

ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ

Εργασία Εξαμήνου

ΟΜΑΔΑ ΦΟΙΤΗΤΩΝ:

Γκρίτσης Ευγένιος
Νικολάου Ελένη
Παναγόπουλος Ηλίας
Πετρούλια Κατερίνα

ΔΙΔΑΣΚΩΝ:

Δρ. Θεόδωρος Ντούσκας

Μάιος 2025

ΠΜΣ στην Ανάπτυξη και Ασφάλεια Πληροφοριακών Συστημάτων
Οικονομικό Πανεπιστήμιο Αθηνών

Περιεχόμενα

Κατάλογος Εικόνων	2
Κατάλογος Πινάκων	3
Εισαγωγή	5
1. Προετοιμασία.....	6
2. Ανίχνευση & Εντοπισμός.....	8
2.1. Συννεντεύξεις.....	8
2.2. Καταγραφή Χώρου	8
2.3. Καταγραφή και Φωτογράφηση πηγών Πειστηρίων.....	11
3. Διαφύλαξη.....	16
3.1. Διαφύλαξη Μνήμης Πειστηρίου Laptop [0001]	16
3.2. Διαφύλαξη Δίσκου Laptop [0005]	18
3.3. Διαφύλαξη πειστηρίου USB [0004].....	20
3.4 Προετοιμασία και μεταφορά πειστηρίων στο εργαστήριο	23
3.4.1 Πειστήριο Laptop [0001] & Δίσκος [0005].....	23
3.4.2 Μνήμη Πειστηρίου Laptop	23
3.4.3 Πειστήριο USB [0004].....	24
4. Ανάλυση	25
4.1 Ανάλυση περιεχομένων μνήμης πειστηρίου Laptop [0001]	25
4.2 Ανάλυση περιεχομένων δίσκου [0005]	26
4.3 Ανάλυση περιεχομένων πειστηρίου USB [0004]	27
5. Παρουσίαση	29
5.1. Εισαγωγή	29
5.2. Συνοπτική Περιγραφή Αποδεικτικών Στοιχείων	29
5.3. Περιγραφή Ανάλυσης Αποδεικτικών Στοιχείων	30
5.4. Περιγραφή Ανάλυσης File System.....	31
5.5. Ανάλυση	32
5.6. Συμπεράσματα	35
Παράρτημα Α – Πίνακας RACI	37
Παράρτημα Β – Συννεντεύξεις.....	37
Παράρτημα Γ – Ανάλυση Μνήμης Πειστηρίου Laptop [0001]	39
Παράρτημα Δ – Ανάλυση Δίσκου Πειστηρίου Laptop [0005] & USB [0004]	54
Παράρτημα Ε – Φόρμες κατάσχεσης και καταγραφής.....	67
Παράρτημα ΣΤ – Εξοπλισμός εργαστηρίου	70
Παράρτημα Ζ – Εξουσιοδότηση Έρευνας	71
Παράρτημα Η – Χρονοδιάγραμμα Ενεργειών Charlie	72
Παράρτημα Θ – Στεγανάλυση	73
Παράρτημα Ι – Λεξικό Όρων.....	79

Κατάλογος Εικόνων

Εικόνα 1: Κάτοψη του Open Space χώρου γραφείου του υπόπτου.....	9
Εικόνα 2: Θέση εργασίας του υπόπτου (AI-Generated)	10
Εικόνα 3: Access Card System, τοποθετημένο στην είσοδο του χώρου	10
Εικόνα 4: Ενεργή φωτεινή ένδειξη A, ο φορητός H/Y είναι ενεργός και σε mode Αδράνεια.	11
Εικόνα 5: Φορητός H/Y	12
Εικόνα 6: Συνδεδεμένα καλώδια στο φορητό H/Y	12
Εικόνα 7: Ενσύρματο ποντίκι, βρισκόταν συνδεδεμένο σε θύρα USB του laptop.....	13
Εικόνα 8: USB, φορητό μέσο αποθήκευσης δεδομένων, βρισκόταν πάνω στην επιφάνεια του γραφείου.....	13
Εικόνα 9: Σκληρός Δίσκος, αφαιρέθηκε μετέπειτα στο Forensics Lab	14
Εικόνα 10: Επιφάνεια εργασίας υπόπτου με ελαχιστοποιημένες 2 διεργασίες	15
Εικόνα 11: Λήψη 1ου πιστού αντιγράφου της μνήμης	16
Εικόνα 12: Λήψη 2ου πιστού αντιγράφου μνήμης	17
Εικόνα 13: Λήψη 1ου αντιγράφου του δίσκου	19
Εικόνα 14: Λήψη 2ου αντιγράφου του δίσκου	19
Εικόνα 15: Στοιχεία δημιουργίας 2ου αντιγράφου του δίσκου	20
Εικόνα 16: Απόκτηση ψηφιακού αντιγράφου του πειστηρίου [0004] με FTK Imager	21
Εικόνα 17: Απόκτηση ψηφιακού αντιγράφου του πειστηρίου [0004] με FTK Imager (2)	21
Εικόνα 18: Απόκτηση αντιγράφου ψηφιακού πειστηρίου [0004] με FEX Imager.....	22
Εικόνα 19: Απόκομμα από κάτοψη ορόφου του γραφείου	30
Εικόνα 20 Πίνακας αρμοδιοτήτων RACI.	37
Εικόνα 21: Πληροφορίες του image της μνήμης	39
Εικόνα 22: Offset	40
Εικόνα 23: Λίστα των ενεργών ή πρόσφατων processes	40
Εικόνα 24 Λίστα των ενεργών ή πρόσφατων processes 2	41
Εικόνα 25 Εύρεση κρυφών διεργασιών.	44
Εικόνα 26 Εύρεση κρυφών διεργασιών 2	44
Εικόνα 27 Εύρεση δικτυακών συνδέσεων.	44
Εικόνα 28 Έυρεση τερματισμένων η απόκρυφων δικτυακών συνδέσεων	45
Εικόνα 29 Συσχέτιση μεταξύ διεργασιών	46
Εικόνα 30 Εντολές μέσω cmd.....	47
Εικόνα 31 Ιστορικό περιήγησης του χρήστη 1	47
Εικόνα 32 Ιστορικό περιήγησης του χρήστη 2	48
Εικόνα 33 Ιστορικό περιήγησης του χρήστη 3	48
Εικόνα 34 Ιστορικό περιήγησης του χρήστη 4	48
Εικόνα 35 Ιστορικό περιήγησης του χρήστη 5	49
Εικόνα 36 Ιστορικό περιήγησης του χρήστη 6	49
Εικόνα 37 Ιστορικό περιήγησης του χρήστη 7	50
Εικόνα 38 Ιστορικό περιήγησης του χρήστη 8	50
Εικόνα 39 Ιστορικό περιήγησης του χρήστη 9	51
Εικόνα 40 Ιστορικό περιήγησης του χρήστη 10	51
Εικόνα 41 Συνδέσεις που έχει ξεκινήσει η κάθε διεργασία	52
Εικόνα 42 Active and loaded hives.....	52
Εικόνα 43 Dump of user passwords	53
Εικόνα 44 Sessions	53

Εικόνα 45 Product Id μηχανήματος	53
Εικόνα 46 Χρονοδιάγραμμα Ενεργειών του Charlie.....	72
Εικόνα 47: Binwalk -e astronaut1.jpg.....	73
Εικόνα 48: Extracted folder	73
Εικόνα 49: Extracted Files	73
Εικόνα 50: Extracted document that contains patent information	74
Εικόνα 51: Astronaut1.jpg	75
Εικόνα 52: microscope1.jpg	76
Εικόνα 53: Στεγανάλυση microscope1.jpg κωδικός immortal	76
Εικόνα 54 Αρχείο .tiff που βρέθηκε εντός του 01.zip.....	77
Εικόνα 55 Αρχείο .tiff που βρέθηκε εντός του 01.zip (2)	78

Κατάλογος Πινάκων

Πίνακας 1: Εργαλεία Forensics	7
Πίνακας 2: Πίνακας Καταγραφής Ψηφιακών Πειστηρίων.	15
Πίνακας 3: Φόρμα στοιχείων μνήμης RAM.....	17
Πίνακας 4: Στοιχεία δημιουργίας 1ου DUMP αντιγράφου	18
Πίνακας 5: Στοιχεία δημιουργίας 2ου DUMP αντιγράφου	18
Πίνακας 6: Στοιχεία δημιουργίας 1ου αντιγράφου του δίσκου	18
Πίνακας 7: Σύνοψη απόκτησης αντιγράφου πειστηρίου [0004] με FTK Imager.....	22
Πίνακας 8: Σύνοψη απόκτησης αντιγράφου ψηφιακού πειστηρίου [0004] με FEX Imager..	22
Πίνακας 9: Βασικές Δομικές Πληροφορίες Πειστηρίου [0005].	27
Πίνακας 10: Βασικές Δομικές Πληροφορίες Πειστηρίου [0004]	28
Πίνακας 11: Πίνακας Αρμοδιοτήτων RACI.	37
Πίνακας 12: Ενεργές ή πρόσφατες διεργασίες.	43
Πίνακας 13 Λίστα των συνδέσεων.....	46
Πίνακας 14 Σχετική αλληλογραφία με την υπόθεση	64
Πίνακας 15 Φόρμα Chain of Custody 1.....	68
Πίνακας 16 Φόρμα Chain of Custody 2.....	68
Πίνακας 17 Φόρμα Στοιχείων Σκληρού Δίσκου.	69

Η σελίδα αυτή έχει σκοπόμως αφεθεί κενή

Εισαγωγή

Η παρούσα αναφορά αφορά στη διεξαγωγή ψηφιακής εγκληματολογικής έρευνας με σκοπό την τεκμηρίωση της διαδικασίας εντοπισμού, διαφύλαξης και ανάλυσης ψηφιακών πειστηρίων που σχετίζονται με πιθανή παράνομη δραστηριότητα.

Η διαδικασία ακολούθησε τις αρχές και τα πρότυπα της ACPO (Association of Chief Police Officers), με έμφαση στη διατήρηση της ακεραιότητας των πειστηρίων, τη λεπτομερή τεκμηρίωση κάθε ενέργειας και τη δυνατότητα επαναληψιμότητας των αποτελεσμάτων. Η προσέγγιση περιελάμβανε συνεντεύξεις με σχετιζόμενα πρόσωπα, καταγραφή του φυσικού χώρου, εντοπισμό και φωτογράφηση πιθανών πηγών πειστηρίων, καθώς και τη διασφάλιση της σωστής μεταφοράς και φύλαξής τους.

Ακολούθησε η τεχνική ανάλυση των συλλεχθέντων δεδομένων, η οποία πραγματοποιήθηκε σε περιβάλλον εργαστηρίου, χρησιμοποιώντας εξειδικευμένα εργαλεία και διαδικασίες. Τα αναλυθέντα πειστήρια περιλάμβαναν μονάδα αποθήκευσης τύπου USB, σκληρό δίσκο και μνήμη από φορητό υπολογιστή.

Η αναφορά είναι δομημένη σε πέντε βασικές ενότητες: προετοιμασία, εντοπισμός και τεκμηρίωση, διαφύλαξη, ανάλυση και παρουσίαση των ευρημάτων. Στα παραρτήματα περιλαμβάνονται υποστηρικτικά στοιχεία, όπως συνεντεύξεις, φόρμες καταγραφής, τεχνικά δεδομένα ανάλυσης και εξοπλισμός που χρησιμοποιήθηκε κατά την έρευνα.

1. Προετοιμασία

Η ομάδα ψηφιακής εγκληματολογικής διερεύνησης έλαβε επίσημη ειδοποίηση από την εταιρεία M57.biz την ώρα 7:30 μ.μ. την Πέμπτη 10/12/2009, σχετικά με ύποπτη δραστηριότητα που ενδέχεται να σχετίζεται με παραβίαση απορρήτου και πιθανή διαρροή ευαίσθητων πληροφοριών. Μετά από αρχική επικοινωνία και αξιολόγηση του αιτήματος, ορίστηκε η ημερομηνία επιτόπιας παρέμβασης για την Παρασκευή 11/12/2009.

Η ομάδα αποτελείτο από τέσσερα μέλη, με ρητή κατανομή αρμοδιοτήτων βάσει του μοντέλου RACI (Responsible, Accountable, Consulted, Informed), το οποίο παρατίθεται στο **Παράρτημα Α**. Τρία μέλη αναλαμβάνουν τον τεχνικό τομέα (Technical Witness), ενώ ένα μέλος εκτελεί ρόλο πραγματογνώμονα (Expert Witness), υπεύθυνο για την τεκμηρίωση και παρουσίαση των ευρημάτων σε δικαστικό ή νομικό πλαίσιο, εφόσον απαιτηθεί. Οι ρόλοι ορίστηκαν ως εξής:

- κύριος 1231, expert witness
- κυρία 1232, technical witness
- κύριος 1233, technical witness
- κυρία 1234, technical witness

Κατά την προετοιμασία, ολοκληρώθηκαν όλα τα απαραίτητα διοικητικά και νομικά βήματα. Υπογράφηκε σύμβαση εμπιστευτικότητας (Non-Disclosure Agreement - NDA), η οποία παρατίθεται στο **Παράρτημα Ζ**. Παράλληλα, εξασφαλίστηκε πλήρης νομική εξουσιοδότηση για την πρόσβαση σε πληροφοριακά συστήματα, υλικό τεκμηρίωσης και φυσικά πειστήρια. Οι υπεύθυνοι της εταιρείας ενημερώθηκαν σχετικά με την ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων, συμπεριλαμβανομένων των διατάξεων του Ν. 2472/97 και έδωσαν τη συναίνεσή τους για τη διενέργεια της έρευνας εντός των προβλεπόμενων ορίων.

Η τεχνική ομάδα εξοπλίστηκε με τα κατάλληλα εργαλεία για την καταγραφή, συλλογή και ανάλυση ψηφιακών πειστηρίων, σύμφωνα με τις απαιτήσεις της έρευνας. Ακολουθεί ο πλήρης κατάλογος εξοπλισμού.

ΠΙΝΑΚΑΣ ΕΞΟΠΛΙΣΜΟΥ FORENSICS
Forensics laptop (HP Envy 13, Windows XP Anvil, VM, Caine Linux)
Forensics USB
Εκτυπωτής, σαρωτής (HP Photosmart C6380 All-in-One)
Σκληροί δίσκοι (Εξωτερικοί USB 1TB, εσωτερικοί SATA 750 GB)
Εφεδρικές μνήμες (16 GB DDR2-DDR3)
Εφεδρικές μητρικές κάρτες
Αναγνώστες μνημών (SanDisk ImageMate All-in-One)
Καλώδια (Ρεύματος, VGA, SATA, micro SATA)
Εξωτερικά CD/DVD/USB Drives
Live CDs/USBs
Λειτουργικά Συστήματα (Windows, Linux, MAC OS X)
Φωτογραφική μηχανή (Canon EOS-1Ds Mark II)
Disk Write Blocker (Tableau Forensic FireWire Bridge (T9))
Καταγραφικό ήχου
Γάντια
Αδιάβροχες σακούλες

Αντιστατικές σακούλες
Αντιστατικά γάντια
Αυτοκόλλητες ετικέτες, ταινία
Ειδικές αριθμημένες τσάντες
Φορητοί κλωβοί Faraday
Εργαλεία (πένσες, κατσαβίδια, τανάλιες, tire up, φακός)
Φόρμες καταγραφής πειστηριών
Σημειωματάρια, μολύβια, στυλό
Κόλλες A4
Εργαλεία δημιουργίας πιστών αντιγράφων μνήμης (Dumpit, dd, FTK Imager, Encase)
Εργαλεία ανάλυσης μνήμης (Volatility Framework, DumpIt, Win32dd)
Εργαλεία πιστών αντιγράφων (R-drive, P2 explorer, Forensics Imager, FTK Imager, Encase)
Εργαλεία ανάλυσης ψηφιακών πειστηρίων (Encase, Access Data FTK, Autopsy, Sleuth, FEX Imager)
Εργαλεία ανάπτυξης κώδικα (Visual studio, eclipse)
Εργαλεία αναπαραγωγής βίντεο (Windows media player, quick player, VLC Media Player)
Εργαλεία επεξεργασίας εγγράφων (Notepad++, MS Word, Open Office)

Πίνακας 1: Εργαλεία Forensics

Στις 11/12/2009 7:30 π.μ., η ομάδα μας αναχώρησε από το εργαστήριο με προορισμό την M57.biz.

2. Ανίχνευση & Εντοπισμός

Στις 11/12/2009 8:32 π.μ. η ομάδα συμβούλων διερεύνησης απέκτησε πρόσβαση στον χώρο όπου πιθανολογείται η διάπραξη του εγκλήματος. Ο χώρος βρίσκεται στον 1^ο όροφο στα κεντρικά γραφεία της M57.biz, Λευκάδος 47, Αθήνα. Επιβεβαιώθηκε ότι ο εν λόγω χώρος αποτελεί ένα ανοιχτού τύπου ¹γραφείο που φιλοξενεί συνολικά 15 θέσεις εργασίας. Ο χώρος τη στιγμή της άφιξης της ομάδας, είχε ήδη απομονωθεί και οι υπόλοιποι εργαζόμενοι έχουν απομακρυνθεί.

Παρόντες από την εταιρεία ήταν ο υπεύθυνος ασφάλειας της εταιρείας, ο IT Admin και ο πιθανός δράστης. Ο Technical Witness 1232 ξεκίνησε άμεσα τη διαδικασία των συνεντεύξεων. Οι Technical Witnesses 1233, 1234 ξεκίνησαν τη διαδικασία καταγραφής του χώρου, καταγραφής και φωτογράφησης πειστηρίων, διαφύλαξης πειστηρίων και προετοιμασίας των πειστηρίων για μεταφορά στο εργαστήριο.

2.1. Συνεντεύξεις

Στις 8:45 π.μ. ξεκίνησαν οι συνεντεύξεις των παρόντων ατόμων, δηλαδή του πιθανού δράστη, του υπεύθυνου ασφάλειας και του IT Admin.

Στις 9:02 π.μ. κλήθηκε για συνέντευξη ο CEO της εταιρείας.

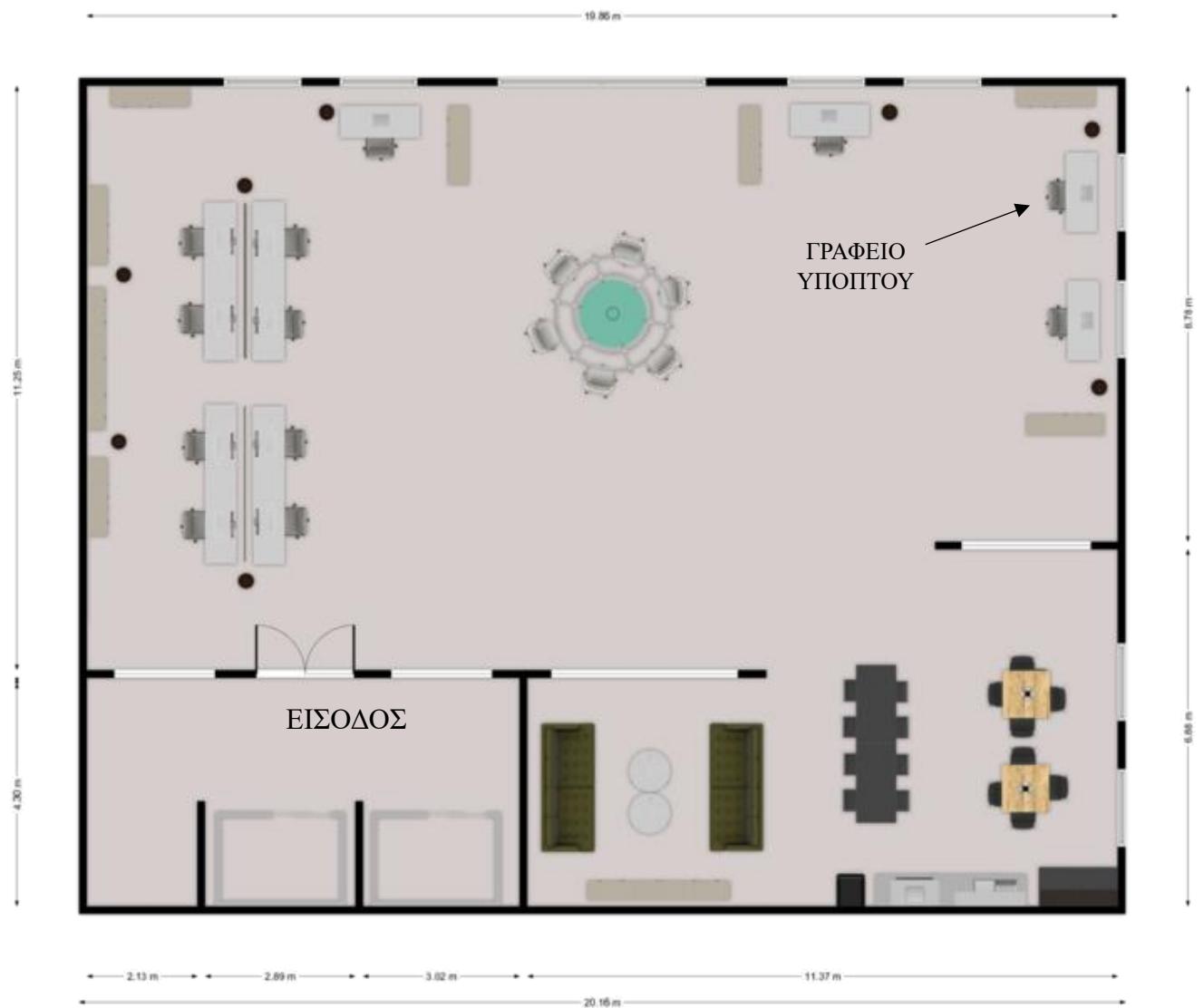
Αναλυτικά οι ερωτήσεις και απαντήσεις βρίσκονται στο **Παράρτημα Β.**

2.2. Καταγραφή Χώρου

Η διαδικασία καταγραφής του χώρου πραγματοποιήθηκε από τον Technical Witness 1233 και ξεκίνησε στις 8:40 π.μ. Η θέση εργασίας του υπόπτου βρίσκεται στην δεξιά γωνία του open space χώρου γραφείου. Ο χώρος συνολικά διαθέτει 12 θέσεις εργασίας που κατανέμονται εντός 300 τ.μ. Η είσοδος στον χώρο βρίσκεται στην κάτω αριστερή γωνία του σχεδίου (Εικόνα 1) και ελέγχεται μέσω ηλεκτρονικού συστήματος πρόσβασης με χρήση κάρτας (access card system).

Στην επιφάνεια του γραφείου του υπόπτου ήταν τοποθετημένος και ενεργοποιημένος ο εταιρικός φορητός υπολογιστής μάρκας DELL, συνδεδεμένος μέσω εξωτερικής μονάδας τροφοδοσίας (τροφοδοτικό). Πάνω στην επιφάνεια του γραφείου εντοπίζονται ένα ποντίκι συνδεδεμένο ενσύρματα με τον φορητό υπολογιστή, όπως και ένα USB stick – φορητό μέσο αποθήκευσης.

¹ Ως Open Space – Ανοιχτού Τύπου χώρος γραφείου νοείται ενιαίος εργασιακός χώρος, χωρίς μόνιμα διαχωριστικά, στον οποίο συνυπάρχουν πολλαπλές θέσεις εργασίας.



Eikόνα 1: Κάτοψη του Open Space χώρου γραφείου των υπόπτων.



Εικόνα 2: Θέση εργασίας του υπόπτου (AI-Generated)



Εικόνα 3: Access Card System, τοποθετημένο στην είσοδο του χώρου

2.3. Καταγραφή και Φωτογράφηση πηγών Πειστηρίων

Η ομάδα προχώρησε στην καταγραφή, απαρίθμηση, σήμανση και φωτογράφηση των πηγών πειστηρίων που ανευρέθηκαν στο χώρο.

Στις 8.45 π.μ. ο Technical Witness 1234, φωτογραφίζει τα ψηφιακά πειστήρια που βρίσκονται πάνω στο γραφείο του υπόπτου.

Στις 8.50 π.μ. ο Technical Witness 1234, έχοντας φωτογραφίσει το γραφείο και τα αντικείμενα του υπόπτου, προχωράει στην μελέτη του φορητού υπολογιστή που φαίνεται ενεργοποιημένος – ενεργή φωτεινή σήμανση πληκτρολογίου (Εικόνα 4). Ωστόσο η οθόνη του φορητού υπολογιστή είναι ανενεργή, δεδομένο που μαρτυρά ότι βρίσκεται σε κατάσταση αναμονής – ενεργή προστασία οθόνης.

Έπειτα από έγκριση του Expert Witness, ο Technical Witness 1234 προχωράει στην επαναφορά του φορητού υπολογιστή σε κατάσταση λειτουργίας. Για να επιτευχθεί αυτό, πραγματοποιήθηκε μία μικρή, αργή και ομαλή κίνηση του ποντικιού προς τα δεξιά. Μόλις η οθόνη ενεργοποιήθηκε, επανήλθε σε λειτουργία ο υπολογιστής χωρίς τη χρήση συνθηματικού ασφαλείας. Στη συνέχεια, έγινε λήψη στιγμάτυπων της ενεργής οθόνης, όπου καταγράφεται το περιεχόμενο της. Στην παραπάνω διαδικασία δεν πατήθηκε κανένα πλήκτρο του πληκτρολογίου. Τέλος, διενεργήθηκε έλεγχος για την ύπαρξη εκτυπωτών, ενεργών εκτυπώσεων και λοιπών απομακρυσμένων ηλεκτρονικών συσκευών εντός του γραφείου, χωρίς να διαπιστωθεί η ύπαρξή τους.

Όλα τα προηγούμενα βήματα έγιναν σύμφωνα με τις οδηγίες κατά ACPO για καταγραφή κατάστασης ενεργού μηχανήματος.

Στις εικόνες 1 έως 5 που ακολουθούν παρατίθενται τα ψηφιακά πειστήρια που καταγράφηκαν στο χώρο του γραφείου.



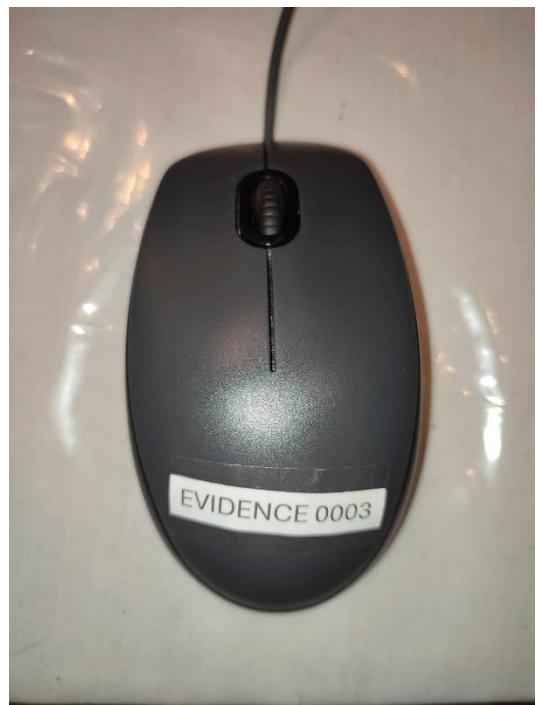
Εικόνα 4: Ενεργή φωτεινή ένδειξη A, ο φορητός H/Y είναι ενεργός και σε mode Αδράνεια



Εικόνα 5: Φορητός H/Y



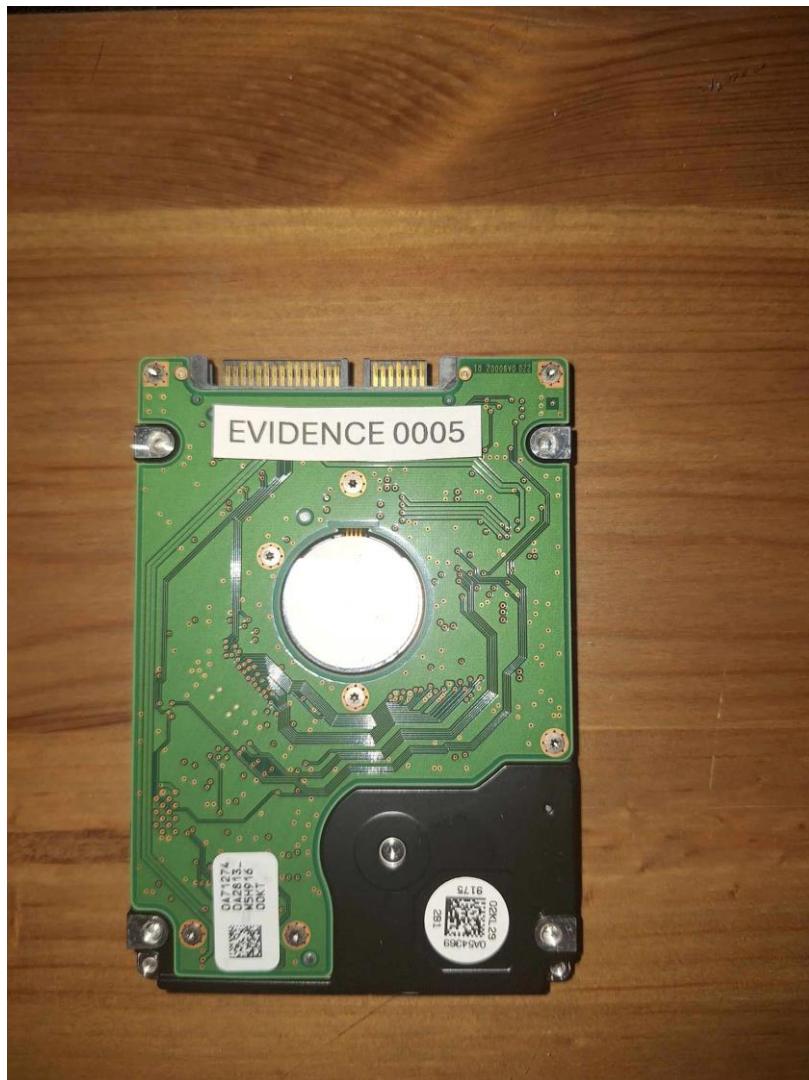
Εικόνα 6: Συνδεδεμένα καλώδια στο φορητό H/Y



Εικόνα 7: Ενσύρματο ποντίκι, βρισκόταν συνδεδεμένο σε θύρα USB του laptop



Εικόνα 8: USB, φορητό μέσo απoθήκευσης δεδομένων, βρισκόταν πάνω στην επιφάνεια τoυ γραφείou



Εικόνα 9: Σκληρός Δίσκος, αφαιρέθηκε μετέπειτα στο Forensics Lab

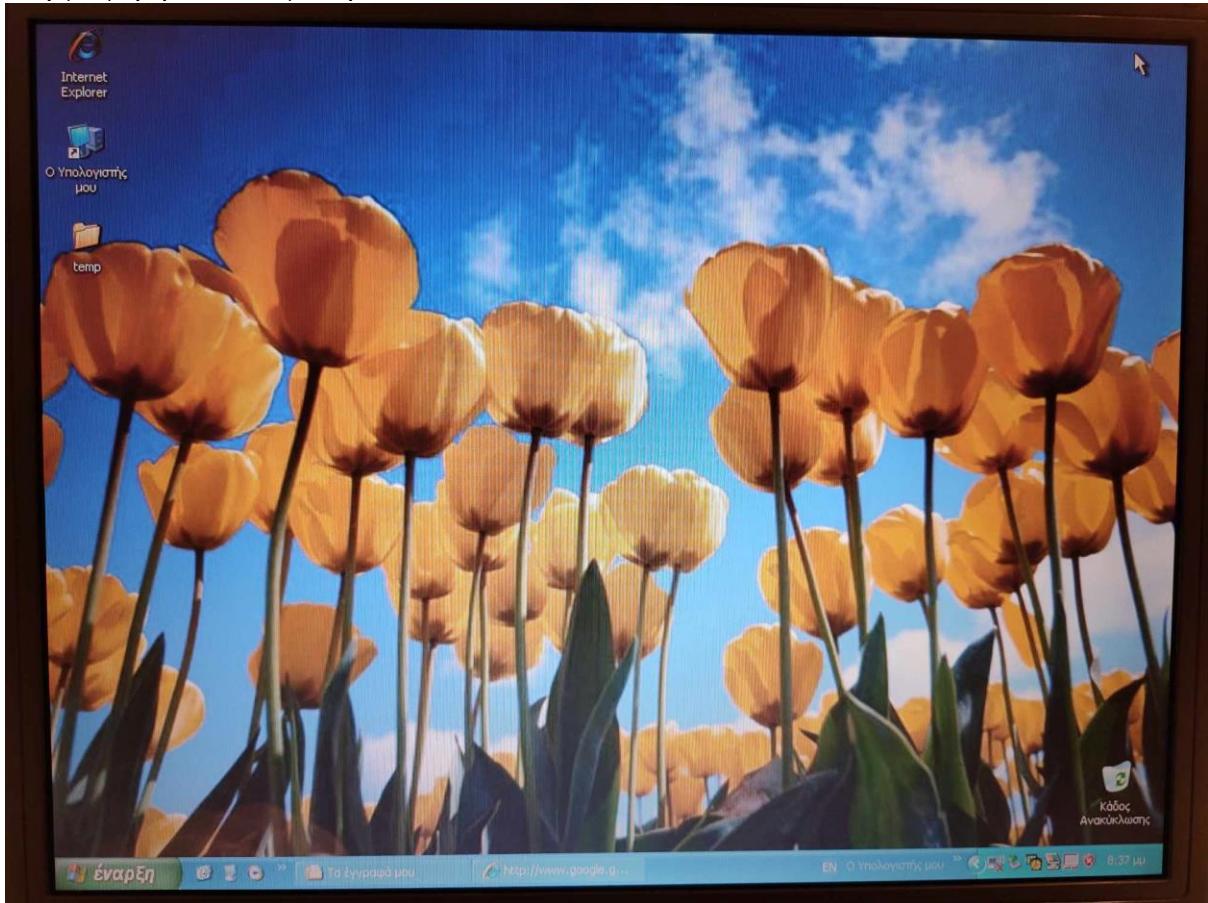
Στη συνέχεια, επισυνάπτεται συνοπτικός πίνακας των πειστηρίων:

ΚΑΤΑΓΕΓΡΑΦΕΝΤΑ ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ			
ΗΜΕΡΟΜΗΝΙΑ:		11-12-2009	
ΑΡΜΟΔΙΟΣ ΕΡΕΥΝΗΤΗΣ:		Technical Witness 1234	
Κωδικός Πειστηρίου	Όνομασία	Serial Number	Κατάσταση
0001	DELL Laptop	DEJ485BIDFGJF	Ενεργό, Συνδεδεμένο με παροχή ρεύματος μέσω πειστηρίου [0002]
0002	Τροφοδοτικό laptop Delta Electronics Inc. AC Adapter – ADP – 65DB	Q4W0406021262	Ενεργό, Συνδεδεμένο με πειστήριο [0001]

0003	Logitech M-U0026 – Ενσύρματο ποντίκι	1939HS01D6W8	Ενεργό, Συνδεδεμένο σε USB port του πειστήριου [0001]
0004	Kingston Data Traveler 2.0 USB Device	2007110203195377	Μη συνδεδεμένο
0005	Σκληρός Δίσκος ZX-500 3.5" (αφαιρέθηκε από το Laptop [0001])	HJ8934FDS923	N/A

Πίνακας 2: Πίνακας Καταγραφής Ψηφιακών Πειστηρίων.

Στις εικόνες 6 έως 8 που ακολουθούν παρατίθενται τα στιγμιότυπα που λήφθηκαν από τον ενεργό φορητό υπολογιστή του υπόπτου.



Εικόνα 10: Επιφάνεια εργασίας υπόπτου με ελαχιστοποιημένες 2 διεργασίες

3. Διαφύλαξη

Ακολουθώντας το πρωτόκολλο λήψης πιστών αντιγράφων ενεργών συσκευών δηλαδή live acquisition αποφασίστηκε να παρθούν πιστά αντίγραφα των volatile δεδομένων όπου η σειρά προτεραιότητας καθορίστηκε από την ευθραυστότητα των δεδομένων RAM, Cache, Registry. Στη συνέχεια ο Technical Witness 1233 προχώρησε στη λήψη των non-volatile δεδομένων πριν μεταφερθεί το laptop στο εργαστήριο.

3.1. Διαφύλαξη Μνήμης Πειστηρίου Laptop [0001]

Στις 2009-12-11 08:57:02 π.μ. συνδέθηκε στο πειστήριο [0001], ο εξωτερικός αφαιρούμενος δίσκος Forensics USB.

Στις 08:59:52 π.μ. ξεκίνησε η λήψη του πρώτου πιστού αντίγραφου με την χρήση του εργαλείου MDD (MoonSols DumpIt) έκδοση 1.3 αφότου άνοιξε το DumpIt σε ένα παράθυρο cmd και πατήθηκε Y.

Στις 09:09:52 π.μ. ολοκληρώθηκε η λήψη του πρώτου αντιγράφου. Καθώς το συγκεκριμένο εργαλείο δεν υπολογίζει αυτόματα hashes κατά τη δημιουργία του αντίγραφου, υπολογίστηκαν χειροκίνητα με την χρήση των παρακάτω εντολών για επαληθεύσουμε ότι το αρχείο δεν αλλοιώθηκε μετά τη δημιουργία μελλοντικά:

```
certutil -hashfile "C:\memdump\charlie-2009-12-11.mddramimage"" MD5
```

```
certutil -hashfile "C:\memdump\charlie-2009-12-11.mddramimage"" SHA1
```

Επιβεβαιώνουμε ότι το μέγεθος του αντιγράφου είναι όσο η αρχική μνήμη ώστε να επαληθεύσουμε την σωστή λήψη του αντιγράφου.

```
C:\Windows\system32>cd C:\Users\lab\Desktop\DumpIt
C:\Users\lab\Desktop\DumpIt>dumpit.exe
DumpIt - v1.3.2.20110401 - One click memory dumper
Copyright <c> 2007 - 2011, Matthieu Suiche <http://www.msuische.net>
Copyright <c> 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size: 2466250752 bytes < 2352 Mb>
Free space size: 9638375424 bytes < 9191 Mb>

* Destination = C:\memdump\charlie-2009-12-11.mddramimage

: Are you sure you want to continue? [y/n] y
Processing... Success.
```

Εικόνα 11: Λήψη Ιου πιστού αντιγράφου της μνήμης

Στις 09:10:05 π.μ. ξεκίνησε η λήψη του δεύτερου αντίγραφου με το εργαλείο Win32dd με την εκτέλεση της εντολής win32dd.exe /f C:\memdump\charlie-2009-12-11-p2.raw /compress και ολοκληρώθηκε στις 09:17:10 π.μ. Το Win32dd υποστηρίζει αυτόματη δημιουργία hashes.

```

C:\moonsols_windows_memory_toolkit_community_edition>win32dd.exe /d /f physmem.dmp
win32dd - 1.3.1.20100417 - (Community Edition)
Kernel land physical memory acquisition
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

      Name          Value
      ----          -----
File type:        Microsoft memory crash dump file
Acquisition method: PFN Mapping
Content:         Memory manager physical memory block
Destination path: physmem.dmp
O.S. Version:    Microsoft Windows 7 Home Premium, 64-bit Service
Pack 1 (build 7601)
Computer name:   CHARLIE
Physical memory in use: 32x
Physical memory size: 83800720 Kb < 8106 Mb>
Physical memory available: 55830004 Kb < 5452 Mb>
Paging file size: 16599592 Kb < 16210 Mb>
Paging file available: 12718696 Kb < 12420 Mb>
Virtual memory size: 2097024 Kb < 2047 Mb>
Virtual memory available: 2044336 Kb < 1996 Mb>
Extended memory available: 0 Kb < 0 Mb>
Physical page size: 4096 bytes
Minimum physical address: 0x0000000000001000
Maximum physical address: 0x0000000023FDFF000
Address space size: 9661579264 bytes (9435136 Kb)
--> Are you sure you want to continue? [y/n] _
```

Eικόνα 12: Λήψη 2ου πιστού αντιγράφου μνήμης

Φόρμα στοιχείων μνήμης RAM

Πεδίο	Παράδειγμα Τιμής
Μάρκα/Μοντέλο	N/A
Λειτουργικό Σύστημα	Windows XP Service Pack 3 x86
Φυσική Μνήμη (RAM)	≈ 2GB
Κατάσταση Συστήματος	Εν λειτουργίᾳ

Πίνακας 3: Φόρμα στοιχείων μνήμης RAM

Στοιχεία δημιουργίας 1^{ου} DUMP αντιγράφου

Πεδίο	Παράδειγμα Τιμής
Εργαλείο	Win32dd
Εντολές	win32dd.exe /f C:\memdump\charlie-2009-12-11-p2.raw /compress
Ημερομηνία	2009-12-11 09:10:05
Τόπος λήψης πιστού αντιγράφου	M57.biz

Αποτέλεσμα	charlie-2009-12-11.mddramimage
Hash MD5	38067cc457546b3156975d9a52d4229f
Hash SHA-1	15c1ae5e2ac3da7a9cdaaa9a162aa9ac9dde3d9d
Ονοματεπώνυμο	Technical Witness 1233
Τίτλος	Technical Witness 1233
Τηλέφωνο	6951767301

Πίνακας 4: Στοιχεία δημιουργίας 1ου DUMP αντιγράφου

Στοιχεία δημιουργίας 2 ^{ου} DUMP αντιγράφου	
Εργαλείο	MDD (MoonSols DumpIt)
Έκδοση	1.3
Ημερομηνία	2009-12-11 08:59:52
Τόπος λήψης πιστού αντιγράφου	M57.biz
Αποτέλεσμα	charlie-2009-12-11-p2.raw
Hash MD5	42367cc457546b3156975d9a52d4229f
Hash SHA-1	72c1da5e2ae3da7a9cdaaa9a214aa9ac9dde3d9d

Πίνακας 5: Στοιχεία δημιουργίας 2ου DUMP αντιγράφου

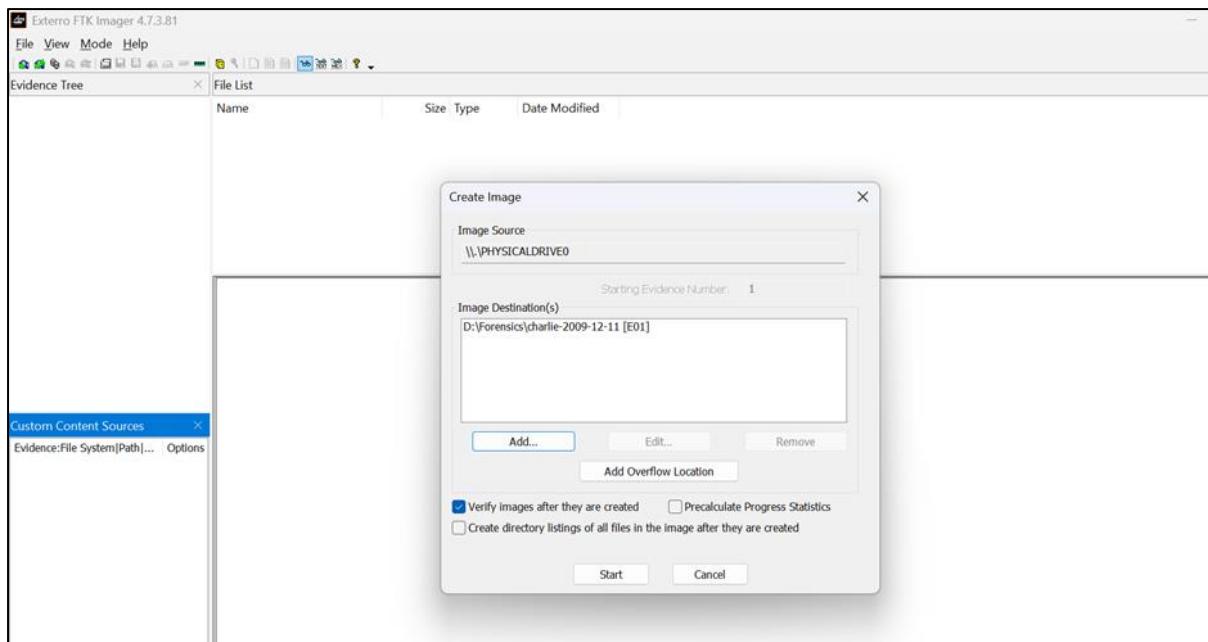
3.2. Διαφύλαξη Δίσκου Laptop [0005]

Στις 2009-12-11 09:12:15 π.μ. ξεκίνησε η λήψη του αντιγράφου του δίσκου. Για την λήψη των αντιγράφων χρησιμοποιήθηκαν τα εργαλεία FTK imager και FEX Imager.

Στοιχεία δημιουργίας 1^{ου} αντιγράφου του δίσκου

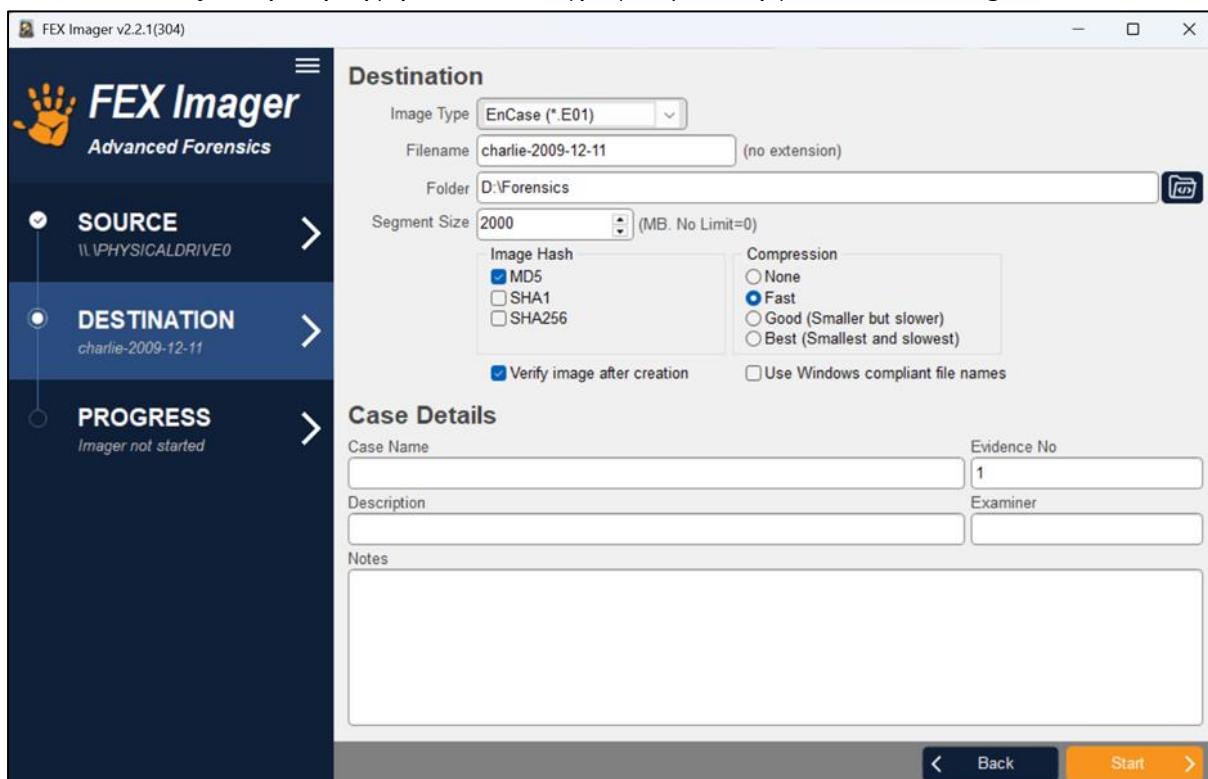
Πεδίο	Παράδειγμα Τιμής
Εργαλείο	FTK imager
Ημερομηνία	2009-12-11 09:12:15 π.μ.
Τόπος λήψης πιστού αντιγράφου	M57.biz
Αποτέλεσμα	charlie-2009-12-11.E01
Hash MD5	0377b3d41bbc295a1c9f00aa07ee174

Πίνακας 6: Στοιχεία δημιουργίας 1ου αντιγράφου του δίσκου



Εικόνα 13: Λήψη 1ου αντιγράφου του δίσκου

Στις 09:23:22 ξεκίνησε η λήψη του 2^{ου} αντιγράφου με το εργαλείο FEX Imager



Εικόνα 14: Λήψη 2ου αντιγράφου του δίσκου

Στοιχεία δημιουργίας 2^{ου} αντιγράφου του δίσκου

Πεδίο

Παράδειγμα Τιμής

Εργαλείο	FEX Imager
Ημερομηνία	2009-12-11 09:23:22 π.μ.
Τόπος λήψης πιστού αντιγράφου	M57.biz
Αποτέλεσμα	charlie-2009-12-11-p2.E01
Hash MD5	0377b3d41bbbc295a1c9f00aa07ee174

Εικόνα 15: Στοιχεία δημιουργίας 2ου αντιγράφου του δίσκου

Στις 09:33:22 π.μ. σταμάτησε να τρέχει και αφαιρέθηκε ο αφαιρούμενος εξωτερικός δίσκος Forensics USB και λήφθηκαν τα hashes του ώστε να επιβεβαιωθεί μελλοντικά τυχόν παραποίηση του:

Hash MD5: 81425ac152766b3101436c9a61f5237g

Hash SHA-1: 63a4ff8a4ad1ed4f0bcade9a214aa6ac9dde139a

Στις 09:33:22 π.μ. ολοκληρώθηκε η διαδικασία διαφύλαξης πειστηρίων του ανοιχτού laptop και αφαιρέθηκε η μπαταρία του κατά ACPO.

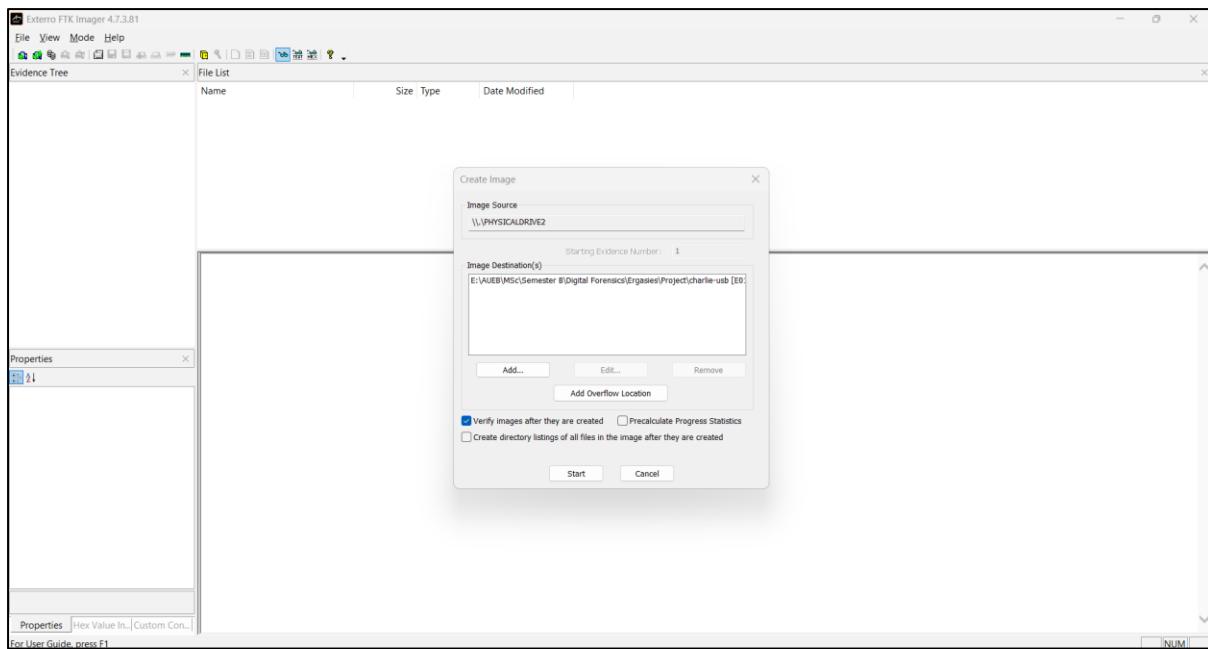
3.3. Διαφύλαξη πειστηρίου USB [0004]

Στις 9:36:54 π.μ. ξεκίνησε η διαδικασία διαφύλαξης του αφαιρούμενου αποθηκευτικού μέσου τύπου USB, που επισημάνθηκε ως στοιχείο [0004] στα εντοπισμένα πειστήρια στον Open space χώρο της εταιρείας M57.biz. Το USB βρισκόταν εκτός υπολογιστή τοποθετημένο πάνω στο γραφείο του υπόπτου υπαλλήλου.

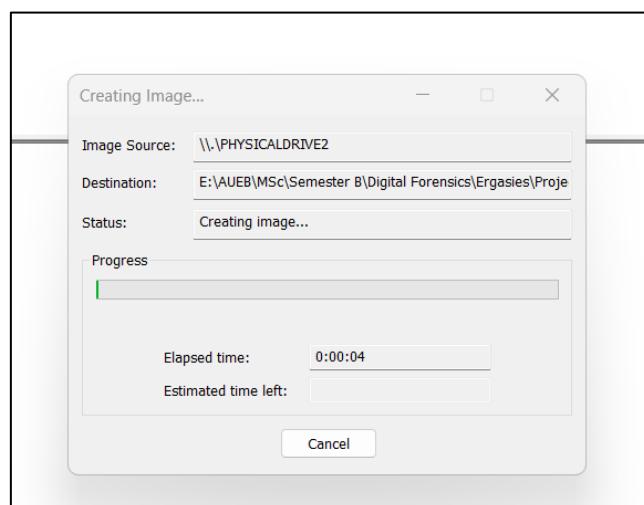
Για την απόκτηση ψηφιακού αντιγράφου από το USB, χρησιμοποιήθηκαν τα εργαλεία FTK Imager και FEX Imager.

Το πειστήριο [0004] συνδέθηκε αρχικά στον φορητό υπολογιστή Forensics laptop (HP Envy 13), απομονωμένο από οποιοδήποτε δίκτυο και διαμορφωμένο αποκλειστικά για χρήση διαφύλαξης ψηφιακών πειστηρίων.

Στις 9:36:54 π.μ. ξεκίνησε η απόκτηση ψηφιακού αντιγράφου με FTK Imager:



Εικόνα 16: Απόκτηση ψηφιακού αντιγράφου του πειστηρίου [0004] με FTK Imager



Εικόνα 17: Απόκτηση ψηφιακού αντιγράφου του πειστηρίου [0004] με FTK Imager (2)

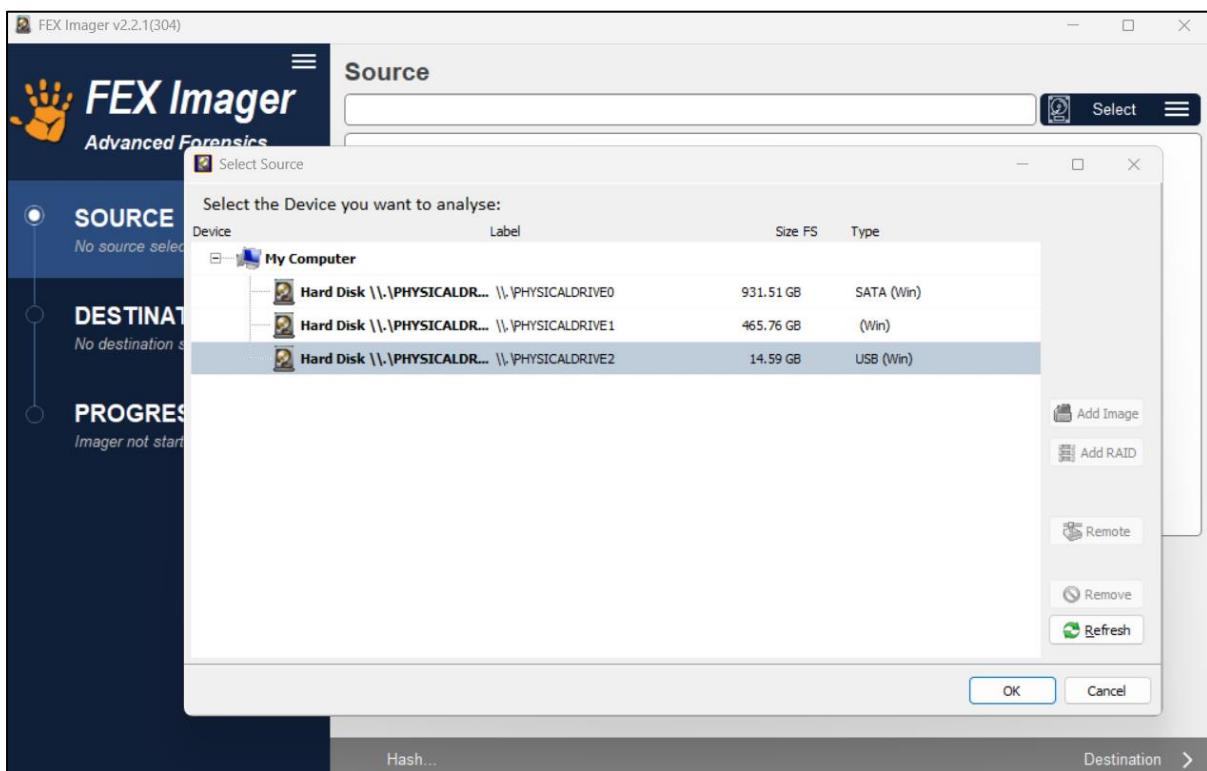
Πεδίο	Τιμή
Εργαλείο	FTK imager
Ημερομηνία	2009-12-11 9:36:54 π.μ
Τόπος λήψης πιστού αντιγράφου	M57.biz
Αποτέλεσμα	Charlie-work-usb-2009-12-11.E01

Hash MD5

9c0de6c8532d7a66ddcf01861dfb6535

Πίνακας 7: Σύνοψη απόκτησης αντιγράφου πειστηρίου [0004] με FTK Imager.

Τυπερα, στις 9:38:21 π.μ. ξεκίνησε η 2^η διαδικασία απόκτησης ψηφιακού αντιγράφου με FEX Imager ως επιβεβαιωτική ενέργεια και για λόγους εγκυρότητας, δημιουργήθηκε και δεύτερη εικόνα:



Εικόνα 18: Απόκτηση αντιγράφου ψηφιακού πειστηρίου [0004] με FEX Imager.

Πεδίο	Τιμή
Εργαλείο	FEX imager
Ημερομηνία	2009-12-11 9:38:21 π.μ.
Τόπος λήψης πιστού αντιγράφου	M57.biz
Αποτέλεσμα	charlie-work-usb-2009-12-11-backup.E01
Hash MD5	9c0de6c8532d7a66ddcf01861dfb6535

Πίνακας 8: Σύνοψη απόκτησης αντιγράφου ψηφιακού πειστηρίου [0004] με FEX Imager.

Τα MD5 Hashes των δύο Images είναι ίδια, επομένως επιβεβαιώνεται η ορθότητα της διαδικασίας του acquisition.

3.4 Προετοιμασία και μεταφορά πειστηρίων στο εργαστήριο

Η διαδικασία πακεταρίσματος και προετοιμασίας των πειστηρίων για τη μεταφορά τους στο εργαστήριο ξεκίνησε στις 9:40 π.μ. με στόχο την ασφαλή μεταφορά τους, χωρίς φθορές και αλλοιώσεις.

Συγκεκριμένα χρησιμοποιήθηκαν:

- Αντιστατικά γάντια,
- Αντιστατικές και αδιάβροχες σακούλες φύλαξης,
- Αυτοκόλλητες ταινίες ασφαλείας για φυσικές θύρες USB και DVD,
- Κατάλληλες ετικέτες με μοναδικά αναγνωριστικά για τα πειστήρια,
- Κούτες με αφρολέξ

3.4.1 Πειστήριο Laptop [0001] & Δίσκος [0005]

Μετά την ολοκλήρωση της λήψης των volatile δεδομένων από το LAPTOP [0001] προχωρήσαμε στις παρακάτω ενέργειες κατά ACPO:

- Αφαιρέθηκε η μπαταρία, χωρίς να πατηθεί το power button,
- Αποσυνδέθηκαν όλα τα περιφερειακά και τα καλώδια, στα οποία τοποθετήθηκαν ετικέτες με αναγνωριστικά και συσκευάστηκαν με κατάλληλο τρόπο ξεχωριστά,
- Προκειμένου να επιβεβαιωθεί η απενεργοποίηση της συσκευής, ανοίχθηκε προσεκτικά το καπάκι και ελέγχθηκε η λειτουργία των ανεμιστήρων,
- Η μπαταρία συσκευάστηκε με προσοχή σε αντιστατική σακούλα με ετικέτα,
- Αφαιρέθηκε ο σκληρός δίσκος, τοποθετήθηκε ετικέτα με κωδικό [0005] και τοποθετήθηκε σε αντιστατική σακούλα,
- Η ίδια η συσκευή τοποθετήθηκε σε αδιάβροχη αντιστατική τσάντα, με τοποθέτηση ταινίας ασφαλείας στις φυσικές θύρες USB και DVD.

3.4.2 Μνήμη Πειστηρίου Laptop

Η μνήμη RAM δεν αφαιρέθηκε φυσικά, αλλά συλλέχθηκε ψηφιακά με live acquisition. Παρόλα αυτά, καθώς αποτελεί ευαίσθητο volatile πειστήριο πραγματοποιήθηκαν οι παρακάτω ενέργειες για την μεταφορά:

- Ο εξωτερικός δίσκος USB FORENSICS που περιείχε τα dumps των RAM τοποθετήθηκε σε αντιστατική σακούλα,
- Επισημάνθηκε με κατάλληλη ετικέτα,
- Καταγράφηκαν και συγκρίθηκαν τα hashes των dumps,
- Τοποθετήθηκε σε κατάλληλο κουτί με αφρολέξ.

3.4.3 Πειστήριο USB [0004]

Το αφαιρούμενο αποθηκευτικό μέσο με κωδικό [0004], με την χρήση αντιστατικών γαντιών τοποθετήθηκε σε κατάλληλη αντιστατική και αδιάβροχη τσάντα με σκληρή επιφάνεια, αφότου είχε τοποθετηθεί η κατάλληλη αναγνωριστική ετικέτα. Υστερα, τοποθετήθηκε εντός κούτας με αφρολέξ.

Τέλος, όλα τα πειστήρια καταγράφηκαν στην κατάλληλη chain of custody φόρμα (βλ. Παράρτημα E)

Όλα τα παραπάνω βήματα διασφαλίζουν την ακεραιότητα και την αποδεικτική ισχύ των ψηφιακών πειστηρίων κατά την περαιτέρω επεξεργασία και ανάλυσή τους στο εργαστήριο.

4. Ανάλυση

Στο παρόν κεφάλαιο παρουσιάζεται η διερεύνηση των ψηφιακών πειστηρίων που συλλέχθηκαν στο πλαίσιο της έρευνας. Η μεθοδολογία που ακολουθήθηκε περιλαμβάνει τη χρήση εξειδικευμένων εργαλείων για τη λήψη και ανάλυση ψηφιακών δεδομένων. Συγκεκριμένα:

- Η μνήμη RAM του πειστηρίου Laptop [0001] αναλύθηκε με το εργαλείο Volatility Framework 2.6 κατόπιν live acquisition κατά την φάση της διαφύλαξης.
- Ο εσωτερικός σκληρός δίσκος του ίδιου Laptop [0001] αναλύθηκε μέσω του εργαλείου Autopsy 4.22.0 κατόπιν δημιουργίας forensic image.
- Τέλος, το αφαιρούμενο αποθηκευτικό μέσο USB [0004] επίσης αναλύθηκε με χρήση του Autopsy 4.22.0, ακολουθώντας όμοια διαδικασία.

Η επιλογή των εργαλείων έγινε βάσει της φύσης των δεδομένων και της δυνατότητας κάθε εργαλείου να προσφέρει αξιόπιστα και τεκμηριωμένα αποτελέσματα.

4.1 Ανάλυση περιεχομένων μνήμης πειστηρίου Laptop [0001]

Η ανάλυση της μνήμης RAM του πειστηρίου πραγματοποιήθηκε με τη χρήση του εργαλείου **Volatility Framework 2.4**, με βάση το αρχείο που προέκυψε από live acquisition με το **MDD (MoonSols DumpIt) έκδοση 1**. Το memory dump αναλύθηκε με στόχο την εξαγωγή τεχνικών και πραγματολογικών δεδομένων που σχετίζονται με την τρέχουσα κατάσταση του συστήματος κατά τη στιγμή της απόκτησης του αντιγράφου.

Η διαδικασία περιλάμβανε τη χρήση ειδικών plugins του Volatility όπως τα pslist, psscan, hashdump, shellbags, svcscan, connscan, consoles, hivelist και printkey, με στόχο την αποκάλυψη ενεργών διεργασιών, δικτυακής δραστηριότητας, ιχνών χρήστη, καταχωρήσεων στο μητρώο (registry), καθώς και πιθανών ενδείξεων κακόβουλης ή ύποπτης δραστηριότητας.

Στο παρόν υποκεφάλαιο παρουσιάζονται οι βασικές δομικές πληροφορίες της καταγραφής μνήμης, το περιβάλλον του λειτουργικού συστήματος, καθώς και μια συνοπτική επισκόπηση των βασικών ευρημάτων που προέκυψαν από την εξέταση της RAM. Ειδικά ευρήματα όπως η παρουσία εργαλείων στεγανογραφίας, η δικτυακή συμπεριφορά του χρήστη, το ιστορικό πρόσβασης σε αρχεία και φάκελους, καθώς και η δομή των διεργασιών παρουσιάζονται αναλυτικά.

Η λεπτομερής εκτέλεση των εντολών με τα αποτελέσματα τους παρατίθενται στο **Παράρτημα Γ**.

Item	Detailed Information
Έναρξη	2009-12-11 08:59:52 π.μ.
Είδος Dump	Physical Memory Dump
Αρχείο Dump	charlie-2009-12-11.mddramimage
Υποπτος Χρήστης	charlie (εμφανίζεται σε hashdump, cmd.exe, explorer.exe)
MD5	38067cc457546b3156975d9a52d4229f (Io αντίγραφο)
SHA-1	15c1ae5e2ac3da7a9cdaaa9a162aa9ac9dde3d9d (Io αντίγραφο)

Εργαλείο Imaging	MDD (MoonSols DumpIt) v1.3
Εργαλείο Ανάλυσης	Volatility 2.4 standalone
Μορφή Dump	RAW Memory Image
Operating System (Profile)	WinXPSP2x86 (<i>προτάθηκε από imageinfo</i>)
KDBG Offset	0x5532e0 (physical), 0x805532e0 (virtual)
Συνολικό Μέγεθος Dump	≈ 2 GB (<i>σύμφωνα με καταγεγραμμένη φυσική μνήμη</i>)
Αριθμός Διεργασιών	26 (σύμφωνα με pslist)
Εντολές CMD	cmd.exe με mdd_1.3.exe (<i>λήψη dump μέσω command prompt</i>)
Shellbags Ευρήματα	Invisible Secrets 2.1\decrypt με timestamp 1970-01-01 (πιθανή αλλοίωση), φακέλους RECYCLER, αρχεία με ύποπτα ονόματα
Δίκτυο - Connections	SMB, HTTP, POP3S, Loopback — από connscan:όπως jusched.exe → 198.189.255.73:80, thunderbird → SSL
Υπηρεσίες (Services)	Ανακτήθηκαν με svchost, συμπεριλαμβανομένων και τερματισμένων ή κρυφών υπηρεσιών
Αρχεία Χρήστη/Ιστορικό	Από Registry Hives (NTUSER.DAT), ιστορικό αρχείων, URLs
Δομή Διεργασιών (pstree)	explorer.exe → thunderbird.exe → cmd.exe → mdd.exe (<i>κανονική ροή ενεργειών</i>)
Visited Files / Downloads	Περιεχόμενο με λέξεις όπως “Quantum Cryptography”, “Patents”, “cygnusfe.zip”, “Immortality”, “Nitroba”
Shellbags Path Analysis	Z:\, πιθανή χρήση USB/δικτυακού drive για μεταφορά δεδομένων
Σχολιασμένα Ευρήματα	Στεγανογραφία, πιθανή απόκρυψη δεδομένων, ύποπτα timestamps, loopback sessions, εξωτερικές HTTP/POP3 συνδέσεις

4.2 Ανάλυση περιεχομένων δίσκου [0005]

Η ανάλυση του σκληρού δίσκου [0005] πραγματοποιήθηκε με τη χρήση του εργαλείου **Autopsy**. Το forensic image αναλύθηκε με στόχο την εξαγωγή τεχνικών και πραγματολογικών δεδομένων που σχετίζονται με το υπό διερεύνηση περιστατικό. Στο παρόν υποκεφάλαιο παρουσιάζονται οι βασικές δομικές πληροφορίες του δίσκου καθώς και μια επισκόπηση του τύπου και του πλήθους των αρχείων που εντοπίστηκαν κατά την αυτοψία. Λεπτομερή ευρήματα και απαντήσεις σε εξειδικευμένα ερωτήματα παρατίθενται στο **Παράρτημα Δ.**

Item	Detailed Information
Έναρξη	2009-12-11 09:12:15 π.μ.
Πειστήριο	Σκληρός Δίσκος [0005]
Αντίγραφο	charlie-2009-12-11.E01
Υποπτος Χρήστης	charlie
MD5	0377b3d41bbc295a1c9f00aa07ee174
SHA-1	ee1d5febb63def90c2900b6984d21a6a137f00ce

Εργαλείο Imaging	FTK imager 4.7.3.81
Μορφή Image	E01 (Expert Witness Compression Format)
Partitions	vol1 (Unallocated: 0-62) vol2 (NTFS / exFAT (0x07): 63-19968794) vol3 (Unallocated: 19968795-19999727)
Bytes ανά Sector	512
Συνολικοί Sectors	19,999,728
Συνολικό Μέγεθος	10.24 GB (10,239,860,736 bytes)
Αρχεία που βρέθηκαν	<ul style="list-style-type: none"> • Εικόνες (45286) • Βίντεο (51) • Ήχος (168) • Archives (553) • Databases (46) • Διαγεγραμμένα Αρχεία (3493) • HTML (873) • Office (29) • PDF (30) • Plain Text (1073) • Rich Text (12) • .exe (1423) • .dll (5227) • .bat (5) • .cmd (2) • .com (18)

Πίνακας 9: Βασικές Δομικές Πληροφορίες Πειστηρίου [0005].

4.3 Ανάλυση περιεχομένων πειστηρίου USB [0004]

Στην παρούσα ενότητα, θα πραγματοποιηθεί η ανάλυση του αποθηκευτικού μέσου τύπου USB (Πειστήριο [0004]) που εντοπίστηκε κατά τη διάρκεια της έρευνας. Το USB stick, το οποίο δεν ήταν συνδεδεμένο κατά την αρχική διαδικασία διαφύλαξης, συνδέθηκε με τον υπολογιστή που χρησιμοποιείται για την ανάλυση και εξετάστηκε με το εργαλείο **Autopsy**. Η ανάλυση επικεντρώθηκε στην αναγνώριση και την ανάκτηση των δεδομένων που περιείχε το USB stick, όπως έγγραφα, εικόνες, αρχεία ήχου και άλλα αρχεία που ενδέχεται να σχετίζονται με την υπόθεση. Κατά τη διάρκεια της ανάλυσης, ελέγχθηκαν οι καταχωρήσεις του συστήματος αρχείων και πραγματοποιήθηκαν εξειδικευμένες αναζητήσεις για να εντοπιστούν σημαντικά αποδεικτικά στοιχεία. Όλα τα αποτελέσματα και τα δεδομένα που προέκυψαν από την ανάλυση καταγράφηκαν και παρατίθενται στο **Παράρτημα Δ** της αναφοράς, περιλαμβάνοντας τις αντίστοιχες εντολές, τα αποτελέσματα και τα αναγνωριστικά των αρχείων που βρέθηκαν

Item	Detailed Information
Έναρξη	2009-12-11 9:36:54 π.μ.
Πειστήριο	Kingston Data Traveler 2.0 USB Device [0004]
Αντίγραφο	charlie-work-usb-2009-12-11.E01
Υποπτος Χρήστης	charlie

MD5	9c0de6c8532d7a66ddcf01861dfb6535
SHA-1	e49bf6048856570cc3d49b1485d6d87aab6ab0a
Εργαλείο Imaging	FTK imager 4.7.3.81
Μορφή Image	E01 (Expert Witness Compression Format)
Partitions	vol1 (Unallocated: 0-0) vol2 (NTFS / exFAT (0x07): 1-2068479)
Bytes ανά Sector	512
Συνολικοί Sectors	2,069,680
Συνολικό Μέγεθος	1.06 GB (1,059,061,760 bytes)
Αρχεία που βρέθηκαν	<ul style="list-style-type: none"> • Εικόνες (11) • Βίντεο (0) • Ήχος (0) • Archives (4) • Databases (1) • Διαγεγραμμένα Αρχεία (2) • HTML (0) • Office (1) • PDF (12) • Plain Text (163) • Rich Text (0) • .exe (2) • .dll (0) • .bat (0) • .cmd (0) • .com (0)

Πίνακας 10: Βασικές Δομικές Πληροφορίες Πειστηρίου [0004]

5. Παρουσίαση

5.1. Εισαγωγή

Η παρούσα αναφορά συντάχθηκε στα πλαίσια έρευνας (Case ID: 00111122009) σχετικά με την εταιρεία M57.biz, μια επιχείρηση που ειδικεύεται στην αναζήτηση διπλωμάτων ευρεσιτεχνίας. Στις 10/12/2009 ημέρα Πέμπτη, η εταιρεία μας DigiFor δέχθηκε τηλεφωνική ενημέρωση από την εταιρεία M57.biz σχετικά με πιθανή ύποπτη δραστηριότητα υπαλλήλου, η οποία ενδέχεται να συνδέεται με παραβίαση εσωτερικών δεδομένων και διαρροή εναίσθητων πληροφοριών. Συγκεκριμένα, ο διευθύνων σύμβουλος της εταιρείας, κύριος Pat McGoo, εξέφρασε ανησυχίες για πιθανή υποκλοπή εταιρικών δεδομένων πελατών – τα οποία διαχειρίζονταν στο πλαίσιο συμφωνιών εμπιστευτικότητας – και για διαρροή ή ακόμη και πώλησή τους σε ανταγωνιστές των εν λόγω πελατών. Συγκεκριμένα, ύποπτος είναι ο υπάλληλος της M57.biz κύριος Charlie, έπειτα από υπόδειξη του IT Administrator, κύριου Terry. Η υπόδειξη βασίστηκε σε ειδοποίηση που έλαβε ο τελευταίος από την αυτόματη υπηρεσία MAILER-DAEMON της εταιρείας, σχετικά με αποτυχία αποστολής e-mail από τον λογαριασμό του εν λόγω υπαλλήλου. Τα πιθανολογούμενα συμβάντα εκτιμάται ότι έλαβαν χώρα εντός του τελευταίου μήνα, με αφετηρία την ημερομηνία πρόσληψης του υπόπτου και εξής. Η διερεύνηση έχει ως στόχο να συλλέξει και να αναλύσει τα ψηφιακά πειστήρια και να εξάγει πληροφορίες και ευρήματα που μπορούν να αποτελέσουν αποδεικτικά στοιχεία σε δικαστικό ή νομικό πλαίσιο.

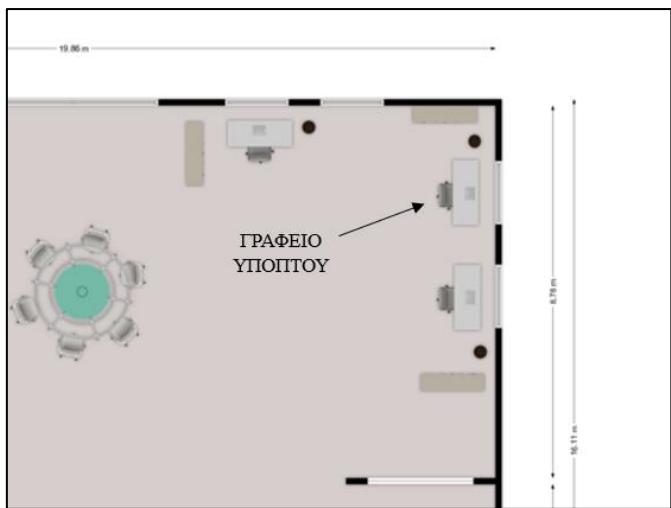
5.2. Συνοπτική Περιγραφή Αποδεικτικών Στοιχείων

Στις 11/12/2009 ημέρα Παρασκευή, η ομάδα της Digifor βρέθηκε στον τόπο του πιθανολογούμενου εγκλήματος και συνέλλεξε όλα εκείνα τα αποδεικτικά στοιχεία που ενδέχεται να αποτελέσουν πηγές ψηφιακών πειστηρίων.

Κατασχέθηκαν ο εταιρικός φορητός υπολογιστής του κυρίου Charlie, μάρκας DELL (σειριακός αριθμός DEJ485BIDFGJF) που βρέθηκε ανοιχτός επάνω στο γραφείο, ένα USB stick (σειριακός αριθμός 2007110203195377) – χωρίς να είναι συνδεδεμένο, το τροφοδοτικό του laptop – συνδεδεμένο (σειριακός αριθμός Q4W0406021262), το ενσύρματο ποντίκι – συνδεδεμένο (σειριακός αριθμός 1939HS01D6W8) – αναλυτικές πληροφορίες (Chain of Custody forms) για τα αποδεικτικά στοιχεία βρίσκονται στο **Παράρτημα Ε**.

Στο χώρο του γραφείου όταν έφτασε η ομάδα μας βρίσκονταν τα παρακάτω άτομα:

Όνοματεπώνυμο	Ρόλος	Σχέση με το συμβάν
Charlie	Υπάλληλος της M57.biz (Patent Researcher)	Ύποπτος
Terry	IT Administrator της M57.biz	Μάρτυρας
Jack	Υπεύθυνος Ασφαλείας της M57.biz	Μάρτυρας



Εικόνα 19: Απόκομμα από κάτοψη ορόφου του γραφείου

5.3. Περιγραφή Ανάλυσης Αποδεικτικών Στοιχείων

Η διαδικασία εφαρμόστηκε σύμφωνα με τις κατευθυντήριες γραμμές και τα πρότυπα της ACPO (Association of Chief Police Officers), δίνοντας ιδιαίτερη έμφαση στη διασφάλιση της ακεραιότητας των πειστηρίων, την αναλυτική καταγραφή κάθε βήματος και τη δυνατότητα επαλήθευσης και αναπαραγωγής των αποτελεσμάτων.

Η μεθοδολογία που ακολουθήθηκε αποτελείται από πέντε (5) διακριτά στάδια: Προετοιμασία – Ανίχνευση – Διαφύλαξη – Ανάλυση – Παρουσίαση.

Το στάδιο της προετοιμασίας περιλαμβάνει τις ενέργειες της ομάδας Digifor από τη στιγμή της ενημέρωσης από την M57.biz έως την άφιξη στον χώρο του εγκλήματος και τοποθετείται χρονικά από τις 10/12/2009 ώρα 7:30 μ.μ. έως τις 10/12/2009 ώρα 10:30 μ.μ. Περιλαμβάνει την οργάνωση και ενημέρωση της ομάδας, τον καθορισμό αρμοδιοτήτων – βλ. **Παράρτημα Α** (RACI matrix), την υπογραφή σχετικών συμβάσεων – βλ. **Παράρτημα Ζ**, την ενημέρωση για τη νομοθεσία και την καταγραφή του απαραίτητου εξοπλισμού και λογισμικού – βλ. Πίνακας 1: Εργαλεία Forensics.

Το στάδιο της ανίχνευσης αφορά στις διαδικασίες που ακολουθήθηκαν από την άφιξη της ομάδας στον χώρο του πιθανολογούμενου εγκλήματος και έχουν ως στόχο τον εντοπισμό και την πλήρη καταγραφή των διαθέσιμων ψηφιακών πειστηρίων. Κατά το στάδιο αυτό πραγματοποιήθηκαν καταγραφή του χώρου εργασίας του υπόπτου (σχέδιο κάτοψης του γραφείου, φωτογράφιση του χώρου) και συνεντεύξεις με τους παρευρισκόμενους – βλ. **Παράρτημα Β**. Χρονικά το συγκεκριμένο στάδιο τοποθετείται στο διάστημα 11/12/2009 ώρα 8:32 π.μ. έως 9:10 π.μ.

Το στάδιο της διαφύλαξης περιλαμβάνει εκείνες τις ενέργειες που αφορούν στην διαφύλαξη της ακεραιότητας των ψηφιακών πειστηρίων στο χώρο του εγκλήματος. Ελήφθησαν πρώτα πιστά αντίγραφα των ευμετάβλητων (volatile) δεδομένων, με προτεραιότητα σε RAM, Cache και Registry. Ακολούθως, καταγράφηκαν και τα μη ευμετάβλητα (non-volatile) δεδομένα (σκληρός δίσκος λάπτοπ και USB) και έγινε και η διαδικασία προετοιμασίας των πειστηρίων για τη μεταφορά τους στο εργαστήριο. Στο στάδιο της διαφύλαξης χρησιμοποιήθηκαν τα εξής εργαλεία: MDD MoonSols DumpIt, για την λήψη 1^ο πιστού αντιγράφου μνήμης, Win32dd για τη λήψη 2^ο πιστού αντιγράφου μνήμης, FTK imager και FEX Imager για τη λήψη αντιγράφου

του σκληρού δίσκου και USB stick. Χρονικά το συγκεκριμένο στάδιο τοποθετείται στο διάστημα 11/12/2009 ώρα 8:57 π.μ. έως 9:39 π.μ.

Τέλος, το στάδιο της ανάλυσης λαμβάνει χώρα πλέον στο εργαστήριο και περιλαμβάνει την ανάλυση των ληφθέντων ψηφιακών πειστηρίων με σκοπό τη διερεύνηση και τον εντοπισμό ιχνών που να επιβεβαιώνουν την τέλεση εγκληματικής πράξης. Στο στάδιο αυτό χρησιμοποιήθηκαν τα εργαλεία: Volatility Framework 2.4, για την ανάλυση του πειστηρίου μνήμης και Autopsy για την ανάλυση του σκληρού δίσκου και του USB stick. Η παραπάνω διαδικασία εξέτασης και τα ευρήματα που προέκυψαν από αυτή παρατίθενται στα **Παραρτήματα Γ και Δ**.

5.4. Περιγραφή Ανάλυσης File System

Τα ψηφιακά πειστηρία που διέθεταν σύστημα αρχείων (file system), συγκεκριμένα ο σκληρός δίσκος και το USB stick, αναλύθηκαν με τη χρήση του εργαλείου Autopsy. Κατά την ανάλυση εντοπίστηκαν συνοπτικά τα εξής δεδομένα στο σύστημα αρχείων τους:

	Laptop / Σκληρός Δίσκος	USB Stick
Λειτουργικό Σύστημα:	Microsoft Windows XP (Version 5.1)	-
Χωρητικότητα	10.24 GB	1.06 GB
MD5 Hash	0377b3d41bbbc295a1c9f00aa07ee174	9c0de6c8532d7a66ddcf01861dfb6535
Αρχεία που βρέθηκαν	<ul style="list-style-type: none"> • Εικόνες (45286) • Βίντεο (51) • Ήχος (168) • Archives (553) • Databases (46) • Διαγεγραμμένα Αρχεία (3493) • HTML (873) • Office (29) • PDF (30) • Plain Text (1073) • Rich Text (12) • .exe (1423) • .dll (5227) • .bat (5) • .cmd (2) • .com (18) 	<ul style="list-style-type: none"> • Εικόνες (11) • Βίντεο (0) • Ήχος (0) • Archives (4) • Databases (1) • Διαγεγραμμένα Αρχεία (2) • HTML (0) • Office (1) • PDF (12) • Plain Text (163) • Rich Text (0) • .exe (2) • .dll (0) • .bat (0) • .cmd (0) • .com (0)
Αριθμός Χρηστών	1 ²	-
Αριθμός Προγραμμάτων	19	-

Αναλυτικότερα τα ευρήματα που προέκυψαν από τα πιστά αντίγραφα δίσκου και USB και αναλύθηκαν με τη βοήθεια του Autopsy περιγράφονται στα **Παραρτήματα Γ και Δ**.

² Χωρίς να καταγράφονται Built-in, Support και Service λογαριασμοί του συστήματος (Administrator, Guest, HelpAssistant, SUPPORT_388945a0)

5.5. Ανάλυση

Στο παρόν κεφάλαιο παρουσιάζεται η ανάλυση των ψηφιακών πειστηρίων που συλλέχθηκαν και μεταφέρθηκαν στο εργαστήριο. Έχει διασφαλιστεί ότι σε όλα τα προηγούμενα στάδια της διαδικασίας τηρήθηκαν πλήρως οι αρχές και οι κατευθυντήριες γραμμές της ACPO, με ιδιαίτερη έμφαση στη διατήρηση της ακεραιότητας των πειστηρίων. Ακολουθεί παρουσίαση των δεδομένων και των ευρημάτων που προέκυψαν κατά την εξέταση των πειστηρίων, εστιάζοντας στα πλέον συναφή και ουσιώδη στοιχεία σε σχέση με την υπό διερεύνηση υπόθεση. Τέλος στο παράρτημα H, επισυνάπτεται και γραφική αναπαράσταση του χρονοδιαγράμματος ενεργειών του υπόπτου Charlie.

I. Πίνακας Αποδεικτικών στοιχείων - Αρχεία

A/A	Όνομα Αρχείου	Πηγή Πειστηρίου	MD5 Hash	Περιγραφή
1.	astronaut1.jpg	Δίσκος: Files	45eade24b3a89b21fed 303310ccbdc54	Αρχείο .jpg το οποίο στο οποίο έχει γίνει στεγανογραφία.
2.	01.zip	Δίσκος: Emails	4fa239c22e5fb7b934a 1bf68e4e0e2e7	Συμπιεσμένος φάκελος που περιείχε αρχεία πατεντών σε μορφή φωτογραφιών.
3.	microscope1.jpg	Δίσκος: Emails	4be2c4abb48c4389ca 798e6c21736ea1	Αρχείο φωτογραφίας (.jpg) που περιείχε τον κωδικό για την αποσυμπίεση του αρχείου 01.zip.

Για περισσότερες λεπτομέρειες σχετικά με την Στεγανάλυση των παραπάνω αρχείων βλ.

Παράρτημα Θ.

II. Πίνακας Αποδεικτικών στοιχείων – Προγράμματα

A/A	Όνομασία	Ημερομηνία Εγκατάστασης	Installation Path
4.	Cygnus Hex Editor Free Edition 1.00	2009-11-24 14:01:10	C:\Program Files\Cygnus FREE EDITION\
5.	Invisible Secrets 2.1	2009-11-19 10:43:32	C:\Program Files\Invisible Secrets 2.1\

III. Αποδεικτικά στοιχεία – Emails

6.	Email ανάθεσης patent search εργασιών για Time Machine στον Charlie		
2009-11-17 10:33:39	Source	[Inbox]	
	From → To	pat@m57.biz-> charlie@m57.biz , jo@m57.biz	
	Subject	ASSIGNMENT OF NITROBA ACCOUNT	
	Body	<p>Jo, Charlie:</p> <p>We have our first contract ! Nitroba wants us to do a prior art investigation in two key areas. Jo, you will be responsible for the teleporter patent search. Charlie, I want you to take the time machine patent search. This is our first real job, so let's make sure we do some quality research. Our reputation will depend on the time and effort that we put into this contract and on Nitroba's satisfaction with our results. Come by my office and we'll talk details.</p> <p>Pat</p>	

7.	Email όπου ο Charlie αφήνει να εννοηθεί η προσδοκία μελλοντικού οικονομικού οφέλους.		
2009-12-01 13:02:34	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com	
	Subject	Pack your bags	
	Body	<p>Alix,</p> <p>Pretty soon I'm going to be able to afford to take you on a nice vacation. Where would you want to go if you could name your destination? I'm getting a hot car too.</p> <p>Charlie</p>	

8.	Αλληλογραφία με Jaime (@project2400.com) κατά την οποία ο Charlie προσφέρει να πουλήσει εμπιστευτικές πληροφορίες της Nitroba έναντι αντιτίμου. Ο Jamie αποδέχεται την προσφορά και λαμβάνει από τον Charlie το αρχείο astronaut1.jpg και τον κωδικό nitro.		
2009-12-02 13:04:29	Source	[Sent]	
	From → To	charlie@m57.biz → jaime@project2400.com	

	Subject	Intrested?
	Body	<p>J,</p> <p>I have something that you'll definitely be interested in. It concerns your competitor. I'm doing a prior art search for them. Want to know what I've found? You know my price. I'll send you the goods after I see half in my account. Make sure you delete this email.</p> <p>C</p>

2009-12-03 09:51:33	Source	[Inbox]
	From → To	jaime@project2400.com → charlie@m57.biz
	Subject	RE:Intrested?
	Body	<p>C,</p> <p>We'll give you 50 large if it's good. I'll put in 10 up front, you'll get the rest when we see the goods.</p> <p>J</p>

2009-12-03 12:16:52	Source	[Sent]
	From → To	charlie@m57.biz → jaime@project2400.com
	Subject	
	Body	<p>J,</p> <p>Nice working with you. Here's the file. Instructions for opening to follow when I see another deposit in my acct.</p> <p>C</p> <p>+Attachment= Astronaut1.jpg</p>

2009-12-04 13:06:23	Source	[Sent]
	From → To	charlie@m57.biz → jaime@project2400.com
	Subject	Instructions
	Body	<p>J,</p> <p>Got the deposit. The password to get the info is nitro. Use the steg program we talked about. And don't forget to delete these emails.</p> <p>C</p>

9.	Αλληλογραφία με Andy (@swexpert.com). Ο Charlie φαίνεται να εκβιάζει τον Andy για 100.000\$ για ένα “immortality patent” στέλνοντας ένα συμπιεσμένο και κλειδωμένο με κωδικό, .zip αρχείο. Στη συνέχεια, αποστέλλει και τον κωδικό με στεγανοφημένο αρχείο jpg.	
	Source	[Sent]

2009-12-04 09:41:47	From → To	charlie@m57.biz → andy@swexpert.com
	Subject	I Found Something
	Body	<p>Andy,</p> <p>Lucky for me, I just happened to stumble across this. I found a prior patent that will definitely invalidate your current immortality patent. You should have used my boss's prior art services, but, oh well, I'll just use your negligence to benefit me. I want 100k or I'll release this publicly. I don't need to tell you how much this will hurt your business if I go public with this. Don't involve the cops or this information will go public. See the attachment for details on what I found. I'll be in touch with my bank acct number. The password for the zip file will be hidden in the next picture I send you.</p> <p>C +Attachment zip file</p>

2009-12-07 11:44:18	Source	[Sent]
	From → To	charlie@m57.biz → andy@swexpert.com
	Subject	Picture
	Body	<p>Andy,</p> <p>Here's the picture I promised... Make sure you delete this.</p> <p>C +Attachment microscope1.jpg</p>

IV. Πίνακας αποδεικτικών στοιχείων – Αναζήτησεις Web

A/A	Ημερομηνία Αναζήτησης	Κλειδί Αναζήτησης	Μηχανή Αναζήτησης
10.	2009-11-19 10:39:24	<i>steganography</i>	http://www.google.com
11.	2009-11-19 10:41:43	<i>steganography tool free</i>	http://www.google.com
12.	2009-11-24 13:57:33	<i>open source hex editor</i>	http://www.google.com

Για περισσότερες λεπτομέρειες σχετικά με όλα τα παραπάνω βλ. Ανάλυση Δίσκου Πειστηρίου Λάπτοπ – **Παράρτημα Δ.**

5.6. Συμπεράσματα

Κατόπιν ολοκληρωμένης ανάλυσης των ψηφιακών πειστηρίων (σκληρός δίσκος laptop, RAM laptop και USB φορητού αποθηκευτικού μέσου), προέκυψαν ευρήματα που ενισχύουν σοβαρά τις υποψίες εις βάρος του υπαλλήλου Charlie, για διάπραξη πολλαπλών παράνομων ενεργειών.

Συγκεκριμένα, κατά την εξέταση του πιστού αντιγράφου σκληρού δίσκου και του πιστού αντιγράφου μνήμης, διαπιστώθηκε η εγκατάσταση και χρήση εργαλείων στεγανογραφίας. Επιπλέον, ανακαλύφθηκαν σχετικές αναζητήσεις στο διαδίκτυο οι οποίες δύναται να υποδηλώσουν πρόθεση και σχεδιασμό απόκρυψης πληροφοριών. Παράλληλα, η ανάλυση των επικοινωνιών μέσω e-mail αποκάλυψε τα εξής:

- **Μη εξουσιοδοτημένη διάθεση εμπιστευτικών πληροφοριών σε τρίτους**, με αντάλλαγμα οικονομικό όφελος, μέσω επικοινωνίας με την ανταγωνίστρια εταιρεία Project2400. Συγκεκριμένα, ο Charlie αποστέλλει αρχείο που περιέχει εμπιστευτικά δεδομένα της Nitroba και λαμβάνει συμφωνηθέν χρηματικό ποσό.
- **Απόπειρα εκβίασης** εις βάρος του εκπροσώπου της εταιρείας SWExpert, Andy, με την απαίτηση ποσού \$100.000 για να μην αποκαλύψει αρχείο που φέρεται να σχετίζεται με "προγενέστερη πατέντα" η οποία θα μπορούσε να ακυρώσει κατατεθειμένο δικαίωμα ευρεσιτεχνίας (immortality patent). Ο εκβιασμός συνοδεύεται από χρήση αρχείων με κρυφές πληροφορίες μέσω στεγανογραφίας.

Από τη στεγαναλυτική διερεύνηση των συνημμένων αρχείων επιβεβαιώθηκε ότι περιείχαν εμπιστευτικές πληροφορίες, αποδεικνύοντας τη χρήση τεχνικών απόκρυψης για την παράνομη μεταφορά ευαίσθητων δεδομένων.

Συνοψίζοντας, ο Charlie φέρεται να έχει διαπράξει τις εξής παράνομες ενέργειες:

1. **Παραβίαση συμφωνιών εμπιστευτικότητας** και μη εξουσιοδοτημένη κοινοποίηση εμπιστευτικών πληροφοριών.
2. **Πώληση ευαίσθητων εταιρικών δεδομένων** σε ανταγωνιστές.
3. **Εκβιασμός** με σκοπό την οικονομική εκμετάλλευση εμπιστευτικού υλικού.
4. **Απόκρυψη και παράνομη μεταφορά δεδομένων** με τη χρήση τεχνικών στεγανογραφίας.
5. **Παραβίαση της εσωτερικής πολιτικής ασφάλειας της εταιρείας M57.biz.**

Τα παραπάνω ευρήματα, υποστηριζόμενα από τεχνική τεκμηρίωση και διατήρηση της αλυσίδας φύλαξης των πειστηρίων, μπορούν να αποτελέσουν βάση για ποινική διερεύνηση και νομική δίωξη.

Παράρτημα Α – Πίνακας RACI

Δραστηριότητα / Βήμα	Expert Witness (1231)	TW1 (1232)	TW2 (1233)	TW3 (1234)
1. Προετοιμασία				
1.1 Εντοπισμός αρμοδιοτήτων και σχεδιασμός διαδικασίας	A/R	C	I	I
1.2 Συγκέντρωση απαραίτητου εξοπλισμού	A	R	R	C
1.3 Έλεγχος νομιμότητας και εξουσιοδοτήσεων	A	I	I	R
2. Ανίχνευση & Εντοπισμός				
2.1 Διενέργεια συνεντεύξεων	A	R	I	I
2.2 Καταγραφή χώρου	A	I	R	I
2.3 Εντοπισμός και καταγραφή πηγών πειστηρίων	A	I	I	R
3. Διαφύλαξη (Preservation)				
3.1 Καταγραφή πειστηρίων	A	R	C	C
3.2 Συμπλήρωση Κατάλληλων Φορμών	A	R	C	I
3.3 Απόσπαση μνήμης και αποθήκευση εικόνων	A	C	R	I
3.4 Μεταφορά πειστηρίων στο εργαστήριο	A	C	R	C
4. Ανάλυση (Analysis)				
4.1 Ανάλυση και Τεκμηρίωση μνήμης	C	R	I	I
4.2 Ανάλυση και Τεκμηρίωση δίσκου	C	I	R	I
4.3 Ανάλυση και Τεκμηρίωση USB	C	I	I	R
4.4 Ερμηνεία ευρημάτων	A/R	C	C	C
5. Παρουσίαση / Αναφορά				
5.1 Σύνταξη τελικής έκθεσης	A/R	C	C	C
5.2 Προετοιμασία παρουσίασης	A/R	R	C	C

Πίνακας 11: Πίνακας Αρμοδιοτήτων RACI.

Παράρτημα Β – Συνεντεύξεις

Πιθανός δράστης

- Ποια ήταν η θέση σας στην εταιρεία και οι βασικές αρμοδιότητές σας;
Απάντηση: Στην εταιρεία εργάζομαι ως ερευνητής για νέες πατέντες. Κύριες αρμοδιότητές μου είναι από τη στιγμή που θα γίνει η σύλληψη της ιδέας, να προσπαθήσω μαζί με τους άλλους ερευνητές να την υλοποιήσουμε.
- Είχατε πρόσβαση σε αρχεία ή δεδομένα που σχετίζονται με ευρεσιτεχνίες;
Απάντηση: Ναι κατείχα πρόσβαση καθώς χρειάζεται για την εργασία μου.
- Χρησιμοποιούσατε προσωπικό εξοπλισμό για την εργασία σας (π.χ. laptop, USB);
Απάντηση: Όχι, ο εξοπλισμός που χρησιμοποιώ είναι εταιρικός.
- Έχετε μεταφέρει αρχεία της εταιρείας εκτός δικτύου;
Απάντηση: Όχι, ό,τι χρησιμοποιούσα ήταν μέσω του δικτύου της εταιρείας είτε τοπικά στις συσκευές που μου έχει παραχωρήσει.
- Γνωρίζατε ότι η χρήση USB συσκευών περιορίζεται βάσει πολιτικής;
Απάντηση: Όχι, δεν μου έχουν πει κάτι τέτοιο.
- Είχατε πρόσφατα κάποιο πρόβλημα με τη διοίκηση ή υπήρξαν διαφωνίες;
Απάντηση: Όχι, καμία διαφωνία. Η διοίκηση μας αφήνει να εργαστούμε χωρίς περιορισμούς.
- Γνωρίζατε για τις ενέργειες παρακολούθησης ή τα συστήματα καταγραφής (monitoring);
Απάντηση: Δεν είναι αντικείμενο της δουλειάς μου αυτό. Δεν γνωρίζω κάτι.
- Είχατε ποτέ λόγο να διακινήσετε πληροφορίες της εταιρείας εκτός συστήματος;

Απάντηση: Όχι, δεν υπήρχε κάποιος λόγος.

Υπεύθυνος ασφάλειας

1. Πότε υποπτευθήκατε κάτι για το πιθανό περιστατικό;
Απάντηση: Δεν υποπτεύθηκα κάτι εγώ.
2. Τηρεί η εταιρεία πολιτική αντιμετώπισης περιστατικών;
Απάντηση: Όχι, ως νεοσύστατη εταιρεία δεν έχουμε προλάβει να δημιουργήσουμε τέτοιο πλάνο.
3. Υπάρχει επίσημη πολιτική για την προστασία πνευματικής ιδιοκτησίας και εναίσθητων δεδομένων;
Απάντηση: Η εταιρεία καθώς διαχειρίζεται εναίσθητα δεδομένα και πληροφορίες δεν επιτρέπεται να τα μοιραζόμαστε με τρίτους. Επίσης ισχύει ότι ορίζουν οι νομικές διατάξεις της χώρας.
4. Υπάρχουν περιορισμοί στη χρήση εξωτερικών μέσων (USB, BYOD);
Απάντηση: Μπορεί να χρησιμοποιείται ότι έχει δοθεί στους εργαζόμενους. Δηλαδή το εταιρικό laptop και μία μονάδα USB, που επιτρέπεται να χρησιμοποιείται μόνο σε εταιρικά laptop.
5. Υπάρχει τακτική εκπαίδευση προσωπικού σε θέματα ασφάλειας πληροφοριών;
Απάντηση: Όχι δεν υπάρχει κάτι.
6. Υπήρξαν ενδείξεις για εσωτερική απειλή πριν το συμβάν;
Απάντηση: Όχι δεν υπήρχε κάποια ένδειξη.
7. Είχατε δει από το access control system κάποια προσέλευση στην εταιρεία σε ώρα που δεν μοιάζει λογική;
Απάντηση: Όχι δεν είχε συμβεί κάτι τέτοιο.
8. Ποια μέτρα λήφθηκαν μέχρι την άφιξή μας για την έρευνα;
Απάντηση: Απομονώθηκε ο χώρος.

IT Admin

1. Πότε εντοπίστηκε για πρώτη φορά η ύποπτη δραστηριότητα;;
Απάντηση: Μου ήρθε μια ειδοποίηση ότι από το λογαριασμό του υποψήφιου δράστη απέτυχε να σταλεί ένα email.
2. Έχουν παρατηρηθεί περιέργεις συνδέσεις, logs ή αλλαγές σε αρχεία;
Απάντηση: Όχι, όλα ήταν όπως θα έπρεπε να είναι.
3. Τηρείται αρχείο καταγραφής συμβάντων; Αν ναι, πού αποθηκεύεται και για πόσο διάστημα;
Απάντηση: Δεν έχουμε προλάβει σαν εταιρεία να οργανωθούμε τόσο πολύ.
4. Έχουν υπάρξει πρόσφατα αλλαγές σε δικαιώματα χρηστών ή στο Active Directory;
Απάντηση: Όχι δεν έχει γίνει κάτι.
5. Έχουν γίνει εξωτερικές συνδέσεις μέσω VPN ή Remote Desktop σε περίεργες ώρες;
Απάντηση: Όχι δεν έχει γίνει κάτι τέτοιο.
6. Τι μέτρα back-up και disaster recovery υπάρχουν;

Απάντηση: Εβδομαδιαίως, κρατείται back up από κάθε μηχάνημα υπαλλήλου της εταιρείας.

7. Έχουν εντοπιστεί traces από malware, keyloggers ή άλλες ύποπτες εφαρμογές;

Απάντηση: Όχι δεν έχει εντοπιστεί κάτι στα συστήματα της εταιρείας.

8. Χρησιμοποιείτε web-based email ή κάποιο client για να διαβάζετε τα emails σας?

Απάντηση: Χρησιμοποιείται client. Ο κάθε υπάλληλος μπορεί να χρησιμοποιήσει όποιον client θέλει.

CEO

1. Έχετε δεχτεί email ή επικοινωνία που φαινόταν ύποπτη;

Απάντηση: Όχι δεν έχω δεχτεί κάτι τέτοιο.

2. Έχει υπάρξει προηγούμενο περιστατικό παραβίασης ή απώλειας δεδομένων;

Απάντηση: Όχι δεν έχει ξανά συμβεί κάτι παρόμοιο.

3. Υπήρξαν πρόσφατες απολύσεις ή εσωτερικές εντάσεις που ίσως σχετίζονται με το συμβάν;

Απάντηση: Δεν έχει υπάρξει κάποιο περιστατικό.

4. Από ποιον ενημερώθήκατε για το συμβάν και τι κάνατε μόλις το μάθατε;

Απάντηση: Ενημερώθηκα από τον διαχειριστή συστημάτων της εταιρείας και μόλις το έμαθα αποφάσισα πως η υπόθεση πρέπει να εξεταστεί αμέσως από επαγγελματίες προτού προλάβει ο υποψήφιος δράστης να κάνει κάποια άλλη ενέργεια. Έτσι επικοινώνησα με εσάς.

5. Τι συνέβη στην εταιρεία μετά την επικοινωνία μαζί μας;

Απάντηση: Έδωσα εντολή να μην εισέλθει κανείς στο χώρο και όλα τα συστήματα να μην πειραχτούν από κανέναν.

Παράρτημα Γ – Ανάλυση Μνήμης Πειστηρίου Laptop [0001]

Η πρώτη εντολή που τρέχουμε με το εργαλείο είναι .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" imageinfo όπου μας δείχνει όλες τις πληροφορίες του image της μνήμης.

```
> .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (C:\memdump\charlie-2009-12-11.mddramimage)
PAE type : No PAE
DTB : 0x39000L
KDBG : 0x805532e0L
Number of Processors : 2
Image Type (Service Pack) : 3
    KPCR for CPU 0 : 0xffdff000L
    KPCR for CPU 1 : 0xf7717000L
    KUSER_SHARED_DATA : 0xfffff0000L
Image date and time : 2009-12-11 16:59:52 UTC+0000
Image local date and time : 2009-12-11 08:59:52 -0800
```

Εικόνα 21: Πληροφορίες του image της μνήμης

Στη συνέχεια προσπαθούμε να βρούμε το offset ώστε να μπορέσουμε να δούμε συγκεκριμένες πληροφορίες του image της μνήμης καθώς αυτό είναι η θέση στη μνήμη όπου ξεκινά η σημαντική **δομή δεδομένων "KDBG"** (Kernel Debugger Block). Η δομή αυτή περιέχει σημαντικές πληροφορίες για το λειτουργικό σύστημα. Χρησιμοποιήθηκε η εντολή `\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 kdbgscan` με βάση το προφίλ που βρέθηκε από το image.info.

```
> .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 kdbgscan
Volatility Foundation Volatility Framework 2.4
*****
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V) : 0x805532e0
Offset (P) : 0x5532e0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64 : 0x805532b8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab) : 2600.xpsp_sp3_gdr.090804-1435
PsActiveProcessHead : 0x80569658 (26 processes)
PsLoadedModuleList : 0x805634c0 (113 modules)
KernelBase : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader) : 5
Minor (OptionalHeader) : 1
KPCR : 0xffffdff000 (CPU 0)
KPCR : 0xf7717000 (CPU 1)
```

Εικόνα 22: Offset

Συμπεραίνουμε ότι το physical offset είναι `--kdbg=0x5532e0` και το virtual offset είναι `0x805532e0` το οποίο μπορούμε να το αξιοποιήσουμε στις μετέπειτα εντολές για μεγαλύτερη ακρίβεια.

Στη συνέχεια εκτελέστηκε η εντολή `\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 pslist` η οποία μας έδωσε τη λίστα των ενεργών ή πρόσφατων processes τη στιγμή λήγυς του αντιγράφου.

```
> .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.4
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0x89bf9c8 System 4 0 64 512 ----- 0
0x89af0460 smss.exe 876 4 3 19 ----- 0 2009-12-11 00:53:21 UTC+0000
0x899fd970 csrss.exe 924 876 11 417 0 0 2009-12-11 00:53:22 UTC+0000
0x89b0b818 winlogon.exe 948 876 17 572 0 0 2009-12-11 00:53:22 UTC+0000
0x89afb5d0 services.exe 992 948 15 265 0 0 2009-12-11 00:53:23 UTC+0000
0x896e01e0 lsass.exe 1004 948 22 354 0 0 2009-12-11 00:53:23 UTC+0000
0x89afa608 svchost.exe 1180 992 17 194 0 0 2009-12-11 00:53:23 UTC+0000
0x89887a78 svchost.exe 1268 992 10 272 0 0 2009-12-11 00:53:24 UTC+0000
0x89387978 svchost.exe 1392 992 74 1523 0 0 2009-12-11 00:53:24 UTC+0000
0x89476da0 svchost.exe 1532 992 5 81 0 0 2009-12-11 00:53:24 UTC+0000
0x8988cc18 svchost.exe 1644 992 11 166 0 0 2009-12-11 00:53:24 UTC+0000
0x893a2ca8 spoolsv.exe 1908 992 10 114 0 0 2009-12-11 00:53:26 UTC+0000
0x8944d9e0 svchost.exe 1796 992 4 108 0 0 2009-12-11 00:53:40 UTC+0000
0x897899e0 avgwdsvc.exe 1728 992 25 962 0 0 2009-12-11 00:53:40 UTC+0000
0x89398160 jqs.exe 320 992 5 117 0 0 2009-12-11 00:53:42 UTC+0000
```

Εικόνα 23: Λίστα των ενεργών ή πρόσφατων processes

0x89395800 explorer.exe	1348	1304	13	481	0	0	2009-12-11 00:53:46 UTC+0000
0x892ccbc0 hkcmd.exe	2684	1348	2	104	0	0	2009-12-11 00:53:51 UTC+0000
0x892d6948 jusched.exe	2804	1348	2	152	0	0	2009-12-11 00:53:51 UTC+0000
0x8990ebe0 ctfmon.exe	2832	1348	1	71	0	0	2009-12-11 00:53:52 UTC+0000
0x89292308 alg.exe	2956	992	6	107	0	0	2009-12-11 00:53:52 UTC+0000
0x892a29e0 soffice.exe	3048	3000	1	20	0	0	2009-12-11 00:53:52 UTC+0000
0x89281da0 soffice.bin	3088	3048	7	216	0	0	2009-12-11 00:53:53 UTC+0000
0x89482718 avgfws9.exe	3936	992	25	762	0	0	2009-12-11 00:54:05 UTC+0000
0x892e57b0 thunderbird.exe	188	1348	10	203	0	0	2009-12-11 16:54:43 UTC+0000
0x899a7020 cmd.exe	3296	1348	1	33	0	0	2009-12-11 16:59:32 UTC+0000
0x8938cb28 mdd_1.3.exe	1768	3296	1	24	0	0	2009-12-11 16:59:51 UTC+0000

Εικόνα 24 Λίστα των ενεργών ή πρόσφατων processes 2.

Offset	Όνομα	PID	PPID	Νήματα	Handles	Session	Έναρξη
0x89bf9c8	System	4	0	64	512	-	-
0x89af0460	smss.exe	876	4	3	19	-	2009-12-11 16:53:21 PST
0x899fd970	csrss.exe	924	876	11	417	0	2009-12-11 16:53:22 PST
0x89b0b818	winlogon.exe	948	876	17	572	0	2009-12-11 16:53:22 PST
0x89afb5d0	services.exe	992	948	15	265	0	2009-12-11 16:53:23 PST
0x896e01e0	lsass.exe	1004	948	22	354	0	2009-12-11 16:53:23 PST
0x89afa608	svchost.exe	1180	992	17	194	0	2009-12-11 16:53:23 PST
0x89887a78	svchost.exe	1268	992	10	272	0	2009-12-11 16:53:24 PST

0x89387978	svchost.exe	1392	992	74	1523	0	2009-12-11 16:53:24 PST
0x89476da0	svchost.exe	1532	992	5	81	0	2009-12-11 16:53:24 PST
0x8988cc18	svchost.exe	1644	992	11	166	0	2009-12-11 16:53:24 PST
0x893a2ca8	spoolsv.exe	1908	992	10	114	0	2009-12-11 16:53:26 PST
0x8944d9e0	svchost.exe	1796	992	4	108	0	2009-12-11 16:53:40 PST
0x897899e0	avgwdsvc.exe	1728	992	25	962	0	2009-12-11 16:53:40 PST
0x89398160	jqs.exe	320	992	5	117	0	2009-12-11 16:53:42 PST
0x89395800	explorer.exe	1348	1304	13	481	0	2009-12-11 16:53:46 PST
0x892ccb0	hkcmd.exe	2684	1348	2	104	0	2009-12-11 16:53:51 PST
0x892d6948	jusched.exe	2804	1348	2	152	0	2009-12-11 16:53:51 PST
0x8990eb0	ctfmon.exe	2832	1348	1	71	0	2009-12-11

								16:53:52 PST
0x89292308	alg.exe	2956	992	6	107	0	2009-12-11 16:53:52 PST	
0x892a29e0	soffice.exe	3048	3000	1	20	0	2009-12-11 16:53:52 PST	
0x89281da0	soffice.bin	3088	3048	7	216	0	2009-12-11 16:53:53 PST	
0x89482718	avgfws9.exe	3936	992	25	762	0	2009-12-11 16:54:05 PST	
0x892e57b0	thunderbird.exe	188	1348	10	203	0	2009-12-11 08:54:43 PST	
0x899a7020	cmd.exe	3296	1348	1	33	0	2009-12-11 08:59:32 PST	
0x8938cb28	mdd_1.3.exe	1768	3296	1	24	0	2009-12-11 08:59:51 PST	

Πίνακας 12: Ενεργές ή πρόσφατες διεργασίες.

Τα αποτελέσματα αυτής της εκτέλεσης μας φαίνονται φυσιολογικά καθώς όλες οι διεργασίες έχουν πατέρα διεργασία. Αυτές που ξεκίνησε ο χρήστης έχουν ppid=1348 και τα υπόλοιπα είναι φυσιολογικά processes του συστήματος. Η τελευταία διεργασία είναι η λήψη του αντιγράφου όπως αναμέναμε. Στη συνέχεια εκτελούμε .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 psscan και για την εύρεση κρυφών διεργασιών η ανωμαλιών που υποδεικνύουν την ύπαρξη rootkit.

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
<hr/>						
0x0000000009281da0	soffice.bin	3088	3048	0x69125000	2009-12-11 00:53:53 UTC+0000	
0x0000000009292308	alg.exe	2956	992	0x6811a000	2009-12-11 00:53:52 UTC+0000	
0x00000000092a29e0	soffice.exe	3048	3000	0x68be5000	2009-12-11 00:53:52 UTC+0000	
0x00000000092ccbc0	hkcmd.exe	2684	1348	0x61b98000	2009-12-11 00:53:51 UTC+0000	
0x00000000092d6948	jusched.exe	2804	1348	0x635b8000	2009-12-11 00:53:51 UTC+0000	
0x00000000092e57b0	thunderbird.exe	188	1348	0x523c3000	2009-12-11 16:54:43 UTC+0000	
0x0000000009387978	svchost.exe	1392	992	0x26627000	2009-12-11 00:53:24 UTC+0000	
0x000000000938cb28	mdd_1.3.exe	1768	3296	0x5ba2e000	2009-12-11 16:59:51 UTC+0000	
0x0000000009395800	explorer.exe	1348	1304	0x571a1000	2009-12-11 00:53:46 UTC+0000	
0x0000000009398160	jqs.exe	320	992	0x50005000	2009-12-11 00:53:42 UTC+0000	
0x00000000093a2ca8	spoolsv.exe	1908	992	0x28f02000	2009-12-11 00:53:26 UTC+0000	
0x000000000944d9e0	svchost.exe	1796	992	0x4fa83000	2009-12-11 00:53:40 UTC+0000	
0x0000000009476da0	svchost.exe	1532	992	0x267bf000	2009-12-11 00:53:24 UTC+0000	
0x0000000009482718	avgfw9.exe	3936	992	0x6df09000	2009-12-11 00:54:05 UTC+0000	
0x00000000096e01e0	lsass.exe	1004	948	0x25b1f000	2009-12-11 00:53:23 UTC+0000	

Εικόνα 25 Εύρεση κρυφών διεργασιών.

0x00000000097899e0	avgwdsvc.exe	1728	992	0x4fb28000	2009-12-11 00:53:40 UTC+0000	
0x0000000009887a78	svchost.exe	1268	992	0x264a1000	2009-12-11 00:53:24 UTC+0000	
0x000000000988cc18	svchost.exe	1644	992	0x26956000	2009-12-11 00:53:24 UTC+0000	
0x000000000990ebe0	ctfmon.exe	2832	1348	0x67f68000	2009-12-11 00:53:52 UTC+0000	
0x00000000099a7020	cmd.exe	3296	1348	0x5b16d000	2009-12-11 16:59:32 UTC+0000	
0x00000000099fd970	csrss.exe	924	876	0x2442d000	2009-12-11 00:53:22 UTC+0000	
0x0000000009af0460	smss.exe	876	4	0x235c9000	2009-12-11 00:53:21 UTC+0000	
0x0000000009afa608	svchost.exe	1180	992	0x262a1000	2009-12-11 00:53:23 UTC+0000	
0x0000000009afb5d0	services.exe	992	948	0x25aa8000	2009-12-11 00:53:23 UTC+0000	
0x0000000009b0b818	winlogon.exe	948	876	0x25892000	2009-12-11 00:53:22 UTC+0000	
0x0000000009bfb9c8	System	4	0	0x0a030000		

Εικόνα 26 Εύρεση κρυφών διεργασιών 2.

Συνεπώς γίνεται αντιληπτό πως δεν υπάρχει κάποια κρυφή διεργασία.

Για την εύρεση δικτυακών συνδέσεων χρησιμοποιήθηκε η εντολή > .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 connections μιας και το λειτουργικό σύστημα είναι windows XP

Offset(V)	Local Address	Remote Address	Pid
<hr/>			
0x897e5008	127.0.0.1:1301	127.0.0.1:1302	188
0x898e4788	127.0.0.1:1302	127.0.0.1:1301	188
0x8979b730	192.168.1.104:1310	192.168.1.1:445	4
0x8946bbe8	192.168.1.104:1208	198.189.255.73:80	2804
0x8997f690	127.0.0.1:1300	127.0.0.1:1299	188
0x899b2cb0	127.0.0.1:1299	127.0.0.1:1300	188

Εικόνα 27 Εύρεση δικτυακών συνδέσεων.

Στη συνέχεια εκτελούμε > .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 connscan που μπορεί να εντοπίσει τερματισμένες ή απόκρυφες συνδέσεις που όντως διαπιστώνουμε ότι βρίσκει περισσότερες συνδέσεις. Η εντολή connscan της Volatility 2.4 χρησιμοποιείται για την ανίχνευση ενεργών δικτυακών συνδέσεων σε εικόνες μνήμης των Windows XP SP2 x86. Αυτή η εντολή σαρώνει τη μνήμη για δομές δεδομένων που σχετίζονται με ενεργές συνδέσεις, όπως οι TCP/IP sockets. Είναι ιδιαίτερα χρήσιμη για την ανακάλυψη κρυφών ή κακόβουλων συνδέσεων που δεν εμφανίζονται σε άλλες πηγές, όπως η εντολή connections.

> .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 connscan			
Offset(P)	Local Address	Remote Address	Pid
0x092c3938	192.168.1.104:1311	192.168.1.1:139	4
0x093ea788	192.168.1.104:1303	63.245.209.10:80	188
0x0946bbe8	192.168.1.104:1208	198.189.255.73:80	2804
0x0979b730	192.168.1.104:1310	192.168.1.1:445	4
0x097e5008	127.0.0.1:1301	127.0.0.1:1302	188
0x0988ac88	192.168.1.104:1304	208.97.132.223:995	188
0x098e4788	127.0.0.1:1302	127.0.0.1:1301	188
0x0997a2c0	192.168.1.104:1307	208.97.132.223:995	188
0x0997f690	127.0.0.1:1300	127.0.0.1:1299	188
0x099b2cb0	127.0.0.1:1299	127.0.0.1:1300	188
0x09a9f2c0	192.168.1.104:1305	63.245.221.11:80	188

Εικόνα 28 Ένρεση τερματισμένων η απόκρυφων δικτυακών συνδέσεων

Παρακάτω παρατίθεται σε πίνακα η λίστα των συνδέσεων.

PI D	Διεργασία	Τοπική Διεύθυνση	Απομακρυσμέ νη Διεύθυνση	Port	Πρωτόκο λλο	Σχόλια
4	System	192.168.1.104: 1311	192.168.1.1:13 9	SMB	TCP	Δικτυακή δραστηριότητα με router (NetBIOS)
188	thunderbird. exe	192.168.1.104: 1303	63.245.209.10: 80	HTTP	TCP	Εξωτερική σύνδεση — Mozilla
280 4	jusched.exe (Java)	192.168.1.104: 1208	198.189.255.73 :80	HTTP	TCP	Εξωτερική σύνδεση
4	System	192.168.1.104: 1310	192.168.1.1:44 5	SMB	TCP	Σύνδεση με router
188	thunderbird. exe	127.0.0.1:1301 ⇒ 1302	Τοπική	Loopba ck	—	Εσωτερική επικοινωνία
188	thunderbird. exe	192.168.1.104: 1304	208.97.132.223 :995	POP3S	TCP	Λήψη email μέσω SSL
188	thunderbird. exe	192.168.1.104: 1307	208.97.132.223 :995	POP3S	TCP	Δεύτερη σύνδεση POP3S

188	thunderbird.exe	192.168.1.104: 1305	63.245.221.11: 80	HTTP	TCP	Εξωτερική σύνδεση (Mozilla)
188	thunderbird.exe	127.0.0.1:1300 ≤ 1299	Τοπική	Loopback	—	—

Πίνακας 13 Λίστα των συνδέσεων

Στη συνέχεια εκτελέστηκε .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 pstree για να δούμε την ιεραρχία των διεργασιών του συστήματος. Αυτό μας δείχνει τις διαδικασίες που ήταν ενεργές κατά τη διάρκεια του dump μνήμης, καθώς και τις σχέσεις μεταξύ τους.

Name	Pid	PPid	Thds	Hnds	Time
0x89bfb9c8: System	4	0	64	512	1970-01-01 00:00:00 UTC+0000
. 0x89af0460:smss.exe	876	4	3	19	2009-12-11 00:53:21 UTC+0000
.. 0x899fd970:csrss.exe	924	876	11	417	2009-12-11 00:53:22 UTC+0000
... 0x89b0b818:winlogon.exe	948	876	17	572	2009-12-11 00:53:22 UTC+0000
.... 0x896e01e0:lsass.exe	1004	948	22	354	2009-12-11 00:53:23 UTC+0000
.... 0x89afb5d0:services.exe	992	948	15	265	2009-12-11 00:53:23 UTC+0000
..... 0x89398160:jqs.exe	320	992	5	117	2009-12-11 00:53:42 UTC+0000
..... 0x89292308:alg.exe	2956	992	6	107	2009-12-11 00:53:52 UTC+0000
..... 0x8944d9e0:svchost.exe	1796	992	4	108	2009-12-11 00:53:40 UTC+0000
..... 0x89afa608:svchost.exe	1180	992	17	194	2009-12-11 00:53:23 UTC+0000
.... 0x89887a78:svchost.exe	1268	992	10	272	2009-12-11 00:53:24 UTC+0000
.... 0x897899e0:avgdsvc.exe	1728	992	25	962	2009-12-11 00:53:40 UTC+0000
.... 0x89482718:avgfw9.exe	3936	992	25	762	2009-12-11 00:54:05 UTC+0000
.... 0x893a2ca8:spoolsv.exe	1908	992	10	114	2009-12-11 00:53:26 UTC+0000
.... 0x89476da0:svchost.exe	1532	992	5	81	2009-12-11 00:53:24 UTC+0000
.... 0x8988cc18:svchost.exe	1644	992	11	166	2009-12-11 00:53:24 UTC+0000
.... 0x89387978:svchost.exe	1392	992	74	1523	2009-12-11 00:53:24 UTC+0000
0x892a29e0:soffice.exe	3048	3000	1	20	2009-12-11 00:53:52 UTC+0000
. 0x89281da0:soffice.bin	3088	3048	7	216	2009-12-11 00:53:53 UTC+0000
0x89395800:explorer.exe	1348	1304	13	481	2009-12-11 00:53:46 UTC+0000
. 0x899a7020:cmd.exe	3296	1348	1	33	2009-12-11 16:59:32 UTC+0000
.. 0x8938cb28:mdd_1.3.exe	1768	3296	1	24	2009-12-11 16:59:51 UTC+0000
. 0x892e57b0:thunderbird.exe	188	1348	10	203	2009-12-11 16:54:43 UTC+0000
. 0x8990eb0:ctfmon.exe	2832	1348	1	71	2009-12-11 00:53:52 UTC+0000
. 0x892d6948:jusched.exe	2804	1348	2	152	2009-12-11 00:53:51 UTC+0000
. 0x892ccb0:hkcmd.exe	2684	1348	2	104	2009-12-11 00:53:51 UTC+0000

Εικόνα 29 Συσχέτιση μεταξύ διεργασιών

Η εκτέλεση της εντολής "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 **consoles** μας επιβεβαίωσε ότι η εντολή που εκτελέστηκε εκείνη την ώρα μέσω cmd ήταν η λήψη του αντιγράφου.

```
y-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 consoles
Volatility Foundation Volatility Framework 2.4
*****
ConsoleProcess: csrss.exe Pid: 924
Console: 0x4f27c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: mdd - 70.66% complete
AttachedProcess: mdd_1.3.exe Pid: 1768 Handle: 0x718
AttachedProcess: cmd.exe Pid: 3296 Handle: 0x678
----
CommandHistory: 0x12b33f8 Application: mdd_1.3.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x718
----
CommandHistory: 0x4f5098 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x678
Cmd #0 at 0x12b32d8: z:\mdd_1.3.exe -o z:\charlie-2009-12-11.ram
----
Screen 0x4f2ea0 X:80 Y:300
Dump:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Charlie>z:\mdd_1.3.exe -o z:\charlie-2009-12-11.ram
-> mdd
-> ManTech Physical Memory Dump Utility
    Copyright (C) 2008 ManTech Security & Mission Assurance

-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
    This is free software, and you are welcome to redistribute it
    under certain conditions; use option '-c' for details.

-> Dumping 2045.98 MB of physical memory to file 'z:\charlie-2009-12-11.ram'.
```

Εικόνα 30 Εντολές μέσω cmd

Ακολουθεί η εκτέλεση "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 **shellbags** με την οποία εντοπίζουμε προτιμήσεις και ιστορικό περιήγησης του χρήστη. Από την έξοδο των Shellbags ορισμένα ευρήματα ξεχωρίζουν ως πιθανώς ύποπτα, είτε λόγω του περιεχομένου είτε λόγω του πλαισίου στο οποίο εμφανίζονται.

```
y-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 shellbags
Volatility Foundation Volatility Framework 2.4
Scanning for registries...
Gathering shellbag items and building path tree...
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellBags\1\Desktop
Last updated: 2009-12-11 00:11:17 UTC+0000
Value          File Name      Modified Date        Create Date        Access Date
File Attr      Unicode Name
-----
ItemPos1280x1024(1)  AVG90-1.LNK  2009-11-09 01:45:18 UTC+0000  2009-11-09 01:45:18 UTC+0000  2009-12-09 16:38:50 UTC+0000
ARC           AVG 9.0.lnk
ItemPos1280x1024(1)  FOXITR-1.LNK  2009-11-17 21:50:46 UTC+0000  2009-11-17 21:50:46 UTC+0000  2009-12-04 21:39:06 UTC+0000
ARC           Foxit Reader.lnk
ItemPos1280x1024(1)  MOZILL~1.LNK  2009-11-13 01:48:06 UTC+0000  2009-11-13 01:48:06 UTC+0000  2009-12-09 16:31:42 UTC+0000
ARC           Mozilla Firefox.lnk
ItemPos1280x1024(1)  MOZILL~2.LNK  2009-11-13 01:52:44 UTC+0000  2009-11-13 01:52:44 UTC+0000  2009-12-09 16:31:42 UTC+0000
ARC           Mozilla Thunderbird.lnk
ItemPos1280x1024(1)  OPENOF~1.LNK  2009-11-10 01:04:22 UTC+0000  2009-11-10 01:04:22 UTC+0000  2009-12-04 21:39:06 UTC+0000
ARC           OpenOffice.org 3.1.lnk
ItemPos1280x1024(1)  web            2009-12-10 00:29:34 UTC+0000  2009-11-17 22:01:28 UTC+0000  2009-12-10 00:29:34 UTC+0000
DIR           web
*****
```

Εικόνα 31 Ιστορικό περιήγησης του χρήστη 1

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU
Last updated: 2009-12-11 16:59:16 UTC+0000
Value   Mru   Entry Type   GUID           GUID Description   Folder IDs
----- -----
1       1     Folder Entry  450d8fba-ad25-11d0-98a8-0800361b1103  My Documents      EXPLORER, MY_DOCUMENTS
0       0     Folder Entry  20d04fe0-3aea-1069-a2d8-08002b30309d  My Computer       EXPLORER, MY_COMPUTER
3       3     Folder Entry  645ff040-5081-101b-9f08-00aa002f954e  Recycle Bin       EXPLORER, RECYCLE_BIN

Value   Mru   File Name   Modified Date   Create Date   Access Date   File Attr
----- -----
2       2     web          2009-11-17 22:01:28 UTC+0000  2009-11-17 22:01:28 UTC+0000  2009-11-17 22:01:28 UTC+0000  DIR
web
*****
```

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0
Last updated: 2009-12-11 16:59:53 UTC+0000
Value   Mru   Entry Type   Path
----- -----
0       1     Volume Name  C:\
3       0     Volume Name  Z:\
*****
```

Εικόνα 32 Ιστορικό περιήγησης του χρήστη 2

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\1
Last updated: 2009-12-10 22:19:47 UTC+0000
Value   Mru   File Name   Modified Date   Create Date   Access Date   File Attr
----- -----
1       3     Patents      2009-11-19 16:49:10 UTC+0000  2009-11-19 16:49:10 UTC+0000  2009-11-19 16:49:10 UTC+0000  DIR
0       1     Patents      2009-11-17 21:50:04 UTC+0000  2009-11-13 01:51:56 UTC+0000  2009-11-17 21:50:04 UTC+0000  DIR
1       0     DOWNLOAD-1    2009-11-17 21:50:04 UTC+0000  2009-11-13 01:51:56 UTC+0000  2009-11-17 21:50:04 UTC+0000  DIR
3       8     MYPICT-1     2009-11-11 01:58:42 UTC+0000  2009-11-11 01:58:22 UTC+0000  2009-11-24 00:51:42 UTC+0000  RO, DIR
2       2     Nitroba       2009-11-19 21:27:46 UTC+0000  2009-11-19 21:27:34 UTC+0000  2009-11-19 21:27:46 UTC+0000  DIR
5       7     NEWCOM-1.ZIP  2009-11-24 21:13:44 UTC+0000  2009-11-24 21:13:44 UTC+0000  2009-11-24 21:13:44 UTC+0000  ARC
4       4     IMMORT-1     2009-11-24 21:13:50 UTC+0000  2009-11-24 21:13:50 UTC+0000  2009-11-24 21:13:50 UTC+0000  DIR
7       6     01             2009-11-24 21:22:20 UTC+0000  2009-11-24 21:22:20 UTC+0000  2009-11-24 21:22:20 UTC+0000  DIR
6       5     01.zip         2009-11-24 21:21:18 UTC+0000  2009-11-24 21:13:44 UTC+0000  2009-11-24 21:21:18 UTC+0000  ARC
8       0     QUANTU-1     2009-12-04 21:53:36 UTC+0000  2009-12-04 21:53:28 UTC+0000  2009-12-04 21:53:36 UTC+0000  DIR
*****
```

Εικόνα 33 Ιστορικό περιήγησης του χρήστη 3

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0
Last updated: 2009-12-08 00:14:59 UTC+0000
Value   Mru   File Name   Modified Date   Create Date   Access Date   File Attr
----- -----
1       2     RECYCLER     2009-11-20 17:23:02 UTC+0000  2009-11-20 17:23:02 UTC+0000  2009-11-20 17:23:02 UTC+0000  HID, SYS, D
IR
0       0     DOCUMENT-1   2009-11-11 01:57:48 UTC+0000  2009-11-08 17:05:48 UTC+0000  2009-11-11 20:02:02 UTC+0000  DIR
C:\Documents and Settings
3       1     PROGRAM-1    2009-11-24 21:19:52 UTC+0000  2009-11-08 17:07:32 UTC+0000  2009-11-24 21:19:54 UTC+0000  RO, DIR
C:\Program Files
2       3     $AVG          2009-11-09 01:45:28 UTC+0000  2009-11-09 01:45:28 UTC+0000  2009-11-20 16:59:16 UTC+0000  HID, DIR
C:$AVG
*****
```

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\4
Last updated: 2009-11-24 20:54:35 UTC+0000
Value   Mru   File Name   Modified Date   Create Date   Access Date   File Attr
----- -----
0       0     MYPICT-1     2009-11-09 01:20:38 UTC+0000  2009-11-09 01:19:38 UTC+0000  2009-11-20 17:42:18 UTC+0000  RO, DIR
My Pictures
*****
```

Εικόνα 34 Ιστορικό περιήγησης του χρήστη 4

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\0
Last updated: 2009-11-24 22:01:13 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
0     0    cygnusfe.zip  2009-11-24 21:58:40 UTC+0000  2009-11-24 21:58:40 UTC+0000  2009-11-24 21:58:40 UTC+0000  ARC
Downloads\cygnusfe.zip
*****
```

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\7
Last updated: 2009-11-24 21:22:30 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
0     0    IMMORT~1    2009-11-24 21:22:20 UTC+0000  2009-11-24 21:22:20 UTC+0000  2009-11-24 21:22:20 UTC+0000  DIR
01\Immortality
*****
```

Εικόνα 35 Ιστορικό περιήγησης του χρήστη 5

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\8
Last updated: 2009-12-10 22:22:16 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
0     0    09145392.zip  2009-12-10 22:20:40 UTC+0000  2009-12-10 22:20:36 UTC+0000  2009-12-10 22:20:40 UTC+0000  ARC
Quantum Cryptography\09145392.zip
*****
```

```
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\Bags\8\Shell
Last updated: 2009-12-10 22:24:02 UTC+0000
Value   File Attr   File Name      Modified Date          Create Date        Access Date
Unicode Name

-----
ItemPos1280x1024(1)  DIR           DOWNLOAD-1    2009-11-24 21:58:40 UTC+0000  2009-11-13 01:51:56 UTC+0000  2009-12-10 22:19:44 UTC+0000
DIR                 Downloads
ItemPos1280x1024(1)  RO, DIR       MYMUSI-1     2009-11-11 01:58:42 UTC+0000  2009-11-11 01:58:22 UTC+0000  2009-12-10 01:55:14 UTC+0000
RO, DIR             My Music
ItemPos1280x1024(1)  RO, DIR       MYPICIT-1   2009-11-11 01:58:42 UTC+0000  2009-11-11 01:58:22 UTC+0000  2009-12-10 22:23:52 UTC+0000
RO, DIR             My Pictures
ItemPos1280x1024(1)  DIR           Nitroba      2009-11-30 16:48:16 UTC+0000  2009-11-19 21:27:34 UTC+0000  2009-12-07 19:52:22 UTC+0000
DIR                 Nitroba
ItemPos1280x1024(1)  DIR           Patents     2009-11-19 16:50:48 UTC+0000  2009-11-19 16:49:10 UTC+0000  2009-12-07 19:52:08 UTC+0000
DIR                 Patents
ItemPos1280x1024(1)  DIR           QUANTU-1     2009-12-10 22:23:40 UTC+0000  2009-12-04 21:53:28 UTC+0000  2009-12-10 22:23:40 UTC+0000
DIR                 Quantum Cryptography
ItemPos1280x1024(1)  ARC           01.zip       2009-11-24 21:21:18 UTC+0000  2009-11-24 21:13:44 UTC+0000  2009-12-04 17:41:48 UTC+0000
ARC                 01.zip
ItemPos1280x1024(1)  PDF           22EE12-1.PDF 2009-11-17 21:54:04 UTC+0000  2009-11-17 21:54:16 UTC+0000  2009-12-09 16:39:32 UTC+0000
*****
```

Εικόνα 36 Ιστορικό περιήγησης του χρήστη 6

```

ItemPos1280x1024(1) 95253S~1.PDF 2009-11-20 21:06:50 UTC+0000 2009-11-20 21:06:50 UTC+0000 2009-12-10 22:21:00 UTC+0000
ARC 95253 SCSI.Mathew+Malizia.pdf
ItemPos1280x1024(1) 97315S~1.PDF 2009-11-20 21:06:50 UTC+0000 2009-11-20 21:06:50 UTC+0000 2009-11-30 16:46:46 UTC+0000
ARC 97315.ScatterGatherIO.Julio+Molock.pdf
ItemPos1280x1024(1) 98521W~1.PDF 2009-11-20 21:06:48 UTC+0000 2009-11-20 21:06:48 UTC+0000 2009-12-09 16:39:04 UTC+0000
ARC 98521.WANS.Greg+Hillier.pdf
ItemPos1280x1024(1) 99262C~1.PDF 2009-11-20 21:06:50 UTC+0000 2009-11-20 21:06:50 UTC+0000 2009-12-09 16:39:32 UTC+0000
ARC 99202.ComplexityTheory.Louisa+Fleet.pdf
ItemPos1280x1024(1) AC7640A9d01.pdf
ItemPos1280x1024(1) ASTRON-2.JPG 2009-11-24 21:43:44 UTC+0000 2009-11-24 21:43:44 UTC+0000 2009-12-10 22:18:38 UTC+0000
ARC astronaut1.jpg
ItemPos1280x1024(1) ASTRON-1.JPG 2009-11-24 21:33:34 UTC+0000 2009-11-24 21:40:30 UTC+0000 2009-12-10 22:18:38 UTC+0000
ARC astronaut.jpg
ItemPos1280x1024(1) desktop.ini 2009-11-11 01:58:42 UTC+0000 2009-11-11 01:58:22 UTC+0000 2009-12-10 22:18:36 UTC+0000
ARC, HID, SYS desktop.ini
ItemPos1280x1024(1) MICRO$-1.JPG 2009-11-24 22:19:22 UTC+0000 2009-11-24 21:40:32 UTC+0000 2009-12-10 22:18:38 UTC+0000
ARC microscopel.jpg
ItemPos1280x1024(1) MICRO$-2.JPG 2009-11-24 21:27:52 UTC+0000 2009-11-24 21:40:32 UTC+0000 2009-12-10 22:18:36 UTC+0000
ARC microscope.jpg
*****
***** Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\0
Last updated: 2009-11-16 21:48:27 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
0     0     Charlie      2009-11-11 01:58:22 UTC+0000  2009-11-11 01:57:48 UTC+0000  2009-11-11 20:02:04 UTC+0000  DIR
C:\Documents and Settings\Charlie
*****
*****
```

Εικόνα 37 Ιστορικό περιήγησης του χρήστη 7

```

***** Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\1
Last updated: 2009-11-20 17:23:13 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
0     0     S-1-5-~1      2009-11-20 17:23:02 UTC+0000  2009-11-20 17:23:02 UTC+0000  2009-11-20 17:23:02 UTC+0000  HID, SYS, D
IR  C:\RECYCLER\S-1-5-21-68200330-329068152-1644491937-1003
*****
***** Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\3
Last updated: 2009-12-07 19:44:09 UTC+0000
Value   Mru   File Name      Modified Date          Create Date        Access Date       File Attr
Path

-----
1     2     CYGNUS~1      2009-11-24 22:01:10 UTC+0000  2009-11-24 22:01:10 UTC+0000  2009-11-24 22:01:12 UTC+0000  DIR
C:\Program Files\Cygnus FREE EDITION
0     1     INVISI~1.1    2009-11-19 18:43:32 UTC+0000  2009-11-19 18:43:32 UTC+0000  2009-11-24 21:19:56 UTC+0000  DIR
C:\Program Files\Invisible Secrets 2.1
2     0     MOZILL~2      2009-12-07 16:43:30 UTC+0000  2009-11-13 01:52:40 UTC+0000  2009-12-07 19:44:10 UTC+0000  DIR
C:\Program Files\Mozilla Thunderbird
*****
```

Εικόνα 38 Ιστορικό περιήγησης του χρήστη 8

*****						File Attr
Registry:	\\Device\\HarddiskVolume1\\Documents and Settings\\Charlie\\NTUSER.DAT			Access Date		File Attr
Key:	Software\\Microsoft\\Windows\\ShellNoRoam\\BagMRU\\0\\0\\4\\0			Create Date		
Last updated:	2009-11-24 20:54:35 UTC+0000	Value	Mru	File Name	Modified Date	
Path						
0	0	SAMPLE~1	2009-11-09 01:21:16 UTC+0000	2009-11-09 01:20:38 UTC+0000	2009-11-10 00:48:34 UTC+0000	RO, DIR
		My Pictures\\Sample Pictures				

Registry:	\\Device\\HarddiskVolume1\\Documents and Settings\\Charlie\\NTUSER.DAT			Access Date		File Attr
Key:	Software\\Microsoft\\Windows\\ShellNoRoam\\BagMRU\\0\\0\\0\\0			Create Date		
Last updated:	2009-12-10 23:56:23 UTC+0000	Value	Mru	File Name	Modified Date	
Path						
1	2	LOCALS~1	2009-11-08 17:07:00 UTC+0000	2009-11-11 01:57:48 UTC+0000	2009-12-10 22:19:44 UTC+0000	HID, DIR
		C:\\Documents and Settings\\Charlie\\Local Settings				
0	0	STARTM~1	2009-11-08 17:07:00 UTC+0000	2009-11-11 01:57:48 UTC+0000	2009-11-11 20:02:04 UTC+0000	RO, DIR
2	1	Recent	2009-12-10 22:29:38 UTC+0000	2009-11-11 01:57:48 UTC+0000	2009-12-10 22:30:12 UTC+0000	RO, HID, DI
R		C:\\Documents and Settings\\Charlie\\Recent				

Εικόνα 39 Ιστορικό περιήγησης του χρήστη 9

*****						File Attr
Registry:	\\Device\\HarddiskVolume1\\Documents and Settings\\Charlie\\NTUSER.DAT			Access Date		File Attr
Key:	Software\\Microsoft\\Windows\\ShellNoRoam\\BagMRU\\0\\0\\3\\0			Create Date		
Last updated:	2009-11-30 16:48:37 UTC+0000	Value	Mru	File Name	Modified Date	
Path						
0	0	decrypt	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR
		C:\\Program Files\\Invisible Secrets 2.1\\decrypt				

Εικόνα 40 Ιστορικό περιήγησης του χρήστη 10

Στα σημαντικότερα ευρήματα συγκαταλέγεται το timestamp 1970-01-01 για το C:\\Program Files\\Invisible Secrets 2.1\\decrypt όπου υποπτεύομαστε timestamp manipulation ενώ παράλληλα το invisible secrets είναι ένα πρόγραμμα στεγανογραφίας/κρυπτογράφησης που υποδηλώνει ότι ο χρήστης πιθανά ήθελε να κρύψει δεδομένα.

Παρατηρούμε πολλά ύποπτα ονόματα αρχείων και εγγράφων όπως Immortality, Nitroba, Quantum Cryptography, Patents, (09145392.zip, 01.zip, cygnusfe.zip in Downloads and Quantum Cryptography που υποδηλώνουν εναίσθητα δεδομένα. Τα αρχεία μπορεί να είναι 95253.SCSI.Mathew+Malizia.pdf, 98521.WANs.Greg+Hillier.pdf μετονομασία κάποιων άλλων δεδομένων σε προσπάθεια απόκρυψης τους.

Ακόμη το Cygnus FREE EDITION που βρέθηκε είναι HEX editor.

Ο φάκελος RECYCLER χρησιμοποιείται για διαγραμμένα αρχεία, και ορισμένοι malware κρύβονται εκεί.

Το \$AVG πιθανώς να σχετίζεται με το antivirus.

Ο δίσκος Z:\\ συνήθως αντιστοιχεί σε εξωτερική μονάδα USB ή χαρτογραφημένο δικτυακό φάκελο. Ο χρήστης μπορεί να αντέγραψε αρχεία ή να μετέφερε εναίσθητα δεδομένα.

Με την εκέλεση της εντολής .\\volatility-2.4.standalone.exe -f "C:\\memdump\\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 verinfo > verinfo_output.txt εξάχθηκαν πληροφορίες έκδοσης από εκτελέσιμα αρχεία (PE files) που βρίσκονται στη μνήμη. Αυτές οι πληροφορίες περιλαμβάνουν όνομα αρχείου, εκδόσεις λογισμικού, κατασκευαστή, ημερομηνίες δημιουργίας, και άλλα metadata. Τα αποτελέσματα αποθηκεύτηκαν σε ένα txt file.

Με την εκέλεση της εντολής "C:\\memdump\\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 sockets παίρνουμε τις συνδέσεις που έχει ξεκινήσει η κάθε διεργασία.

y-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 sockets							
Volatility Foundation Volatility Framework 2.4	Offset(V)	PID	Port	Proto	Protocol	Address	Create Time
0x89301958	2804	1208	6	TCP		0.0.0.0	2009-12-11 11:42:16 UTC+0000
0x895744f8	4	138	17	UDP		192.168.1.104	2009-12-11 00:53:26 UTC+0000
0x898b6a58	4	0	47	GRE		0.0.0.0	2009-12-11 00:58:52 UTC+0000
0x89a2bbb8	188	1299	6	TCP		127.0.0.1	2009-12-11 16:54:45 UTC+0000
0x899692a0	1004	500	17	UDP		0.0.0.0	2009-12-11 00:53:43 UTC+0000
0x89427260	1392	123	17	UDP		192.168.1.104	2009-12-11 00:53:46 UTC+0000
0x89926a00	4	445	6	TCP		0.0.0.0	2009-12-11 00:53:06 UTC+0000
0x897c2e98	1268	135	6	TCP		0.0.0.0	2009-12-11 00:53:24 UTC+0000
0x89868e98	188	1302	6	TCP		0.0.0.0	2009-12-11 16:54:51 UTC+0000
0x89878208	4	1310	6	TCP		0.0.0.0	2009-12-11 16:59:28 UTC+0000
0x89395cb8	1392	123	17	UDP		127.0.0.1	2009-12-11 00:53:46 UTC+0000
0x897c1af0	1004	0	255	Reserved		0.0.0.0	2009-12-11 00:53:43 UTC+0000
0x892d1ad8	1644	1900	17	UDP		192.168.1.104	2009-12-11 00:53:52 UTC+0000
0x8955c7e0	4	139	6	TCP		192.168.1.104	2009-12-11 00:53:26 UTC+0000
0x897ffe98	188	1301	6	TCP		127.0.0.1	2009-12-11 16:54:51 UTC+0000
0x89909ae8	2956	1034	6	TCP		127.0.0.1	2009-12-11 00:53:54 UTC+0000
0x8991be98	188	1300	6	TCP		0.0.0.0	2009-12-11 16:54:45 UTC+0000
0x89691468	4	137	17	UDP		192.168.1.104	2009-12-11 00:53:26 UTC+0000
0x892a8938	1644	1900	17	UDP		127.0.0.1	2009-12-11 00:53:52 UTC+0000
0x89a82a20	1004	4500	17	UDP		0.0.0.0	2009-12-11 00:53:43 UTC+0000
0x893a0cc0	320	5152	6	TCP		127.0.0.1	2009-12-11 00:53:43 UTC+0000
0x8997da68	4	445	17	UDP		0.0.0.0	2009-12-11 00:53:06 UTC+0000
0x89884248	4	1045	6	TCP		0.0.0.0	2009-12-11 00:58:52 UTC+0000

Εικόνα 41 Συνδέσεις που έχει ζεκτινήσει η κάθε διεργασία

Η εντολή volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 **svcscan** χρησιμοποιεί το plugin svcscan του Volatility Framework για να σαρώσει τη μνήμη και να εντοπίσει υπηρεσίες Windows (*services*) ακόμα κι αν αυτές έχουν σταματήσει ή αποκρύπτονται από το Service Control Manager (SCM). Τα αποτελέσματα αποθηκεύτηκαν σε txt file.

Η εντολή .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 **hivelist** τυπώνει όλα τα active και loaded hives όπως NTUSER.DAT (per-user settings and activity), SOFTWARE, SYSTEM, SAM, SECURITY (global Windows config and security) και UsrClass.dat.

y-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 hivelist						
Virtual	Physical	Name				
0xe2e13b60	0x64473b60	\Device\HarddiskVolume1\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat				
0xe1b44b60	0x2616bb60	\Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT				
0xe1ba0008	0x2690d008	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat				
0xe1ba1598	0x268ee598	\Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT				
0xe1b6fb60	0x2642cb60	\Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat				
0xe1b74758	0x2640b758	\Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT				
0xe14ee4c0	0x235c74c0	\Device\HarddiskVolume1\WINDOWS\system32\config\software				
0xe14e56b8	0x235e36b8	\Device\HarddiskVolume1\WINDOWS\system32\config\default				
0xe14feb60	0x2360cb60	\Device\HarddiskVolume1\WINDOWS\system32\config\SAM				
0xe14eb5b0	0x235e3b60	\Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY				
0xe1390b60	0x0a3f7b60	[no name]				
0xe1037008	0x0a08c008	\Device\HarddiskVolume1\WINDOWS\system32\config\system				
0xe102f008	0x0a095008	[no name]				

Εικόνα 42 Active and loaded hives

Με τη γνώση της τοποθεσίας κάθε registry hive μπορέσαμε να καταφέραμε να τυπώσουμε τη λίστα με τα urls που επισκέφτηκε και τη λίστα των αρχείων που είχε ανοίξει πρόσφατα. Η εντολή **hashdump** έκανε dump τα passwords των χρηστών.

```
y-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 hashdump
Volatility Foundation Volatility Framework 2.4
Administrator: 500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest: 501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant: 1000:c84fa92b5e90e68cdf2b9bc99a6ddf59:fc20a40d2ee88511f2093e88e4e90d03:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:a92937cd0574859facc0017cd2e8bdb:::
Charlie: 1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PS C:\Users\katep\Downloads\Msc\2o εξάμηνο\Ψηφιακα Πειστηρια\volatility_2.4.win.standalone> |
```

Eikόνα 43 Dump of user passwords

Τα παρακάτω hashes του χρήστη Charlie αντιστοιχούν σε λογαριασμό χρήστη που δεν έχει θέσει κωδικό καθώς τα hashes είναι default.

- LM Hash: aad3b435b51404eeaad3b435b51404ee
- NTLM Hash: 31d6cfe0d16ae931b73c59d7e0c089c0

Από την εντολή sessions βλέπουμε ότι πριν την λήψη του αντιγράφου μνήμης έχουμε αλληλεπίδραση με το thunderbird.

```
Process: 188 thunderbird.exe 2009-12-11 16:54:43 UTC+0000
Process: 3296 cmd.exe 2009-12-11 16:59:32 UTC+0000
Process: 1768 mdd_1.3.exe 2009-12-11 16:59:51 UTC+0000
```

Eikόνα 44 Sessions

Με την εντολή .\volatility-2.4.standalone.exe -f "C:\memdump\charlie-2009-12-11.mddramimage" --profile=WinXPSP2x86 printkey -o 0xe14ee4c0 -K "Microsoft\Windows NT\CurrentVersion" εντοπίζουμε το product id του μηχανήματος

Values:
REG_SZ SubVersionNumber : (S)
REG_SZ CurrentBuild : (S) 1.511.1 () (Obsolete data - do not use)
REG_DWORD InstallDate : (S) 1257729947
REG_SZ ProductName : (S) Microsoft Windows XP
REG_SZ RegDone : (S)
REG_SZ RegisteredOrganization : (S) M57.biz
REG_SZ RegisteredOwner : (S) Charlie
REG_SZ SoftwareType : (S) SYSTEM
REG_SZ CurrentVersion : (S) 5.1
REG_SZ CurrentBuildNumber : (S) 2600
REG_SZ BuildLab : (S) 2600.xpsp_sp3_gdr.090804-1435
REG_SZ CurrentType : (S) Multiprocessor Free
REG_SZ CSDVersion : (S) Service Pack 3
REG_SZ SystemRoot : (S) C:\WINDOWS
REG_SZ SourcePath : (S) D:\I386
REG_SZ PathName : (S) C:\WINDOWS
REG_SZ ProductId : (S) 76487-027-5250835-22765
REG_BINARY DigitalProductId : (S)

Eikόνα 45 Product Id μηχανήματος

Παράρτημα Δ – Ανάλυση Δίσκου Πειστηρίου Laptop [0005] & USB [0004]

1) Ποιες είναι οι τιμές κατακερματισμού (MD5 & SHA-1) όλων των εικόνων;

Ταιριάζει η τιμή κατακερματισμού απόκτησης και επαλήθευσης;

Απάντηση	Class	Hash Algo.	Hash value
Δίσκος [0005]	MD5	0377b3d41bbbc295a1c9f00aa07ee174	
	SHA-1	ee1d5febb63def90c2900b6984d21a6a137f00ce	
USB [0004]	MD5	9c0de6c8532d7a66ddcf01861dfb6535	
	SHA-1	e49bf6048856570cc3d49b1485d6d87aab6ab0a	
Παρατηρήσεις	Οι τιμές κατακερματισμού και των δύο εικόνων ταιριάζουν με τους κατακερματισμούς απόκτησης, επιβεβαιώνοντας την ακεραιότητα και τη γνησιότητα των αποδεικτικών στοιχείων.		

2) Προσδιορίστε τις πληροφορίες κατάτμησης της εικόνας [0005] του Laptop

Απάντηση	No.	Bootable	File system	Start Sector	Total Sectors	Size
	1	No	-	0	63	0,003 MB
	2	Yes	NTFS / exFAT (0x07)	63	19968732	9.52 GB
	3	No	-	19968795	30933	15.15 MB
Παρατηρήσεις	N/A					

3) Εξηγήστε λεπτομερώς τις πληροφορίες για το εγκατεστημένο λειτουργικό σύστημα

Απάντηση	OS Name	Microsoft Windows XP
	Version	5.1
	Build Number	2600
	Registered Owner	Charlie
	System Root	C:\Windows
	Install Date	2009-11-08 05:25:47 PM (PST)
Παρατηρήσεις	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	

4) Ποία είναι η ρύθμιση της ζώνης ώρας;

Απάντηση	Timezone	Pacific Standard Time (UTC-8)
	Daylight Time Bias	-60 minutes (for daylight saving time)
Παρατηρήσεις	HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation	

5) Ποιό είναι το όνομα του υπολογιστή;

Απάντηση	M57-CHARLIE
Παρατηρήσεις	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ComputerName (value: ComputerName) HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters (value: Hostname)

6) Καταγράψτε όλους τους λογαριασμούς στο λειτουργικό σύστημα εκτός από τους λογαριασμούς συστήματος: Administrator, Guest, systemprofile, LocalService, NetworkService, (Account name, login count, last logon date...)

Απάντηση (Εφαρμόζεται η ζώνη ώρας)	Account	SID	NT Hash	Status	Login Count	Account Created Time	Last Login Time	Login Failure Time
	HelpAssistant	1000	(a)	N/A	N/A	N/A	N/A	N/A
	Charlie	1003	(b)	Enabled	528	N/A	2009-11-08 17:25:47 (PST)	N/A

	SUPPORT_38 8945a0	1002	(c)	Enabled	Not Tracked	N/A	N/A	N/A
Παρατηρήσεις	<ul style="list-style-type: none"> - HKLM\SAM\~ - SYSTEM hive is required for calculating hash values of passwords. - NT Hashes <ul style="list-style-type: none"> (a) 828BA628782E9D13A1F40462E8030000 (b) 828BA628782E9D13A1F40462EB030000 (c) 06139998CE87AB50F7E32B2BCBBB0582 							

7) Ποιός ήταν ο τελευταίος χρήστης που συνδέθηκε στο Laptop [0001]?

Απάντηση	Charlie
Παρατηρήσεις	HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon (Value: DefaultUserName)

8) Πότε ήταν η τελευταία καταγεγραμμένη ημερομηνία/ώρα διακοπής λειτουργίας;

Απάντηση	Friday, December 11, 2009, 9:09:57.515 AM PST
Παρατηρήσεις	HKLM\SYSTEM\ControlSet001\Control\Windows (value: ShutdownTime)

9) Εξηγήστε τις πληροφορίες για τη διασύνδεση/διασυνδέσεις δικτύου με διεύθυνση IP που έχει εκχωρηθεί από το DHCP.

Απάντηση	Device Name	Intel(R) PRO/1000 MT Network Connection
	IP Address	192.168.1.104
	Subnet Mask	255.255.255.0
	Name Server	192.168.1.1
	Domain	m57.biz
	Default Gateway	192.168.1.1
	DHCP Usage	Yes
	DHCP Server	192.168.1.1
Παρατηρήσεις	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{B15FB27D-C44F-4540-AB9C-7C789450051B}	HKAM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\0008 {value: DriverDesc}
	Επιπλέον, εντοπίστηκαν δύο ακόμη διεπαφές δικτύου. Και οι δύο είχαν διευθύνσεις IP ορισμένες στο 0.0.0.0, με απενεργοποιημένο το DHCP και χωρίς διαμορφωμένη προεπιλεγμένη πύλη ή DNS. {0739C3D2-07C9-427E-9D5A-E41CEBFD1029} και {E23C0DB8-617C-46F7-80E7-3BE2280460FC}.	

10) Ποίες εφαρμογές εγκαταστάθηκαν από τον ύποπτο μετά την εγκατάσταση του λειτουργικού συστήματος;

Απάντηση	Installation Time	Name	Version	Manufacturer	Installation Path
(Εφαρμόζεται η ζώνη ώρας)	2009-11-24 13:19:52	7-Zip	4.65	N/A	C:\Program Files\7-Zip
	2009-11-18 13:04:30	Adobe Flash Player Plugin	10.0.32.18	Adobe Systems Inc.	C:\WINDOWS\System32\Macromed\Flash\
(Δεν περιλαμβάνονται Windows Security Patches & Updates)	2009-11-09 17:44:32	Avg90Full	9.0	AVG Technologies	C:\Program Files\AVG\AVG9\
	2009-11-24 14:01:10	Cygnus Hex Editor Free Edition 1.00	1.00	SoftCircuits	C:\Program Files\Cygnus FREE EDITION\
	2009-11-17 13:50:44	Foxit Reader	3.1.3.1030	Foxit Software Company	C:\Program Files\Foxit Software\Foxit Reader\
	2009-11-10 16:40:00	Windows Internet Explorer 8	20090308.140743	Microsoft Corporation	C:\WINDOWS\Internet Explorer\
	2009-11-19 10:43:32	Invisible Secrets 2.1	2.0.19	Neobyte Solutions	C:\Program Files\Invisible Secrets 2.1\

	2009-11-13 17:48:03	Mozilla Firefox	3.5.5 (en-US)	Mozilla	C:\Program Files\Mozilla Firefox\
	2009-11-13 17:52:43	Mozilla Thunderbird	2.0.023 (en-US)	Mozilla	C:\Program Files\Mozilla Thunderbird\
	2009-11-19 13:11:26	QuickTime	7.65.17.80	Apple Inc.	C:\Program Files\QuickTime\
	2009-11-10 17:27:39	Java™ 6 Update 17	6.0.170	Sun Microsystems, Inc.	C:\Program Files\Java\jre6\
	2009-11-11 17:58:41	WebFldrs XP	9.50.7523	Microsoft Corporation	C:\WINDOWS\System32\
	2009-11-19 13:10:36	Apple Application Support	1.1.0	Apple Inc.	-
	2009-11-19 13:10:16	Apple Software Update	2.1.1.116	Apple Inc.	C:\Program Files\Apple Software Update\
	2009-11-09 17:44:29	Microsoft Visual C++ 2005 Redistributable	8.0.5913	Microsoft Corporation	-
	2009-11-30 09:11:15	Brother HL-2170W	1.00	Brother	C:\Program Files\Brother\BRHL2170\
	2009-11-10 17:04:29	OpenOffice.org 3.1	3.1.9420	OpenOffice.org	C:\Program Files\
	2009-11-13 17:57:04	Python 2.6.4	2.6.4150	Python Software Foundation	C:\Python26\
Παρατηρήσεις	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~				

11) Ποια προγράμματα περιήγησης ιστού χρησιμοποιήθηκαν;

Απάντηση	- Microsoft Internet Explorer v.8.0.6001.18702 - Mozilla Firefox v.1.9.1.5 (updated to 3.5.5 en-US)
Παρατηρήσεις	HKLM\SOFTWARE\Microsoft\Internet Explorer (value: svcVersion) HKLM\SOFTWARE\Mozilla\Mozilla Firefox

12) Προσδιορίστε τις διαδρομές καταλόγων/αρχείων που σχετίζονται με το ιστορικό του προγράμματος περιήγησης ιστού.

Απάντηση	MS IE	<ul style="list-style-type: none"> • C:\Documents and Settings\Administrator\Application Data\Cookies\index.dat • C:\Documents and Settings\Charlie\Application Data\Microsoft\Internet Explorer\UserData\index.dat • C:\Documents and Settings\Charlie\Local Settings\History\History.IE5\~ • C:\Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\~ • C:\ Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Internet Explorer\~ • C:\Documents and Settings\Charlie\IETidCache\index.dat • C:\Documents and Settings\LocalService\IETidCache\index.dat
	Mozilla Firefox	<ul style="list-style-type: none"> • C:\Documents and Settings\Charlie\Application Data\Microsoft\Mozilla\Firefox\Profiles\2usvf7i1.default\places.sqlite • C:\ Documents and Settings\Charlie\Application Data\Microsoft\Mozilla\Firefox\Profiles\2usvf7i1.default\cookies.sqlite • C:\Documents and Settings\Charlie\Local Settings\Application Data\Microsoft\Mozilla\Firefox\Profiles\2usvf7i1.default\~ • C:\ Documents and Settings\Charlie\Application Data\Cookies\index.dat
Παρατηρήσεις		

Charlie-DFIR - Autopsy 4.22.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources

- charlie-2009-12-11.E01_1 Host
 - vol1 (Unallocated: 0-62)
 - vol2 (NTFS / exFAT (0x07): 63-19968794)
 - OrphanFiles (0)
 - SAVG (4)
 - ScarvedFiles (2)
 - \$Extend (7)
 - \$Unalloc (2)
 - 32bits_386 (10)
 - dell (3)
 - Documents and Settings (8)
 - Administrator (20)
 - All Users (9)
 - Charlie (20)
 - idler (4)
 - Application Data (12)
 - Adobe (3)
 - Foxit (3)
 - Identities (3)
 - Macromedia (3)
 - Microsoft (11)
 - Mozilla (5)
 - Extensions (3)
 - Firefox (5)
 - Crash Reports (3)
 - Profiles (3)
 - 2usvf71.default (40)
 - OpenOffice.org (3)
 - Sun (3)
 - Thunderbird (5)
 - Cookies (22)
 - Desktop (3)
 - Favorites (5)
 - IETldCache (3)
 - Local Settings (7)
 - My Documents (22)

Listing /img Charlie-2009-12-11.E01_1/vol_vol2/Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf71.default 40 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
extensions.cache				2009-11-12 17:50:53 GMT-08:00	2009-11-12 17:50:53 GMT-08:00	2009-12-10 08:31:24 GMT-08:00	2009-11-12 17:50:48 GMT-08:00	275
extensions.ini				2009-11-12 17:50:53 GMT-08:00	2009-11-12 17:50:53 GMT-08:00	2009-12-10 08:31:24 GMT-08:00	2009-11-12 17:50:48 GMT-08:00	322
extensions.rdf				2009-11-12 17:50:53 GMT-08:00	2009-11-12 17:50:54 GMT-08:00	2009-12-10 08:31:24 GMT-08:00	2009-11-12 17:50:47 GMT-08:00	3155
formhistory.sqlite				2009-12-10 14:19:18 GMT-08:00	2009-12-10 14:19:18 GMT-08:00	2009-12-10 14:19:18 GMT-08:00	2009-11-12 17:49:40 GMT-08:00	6144
key3.db				2009-12-10 16:11:11 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	2009-11-12 17:49:41 GMT-08:00	16384
localStorage.rdf				2009-12-10 16:11:11 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	6785
mimetypes.rdf				2009-12-10 14:19:43 GMT-08:00	2009-12-10 14:19:43 GMT-08:00	2009-12-10 14:19:43 GMT-08:00	2009-12-10 14:19:43 GMT-08:00	4726
mozrepl.tmpjs				2009-12-10 13:06:16 GMT-08:00	2009-12-10 13:06:16 GMT-08:00	2009-12-10 13:06:16 GMT-08:00	2009-11-17 14:04:23 GMT-08:00	32
permissions.sqlite				2009-11-12 17:50:52 GMT-08:00	2009-11-12 17:50:52 GMT-08:00	2009-12-10 16:11:11 GMT-08:00	2009-11-12 17:49:37 GMT-08:00	2048
places.sqlite				2009-12-10 16:11:10 GMT-08:00	2009-12-10 16:11:10 GMT-08:00	2009-12-10 16:11:10 GMT-08:00	2009-11-12 17:49:38 GMT-08:00	77414
places.sqlite-journal				2009-12-10 16:11:00 GMT-08:00	2009-12-10 16:11:00 GMT-08:00	2009-12-10 16:11:00 GMT-08:00	2009-11-12 17:49:38 GMT-08:00	0

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Table moz_places 845 entries Page 2 of 9 Export to CSV

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frequency	last_visit_...
462	http://www...	Real time machine tool error ... - Google Patent Search	moc.eligoo...	1	0	0	6	60	125864952...
463	http://www...	url	moc.eligoo...	1	0	0		60	125864953...
464	http://www...	Class Definition for Class 700 - DATA PROCESSING: GENERI...	vog.otpstu...	1	0	0	15	60	125864952...
465	http://en...	en.wikipedia.org	gro.idelp...	1	0	0		60	125864969...
466	http://en...	Wikipedia, the free encyclopedia	gro.idelp...	1	0	0	12	60	125865609...
467	http://en...	steganography - Google Search	moc.eligoo...	2	0	0	6	125	125865609...
468	http://en...	Steganography - Wikipedia, the free encyclopedia	gro.idelp...	1	0	0	12	60	125865596...
469	http://inco...	: incoherence.co.uk - hide image ...	kurocune...	1	0	1	30	1234	125865601...
470	http://ho...	Steganography Software	tent.sacm...	1	0	1		1234	125865605...

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Table moz_places 845 entries Page 4 of 9 Export to CSV

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frequency	last_visit_...
877	http://patf...	United States Patent: 5026637	vog.otpstu...	1	0	0	16	82	125909686...
878	http://patf...	Publication Images	vog.otpstu...	1	0	0	34	82	125909720...
879	http://patf...	Patent Database Search Results: ttl:immortality in US Patents Text Coll	vog.otpstu...	1	0	0	16	82	125909728...
880	http://patf...	Patent Database Search Results: ttl:immortal in US Patent Collection	vog.otpstu...	1	0	0	16	82	125909729...
881	http://patf...	United States Patent: 6962168	vog.otpstu...	1	0	0	16	82	125909733...
882	http://patf...	Publication Images	vog.otpstu...	1	0	0	36	82	125909734...
883	http://www...	7zip - Google Search	moc.eligoo...	1	0	0	6	82	125909756...
884	http://www...	7-Zip	gro.idelp...	7	0	0		82	125909756...
885	http://do...	7z465.exe	tenegrofe...	1	0	0		82	125909756...

13) Λίστα με websites που επισκεπτόταν ο ύποπτος?

Πίνακας με websites για patent searching.

Απάντηση	Timestamp	URL	Browser
(Εφαρμόζεται η ζώνη ώρας Pacific Standard Time)	2009-11-12 17:50:37 PST	http://www.google.com/patents	Mozilla Firefox
	2009-11-12 17:55:02 PST	http://www.espacenet.com/	Mozilla Firefox
	2009-11-16 13:30:16 PST	http://www.wipo.int/patentscope/search/en/search.jsf	Mozilla Firefox
	2009-11-16 13:30:46 PST	http://patft.uspto.gov/	Mozilla Firefox
	2009-11-18 13:36:15 PST	http://usms.nist.gov/resources/MNs/MNspreadsheetTagged.csv	Mozilla Firefox
	2009-11-19 13:28:57 PST	http://www.epo.org/	Mozilla Firefox
	2009-11-19 13:29:01 PST	http://www.european-patent-office.org/	Mozilla Firefox

	2009-12-07 12:56:15 PST	http://www.peertopatent.org/	Mozilla Firefox
	2009-11-19 08:47:34 PST	http://www.google.com/patents/download/PNEUMATIC_BOXING_G_LOVE.pdf?id=InUBAAAAEBAJ&output=pdf&sig=ACfU3U2liBDli7vLKJlms2Qre0ZD2bUWuA&source=gbs_overview_r&cad=0	Mozilla Firefox
	2009-11-19 08:49:02 PST	http://www.google.com/patents/download/Method_of_real_time_machine_path_plannin.pdf?id=KccjAAAEBAJ&output=pdf&sig=ACfU3U0CT6HhoiOuysi9h9WLWz5bS_g-IQ&source=gbs_overview_r&cad=0	Mozilla Firefox
	2009-12-02 13:29:41 PST	http://www.wipo.int/patentscope/search/en/detail.jsf?docId=WO1987005929&rrecNum=49&docAn=US1987000710&office=&queryString=immortality&prevFilter=&sortOption=Relevance&maxRec=12343 Title: WO/1987/005929 IMMORTALIZED CELLS WHICH PRODUCE TISSUE-SPECIFIC PRODUCTS	Mozilla Firefox
Παρατηρήσεις	Τα δεδομένα βρέθηκαν στο path /Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/places.sqlite		

Πίνακας με websites λογισμικού

Απάντηση (Εφαρμόζεται η ζώνη ώρας Pacific Standard Time)	Timestamp	URL	Browser
	2009-11-12 17:50:37 PST	http://wiki.github.com/bard/mozrepl	Mozilla Firefox
	2009-11-12 17:55:10 PST	http://www.python.org/ftp/python/2.6.4/python-2.6.4.msi	Mozilla Firefox
	2009-11-17 13:49:48 PST	http://www.foxitsoftware.com/pdf/reader/	Mozilla Firefox
	2009-11-18 13:39:08 PST	http://www.easc.noaa.gov/Security/webfile/erso.doc.gov/briefings/STU.doc	Mozilla Firefox
	2009-11-19 10:40:13 PST	http://incoherency.co.uk/hideimage.php	Mozilla Firefox
	2009-11-19 10:40:55 PST	http://home.comcast.net/~ebm.md/stego/softwarewindows.html	Mozilla Firefox
	2009-11-19 10:41:10 PST	http://utilitymill.com/edit/Steganography_Encode	Mozilla Firefox
	2009-11-19 10:41:48 PST	http://www.brothersoft.com/downloads/steganography-tool.html	Mozilla Firefox
	2009-11-19 10:41:53 PST	http://3d2f.com/tags/steganography/	Mozilla Firefox
	2009-11-19 10:42:08 PST	http://www.prospector.cz/Freeware/Utilities/Security/Steganography/	Mozilla Firefox
	2009-11-19 10:42:12 PST	http://www.invisiblesecrets.com/ver2/index.html	Mozilla Firefox
	2009-11-19 10:42:17 PST	http://www.neobytesolutions.com/downloads/invsecr2.exe	Mozilla Firefox
	2009-11-19 10:43:05 PST	http://steghide.sourceforge.net/index.php	Mozilla Firefox
	2009-11-19 13:07:51 PST	http://www.apple.com/quicktime/download/	Mozilla Firefox
	2009-11-19 13:17:07 PST	http://www.alternatiff.com/distribution/alternatiff-1_9_1.exe	Mozilla Firefox
	2009-11-24 13:19:22 PST	http://www.7-zip.org/	Mozilla Firefox
	2009-11-24 13:57:49 PST	http://www.physics.ohio-state.edu/~prewett/hexedit/	Mozilla Firefox
	2009-11-24 13:58:10 PST	http://www.softcircuits.com/cygnus/fe/	Mozilla Firefox
	2009-11-24 16:11:09 PST	http://trilinos.sandia.gov/changelog-6.0.html	Mozilla Firefox
	2009-12-03 09:42:34 PST	http://www.us-cert.gov/control_systems/csvuls.html	Mozilla Firefox
	2009-12-03 13:39:26 PST	http://netlib.sandia.gov/bibnet/journals/appnummath.ps.gz	Mozilla Firefox
	2009-12-04 16:15:42 PST	http://afni.nimh.nih.gov/pub/dist/doc/program_help/3dsvm.html	Mozilla Firefox
Παρατηρήσεις	Τα δεδομένα βρέθηκαν στο path /Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/places.sqlite		

Πίνακας με websites λοιπού περιεχομένου

	Timestamp	URL	Browser
--	-----------	-----	---------

Απάντηση (Εφαρμόζεται η ζώνη ώρας Pacific Standard Time)	2009-11-16 13:14:00 PST	http://en.wikipedia.org/wiki/Internet_as_a_source_of_prior_art	Mozilla Firefox
	2009-11-17 10:29:53 PST	http://www.controller.com/	Mozilla Firefox
	2009-11-18 12:57:14 PST	http://www.turtlefiji.com/	Mozilla Firefox
	2009-11-19 13:20:30 PST	http://www.gulfstream.com/	Mozilla Firefox
	2009-11-19 10:39:24 PST	http://en.wikipedia.org/wiki/Steganography	Mozilla Firefox
	2009-12-02 08:56:07 PST	http://autos.aol.com/gallery/hot_sports_cars	Mozilla Firefox
	2009-12-01 12:59:15 PST	http://www.supercars.net/index.html	Mozilla Firefox
	2009-12-07 12:56:08 PST	http://en.wikipedia.org/wiki/Inequitable_conduct	Mozilla Firefox
	2009-12-07 13:39:56 PST	http://www.friendlyplanet.com/	Mozilla Firefox
	Παρατηρήσεις	Τα δεδομένα βρέθηκαν στο path /Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/places.sqlite	

14) List all search keywords using web browsers. (Timestamp, URL, keyword)

Απάντηση (Some duplicated and meaningless items are excluded) (Εφαρμόζεται η ζώνη ώρας)	Timestamp	Keyword (URL)	Browser
	2009-11-12 17:50:27	mozrepl (http://www.google.com/search?q=mozrepl&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-11-12 17:54:56	python (http://www.google.com/search?q=python&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-11-19 08:48:47	time machine (http://www.google.com/patents?q=time+machine&btnG=Search+Patents)	Mozilla Firefox
	2009-11-19 08:49:43	time travel (http://www.google.com/patents?q=time+travel&btnG=Search+Patents)	Mozilla Firefox
	2009-11-19 10:39:24	steganography (http://www.google.com/search?q=steganography&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-11-19 10:41:43	steganography tool free (http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=0lr&q=steganography+tool+free&aq=f&oq=&aqi=)	Mozilla Firefox
	2009-11-24 13:19:22	7zip (http://www.google.com/search?q=7zip&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-11-24 13:57:33	open source hex editor (http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=uXO&q=open+source+hex+editor&aq=f&oq=&aqi=gsx2g-msx3)	Mozilla Firefox
	2009-12-02 08:55:58	hot sports cars (http://www.google.com/search?q=hot+sports+cars&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-12-08 13:01:37	mediterranean vacation packages (http://www.google.com/search?q=mediterranean+vacation+packages&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox
	2009-12-08 14:17:01	exotic car dealer (http://www.google.com/search?q=exotic+car+dealer&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Mozilla Firefox

	2009-12-08 14:17:34	ford car dealer (http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=kXT&q= ford+car+dealer &aq=f&oq=&aqi=g10)	Mozilla Firefox
	2009-11-13 18:46:29	http://www.google.com/	Internet Explorer
	2009-11-12 15:46:32	firefox	Internet Explorer
Παρατηρήσεις	<p>Τα keywords του Mozilla βρέθηκαν στο: /Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/places.sqlite</p> <p>Τα keywords του Internet Explorer βρέθηκαν στο: \Documents and Settings\Charlie\Local Settings\Temporary Internet Files\Content.IE5\index.dat</p> <p>Internet Explorer urls typed βρέθηκαν στο:</p> <p>HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs</p>		

15) Λίστα με user keywords στην μπάρα αναζήτησης του Windows Explorer.

Απάντηση	Timestamp (PST Timezone is applied)	Search Keyword
	-	-
Παρατηρήσεις	<p>Τα σχετικά registry keys δεν υπάρχουν στο C:\Documents and Settings\Charlie\NTUSER.DAT</p> <p>Έγινε αναζήτηση στα παρακάτω κλειδιά</p> <p>Software\Microsoft\Search Assistant\ACMru</p> <pre>C:\Users\HELENA\Downloads\RECmd\RECmd\RECmd.exe -f "C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT" --kn "Software\Microsoft\Search Assistant\ACMru" --csv "output.csv" "Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery" RECmd version 2.1.0.0 Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/RECmd Note: Enclose all strings containing spaces (and all RegEx) with double quotes Command line: -f C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT --kn Software\Microsoft\Search Assistant\ACMru --csv output.csv "Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery" Processing hive C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT Key Software\Microsoft\Search Assistant\ACMru not found</pre> <p>Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery</p> <pre>C:\Users\HELENA\Downloads\RECmd\RECmd\RECmd.exe -f "C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT" --kn "Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery" --csv "output.csv" RECmd version 2.1.0.0 Author: Eric Zimmerman (saericzimmerman@gmail.com) https://github.com/EricZimmerman/RECmd Note: Enclose all strings containing spaces (and all RegEx) with double quotes Command line: -f C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT --kn Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery --csv output.csv Processing hive C:\Users\HELENA\Documents\Master\DigitalForensics\Charlie\DFIR - Charlie\NTUSER.DAT Key Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery not found</pre> <p>+ Βλ. Ερώτηση 29</p>	

16) What application was used for e-mail communication?

Απάντηση	Mozilla Thunderbird
Παρατηρήσεις	REGISTRY_USER_NTUSER_S-1-5-21...\Software\Mozilla\Thunderbird\Profiles\4xjz34s9h.default

17) Where is the e-mail file located?

Απάντηση	/img_charlie-2009-12-11.E01/vol_vo12/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Inbox
Παρατηρήσεις	<ul style="list-style-type: none"> - Mozilla Thunderbird <p>REGISTRY_USER_NTUSER_S-1-5-21...\Software\Mozilla\Thunderbird\Profiles\4xjz34s9h.default</p>

18) What was the e-mail account used by the suspect?

Απάντηση	charlie@m57.biz
Παρατηρήσεις	- See Question 19.

19) List all e-mails of the suspect. If , identify deleted e-mails. (You can identify the following items: Timestamp, From, To, Subject, Body, and Attachment) [Hint: just examine the OST file only.]

Απάντηση (Εφαρμόζεται η ζώνη ώρας)	Timestamp	E-Mail Communication	
	2009-11-17 10:30:59	Source	[Inbox]
		From → To	pat@m57.biz-> charlie@m57.biz , cjo@m57.biz
		Subject	M57.BIZ PRIOR ART INVESTIGATION SERVICES
		Body	<p>----- Original Message ----- From: Alex Monroe To: Pat McGoo Sent: Tuesday, November 17, 2009 8:58 AM Subject: Re: M57.BIZ PRIOR ART INVESTIGATION SERVICES</p> <p>Dear Pat,</p> <p>Yes, we are very interested in using your prior art investigation services. Our R&D department is currently applying for patents in two key areas that we are counting on to gain market share over our major competitor, project2400.com. I am counting on you and your firm to keep these research areas in strict confidentiality. We wouldn't want project2400 to know about our research interests.</p> <p>We will hire you to do prior art searches on these two areas:</p> <ul style="list-style-type: none"> a.. Time machines b.. Teleporters <p>Please send me a quote for these two investigations.</p> <p>Regards,</p> <p>Alex</p> <p>CEO - Nitroba.com</p> <p>On Nov 16, 2009, at 2:49 PM, Pat McGoo wrote:</p> <p>Alex,</p> <p>I enjoyed talking with you at the patent conference in San Francisco last week. I remember that you said that you would be interested in our prior art investigation services.</p> <p>If you are still interested in our services, then I can fax you over a service agreement right away. I hope to hear from you soon. Please do not hesitate to give me a call or email if you have any questions, concerns, or comments.</p> <p>Regards,</p>

			Pat McGoo CEO, M57.biz pat@m57.biz 831-555-1234 [Inbox] pat@m57.biz-> charlie@m57.biz, cjo@m57.biz
2009-11-17 10:33:39	Source	[Inbox]	
	From → To	pat@m57.biz-> charlie@m57.biz , jo@m57.biz	
	Subject	ASSIGNMENT OF NITROBA ACCOUNT	
	Body	Jo, Charlie: We have our first contract ! Nitroba wants us to do a prior art investigation in two key areas. Jo, you will be responsible for the teleporter patent search. Charlie, I want you to take the time machine patent search. This is our first real job, so let's make sure we do some quality research. Our reputation will depend on the time and effort that we put into this contract and on Nitroba's satisfaction with our results. Come by my office and we'll talk details. Pat	
2009-11-16 13:26:16	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com, rubinfritz31@mail.com	
	Subject	New email address	
	Body	Hey everybody. I started working at the new company today. It's pretty slow going so far, we're just getting set up and figuring out where everything is. I got my new email set up, so you can send to me at this address. Charlie	
2009-12-01 13:02:34	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com	
	Subject	Pack your bags	
	Body	Alix, Pretty soon I'm going to be able to afford to take you on a nice vacation. Where would you want to go if you could name your destination? I'm getting a hot car too. Charlie	
2009-12-02 13:04:29	Source	[Sent]	
	From → To	charlie@m57.biz → jaime@project2400.com	
	Subject	Interested?	
	Body	J, I have something that you'll definitely be interested in. It concerns your competitor. I'm doing a prior art search for them. Want to know what I've found? You know my price. I'll send you the goods after I see half in my account. Make sure you delete this email. C	

	2009-12-03 12:16:52	Source	[Sent]	
		From → To	charlie@m57.biz → jaime@project2400.com	
		Subject		
		Body	J, Nice working with you. Here's the file. Instructions for opening to follow when I see another deposit in my acct. C +Attachment= Astronaut1.jpg	
	2009-12-04 09:41:47	Source	[Sent]	
		From → To	charlie@m57.biz → andy@swexpert.com	
		Subject	I Found Something	
		Body	Andy, Lucky for me, I just happened to stumble across this. I found a prior patent that will definitely invalidate your current immortality patent. You should have used my boss's prior art services, but, oh well, I'll just use your negligence to benefit me. I want 100k or I'll release this publicly. I don't need to tell you how much this will hurt your business if I go public with this. Don't involve the cops or this information will go public. See the attachment for details on what I found. I'll be in touch with my bank acct number. The password for the zip file will be hidden in the next picture I send you. C +Attachment zip file	
	2009-12-04 13:06:23	Source	[Sent]	
		From → To	charlie@m57.biz → jaime@project2400.com	
		Subject	Instructions	
		Body	J, Got the deposit. The password to get the info is nitro. Use the steg program we talked about. And don't forget to delete these emails. C	
		Source	[Inbox]	
		From → To	MAILER-DAEMON-> charlie@m57.biz	
		Subject	Undelivered Mail Returned To Sender	
		Body	This is the Spam & Virus Firewall at mustang.nps.edu. I'm sorry to inform you that the message below could not be delivered. When delivery was attempted, the following error was returned. < jaime@project2400.com >: host mx2.sub3.homie.mail.dreamhost.com[208.97.132.222] said: 550 5.1.1 < jaime@project2400.com >: Recipient address rejected: User unknown in virtual alias table (in reply to RCPT TO command) +2 attachments	

	2009-12-07 11:44:18	Source	[Sent]
		From → To	charlie@m57.biz → andy@swexpert.com
		Subject	Picture
		Body	<p>Andy,</p> <p>Here's the picture I promised... Make sure you delete this.</p> <p>C +Attachment microscope1.jpg</p>
2009-12-03 09:51:33	Source	[Inbox]	
		From → To	jaime@project2400.com → charlie@m57.biz
		Subject	RE:Intrested?
		Body	<p>C,</p> <p>We'll give you \$0 large if it's good. I'll put in \$10 up front, you'll get the rest when we see the goods.</p> <p>J</p> <p>> J, > > I have something that you'll definitely be interested in. It concerns > your competitor. I'm doing a prior art search for them. Want to know > what I've found? You know my price. I'll send you the goods after I > see half in my account. Make sure you delete this email. > > C > ></p>
2009-12-11 08:55:53	Source	[Inbox]	
		From → To	pat@m57.biz-> terry@m57.biz, charlie@m57.biz , jo@m57.biz
		Subject	Important Meeting
		Body	<p>Team,</p> <p>we are going to have a meeting first thing this morning. As soon as you get in please come in to the conference room. I received a call yesterday from the Police - they are going to be here to talk to us.</p> <p>Pat</p>
Παρατηρήσεις	- Βρέθηκε Στεγανογραφία σε 2 εικόνες που στάλθηκαν μέσω mail.		

Πίνακας 14 Σχετική αλληλογραφία με την υπόθεση

20) List external storage devices attached to Laptop

Απάντηση	Device Name	Volume Name	Serial No.	First Connected Time	Connected Time After Reboot
	Kingston Data Traveler 2.0 USB Device (Charlie's USB [0004])	F: Volume{fd7018a2-d5f8-11de-a023-000bdb4f6b10}	2007110203195377	2009/11/20 09:20:25 PST	-
	LaCie Rugged FW/USB USB Device	-	00D04B881007C255	2009/11/16 16:25:20 PST	-

	SanDisk Cruzer USB Device	Volume {ee9b4 db1-d3aa- 11de-a020- 000bdb4f6b10 }	43175107A4C24AD4	2009/11/17 13:09:13 PST	-
	USB 2.0 Flash Disk USB Device (Terry's USB)	Volume {ee9b4 db0-d3aa- 11de-a020- 000bdb4f6b10 }	51491E64	2009/11/17 10:56:37 PST	-
Παρατηρήσεις	<ul style="list-style-type: none"> - Device Name: HKLM\SYSTEM\ControlSet###\Enum\USBSTOR\###<USB_NAME>###\###<SN>###\FriendlyName - Volume: we bind the value found in HKLM\SYSTEM\ControlSet###\Enum\USBSTOR\###<USB_NAME>###\###<SN>###\ParentIdPrefix With HKLM\SYSTEM\MountedDevices - Serial Number: HKLM\SYSTEM\ControlSet###\Enum\USBSTOR\###<USB_NAME>###\ - First Connected Time: C:\Windows\inf\setupapi.log - Connected Time After Reboot: - 				

21) Εντοπίστε όλα τα ίχνη που σχετίζονται με τη «μετονομασία» αρχείων στους φακέλους "Τα Έγγραφά μου" (My Documents) και "Λήψεις" (Downloads) των Windows. (Θα πρέπει να ληφθούν υπόψη μόνο ενέργειες που πραγματοποιήθηκαν στο χρονικό διάστημα από 11/12/2009 έως 12/12/2009.)

Απάντηση	Timestamp	USN	Path (Of course, just file names are OK)	Event
(Εφαρμόζεται η ζώνη ώρας)	18/11/2009 16:39	74951376	.\Documents and Settings\Charlie\Desktop\web\Copy of urlspersona.txt	RenameOldName
		74951488	.\Documents and Settings\Charlie\Desktop\web\urls_personal.txt	RenameNewName
	10/12/2009 22:23	80488896	.\Documents and Settings\Charlie\My Documents\Quantum Cryptography\New Text Document.txt	RenameOldName
		80489000	.\Documents and Settings\Charlie\My Documents\Quantum Cryptography\OCR.txt	RenameNewName
Παρατηρήσεις	<ul style="list-style-type: none"> - NTFS journal file analysis (→ \$UsnJrnl) - \\$Extend\\$UsnJrnl:\$J (+ \$MFT for identifying full paths of files) 			

22) What is the IP address of company's shared network drive?

Απάντηση	192.168.1.1
Παρατηρήσεις	\Charlie\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU > data: \\\192.168.1.1\m57\ram \Documents and Settings\Charlie\NTUSER.DAT\Network/Z >mapping:Z

23) Καταχωρίστε όλους τους καταλόγους που διασχίστηκαν στη μονάδα USB [0004]

Απάντηση	Timestamp	Directory Path	Source
(Εφαρμόζεται η ζώνη ώρας)	2009-11-24 14:19:24 PST	F:\	
	2009-12-12 14:29:37 PST	F:\Email\other	
Παρατηρήσεις	HKU\charlie\Software\~		

24) Καταχωρίστε όλα τα αρχεία που άνοιξαν στη μονάδα USB [0004]

Απάντηση	Timestamp	Directory Path	Source
(Εφαρμόζεται η ζώνη ώρας)	2009-11-24 14:08:33 PST	F:\Copy of microscope.jpg	
	2009-11-24 14:09:20 PST	F:\microscope.jpg	
	2009-12-04 13:39:45 PST	F:\Email\Charlie_2009-11-20_0957_99202.ComplexityTheory.Louisa+Fleet.pdf	
	2009-12-04 13:40:21 PST	F:\Email\Charlie_2009-11-20_0957_Received_95253.SCSI.Mathew+Malizia.pdf	
	2009-12-04 13:40:28 PST	F:\Email\Charlie_2009-11-20_0957_Received_97315.ScatterGatherIO.Julio+Molock.pdf	
	2009-12-04 13:40:35 PST	F:\Email\Charlie_2009-11-20_0957_Received_98521.WANs.Greg+Hillier.pdf	
	2009-12-04 13:41:17 PST	F:\Email\Charlie_2009-11-20_1055_Received_PETEFFS.pdf	
	2009-12-04 13:42:26 PST	F:\Email\Charlie_2009-11-30_0854_Received_US5041044.pdf	
	2009-12-10 14:28:05 PST	F:\Email\other\QC Project.eml	
	2009-12-10 14:28:17 PST	F:\Email\other\Picture.eml	
	2009-12-10 14:29:37 PST	F:\Email\other\Picture_a1.jpg	
Παρατηρήσεις	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs		

25) Καταχωρίστε όλους τους καταλόγους που διασχίστηκαν στη μονάδα δίσκου δικτύου της εταιρείας

Απάντηση	Timestamp	Directory Path	Source
(Εφαρμόζεται η ζώνη ώρας)		Desktop\My Computer\Z:\	Registry Explorer
	2009-12-04 16:39:46 PST	Desktop\My Computer\Z:\windd	Registry Explorer
	2009-12-05 08:37:24 PST	Desktop\My Computer\Z:\windd\32bits_i386	Registry Explorer
Παρατηρήσεις	- Z:/ is mapped on \\192.168.1.1\\		
	HKU\charlie\Software\~		

26) Καταχωρίστε όλα τα αρχεία που άνοιξαν στη μονάδα δίσκου δικτύου της εταιρείας.

Απάντηση	Timestamp	Directory Path	Source

(Εφαρμόζεται η ζώνη ώρας)			
Παρατηρήσεις	- Z: is mapped on \\192.168.1.1 - HKU\charlie\Software\~ - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs Από την αναζήτηση στο NTUSER.DAT δεν προέκυψε κάποιο σχετικό εύρημα		

27) Βρείτε ίχνη που σχετίζονται με υπηρεσίες cloud στο Laptop [0001]. (Service name, log files...).

Απάντηση	Cloud Service	Type	Traces
Παρατηρήσεις	Από την αναζήτηση δεν προέκυψε κάποιο σχετικό εύρημα - Από την ερώτηση 10 δεν προέκυψε κάτι - HKLM\SOFTWARE - HKLM\SOFTWARE\Microsoft\Windows\Current Version\Uninstall - HKCU\Software\Microsoft\Windows\CurrentVersion\Run		

28) Ποια αρχεία διαγράφηκαν από το Dropbox; Βρείτε το όνομα αρχείου και την τροποποιημένη χρονική σήμανση του αρχείου.

Απάντηση (Εφαρμόζεται η ζώνη ώρας)	Timestamp	File name	Modified Time (UTC-05)
Παρατηρήσεις	Από προηγούμενο ερώτημα προέκυψε πως δεν έχει εγκατασταθεί το Dropbox στο μηχάνημα οπότε δεν υπάρχει κάποιο εύρημα		

29) Τι είδους δεδομένα αποθηκεύτηκαν στο Windows Search database?

Απάντηση	-
Παρατηρήσεις	- Δεν βρέθηκαν.wci αρχεία στο <ul style="list-style-type: none">• /img_charlie-2009-12-11.E01/vol_vvol2/System Volume Information/• Ή στο /img_charlie-2009-12-11.E01/WINDOWS/system32/CatRoot2• Και το Indexing Service (cisvc) στο HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cisvc είχε τιμή 3 που δείχνει ότι εγκαταστάθηκε αλλά ποτέ δεν έτρεξε στο σύστημα, αφήνωντας μη χρησιμοποιήσιμη ΒΔ για ανάλυση

Παράρτημα Ε – Φόρμες κατάσχεσης και καταγραφής

Εντυπο Παρακολούθησης Αλυσίδας Κατοχής Αποδεικτικών Στοιχείων

Αριθμός Υπόθεσης: 00111122009

Αδίκημα: Διαρροή δεδομένων

Επιθεωρητής: Technical Witness 1232

Θύμα: M57.Biz

Υποπτος: Charlie

Ημερομηνία/Ωρα Κατάσχεσης: 11/12/2009

Τοποθεσία Κατάσχεσης: Γραφεία M57.Biz

Περιγραφή Πειστηρίων		
Πειστήριο #	Ποσότητα	Περιγραφή (Μοντέλο, Σ/Α #, Κατάσταση, Σημάδια, Γρατζουνιές)
0001	1	DELL Laptop, DEJ485BIDFGJF, Ενεργό, Συνδεδεμένο με παροχή ρεύματος μέσω πειστηρίου 0002
0002	1	Τροφοδοτικό laptop Delta Electronics Inc. AC Adapter – ADP – 65DB, Q4W0406021262, Ενεργό, Συνδεδεμένο με πειστήριο [0001]
0003	1	Logitech M-U0026 – Ενσύρματο ποντίκι, 1939HS01D6W8, Μη συνδεδεμένο, Γρατζουνιές στην δεξιά πλευρά
0004	1	Kingston Data Traveler 2.0 USB Device, 2007110203195377, Μη συνδεδεμένο
0005	1	Σκληρός Δίσκος ZX-500 3.5" (αφαιρέθηκε από το Laptop [0001]), HJ8934FDS923

Πίνακας 15 Φόρμα Chain of Custody 1.

Chain of Custody				
Πειστήριο #	Ημερομηνία	Παραδόθηκε από (Υπογραφή & Αρ. Ταυτότητας)	Παραλήφθηκε από (Υπογραφή & Αρ. Ταυτότητας)	Σχόλια/Τοποθεσία
0001	11/12/2009	M57.Biz IT Admin	Technical Witness 1233	M57.Biz / Γραφεία 1 ^{ου} ορόφου
0002	11/12/2009	M57.Biz IT Admin	Technical Witness 1233	M57.Biz / Γραφεία 1 ^{ου} ορόφου
0003	11/12/2009	M57.Biz IT Admin	Technical Witness 1233	M57.Biz / Γραφεία 1 ^{ου} ορόφου
0004	11/12/2009	M57.Biz IT Admin	Technical Witness 1233	M57.Biz / Γραφεία 1 ^{ου} ορόφου
0005	11/12/2009	M57.Biz IT Admin	Technical Witness 1233	M57.Biz / Γραφεία 1 ^{ου} ορόφου
0001	29/12/2009	Technical Witness 1233	M57.Biz IT Admin	FORENSICS LAB
0002	29/12/2009	Technical Witness 1233	M57.Biz IT Admin	FORENSICS LAB
0003	29/12/2009	Technical Witness 1233	M57.Biz IT Admin	FORENSICS LAB
0004	29/12/2009	Technical Witness 1233	M57.Biz IT Admin	FORENSICS LAB
0005	29/12/2009	Technical Witness 1233	M57.Biz IT Admin	FORENSICS LAB

Πίνακας 16 Φόρμα Chain of Custody 2.

Φόρμα στοιχείων σκληρού δίσκου

Τεχνικές Προδιαγραφές Σκληρού δίσκου	
Case ID	00111122009

Item ID	[0005]					
Reference Device ID	[0001] / DELL Laptop					
Κατασκευαστής	ZX-500					
S/N	HJ8934FDS923					
Κύλινδροι	1,253					
Κεφαλές	255					
Δίσκοι	1					
Χωρητικότητα	10.24 GB (10,239,860,736 bytes)					
Λεπτομέρειες κατάσχεσης σκληρού δίσκου						
Ήταν προσαρτημένος ο δίσκος;	ΝΑΙ					
Ήταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;	ΟΧΙ					
Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε; Η μπαταρία αφαιρέθηκε χωρίς να πατηθεί το power button. Ελέγχθηκε η λειτουργία των ανεμιστήρων, όλα τα καλώδια και περιφερειακά αποσυνδέθηκαν, επισημάνθηκαν και συσκευάστηκαν. Ο σκληρός δίσκος αφαιρέθηκε και τοποθετήθηκε σε αντιστατική σακούλα με κατάλληλη επισήμανση.						
Ήταν ο δίσκος προστατευμένος με κωδικό πρόσβασης;	ΟΧΙ					
Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι; ΟΧΙ						
Δημιουργία αντιγράφου						
Εφαρμογή δημιουργίας αντιγράφου	FTK Imager	Έκδοση	4.7.3.81			
Τόπος λήψης πιστού αντιγράφου	Γραφεία M57.Biz					
Ημερομηνία λήψης πιστού αντιγράφου	2009-12-11 09:12:15 π.μ.					
hashes	0377b3d41bbbc295a1c9f00aa07ee174					
Εγκληματολόγος ερευνητής που έκανε την κατάσχεση						
Όνοματεπώνυμο	Technical Witness 1233	Τίτλος	Ερευνητής/Αναλυτής			
Τηλέφωνο	6938677621	Τμήμα	Digital Forensics			
Υπογραφή	TW1233	Ημ/νια	11/12/2009			
Σχόλια	Καμία πρόσθετη παρατήρηση κατά την κατάσχεση. Όλα τα μέτρα λήφθηκαν σύμφωνα με τις οδηγίες του ACPO.					

Πίνακας 17 Φόρμα Στοιχείων Σκληρού Δίσκου.

Παράρτημα ΣΤ – Εξοπλισμός εργαστηρίου

Το εργαστήριο ψηφιακής εγκληματολογίας στεγάζεται σε ειδικά διαμορφωμένο χώρο, σχεδιασμένο με αυστηρά μέτρα ασφαλείας και τεχνικές προδιαγραφές που διασφαλίζουν την ακεραιότητα των αποδεικτικών στοιχείων και την εμπιστευτικότητα της ανάλυσης. Ο χώρος βρίσκεται εντός εσωτερικού δωματίου, πλήρως απομονωμένου από εξωτερικά δίκτυα και σήματα. Χρησιμοποιούνται τεχνολογίες θωράκισης (shielding) για την αποτροπή ηλεκτρομαγνητικών παρεμβολών και την απομόνωση από σήματα Wi-Fi, Bluetooth, κινητής τηλεφωνίας και άλλων ασύρματων επικοινωνιών.

Η είσοδος στον χώρο πραγματοποιείται αποκλειστικά μέσω ηλεκτρονικού συστήματος ελέγχου πρόσβασης (access control) με τη χρήση προσωπικών μαγνητικών καρτών. Η πρόσβαση επιτρέπεται μόνο σε εξουσιοδοτημένα μέλη του προσωπικού με κατάλληλα δικαιώματα. Επιπλέον, ολόκληρος ο χώρος παρακολουθείται από σύστημα συνεχούς βιντεοεπιτήρησης (CCTV), με κάμερες υψηλής ευκρίνειας που καταγράφουν 24/7 όλες τις κινήσεις εντός και εκτός του εργαστηρίου.

Στο εσωτερικό του εργαστηρίου βρίσκονται απομονωμένοι (air-gapped) σταθμοί εργασίας, οι οποίοι δεν διαθέτουν σύνδεση στο διαδίκτυο ή σε οποιοδήποτε εξωτερικό δίκτυο. Οι υπολογιστές αυτοί είναι αφιερωμένοι αποκλειστικά στην ανάλυση ψηφιακών αποδεικτικών στοιχείων και είναι εξοπλισμένοι με πλήρες λογισμικό forensics, συμπεριλαμβανομένων των εργαλείων **Autopsy**, **FTK Imager**, **EnCase**, **X-Ways Forensics**, **Magnet AXIOM** και άλλων εξειδικευμένων βοηθημάτων.

Επιπλέον, στο εργαστήριο υπάρχουν **συσκευές write blocker** (υλικού και λογισμικού επιπέδου), που διασφαλίζουν την ακεραιότητα των δεδομένων κατά τη διάρκεια της ανάλυσης, καθώς και **φορητοί σαρωτές**, **storage duplicators**, **forensic dongles** και **εξειδικευμένα κιτ κατάσχεσης (field kits)** για επιτόπιες επιχειρήσεις. Όλα τα δεδομένα που συλλέγονται ή δημιουργούνται φυλάσσονται σε **κρυπτογραφημένα μέσα αποθήκευσης**, τα οποία τηρούνται σε ασφαλές ερμάριο εντός του χώρου.

Παράρτημα Ζ – Εξουσιοδότηση Έρευνας

Αθήνα 10 Δεκεμβρίου 2009

ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΕΡΓΟΥ

Με την παρούσα, εξουσιοδοτούμε την ομάδα ψηφιακής εγκληματολογικής διερεύνησης να προχωρήσει σε όλες τις απαραίτητες ενέργειες που σχετίζονται με:

- Την επιτόπια αυτοψία και καταγραφή χώρων εργασίας και εξοπλισμού.
- Τη συλλογή, καταγραφή και αποτύπωση πιθανών ψηφιακών πειστηρίων.
- Την απόσπαση, αποθήκευση και ανάλυση δεδομένων από υπολογιστικά συστήματα, αποθηκευτικά μέσα ή άλλες ηλεκτρονικές συσκευές που βρίσκονται εντός των εγκαταστάσεων ή υπό την ευθύνη της εταιρείας.
- Τη μεταφορά των πειστηρίων προς ανάλυση σε εργαστηριακό περιβάλλον, εφόσον απαιτείται.

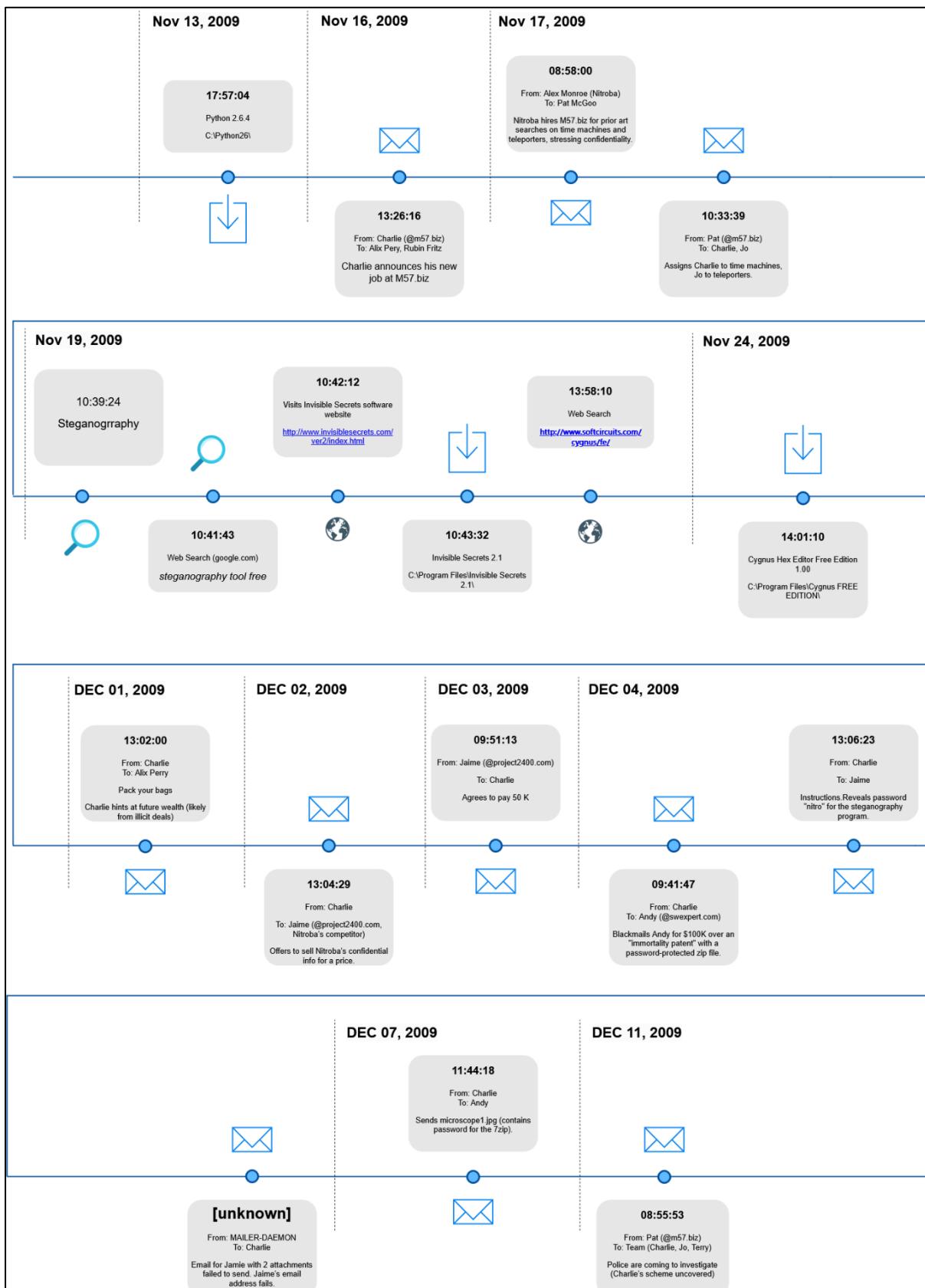
Η εξουσιοδότηση αυτή παρέχεται στο πλαίσιο της διερεύνησης πιθανής παραβίασης της ασφάλειας πληροφοριακών συστημάτων της εταιρείας και τυχόν διαρροής ευαίσθητων ή εμπιστευτικών δεδομένων.

Η ομάδα έχει λάβει πλήρη και έγγραφη δέσμευση εμπιστευτικότητας (NDA), η οποία ισχύει καθ' όλη τη διάρκεια της διαδικασίας και μετά την ολοκλήρωσή της.

Επισημαίνεται ότι η εταιρεία έχει ενημερωθεί από την ομάδα σχετικά με τις νομικές υποχρεώσεις και τους περιορισμούς της έρευνας, ιδίως σε σχέση με την προστασία προσωπικών δεδομένων σύμφωνα με Ν. 2472/97), και παρέχει ρητή συγκατάθεση για την επεξεργασία των σχετικών πληροφοριών.

Η παρούσα εξουσιοδότηση τίθεται σε ισχύ από την ημερομηνία υπογραφής και ισχύει μέχρι την ολοκλήρωση της έρευνας, εκτός αν ανακληθεί εγγράφως από την εταιρεία.

Παράρτημα Η – Χρονοδιάγραμμα Ενεργειών Charlie



Εικόνα 46 Χρονοδιάγραμμα Ενεργειών του Charlie..

Παράρτημα Θ – Στεγανάλυση

Στην αλληλογραφία του κατηγορούμενου εντοπίστηκαν αρκετά mail στα οποία γίνεται αναφορά σε στεγανογραφικά εργαλεία, υπάρχουν συμπιεσμένα/κρυπτογραφημένα αρχεία των οποίων ο κωδικός βρίσκεται σε κάποια απεσταλμένη εικόνα. Συγκεκριμένα εντοπίστηκαν δυο εικόνες που περιέχουν στεγανογραφία μία για την κάθε διαφορετική επικοινωνία του με κάποιον με παράνομο τρόπο. Έχουμε 2 παράνομα περιστατικά.

A. Παράνομη πώληση εμπιστευτικών πληροφοριών σε αντίταλους συγκεκριμένα στον jaime@project2400.com στον οποίον έστειλε την στεγανογραφημένη εικόνα astronaut1.jpg με τον κωδικό nitro. Η αρχική εικόνα astronaut.jpg βρέθηκε στο USB. Πριν την έναρξη της διαδικασίας στεγανάλυσης, επιβεβαιώνουμε την ακεραιότητα της εικόνας με τη σύγκριση των hashes της εικόνας :

MD5: 45eade24b3a89b21fed303310ccbdc54

SHA-256: f57e2e43101088191f9929e1be088baeaeb3ae4df18200701f4f814d6b551b32

Για την στεγανάλυση της ακολουθήθηκε η παρακάτω διαδικασία :

- Έγιναν extract ενσωματωμένα δεδομένα με την εντολή binwalk -e astronaut1.jpg και έδωσαν σαν αποτέλεσμα τον φάκελο _astronaut1.jpg.extracted με δυο αρχεία μέσα το AC.zlib και το AC

```
(katkali㉿kali)-[~/shared]$ binwalk -e astronaut1.jpg

DECIMAL      HEXADECIMAL      DESCRIPTION
_____
172          0xAC            Zlib compressed data, best compression

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

Eikόνα 47: Binwalk -e astronaut1.jpg

```
(katkali㉿kali)-[~/shared]$ ls
astronaut1.jpg           _astronaut1.jpg.extracted
```

Eikόνα 48: Extracted folder

```
(katkali㉿kali)-[~/shared]
$ cd _astronaut1.jpg.extracted/
(katkali㉿kali)-[~/shared/_astronaut1.jpg.extracted]
$ ls
AC  AC.zlib
```

Eikόνα 49: Extracted Files

- Στη συνέχεια με την εκτέλεση την AC document.odt μετατρέπουμε το AC με κατάληξη .odt και το αποσυμπιέζουμε με την εντολή unzip -l document.odt καθώς τα αρχεία OpenDocument είναι στην πραγματικότητα αρχεία ZIP με δομημένη XML μέσα και ανοίγοντας το αρχείο document.odt με word εντοπίζουμε κείμενο σχετικό με την πατέντα time machines της Nitroba:

```
(katkali㉿kali)-[~/shared/_astronaut1.jpg.extracted]
$ unzip -l document.odt
Archive: document.odt
Length      Date    Time   Name
-----  ----  ----
      39  2009-11-19 21:26  mimetype
       0  2009-11-19 21:26  Configurations2/statusbar/
       0  2009-11-19 21:26  Configurations2/accelerator/current.xml
       0  2009-11-19 21:26  Configurations2/floater/
       0  2009-11-19 21:26  Configurations2/popupmenu/
       0  2009-11-19 21:26  Configurations2/progressbar/
       0  2009-11-19 21:26  Configurations2/menubar/
       0  2009-11-19 21:26  Configurations2/toolbar/
       0  2009-11-19 21:26  Configurations2/images/Bitmaps/
  9111  2009-11-19 21:26  content.xml
11435  2009-11-19 21:26  styles.xml
 1033  2009-11-19 21:26  meta.xml
  3430  2009-11-19 21:26  Thumbnails/thumbnail.png
  8086  2009-11-19 21:26  settings.xml
 1889  2009-11-19 21:26  META-INF/manifest.xml
-----  -----
 35023                               15 files
```

Eikόνα 50: Extracted document that contains patent information

Time Machine Prior Art:

Pub. No.:WO/2009/056125 International Application No.:PCT/DE2008/001787 Publication Date:07.05.2009 International Filing Date:28.10.2008

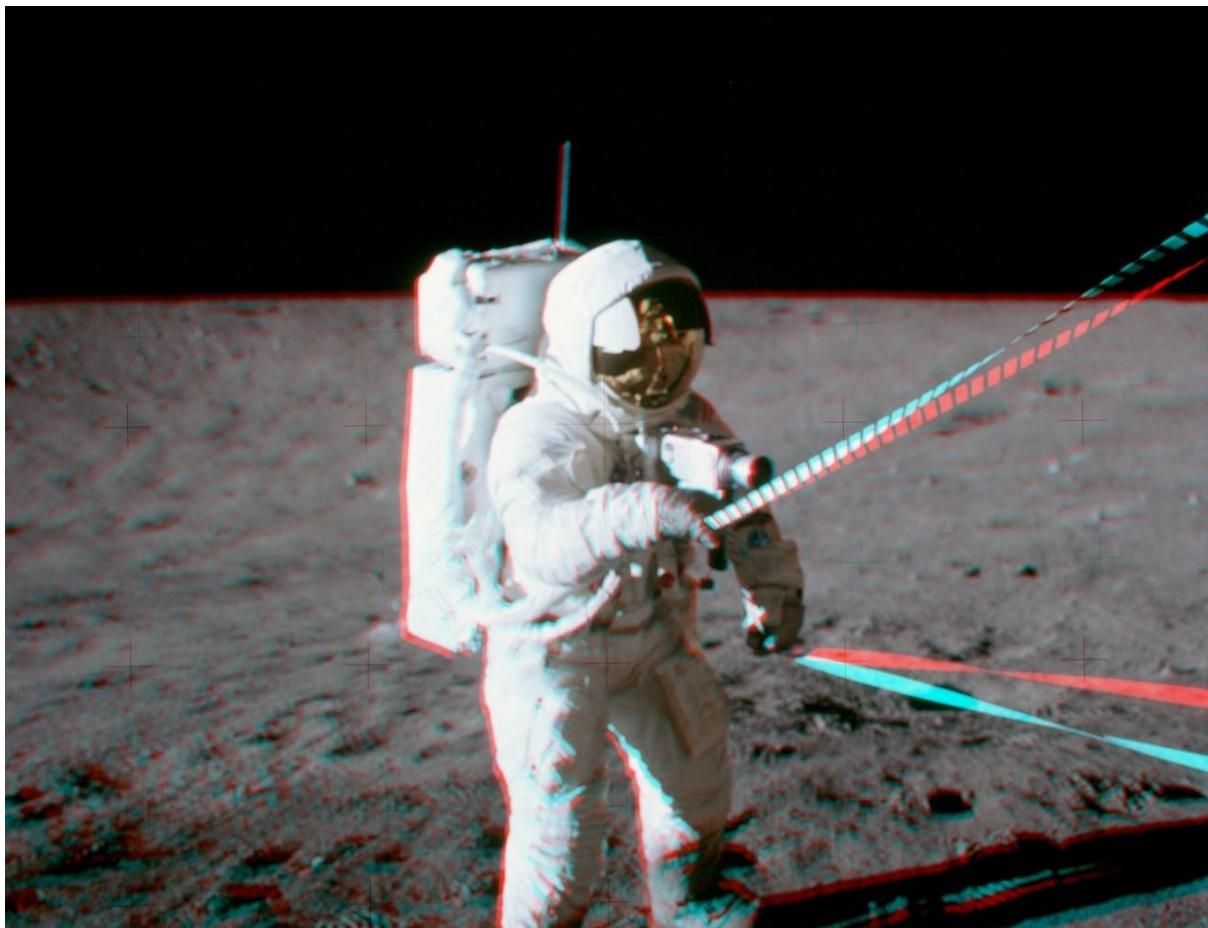
<i>Pub. No.:</i>	<i>WO/2008/143237</i>	<i>International Application No.:</i>	<i>PCT/JP2008/059191</i>
<i>Publication Date:</i>	<i>27.11.2008</i>	<i>International Filing Date:</i>	<i>20.05.2008</i>

Pub. No.:WO/2008/094611 International Application No.:PCT/US2008/001241 Publication Date:07.08.2008 International Filing Date:30.01.2008

PriorityData:

11/700,015 31.01.2007 US

Title: SIMULATION SYSTEM IMPLEMENTING REAL-TIME MACHINE DATA



Εικόνα 51: Astronaut1.jpg

B. Η δεύτερη περίπτωση αφορά εκβιασμό γνωστοποίησης δημόσια, εναίσθητων πληροφοριών με σκοπό την απόσπαση χρημάτων από τον andy@swexpert.com μέσω mail σχετικά με την πατέντα του στο quantum cryptography. Στα mail βρέθηκε το κρυπτογραφημένο 01.zip αρχείο το οποίο χρειάζεται κωδικό για να ανοίξει. Ο κωδικός βρέθηκε στην φωτογραφία microscope1.jpg που βρέθηκε σε επόμενο mail όταν ανοίχτηκε στο autopsy σε δεκαεξαδική μορφή. Τα hashes του microscope1.jpg είναι:

MD5: 4be2c4abb48c4389ca798e6c21736ea1

SHA-256: 99d057377f176c010166cde2c3e5ad517a7a3db7443810f048e38e4c32da0b29



Eikόνα 52: microscope1.jpg

Charlie - Autopsy 4.22.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case Keyword Lists Keyword Search

Listing /img_charlie-2009-12-11.E01/vol.vol2/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Sent 3 Results

Table Thumbnail Summary Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
01.zip		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	108438	Allocated	Allocated	unkn
astronaut.jpg		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	722717	Allocated	Allocated	unkn
microscope1.jpg		1		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	136274	Allocated	Allocated	unkn

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of 9 Page Go to Page: 1 Jump to Offset Launch in HxD

```

0x00000000: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 90 .....JFIF.....
0x00000010: 00 90 00 00 FF DB 00 43 00 01 01 01 01 01 01 01 01
0x00000020: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000030: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000040: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000050: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000060: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000070: 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
0x00000080: 70 61 73 73 77 6F 72 64 3D 69 6D 6F 72 74 61 password=immortal
0x00000090: 6C 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 FF C0
0x000000A0: 00 11 00 02 65 01 73 03 01 22 00 02 11 01 03 11
0x000000B0: 01 FF C0 00 1F 00 00 01 05 01 01 01 01 01 01 00
0x000000C0: 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09
0x000000D0: CA 08 FF C4 00 B5 10 00 02 01 03 03 02 04 03 05
0x000000E0: 05 04 04 00 00 01 70 01 02 03 00 04 11 05 12 21
0x000000F0: 31 41 06 13 51 61 07 22 71 14 32 01 91 A1 08 23 1A..Qa..q.2...#
0x00000100: 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B...R..3Bkr....
0x00000110: 10 19 1A 25 26 27 20 29 2A 34 35 36 37 38 39 3A ...%`!)*456789:
0x00000120: 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJKLMNOPQRSTUVWXYZ
0x00000130: 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijklmnopqrstuvwxyz
0x00000140: 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99
0x00000150: 8A 87 81 84 85 88 89 8A 8B 8B 87 83 84 85 86 87

```

Eikόνα 53: Στεγανάλυση microscope1.jpg κωδικός immortal



US006982168B1

(12) United States Patent
Topalian et al.(10) Patent No.: US 6,982,168 B1
(45) Date of Patent: Jan. 3, 2006(54) IMMORTAL HUMAN PROSTATE
EPITHELIAL CELL LINES AND CLONES
AND THEIR APPLICATIONS IN THE
RESEARCH AND THERAPY OF PROSTATE
CANCER

(75) Inventors: Suzanne L. Topalian, Brookeville, MD (US); W. Marston Linehan, Rockville, MD (US); Robert K. Bright, Portland, OR (US); Cathy D. Vocke, Germantown, MD (US)

(73) Assignee: The United States of America as represented by the Department of Health and Human Services, Washington, DC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 08/913,770

(22) PCT Filed: Jan. 30, 1997

(86) PCT No.: PCT/US97/01430

§ 371 (c)(1),
(2), (4) Date: Sep. 22, 1997

(87) PCT Pub. No.: WO97/28255

PCT Pub. Date: Aug. 7, 1997

Related U.S. Application Data
(60) Provisional application No. 60/011,042, filed on Feb. 2, 1996.(51) Int. Cl.
C12N 15/85 (2006.01)(52) U.S. Cl. 435/325; 435/366; 435/371;
435/384; 435/385; 435/386(58) Field of Classification Search 424/184.1,
424/277.1, 93.7; 435/7.23, 325, 366, 378
See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS

5,026,637 A	6/1991	Soule et al.	435/29
5,376,542 A	12/1994	Schlegel	435/172.2
5,436,152 A	7/1995	Soule et al.	435/240.2
5,443,954 A	8/1995	Reddel et al.	435/7.21
5,462,870 A	10/1995	Chopra	435/240.2
5,576,206 A	11/1996	Schlegel	435/240.2
5,716,830 A	2/1998	Webber et al.	435/6
5,824,488 A	* 10/1998	Webber et al.	435/7.23

FOREIGN PATENT DOCUMENTS

WO	WO 92/16645	10/1992
WO	WO 95/29990	11/1995
WO	WO 95/29994	11/1995

OTHER PUBLICATIONS

Chiarclo, E, Oncogene 16: 541-545, 1998.*
Kelemen. Genes Chromosomes Cancer 11:195-198, 1994.*
Drexler. Leukemia & Lymphoma 9:1-25, 1993.*
Embleton, Immunol. Ser. 23:181-207, 1984.*
Heu, In: Tissue Culture Meth & Applications, Kruse & Patterson, Eds, p. 764, 1973.*
Mustafa O. Int'l. J. Oncol. 8(5):883-888, 1996.*
ATCC Catalogue of Cell Lines & Hybridomas, 6th edition, pp. 145 and 222, 1988.*

Bernardino et al. "Characterization of Chromosome changes in two human prostatic carcinoma cell lines (PC-3 and DU 145) using chromosome painting and comparative genomic hybridization" Cancer Genet. Cytogenet. vol. 96, pp. 123-128, 1997.*

Freshney, Culture of Animal Cells, A manual of basic techniques chapter 13, p. 130, 1983.*

Smith, R. T. "Cancer and the immune system" Clinical Immunology. vol. 41 No. 4, pp. 841-850, Aug. 1994.*

McInerney J. M et al. Gene Therapy 7(8): 653-63, 2000.*

Parda et al. "Neoplastic Transformation of a Human Prostate Epithelial Cell Line by the v-Ki-ras Oncogene", *The Prostate* 23:91-98 (1993).

Hayward et al. "Establishment and Characterization of an Immortalized But Non-Transformed Human Prostate Epithelial Cell Line: BPH-1", *In Vitro Cell Dev. Biol.* 31A:14-24, Jan. 1995.

Castagnetti et al, "Prostate Long-Term Epithelial Cell Lines", *Annals of The New York Academy of Sciences*, vol. 595, pp. 149-164, 1990.

Boudou et al. "Distinct Androgen 5 α -Reduction Pathways in Cultured Fibroblasts and Immortalized Epithelial Cells From Normal Human Adult Prostate", *The Journal of Urology* vol. 152, 226-231, Jul. 1994.

Narayan et al. "Establishment and Characterization of a Human Primary Prostatic Adenocarcinoma Cell Line (ND-1)", *The Journal of Urology*, vol. 148, 1600-1604, Nov. 1992.

Rhim et al. "Stepwise immortalization and transformation of adult human prostate epithelial cells by a combination of HPV-18 and v-Ki-ras", *Proc. Natl. Acad. Sci. USA*, vol. 91, pp. 11874-11878, Dec. 1994.

(Continued)

Primary Examiner—Susan Ungar

Assistant Examiner—Minh-Tam Davis

(74) Attorney, Agent, or Firm—Leydig, Voit & Mayer, Ltd.

(57) ABSTRACT

The present invention relates to immortalized, malignant, human, adult prostate epithelial cell lines or cell lines derived therefrom useful in the diagnosis and treatment of prostate cancer. More particularly, the present invention relates to cloned, immortalized, malignant, human, adult prostate epithelial cell lines and uses of these cell lines for the diagnosis and treatment of cancer. Furthermore, the present invention provides for the characterization of said cell lines through the analysis of specific chromosomal deletions.

21 Claims, 6 Drawing Sheets

United States Patent [19]
Soule et al.

[11] Patent Number: **5,026,637**
[45] Date of Patent: **Jun. 25, 1991**

[54] **IMMORTAL HUMAN MAMMARY
EPITHELIAL CELL LINES**

[76] Inventors: **Herbert Soule**, 6344 Jonathan,
Dearborn, Mich. 48126; **Charles M.
McGrath**, 6669 Beach, Troy, Mich.
48098

[21] Appl. No.: **317,610**

[22] Filed: **Feb. 28, 1989**
(Under 37 CFR 1.47)

[51] Int. Cl.5 **C12Q 1/02; C12Q 1/18;
C12N 5/06**

[52] U.S. Cl. **435/29; 435/32;
435/172.1; 435/240.1; 435/240.2; 436/63;
436/813**

[58] Field of Search **435/29, 23, 7, 320,
435/6, 252.8, 219, 32, 172.1, 240.1, 240.2;
436/63, 813; 536/27; 935/9; 424/85.2, 85.1,
85.8, 85.91, 1.1; 514/317, 428, 648; 530/14, 395,
415, 829**

[56] **References Cited**
PUBLICATIONS

Jones et al., Breast Cancer Research Group and Pathology Dept., Michigan Cancer Foundation, Detroit, Mich. 48201, Proceedings of AACR, vol. 29, (Mar. 1988).

In Vitro, vol. 20, No. 8, Aug. 1984, "Calcium Regulation of Normal Human Mammary Epithelial Cell

Growth in Culture", Charles M. McGrath and Herbert D. Soule, pp. 653-662.

In Vitro Cellular & Developmental Biology, vol. 33, No. 1, Jan. 1986, "A Simplified Method for Passage and Long-Term Growth of Human Mammary Epithelial Cells", Herbert D. Soule and Charles M. McGrath, pp. 6-12.

Proceedings of AACR, vol. 29, Mar. 1988, #1780, p. 448.

Primary Examiner—Esther L. Kepplinger
Assistant Examiner—Toni R. Scheiner
Attorney, Agent, or Firm—Robert L. Kelly; Dykema Gossett

[57] **ABSTRACT**

Immortalized human epithelial cell sublines are provided. The novel cell lines do not undergo terminal differentiation and senescence upon exposure to high calcium concentrations. The novel cells exhibit positive reactivity with milk-fat globule membrane antigen and cytokeratin anti-serum. The cells are non-tumorigenic in athymic mice, and exhibit both three-dimensional growth in collagen and dome formation in confluent cultures. The cell sublines demonstrate growth control by hormones and growth factors. The novel cell sublines are useful in evaluating the capacity of preselected agents to bring about a change in epithelial cell growth and in the production of proteins.

3 Claims, 3 Drawing Sheets

Παράρτημα I – Λεξικό Όρων

MD5:

Αλγόριθμος κατακερματισμού (hashing) που παράγει μια μοναδική ακολουθία 128-bit (συνήθως 32 χαρακτήρες σε δεκαεξαδική μορφή) από δεδομένα. Χρησιμοποιείται για την επαλήθευση της ακεραιότητας αρχείων. Θεωρείται πλέον επισφαλής για κρυπτογραφικούς σκοπούς λόγω πιθανών συγκρούσεων (collisions).

SHA-1:

Άλλος αλγόριθμος κατακερματισμού, που παράγει 160-bit hash value. Είναι ασφαλέστερος από τον MD5 αλλά και αυτός έχει θεωρηθεί πλέον ακατάλληλος για κρυπτογραφική ασφάλεια (λόγω επιτυχημένων επιθέσεων). Χρησιμοποιείται ακόμα για επαλήθευση ακεραιότητας αρχείων ή forensic image.

Live acquisition: Απόκτηση δεδομένων ενώ ο υπολογιστής είναι ακόμα ενεργός (π.χ. RAM, δίκτυο).

Volatile data: Δεδομένα που χάνονται όταν ένας υπολογιστής απενεργοποιηθεί, όπως η μνήμη RAM ή οι προσωρινοί πίνακες δικτύου.

Απόκτηση (Acquisition): Η διαδικασία κατά την οποία το ψηφιακό αποδεικτικό υλικό αντιγράφεται, διπλασιάζεται ή αποκτάται ως είδωλο (image).

Ανάλυση (Analysis): Η αξιολόγηση των αποτελεσμάτων της εξέτασης με σκοπό την εξαγωγή χρήσιμων ή αποδεικτικών στοιχείων για την υπόθεση.

BIOS: Βασικό Σύστημα Εισόδου/Εξόδου. Ένα σύνολο οδηγιών αποθηκευμένο στη μνήμη ROM που επιτρέπει την εκκίνηση του λειτουργικού συστήματος και την επικοινωνία με τις συσκευές του υπολογιστή, όπως ο σκληρός δίσκος, το πληκτρολόγιο, η οθόνη, ο εκτυπωτής κ.λπ.

CD-RW: Επαναεγγράψιμος οπτικός δίσκος, στον οποίο μπορούν να αποθηκευτούν και να διαγραφούν δεδομένα πολλές φορές.

CMOS: Ημιαγωγός οξειδίου μετάλλου συμπληρωματικού τύπου. Τσιπ που χρησιμοποιείται για την αποθήκευση ρυθμίσεων του BIOS.

Συμπιεσμένο Αρχείο (Compressed file): Αρχείο του οποίου το μέγεθος έχει μειωθεί μέσω αλγορίθμου συμπίεσης για εξοικονόμηση χώρου. Το αρχείο πρέπει να αποσυμπιεστεί για να είναι αναγνώσιμο από τα περισσότερα προγράμματα.

Αντίγραφο (Copy): Πιστή αναπαραγωγή των πληροφοριών ενός φυσικού αντικειμένου, ανεξάρτητα από την αρχική ηλεκτρονική συσκευή αποθήκευσης. Περιεχόμενο διατηρείται, αλλά ορισμένα χαρακτηριστικά μπορεί να αλλάξουν.

Διεγραμμένα Αρχεία (Deleted files): Αρχεία που έχουν διαγραφεί σκόπιμα, συχνά για την απόκρυψη ενοχοποιητικών στοιχείων. Ωστόσο, με κατάλληλες τεχνικές, μπορούν συχνά να ανακτηθούν εν μέρει ή πλήρως από ειδικούς.

Ψηφιακό Αποδεικτικό Υλικό (Digital evidence): Πληροφορία αποθηκευμένη ή μεταδιδόμενη σε δυαδική μορφή που μπορεί να χρησιμοποιηθεί σε δικαστικές διαδικασίες.

Ακριβές Αντίγραφο (Duplicate): Ψηφιακή αναπαραγωγή όλων των δεδομένων ενός μέσου αποθήκευσης, με πλήρη διατήρηση περιεχομένου και χαρακτηριστικών (bit stream, bit copy).

Ηλεκτρομαγνητική Παρεμβολή (Electromagnetic interference): Παρεμβολή που μπορεί να επηρεάσει αρνητικά τη λειτουργία ηλεκτρονικών συσκευών.

Κρυπτογράφηση (Encryption): Διαδικασία μετατροπής ενός μηνύματος σε μορφή που δεν μπορεί να διαβαστεί χωρίς το κατάλληλο κλειδί, για την προστασία των δεδομένων.

Εξέταση (Examination): Τεχνική διαδικασία που καθιστά τα δεδομένα ορατά και έτοιμα για ανάλυση. Περιλαμβάνει δοκιμές για τον εντοπισμό ή μη συγκεκριμένων στοιχείων.

Ανωμαλία Ονόματος Αρχείου (File name anomaly): Μη αντιστοιχία μεταξύ του ονόματος/επέκτασης του αρχείου και του περιεχομένου του.

File Slack: Ο χώρος ανάμεσα στο λογικό τέλος ενός αρχείου και το τέλος του τελευταίου τομέα που του έχει αποδοθεί.

Δομή Αρχείου (File structure): Ο τρόπος με τον οποίο μια εφαρμογή αποθηκεύει δεδομένα μέσα σε ένα αρχείο.

Σύστημα Αρχείων (File system): Ο τρόπος με τον οποίο το λειτουργικό σύστημα παρακολουθεί και οργανώνει τα αρχεία σε έναν δίσκο.

Forensically Clean: Ψηφιακά μέσα καθαρισμένα από μη απαραίτητα ή υπολειμματικά δεδομένα, ελεγμένα για ιούς και επαληθευμένα πριν από τη χρήση.

Hashing: Η εφαρμογή μαθηματικού αλγορίθμου σε δεδομένα ώστε να παραχθεί ένας μοναδικός αριθμητικός δείκτης (hash value) που αντιπροσωπεύει τα δεδομένα.

Host Protected Area (HPA): Προστατευμένο τμήμα σε IDE δίσκους που δεν είναι προσβάσιμο από το λειτουργικό σύστημα, σύμφωνα με το πρότυπο ATA.

IDE: Ενσωματωμένα Ηλεκτρονικά Δίσκου. Διεπαφή επικοινωνίας που χρησιμοποιείται συνήθως με συσκευές αποθήκευσης.

Είδωλο (Image): Ψηφιακή αναπαράσταση όλων των δεδομένων ενός μέσου αποθήκευσης, συμπεριλαμβανομένων μεταδεδομένων (π.χ. CRC, hash value).

ISP (Πάροχος Υπηρεσιών Διαδικτύου): Οργανισμός που παρέχει πρόσβαση στο διαδίκτυο.

Διεύθυνση MAC (MAC address): Μοναδικός αριθμός που είναι ενσωματωμένος σε κάθε κάρτα δικτύου για σκοπούς αναγνώρισης.

MO (Magneto-Optical): Μέσο αποθήκευσης που συνδυάζει μαγνητική και οπτική τεχνολογία για δημιουργία αντιγράφων ασφαλείας.

Δίκτυο (Network): Σύνολο υπολογιστών που συνδέονται μεταξύ τους για ανταλλαγή πληροφοριών και κοινή χρήση πόρων.

Αρχικό Αποδεικτικό Υλικό (Original evidence): Το φυσικό αντικείμενο και τα δεδομένα του όπως κατασχέθηκαν.

Προστασία με Κωδικό (Password protected): Αρχεία που απαιτούν κωδικό πρόσβασης για να ανοιχτούν. Συχνά η προστασία αυτή μπορεί να παρακαμφθεί από ειδικούς.

Διαταγή Διατήρησης (Preservation Order): Νομικό έγγραφο που απαιτεί από ένα άτομο ή εταιρεία να διατηρήσει ενδεχόμενα αποδεικτικά στοιχεία.

Ιδιωταγές Λογισμικό (Proprietary software): Λογισμικό που ανήκει σε συγκεκριμένο πρόσωπο ή εταιρεία και απαιτεί άδεια χρήσης.

Αφαιρούμενα Μέσα (Removable media): Μέσα αποθήκευσης που μπορούν να αφαιρεθούν εύκολα (π.χ. CD, DVD, USB, κασέτες).

SCSI: Διεπαφή επικοινωνίας που χρησιμοποιείται με ορισμένα είδη αποθηκευτικών συσκευών.

Στεγανογραφία (Steganography): Τεχνική απόκρυψης ενός αρχείου μέσα σε άλλο με τρόπο που δεν είναι άμεσα αντιληπτός.

Διαχειριστής Συστήματος (System Administrator): Το άτομο που έχει δικαιώματα εποπτείας και πλήρους πρόσβασης σε ένα υπολογιστικό σύστημα.

Μη Δεσμευμένος Χώρος (Unallocated space): Τμήματα του δίσκου που δεν έχουν εκχωρηθεί σε ενεργά αρχεία αλλά μπορεί να περιέχουν υπολειμματα παλαιών αρχείων.

Προστασία Εγγραφής (Write protection): Μέθοδοι που αποτρέπουν την εγγραφή δεδομένων σε κάποιο μέσο