32:57 EEST	2017-07-06 16:07:
{10CD22AC-624C-11E7-9736-000C296D71A7}.dat	2017-07-06 16:51:59 EEST	2017-07-06 16:51:59 EEST	2017-07-06 16:07:
{724E5E84-624C-11E7-9736-000C296D71A7}.dat	2017-07-06 16:51:59 EEST	2017-07-06 16:51:59 EEST	2017-07-06 16:10:
RecoveryStore.{10CD22A9-624C-11E7-9736-000C296D71A7}.dat	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:
{10CD22AB-624C-11E7-9736-000C296D71A7}.dat	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:
{859A7C35-624E-11E7-9736-000C296D71A7}.dat	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:

Εικόνα 21: Αρχεία στον φάκελο Recovery για τον MSEdge

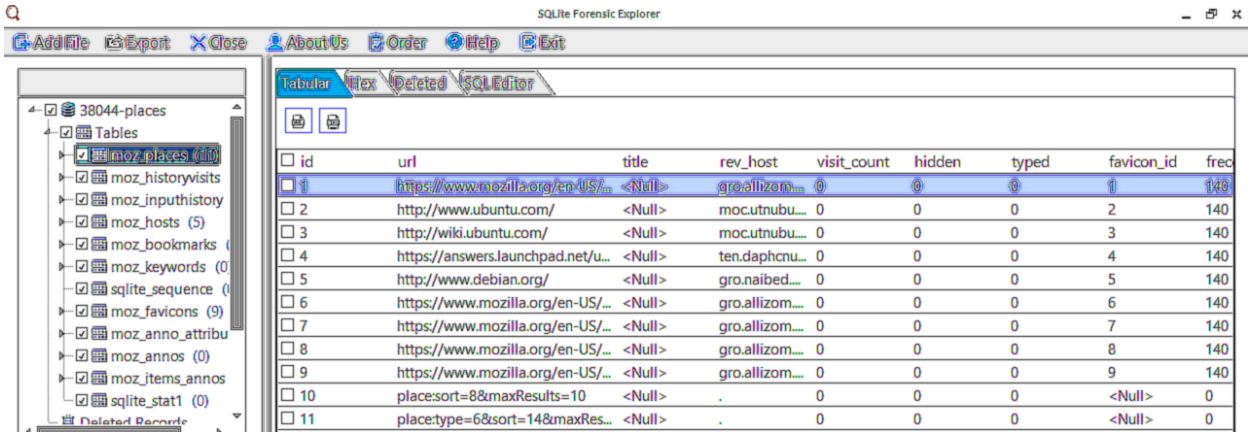
```
Root Entry
KjjaqfajN2c0uzgvll4qy5nfWe
TravelLog
Root Entry
KjjaqfajN2c0uzgvll4qy5nfWe
TravelLog
TL10
 i3%
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
text/html$
AVoi-45e
agelis_exogiinos
https://www.facebo
https://www.facebook.com/
Facebook - Log In or Sign Up
@hotmail.com
eyJ3IjoxMzYyLCJoIjo2NTMsImF3IjoxMzYyLCJhaCI6NjEzLCJjIjoyNH0=
060950_WjIH
1499346589
AAAAfVq/qKVVVVVAAAAAAAAKAAAAAAAAAAAAAAAAAAAANff/NNNAAQDBE
en_US
login_bluebar
AVoi-45e
TRST
TRST
TRST
TRST
```

Εικόνα 22: Περιεχόμενο αρχείου dat από το φάκελο recovery

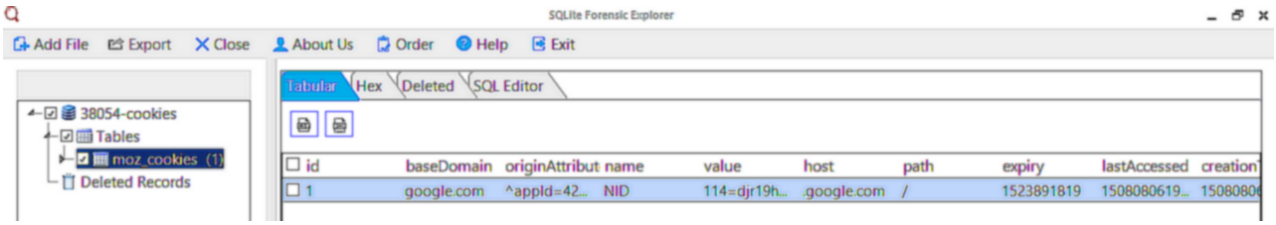
Αποτελέσματα ανάλυσης δίσκου Linux::

Firefox::

Μετά από ανάλυση του δίσκου δε βρέθηκαν εναπομείναντα στοιχεία από την περιήγηση μας, και εδώ ο Firefox δε φαίνεται να γράφει στο δίσκο κάτι ή τουλάχιστον διαγράφει ότι έχει γράψει με τρόπο ασφαλή οπότε η ανάκτηση είναι δύσκολη έως αδύνατη. Επόμενο βήμα να ελέγχουμε και δω τις sqlite βάσεις οι οποίες λόγω ιδιωτικής περιήγησης δεν έχουν εγγραφές από τους ιστοτόπους που επισκεφθήκαμε.



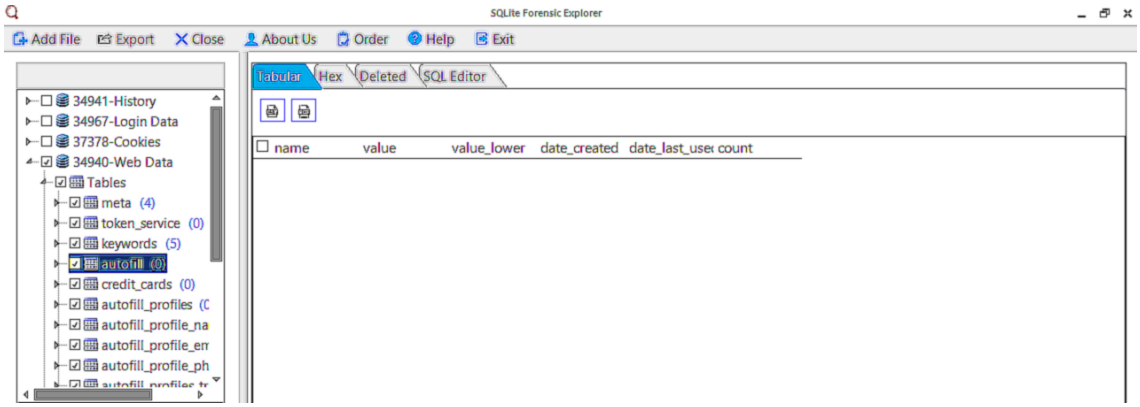
Εικόνα 23: Places.sqlite βάση του Firefox, δεν υπάρχει εγγραφή για το protagon



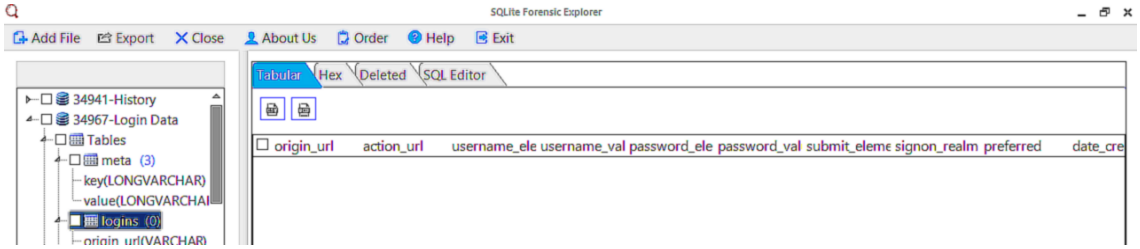
Εικόνα 24: Cookies.sqlite βάση του Firefox, μόνο cookie της google για τις επιλογές του χρήστη

Chrome:

Και εδώ ισχύουν τα ίδια με τον Firefox τίποτα δε γράφετε στο δίσκο και αν γράφετε διαγράφετε με ασφαλή τρόπο.



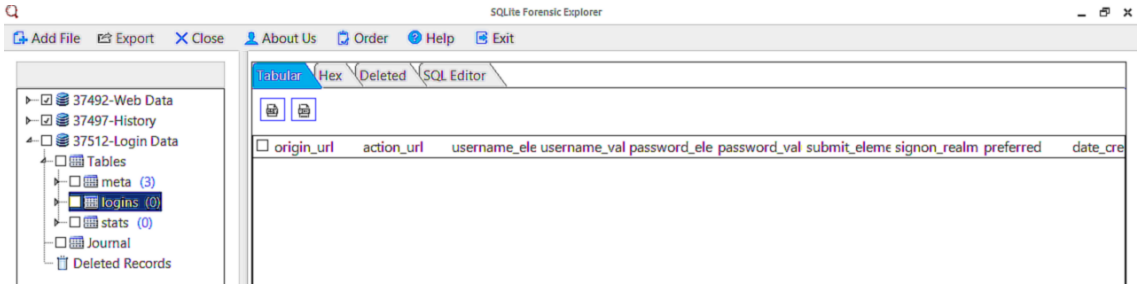
Εικόνα 25: Webdata.sqlite βάση δεν έχει εγγραφές



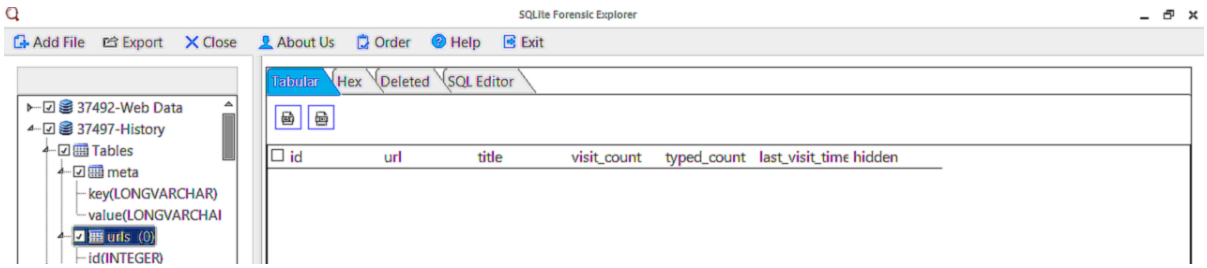
Εικόνα 26: Logindata βάση, δεν περιέχει όνομα χρήστη και κωδικό από το mail

Opera:

Και εδώ δε βρήκαμε τίποτα αξιόλογο στο δίσκο και στις βάσεις ειδικότερα. Παρακάτω θα δούμε τη βάση των συνδέσεων (login) και τα url στη βάση ιστορικού οι οποίες είναι άδειες κανένα στοιχείο ότι συνδεθήκαμε στο facebook.



Εικόνα 27: Βάση login, δεν περιέχει στοιχεία απο το facebook



Εικόνα 28: Βάση ιστορικού, δεν περιέχει το σύνδεσμο του facebook

Γενικές παρατηρήσεις:

Κλείνοντας να πούμε ότι και στα δυο λειτουργικά οι μνήμες μετά από sleep/hibernation ήταν ίδιες δηλαδή στις ίδιες θέσεις μνήμης βρήκαμε τους browsers που είχαμε ανοιχτούς. Αυτό συμβαίνει διότι στο μεν sleep mode ο υπολογιστής είναι σε κατάσταση χαμηλής ενέργειας και τροφοδοτείτε με ρεύμα τόσο ώστε να λειτουργεί η μνήμη στο δε hibernation mode όλη η μνήμη περνάει στον σκληρό δίσκο (δημιουργείτε ένα ακριβές αντίγραφό της) και ο υπολογιστής κλείνει σαν να έχουμε πατήσει το κουμπί power. Όταν κάνουμε επανεκκίνηση και τα δυο mode μας επαναφέρουν στην κατάσταση που ήμασταν πριν βάλουμε τον υπολογιστή σε sleep/hibernation με όλα τις εφαρμογές ανοικτές και ότι άλλο είχαμε ανοιχτό. Και στις δυο περιπτώσεις δεν αλλάζει κάτι στις θέσεις μνήμης γιατί στην πρώτη η μνήμη μένει ανέπαφη στη δεύτερη επαναφέρουμε τη μνήμη από το δίσκο όπως ήταν πριν. Μάλιστα στα windows μπορούμε να βρούμε το hiberfile.sys στην ίδια θέση με το pagefil.sys αρχείο στο σκληρό μας δίσκο και μπορεί κι αυτό να μας προσφέρει στοιχεία για την περιήγηση μας στο διαδίκτυο.

Τελικά όπως βλέπουμε και στο πίνακα στοιχεία μπορούμε να βρούμε κυρίως στη RAM ενώ στον MSEdge μπορούμε και στο δίσκο. Παρ' όλα αυτά πρέπει να έχουμε στο μυαλό μας και αλληλεπιδράσεις άλλον εφαρμογών και συγκεκριμένα των αντιικών προγραμμάτων. Συγκεκριμένα στα Windows βρέθηκε μια βάση με το όνομα url.db μέσα στο φάκελο του αντιικού προγράμματος AVG με όλα τα url που είχαμε επισκεφθεί ακόμα κι αυτά σε ιδιωτική περιήγηση. Επίσης μη ξεχνάμε ότι τα Windows μπορούν να συγχρονίζονται μεταξύ υπολογιστών που χρησιμοποιούμαι ή ακόμα και λογαριασμοί όπως της Google. Αυτά θα μπορούσαν να διερευνηθούν σε κάποια άλλη έρευνα μαζί και με τις προεκτάσεις(extensions) και plugins των browsers.

Συνολικός Πίνακας ευρημάτων

		MS Edge	Firefox	Chrome	Opera
WINDOWS	RAM	NAI	NAI	NAI	NAI
	DISK	NAI	OXI	OXI	OXI
LINUX	RAM		NAI	NAI	NAI
	DISK		OXI	OXI	OXI

ΣΥΜΠΕΡΑΣΜΑΤΑ

Από την ανάλυση των δεδομένων μας διαπιστώσαμε ότι γενικά ο ποιο σίγουρος τρόπος να εξάγουμε στοιχεία για τη διαδικτυακή συμπεριφορά μας όταν χρησιμοποιούμε τον φυλλομετρητή σε κατάσταση ιδιωτικής περιήγησης είναι η ανάλυση της μνήμης RAM. Όλοι οι φυλλομετρητές είχαν αφήσει στοιχεία στη μνήμη, να έχουμε υπόψιν μας όμως ότι η ανάλυση μνήμης προϋποθέτει να μην έχει κλείσει ο υπολογιστής, άρα θέλει άμεση εξαγωγή της κάτι που δεν είναι εφικτό πάντα.

Σε επίπεδο ανάλυσης δίσκου οι Firefox, Chrome και Opera δεν φαίνεται να αφήνουν κάτι στο δίσκο. Αντίθετα ο MSEdge μπορεί να διαγράφει τα αρχεία αυτά όμως μπορούν να ανακτηθούν με τα κατάλληλα εργαλεία. Επίσης να μη ξεχνάμε ότι στα Windows ένα επιπλέον αρχείο, η εικονική μνήμη (pagefile.sys), είναι πλούσιο σε στοιχεία επίσης. Όσον αφορά τις βάσεις δεδομένων που χρησιμοποιούν αυτές δεν περιέχουν κάποια στοιχεία κυρίως λόγο ότι πολλά απ αυτά δεν αποθηκεύονται από τους φυλλομετρητές.

Κλείνοντας συμπεραίνουμε ότι το αδύναμο σημείο είναι η μνήμη για όλους τους φυλλομετρητές, παρ' όλα αυτά όσον αφορά τους απλούς χρήστες είναι μάλλον απίθανο να καταλάβουν τι σελίδες επισκεφθήκαμε σε κατάσταση ιδιωτικής περιήγησης. Φυσικά να μη ξεχνάμε ότι δε γινόμαστε αόρατοι όταν χρησιμοποιούμε την ιδιωτική περιήγηση. Οι πάροχοι διαδικτύου ή οι υπεύθυνοι του δικτύου θα μπορούν να βλέπουν ποιους ιστοτόπους επισκεπτόμαστε. Επίσης η ιδιωτική περιήγηση σε σταματάει το tracking που έχουν πολλά site. Από τους τέσσερις φυλλομετρητές ο Chrome, Firefox και Opera έχουν την ποιο καλή κατάσταση ιδιωτικής περιήγησης ενώ ο MSEdge έχει ακόμα κάποια θέματα όπως προείπαμε που πρέπει να λύσει. Ακόμα πρέπει να λαμβάνουμε υπόψιν μας τους λογαριασμούς που έχουμε όπως στη google που μπορεί να συγχρονίζει τους browser ή τα Windows που μπορούν να κάνουνε το ίδιο όταν έχουμε 2 ή παραπάνω συσκευές που συνδεόμαστε με τος κωδικούς μας. Τέλος μη ξεχνάμε την αλληλεπίδραση των σύγχρονων εφαρμογών μεταξύ τους και το τι δεδομένα μπορεί να ανταλλάσουν εν αγνοία μας όπως τα αντιικά προγράμματα. Τελικά η ιδιωτική περιήγηση είναι μια αμφιλεγόμενη έννοια αφού βλέπουμε ότι μπορούμε να βρούμε ευρήματα της διαδικτυακής μας δραστηριότητας. Αν και για τον μέσο χρήστη δεν είναι εύκολο να κάνει ανάλυση σίγουρα η δραστηριότητα του δεν είναι τόσο ιδιωτική όσο νομίζουμε όταν μπορούν να τη δει και κάποιος άλλος είτε είναι ο πάροχος ιντερνετ είτε κάποιο διαδικτυακός ιστότοπος είτε κάποια εφαρμογή που συλλέγει στοιχεία εν αγνοία μας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] https://en.wikipedia.org/wiki/Forensic_science

[2] https://en.wikipedia.org/wiki/Computer_forensics

[3] https://digital-forensics.sans.org/blog/category/browser-forensics

[4] http://kb.digital-detective.net/display/BF/Browser+Forensics+and+Analysis

[5] https://www.the-parallax.com/2016/08/30/timeline-of-web-browser-security/

[6] http://www.forensicswiki.org/wiki/Google_Chrome

[7] http://forensicswiki.org/wiki/Internet_Explorer

[8] http://www.forensicswiki.org/wiki/Opera

[9] http://www.forensicswiki.org/wiki/Mozilla_Firefox

[10] https://csrc.nist.gov/publications/detail/sp/800-86/final

[11] https://www.sans.org/security-resources/posters/windows-forensics-evidenceof/75/download

[12] Kiavash Satvat, Matthew Forshaw, Feng Hao, Ehsan Toreini "On the Privacy of Private Browsing – A Forensic Approach"

[13] Emad Sayed Noorulla "Web Browser Private Mode Forensics Analysis

[14] Ashley Hedberg "The Privacy of Private Browsing"

[15] Google Incognito mode "https://support.google.com/chrome/answer/7440301"

[16] Firefox Private Browsing "https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history"

[17] Opera Private Browsing "http://help.opera.com/Mac/12.00/en/private.html"

[18] Internet Explorer Inprivate "https://www.microsoft.com/nz/ie9/features/inprivatebrowsing.aspx"

[19] https://www.sleuthkit.org/autopsy/

[20] https://www.brimorlabs.com/

[21] https://github.com/504ensicsLabs/LiME

[22] http://forensicswiki.org/wiki/Dcfldd

[23] http://www.winhex.com/winhex/hex-editor.html

[24] http://www.sqliteviewer.org/

[25] http://www.nirsoft.net/

[26] Nikolaos Tsalis, Alexios Mylonas, Antonia Nisioti, Dimitris Gritzalis, Vasilios Katos"Exploring the protection of private browsing in desktop browsers"

[27] Howard Chivers "Private browsing: A window of forensic opportunity"

[28] Donny J Ohana, Narasimha Shashidhar "Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions"

[29] Gaurav Aggarwal, Elie Bursztein, Collin Jackson, Dan Boneh “An Analysis of Private Browsing Modes in Modern Browsers”

[30] Andrew Marrington, Ibrahim Baggili “Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers

[31] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor “Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing”

[32] Xianyi Gao, Ylong Yang, Huiqing Fu, Janne Lindqvist, Yang Wang “Private Browsing: an Inquiry on Usability and Privacy Protection

[33] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, Blase Ur “Your Secrets Are Safe: How Browsers Explanations Impact Misconceptions About Private Browsing Mode”

[34] https://www.csoonline.com/article/3268813/antivirus-software/law-enforcement-uses-anti-virus-software-to-recover-suspects-web-history.html