



ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΑΝΑΠΤΥΞΗ & ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ψηφιακά Πειστήρια

Τελική Εργασία

Νικόλαος Αργυρίου f3312301

Ελευθέριος Γεωργιάδης f3312304

Ευάγγελος Γκίνης f3312303

Επιβλέπων Καθηγητής: Ντούσκας Θεόδωρος

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή	5
1. Προετοιμασία	7
2. Ανίχνευση και Εντοπισμός	11
2.1 Άφιξη στο χώρο	11
2.2 Συνεντεύξεις.....	11
2.3 Καταγραφή Χώρου	12
2.4 Καταγραφή και Φωτογράφιση πηγών πειστηρίων	13
3. Διαφύλαξη	15
3.1 Διαφύλαξη μνήμης πειστηρίου H/Y Laptop	16
3.2 Διαφύλαξη δίσκου πειστηρίου H/Y Laptop	16
3.3 Διαφύλαξη USB πειστηρίου H/Y Laptop	16
3.4 Συγκέντρωση αποτελεσμάτων	16
3.5 Προετοιμασία και μεταφορά πειστηρίων στο εργαστήριο.....	17
4. Ανάλυση	21
4.1 Ανάλυση περιεχομένων μνήμης H/Y Laptop	21
4.2 Ανάλυση περιεχομένων δίσκου H/Y Laptop	22
4.3 Ανάλυση περιεχομένων USB	28
5. Παρουσίαση	31
Παράρτημα Α – Αρχική Συνομιλία	42
Παράρτημα Β – Συνεντεύξεις	42
Συνέντευξη με τον Υπεύθυνο ασφάλειας (CISO) της εταιρείας	42
Συνέντευξη με τον IT Administrator(Terry) της εταιρείας	43
Συνέντευξη με τον πιθανό δράστη (Charlie)	44
Παράρτημα Γ – Διαφύλαξη πειστηρίων	45
Παράρτημα Δ – Ανάλυση μνήμης H/Y Laptop	52
Παράρτημα Ε – Ανάλυση δίσκου H/Y Laptop	54

Παράρτημα ΣΤ – Ανάλυση USB	71
Παράρτημα Ζ – Εξοπλισμός Εργαστηρίου	74
Hardware Εξοπλισμός	74
Software Εξοπλισμός	80
Παράρτημα Η – RACI Matrix	82
Παράρτημα Θ – Chain of Custody Φόρμα	84
Παράρτημα Ι – Νομοθεσία	85
Παράρτημα ΙΑ – Σύμβαση	86
Παράρτημα ΙΒ – Καταγραφή φόρμας σκληρού δίσκου	87
Παράρτημα ΙΓ – Εικόνες	89
Παράρτημα ΙΔ – Πίνακες	90
Λεξικό Όρων	91
Βιβλιογραφία	92

Εισαγωγή

Η υπόθεση ξεκινάει όταν η εταιρεία M57Biz δέχεται τηλεφώνημα από την αστυνομία. Η ενημέρωση ήταν ότι ο υπάλληλος εν ονόματι Charlie απείλησε παλιό πελάτη της M57Biz, τον Andy, απαιτώντας χρηματικό ποσό. Η απειλή επρόκειτο για διαρροή δεδομένων. Εάν ο Andy δεν έδινε ένα δεδομένο χρηματικό ποσό, ο Charlie θα δημοσίευε πατέντες οι οποίες θα ανέτρεπαν την εταιρεία του Andy – SWEXPERT – από τον ανταγωνισμό.

Η εταιρεία M57 αναζητάει πατέντες εκ μέρους άλλων εταιρειών όπου είναι πελάτες της. Συγκεκριμένα, απασχολεί ερευνητές προκειμένου να αναζητούν σε ιστοσελίδες κατοχύρωσης πατέντων ερευνητικά έγγραφα για τα θέματα που φάχνουν. Η εταιρεία τον τελευταίο καιρό έκανε αναζητήσεις για quantum cryptography, teleportation, immortality, cryogenics.

Για αυτό το λόγο, αναθέτει στην ομάδα διερεύνησης ψηφιακών πειστηρίων “Crime Seen” την ανάλυση και εξιχνίαση του εγκλήματος. Ως επιπλέον πληροφορίες, ο οργανισμός αναφέρει ότι το γραφείο του πιθανού δράστη βρίσκεται στην δεξιά γωνία ενός «open-space» γραφείου, στον 1ο όροφο. Ο πιθανός ένοχος, δουλεύει κυρίως σε εταιρικό laptop προκειμένου να πηγαίνει σε πελάτες ή σε συνέδρια. Την ημέρα που η ομάδα διερεύνησης φτάνει στο χώρο βρίσκει το laptop στο γραφείο του ενεργοποιημένο και ένα USB στο γραφείο. Ακόμη, η είσοδος στους χώρους της εταιρίας παρακολουθείται από Access Card system. Παρόντες στη σκηνή του η-εγκλήματος ήταν ο Υπεύθυνος Ασφάλειας της εταιρίας (CISO), ο IT Admin και ο πιθανός δράστης (Charlie).

Η ομάδα “Crime Seen” αποτελείται από έναν Expert Witness (**Αργυρίου Νικόλαος**) και δύο Technical Witnesses (**Γκίνης Ευάγγελος, Γεωργιάδης Ελευθέριος**). Το κάθε μέλος αναλαμβάνει διαφορετικές αρμοδιότητες στο κομμάτι της έρευνας, οι οποίες θα αναλυθούν παρακάτω (βλ. [Παράρτημα Η](#)). Οι πρακτικές που ακολουθεί η ομάδα είναι συμβατές με βάση τα διεθνή πρότυπα και πρακτικές (ACPO Guidelines).

Η διαδικασία εξιχνίασης διασπάται σε πέντε διακριτά στάδια, καθένα το οποίο είναι εξίσου σημαντικό και απαραίτητο για τη σωστή διεξαγωγή της έρευνας. Πιο συγκεκριμένα, οι φάσεις είναι:

- Προετοιμασία
- Ανίχνευση και Εντοπισμός
- Διαφύλαξη
- Ανάλυση
- Παρουσίαση

και εκτελούνται σειριακά. Στις επόμενες σελίδες, θα αναλυθεί το κάθε βήμα ξεχωριστά και αναλυτικά.

Επιπρόσθετα, κατά την διεξαγωγή της έρευνας στο εργαστήριο της ομάδας, διαπιστώθηκε ότι ο Charlie διέπραξε και δεύτερο έγκλημα, το οποίο αφορά και πάλι πελάτη της M57Biz. Ο Charlie εργαζόταν σε μία πατέντα για την εταιρεία Nitroba. Μέσω email επικοινώνησε με ανταγωνιστή της Nitroba, την project2400, και έναντι χρηματικού ποσού διέρρευσε πληροφορίες για τις πατέντες της Nitroba.

Για την εκπλήρωση των παραπάνω, ο Charlie χρησιμοποίησε λογισμικό το οποίο κρυπτογραφεί αρχεία, και με στεγανογραφία κρύβει πληροφορία μέσα σε αρχεία. Μάλιστα, ανιχνεύθηκαν:

- Σε μία εικόνα, στεγανογραφία
- Σε ένα zip αρχείο, κρυπτογραφία και προστασία με κωδικό
- Σε μία άλλη εικόνα, κρυμμένη μία πρόταση με τον κωδικό πρόσβασης για το παραπάνω zip αρχείο

Σχετικά με τον συγκεκριμένο τύπο ηλεκτρονικού εγκλήματος:

Πρόκειται για πραγματοποίηση απειλής εκ των έσω, δηλαδή για insider. Ως insider ορίζουμε «οποιοδήποτε άτομο είχε ή έχει εξουσιοδοτημένη πρόσβαση στο Πληροφοριακό Σύστημα (Π.Σ.) ενός οργανισμού και προβαίνει σε χρήση η οποία αντίκειται στους κανόνες που ορίζει η πολιτική ασφάλειας του οργανισμού». Ένας insider μπορεί να:

- Διαρρεύσει δεδομένα
- Αλλοιώσει δεδομένα
- Κατασκοπεύσει την επιχειρηματική δραστηριότητα του οργανισμού
- Εκβιάσει άλλα μέλη του προσωπικού, κ.ά.

Στην περίπτωση της εταιρείας M57Biz, ο insider είναι ο Charlie, και ως εργαζόμενος στην εταιρεία, ανακάλυψε νέες πατέντες οι οποίες αποτελούν απόρρητο της εταιρείας. Απείλησε μέσω email ότι θα διαρρεύσει τα αρχεία εάν δεν του αποδοθεί ένα συγκεκριμένο ποσό λύτρων (100χιλ. ευρώ). Προσπάθησε επίσης να έρθει σε επαφή με ανταγωνιστές ώστε να τους πουλήσει την πατέντα της εταιρείας M57Biz.

1. Προετοιμασία

Η ομάδα σε αυτό το στάδιο καλείται να δώσει απαντήσεις σε συγκεκριμένα ερωτήματα. Για τη σωστή διεξαγωγή όλης της έρευνας είναι πολύ σημαντικό το συγκεκριμένο στάδιο, καθώς λάθη σε αυτή τη φάση μπορεί να αποφανθούν καταστροφικά για την συνέχεια.

Απαραίτητο είναι να:

1. Συγκεντρωθούν οι απαραίτητες άδειες και συμβάσεις που αποδεικνύουν την δικαιοδοσία της ομάδας στο να προβεί στην διερεύνηση και εξιχνίαση του ηλεκτρονικού εγκλήματος, για την εταιρεία M57Biz.
2. Γίνει επικοινωνία με τους υπεύθυνους της εταιρείας M57Biz έτσι ώστε να ληφθούν αρχικές πληροφορίες για την φύση του η-εγκλήματος.
3. Κληθούν τα κατάλληλα άτομα ώστε να γίνει διακριτός καθορισμός ρόλων και η διαμόρφωση της ομάδας η οποία θα διερευνήσει το η-έγκλημα.
4. Επιλεχθούν τα κατάλληλα εργαλεία (λογισμικό και υλικό) που θα χρησιμοποιηθούν κατά την διαδικασία.
5. Ενημερωθεί η ομάδα σχετικά με την ισχύουσα νομοθεσία για την φύση του συγκεκριμένου η-εγκλήματος (data leakage).
6. Αποφασιστεί η διαδικασία βάσει της οποίας θα πραγματοποιηθεί η έρευνα με στόχο τη συλλογή του μέγιστου αριθμού των αποδείξεων στον ελάχιστο δυνατό χρόνο, ελαχιστοποιώντας τις επιπτώσεις στο θύμα.

Αναλυτικότερα:

1. Συγκέντρωση απαραίτητων εγγράφων και συμβάσεων. Σε αυτό το σημείο ο Expert Witness λαμβάνει την επίσημη σύμβαση από την εταιρεία, που εξουσιοδοτεί την ομάδα "Crime Seen" να διεξάγει την έρευνα. Ο Expert Witness διαβάζει με προσοχή τους όρους της σύμβασης και υπογράφει το έγγραφο. Η σύμβαση περιλαμβάνει τη δικαιοδοσία που δίνεται στα μέλη της ομάδας, τους όρους της συμφωνίας όπως χρηματική αμοιβή, διασφάλιση εμπιστευτικότητας κ.α. Το έντυπο της σύμβασης που έστειλε η εταιρεία M57Biz είναι προσφέρεται ως επισυναπτόμενο έγγραφο (βλ. [Παράρτημα IA](#)).
2. Πρώτη επικοινωνία με την εταιρεία: Ο Expert Witness ενημερώνεται από την εταιρεία τηλεφωνικώς για το συμβάν. Πιο συγκεκριμένα, η εταιρεία σε αυτό το σημείο ενημερώνει λεπτομερώς για το τι έχει γίνει και απαντάει. Η συνομιλία είναι καταγεγραμμένη στο [Παράρτημα A](#). Η σημαντική πληροφορία που αποκομίστηκε ήταν ότι το έγκλημα έχει να κάνει με data leakage από insider στην εταιρεία με χρήση απειλητικών email. Τότε ενεργοποιείται η κατάλληλη πολιτική η οποία έχει

εδραιωθεί σε προηγούμενο χρόνο, κατά τον σχεδιασμό του Incident Handling Procedure.

3. **Σύσταση Ομάδας ρόλοι και Αρμοδιότητες:** Όπως έχει ήδη αναφερθεί η ομάδα που διεξάγει την έρευνα αποτελείται από τον Expert Witness και από δύο Technical Witnesses. Το κάθε μέλος είναι υπεύθυνο για διαφορετικά μέρη της έρευνας. Για τον καθορισμό των ρόλων θα χρησιμοποιηθεί το RACI (Responsible Accountable Consulted Informed) Matrix. Ο πίνακας αναγράφεται σε παράρτημα παρακάτω (βλ. [Παράρτημα H](#)).
4. Τώρα, με βάση τις πληροφορίες που έχει ήδη συλλέξει η ομάδα καλείται να αποφασίσει ποια εργαλεία λογισμικού, υλικού, και λοιπού σχετικού εξοπλισμού θα χρησιμοποιήσει ώστε να μπορέσει να πραγματοποιήσει αποτελεσματικά την έρευνα, διασφαλίζοντας ότι θα ακολουθήσουν τις βέλτιστες και ταυτόχρονα νόμιμες πρακτικές. Παρακάτω φαίνεται ένα checklist με τα εργαλεία αυτά.

Forensic Equipment	
○	Λάπποπ με εγκατεστημένα τα απαραίτητα προγράμματα για forensics <ul style="list-style-type: none">i. FTK Imager για λήψη πιστού αντίγραφου μνήμης και δίσκουii. Εργαλεία αναπαραγωγής βίντεοiii. Εργαλεία επεξεργασίας εγγράφων
○	Bootable USBs με έξτρα forensics tools
○	Υλικό αποθηκευτικού χώρου με επαρκή χωρητικότητα για αποθήκευση πειστηρίων <ul style="list-style-type: none">i. HDD 1ii. HDD 2iii. USB Type Civ. SD Card
○	Wi-Fi Detector
○	Οδηγοί Οπτικών Μέσων (CD/DVD readers)
○	Καλώδια συνδεσιμότητας (usb type c, micro usb κλπ.)
○	Καλώδια δικτύων
Εργαλεία για αποσυναρμολόγηση υλικού υπολογιστών/κινητών συσκευών	
○	Κατσαβίδια
○	Κοφτάκια
○	Πένσες
○	Τσιμπιδάκια

○	Smartphone Repair Tool Kit
Εργαλεία και υλικά για μεταφορά και πακετάρισμα	
○	Χαρτάκια/Ταμπέλες με αναγνωριστικό αποδεικτικού
○	Κλωβοί Faraday για απομόνωση κινητών τηλεφώνων
○	Power banks
○	Ψηφιακή κάμερα για λήψη φωτογραφιών και βίντεο
○	Ζελοτέιπ
○	Αδιάβροχες και αντιστατικές σακούλες
○	Evidence tape
○	Χάρτινα κουτιά
Λοιπός εξοπλισμός	
○	Γάντια
○	Μάσκες
○	Στυλό / Μαρκαδόροι
○	Σημειωματάρια
○	Λαστιχάκια
○	Μεγεθυντικοί φακοί

5. Ενημέρωση ομάδας για την ισχύουσα νομοθεσία για την φύση του συγκεκριμένου η-εγκλήματος: Η ομάδα οφείλει να ενημερωθεί για την νομοθεσία. Οι ενέργειες που έγιναν στο συγκεκριμένο περιστατικό μπορεί να χαρακτηριστούν ως παραβίαση ασφάλειας δεδομένων, κακόβουλη διαρροή πληροφοριών, κατασκοπεία επιχειρηματικών μυστικών και εκβιασμός. Μπορούν να αποτελέσουν ποινικά αδικήματα όπως παραβίαση απορρήτου, κλοπή πνευματικής ιδιοκτησίας, εκβιασμός και παραβίαση εμπιστευτικών συμφωνιών. Επίσης, εφόσον η αποκάλυψη των μυστικών προκάλεσαν σημαντική οικονομική ή όποια άλλη ζημιά στην εταιρία (π.χ., ζημία στο κύρος αυτής) έχει το δικαίωμα να εγείρει αγωγή εναντίον του μέσω των διατάξεων περί αδικοπραξίας (ά. 914 ΑΚ) και τα φυσικά πρόσωπα μπορούν να αιτηθούν αποκατάσταση για ηθική βλάβη. Τέλος όλοι ενημερώθηκαν για την άρση ευαίσθητων προσωπικών δεδομένων σε περίπτωση που αυτό κριθεί σκόπιμο.
6. Η ομάδα οφείλει να ελαχιστοποιήσει την ζημιά στο θύμα ενώ ταυτόχρονα μεγιστοποιείται το όφελος από την πληροφορία που λαμβάνεται σε κάθε βήμα της διαδικασίας για την εξιχνίαση του εγκλήματος. Το σενάριο πλέον είναι γνωστό, έχουν ληφθεί τα απαραίτητα μέτρα και η πολιτική και οι διαδικασίες είναι προκαθορισμένες για τον τύπο αυτού του η-εγκλήματος. Για να επιτευχθεί ο στόχος αυτός, η ομάδα όταν καταφτάσει στον τόπο του εγκλήματος θα ακολουθήσει τα εξής βήματα οπτικοποιημένα στο παρακάτω διάγραμμα:



Εικόνα 1 Βήματα Διαδικασίας

2. Ανίχνευση και Εντοπισμός

2.1 Άφιξη στο χώρο

Στις **08:56** η ομάδα έφτασε στον χώρο του πιθανού εγκλήματος. Επιβεβαιώνεται ότι ο χώρος σφραγίστηκε. Παρόντες στο χώρο βρέθηκαν ο Υπεύθυνος Ασφάλειας της εταιρίας, ο IT Admin και ο πιθανός δράστης. Αμέσως τότε ξεκίνησε η διαδικασία των συνεντεύξεων ξεχωριστά στον καθένα και η διαδικασία αποτύπωσης του χώρου και των πιθανών ψηφιακών και μη πειστηρίων.

2.2 Συνεντεύξεις

Στις **09:10** ξεκίνησε η συνέντευξη του CISO της εταιρείας. Λήφθηκε γενική γνώση για κάποιες παραμέτρους ασφαλείας της εταιρείας. Ο χώρος φυλάσσεται από Access Card system και κάμερες ασφαλείας και εφαρμόζεται least privilege principle κάθε χρήστη εντός του domain.

Στις **09:34** χρειάστηκε να κληθεί ο IT Admin της εταιρείας για τις ερωτήσεις τεχνικής φύσεως. Από τον IT Admin έγιναν γνωστές πληροφορίες για το domain της εταιρείας. Ο πάροχος υπηρεσιών email και identity management γίνεται από την Microsoft. Δόθηκε η τοπολογία του δικτύου καθώς και διάγραμμα του open space χώρου.

Στις **09:58** ξεκίνησε η συνέντευξη του Charlie (πιθανού ύποπτου). Δεν λογοδότησε εξαρχής στην συνέντευξη, αρνήθηκε να δώσει πληροφορίες για το ίδιο το έγκλημα, καθώς και μερικές πιο προσωπικές. Δήλωσε ικανοποιημένος με τις συνθήκες εργασίας του.

Στις **10:20** τελείωσαν όλες οι συνεντεύξεις.

Στο [Παράρτημα Β](#) φαίνονται οι συνεντεύξεις αναλυτικά.

2.3 Καταγραφή Χώρου

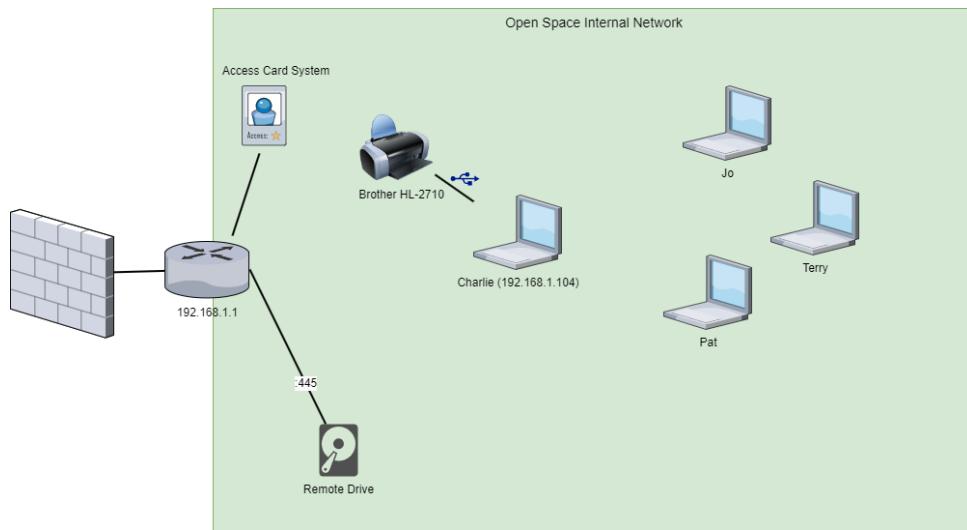
Στις **10:21** ξεκίνησε η καταγραφή του χώρου. Δόθηκε σχετικό σχεδιάγραμμα.



Εικόνα 2 Κάτοψη χώρου εταιρείας M57

Στην εταιρεία οι υπάλληλοι εργάζονται σε open space χώρο, που σημαίνει ότι δεν υπάρχει προκαθορισμένο γραφείο για τον κάθε υπάλληλο. Αντ' αυτού, υπάρχει ένας ενιαίος χώρος στον οποίο εργάζονται, και επιλέγει ο καθένας το γραφείο στο οποίο επιθυμεί να δουλέψει. Όταν έγινε γνωστοποίηση του η-εγκλήματος, ο Charlie βρισκόταν στην δεξιά γωνία του χώρου. Εκεί βρέθηκε το εταιρικό του laptop ανοιχτό και δίπλα του το USB stick (ένδειξη κόκκινου κύκλου πάνω δεξιά στην εικόνα).

Στις **10:40** έγινε λεπτομερής καταγραφή της τοπολογίας δικτύου του χώρου.



Εικόνα 3 Τοπολογία δικτύου της εταιρείας

Παραπάνω φαίνεται η τοπολογία του δικτύου. Περιλαμβάνει:

- Router που λειτουργεί και ως Wi-Fi access point
- Firewall για DMZ δίκτυο στον όροφο του open space
- To Access Card System επικοινωνεί με το router για να μπορεί να στέλνει logs τα οποία καταγράφονται
- Remote network location <\\192.168.1.1\m57\ram>

Δεν υπάρχουν άλλα access points ή δικτυακές συσκευές.

Δεν υπήρξε συσκευή στην οποία απαγορεύτηκε πρόσβαση στην ομάδα διερεύνησης.

2.4 Καταγραφή και Φωτογράφιση πηγών πειστηρίων

Όπως προαναφέρθηκε, στο γραφείο του Charlie βρέθηκε το laptop του και ένα usb stick.

Στις **08:58** φωτογραφήθηκε η πρώτη πηγή πειστηρίων, το laptop του Charlie. Στην παρακάτω εικόνα φαίνεται φωτογραφία του laptop όπως ακριβώς βρέθηκε. Δεν ήταν συνδεδεμένα καλώδια για παροχή δικτύου. Το καλώδιο τροφοδοσίας ρεύματος ήταν συνδεδεμένο. Δεν φαινόντουσαν ανοιχτά προγράμματα να τρέχουν, ή εικονίδια.



Εικόνα 4 Οθόνη στο laptop του Charlie, όπως αυτή βρέθηκε

Στις **09:00** φωτογραφήθηκε η δεύτερη πηγή πειστηρίων, το USB. Παρακάτω φαίνεται φωτογραφία του USB στο γραφείο, όπως ακριβώς βρέθηκε.



Εικόνα 5 USB δίπλα από το laptop του Charlie, όπως αυτό βρέθηκε

Συλλεχθέντες πηγές πειστηρίων (artifacts):

Είδος συσκευής	Κατάσταση
Laptop	Ενεργό
USB	Αποσυνδεδεμένο

Πίνακας 1 Πηγές Πειστηρίων

3. Διαφύλαξη

Στο στάδιο αυτό καλούμαστε να πάρουμε τα πιστά αντίγραφα που μας ενδιαφέρουν. Συγκεκριμένα αυτά περιλαμβάνουν:

1. Πιστό αντίγραφο μνήμης
2. Πιστό αντίγραφο σκληρού δίσκου
3. Πιστό αντίγραφο USB

Για να γίνει αυτό χρησιμοποιούνται τα εργαλεία:

- mdd_1.3
- Access Data FTK Imager 4.7.1.2

Θα χρησιμοποιηθούν και τα δύο εργαλεία για να λάβουμε διπλά αντίγραφα μνήμης. Οι τεχνικές λεπτομέρειες αποτυπώνονται στο [Παράρτημα Γ.](#)

Στις **08:58** προετοιμάστηκε ο εξοπλισμός που χρειαζόμασταν για την διαφύλαξη των πειστηρίων του συγκεκριμένου εγκλήματος. Οι technical experts έπειτα από συζήτηση χρησιμοποίησαν συγκεκριμένο USB stick από το οποίο περιέχει το απαιτούμενο λογισμικό.

Στις **08:59** συνδέθηκε το USB της ομάδας στο laptop. Δίνονται τεχνικές λεπτομέρειες του USB των technical experts:

	
Κατασκευάστρια εταιρεία	Samsung
Μοντέλο	Fit Plus
Ονομασία/Ταμπέλα	LiveForensicsTools (F:\)
Χωρητικότητα	64 GB
Serial No.	AA000000000000489
Εγκατεστημένα προγράμματα	<ul style="list-style-type: none">• Access Data FTK Imager 4.7.1.2• mdd_1.3• Encase• Volatility 2.4• LiveResponseCollection

MD5 Hash	62ed973d963913bb55111a7b8116ace1
SHA1 Hash	c950059e02a519e254e1bcfeed662e5691e79cdb

Πίνακας 2 Forensics Team USB Flash

3.1 Διαφύλαξη μνήμης πειστηρίου H/Y Laptop

Στις **08:59** ξεκίνησε η διαδικασία διαφύλαξης μνήμης με το εργαλείο FTK Imager.

Μόλις τελειώσει η διαδικασία θα πρέπει να έχουμε τα αρχεία στο directory που επιλέξαμε.

Στις **09:20** ξεκίνησε η λήψη πιστού αντιγράφου μνήμης με το εργαλείο mdd_1.3.

3.2 Διαφύλαξη δίσκου πειστηρίου H/Y Laptop

Στις **09:30** ξεκίνησε η διαδικασία διαφύλαξης δίσκου με το εργαλείο FTK Imager. Κρίθηκε ότι για το δεδομένο μέγεθος δίσκου, ο χρόνος επαρκεί για να εκτελεστεί το imaging στον τόπο του εγκλήματος.

3.3 Διαφύλαξη USB πειστηρίου H/Y Laptop

Στις **10:05** ξεκίνησε η διαδικασία διαφύλαξης USB πειστηρίου με το εργαλείο FTK Imager.

3.4 Συγκέντρωση αποτελεσμάτων

Στις **10:55** παράγονται τα MD5 και SHA1 values των πειστηρίων που συλλέχθηκαν.

Παίρνουμε ένα csv αρχείο, των οποίων τα αποτελέσματα φαίνονται στους παρακάτω πίνακες.

Όνομα αρχείου	charlie-2001-12-11.mddramimage
MD5 value	A70415FC1321E5C5CC145B32F9B871D6

SHA1 value	40B0CF7ADE174B36D508180F38C5271DD4EA289A
-------------------	--

Πίνακας 3 RAM Details



Όνομα αρχείου	charlie-2001-12-11.E01
MD5 value	A459F1AA45941AD4FA22D5CB9D35F7FC
SHA1 value	EE1D5FEBB63DEF90C2900B6984D21A6A137F00CE

Πίνακας 4 HDD Details



Όνομα αρχείου	charlie-work-usb-2001-12-11.E01
MD5 value	8C23941655B3313F4A31A1A66085BE86
SHA1 value	E49BF6048856570CC3D49B1485D6D87AAAB6AB0A

Πίνακας 5 USB Details

3.5 Προετοιμασία και μεταφορά πειστηρίων στο εργαστήριο

Στις **13:50** αφού είχε κριθεί ότι λήφθηκαν όλα τα δεδομένα τα οποία είναι ευάλωτα (δηλ. μπορεί να χαθούν), ξεκίνησε η προετοιμασία μεταφοράς πειστηρίων στο εργαστήριο. Αρχικά, η ομάδα τερμάτισε την λειτουργία του laptop του Charlie. Αποσπάστηκε η μπαταρία και ο σκληρός δίσκος.

Στις **14:00** η συσκευή και τα επιμέρους κομμάτια της τοποθετήθηκαν σε αντιστατικές σακούλες.

Συνολικά, συλλέχθηκαν από την σκηνή του εγκλήματος τα εξής:

- Το laptop του Charlie
- Το USB που ήταν στο γραφείο του Charlie
- Ο σκληρός δίσκος ο οποίος αφαιρέθηκε από έναν technical expert
- Το καλώδιο τροφοδοτικού του laptop
- Η μπαταρία του laptop του Charlie



Εικόνα 6 Charlie's Laptop



Εικόνα 7 Charlie's USB



Eικόνα 8 Charlie's Laptop HDD



Eικόνα 9 Charlie's Laptop Power Supply Unit



Eικόνα 10 Charlie's Laptop Battery

Για την ασφαλή μεταφορά των αντικειμένων, πρώτα τα αφήσαμε να κρυώσουν. Το κάθε ένα από αυτά τοποθετήθηκε σε αντιστατική σακούλα ξεχωριστά. Αποθηκεύτηκαν ασφαλώς σε ένα σκληρό χάρτινο κουτί. Το λάπποπ τοποθετήθηκε στο κάτω μέρος, και τα υπόλοιπα από πάνω για να αποφευχθούν ζημιές.

Στις **15:00** η ομάδα έφτασε στο εργαστήριο, όπου και παρέδωσε το κατασχεθέν υλικό. Αποφασίστηκε ότι η εργαστηριακή έρευνα θα ξεκινήσει την επόμενη ημέρα. Η ομάδα πριν φύγει από το εργαστήριο ενημέρωσε την Chain of Custody φόρμα, έφτιαξε τριπλό αντίγραφο(ένα για κάθε μέλος) του πιστού για τη μνήμη, το δίσκο και το USB ώστε να δουλέψει πάνω σε αυτά κατά τη διάρκεια της έρευνας. Τέλος, το υλικό αποθηκεύτηκε με ασφάλεια σε κατάλληλα διαμορφωμένο χώρο στο εργαστήριο.

4. Ανάλυση

Την επόμενη ημέρα, στις **12/12/2009** ώρα **09:00** ξεκίνησε η το στάδιο της ανάλυσης. Θα πρέπει να αναλυθούν τα πειστήρια της μνήμης, του δίσκου και του USB και να μεγιστοποιηθεί η ωφέλιμη πληροφορία που δύναται να εξαχθεί. Για τους σκοπούς αυτούς, στο εργαστήριο χρησιμοποιήθηκε υπολογιστής με λειτουργικό σύστημα Windows 10.

4.1 Ανάλυση περιεχομένων μνήμης H/Y Laptop

Σε αυτό το στάδιο γίνεται ανάλυση των volatile data(ώρα **09:20**). Πιο συγκεκριμένα, έχοντας πάρει από τον ανοιχτό υπολογιστή στον τόπο του εγκλήματος το memory dump επιστρέφουμε στο εργαστήριο για να κάνουμε ανάλυση της μνήμης με το εργαλείο volatility. Στόχος αυτής της φάσης είναι να πάρουμε όσες περισσότερες πληροφορίες μπορούμε για το ανοιχτό μηχάνημα, που δεν θα μπορούσαμε να πάρουμε από την ανάλυση του δίσκου. Οι τεχνικές λεπτομέρειες της έρευνας για τη μνήμη βρίσκονται στο Παράρτημα Δ.

Στις **09:21** ο αρμόδιος τεχνικός ανέλαβε να ξεκινήσει να τρέχει τις εντολές του εργαλείου volatility. Αρχικά ξεκίνησε με την εντολή *imageinfo* η οποία επιστρέφει το λειτουργικό σύστημα και την έκδοσή του. Ασφαλώς προέκυψε ότι είναι Windows XP όπως γνωρίζαμε, και η ώρα συστήματος.

Στις **09:30** με την εντολή *pslist* εντοπίστηκαν οι διεργασίες (τα προγράμματα) οι οποίες ήταν ενεργές την ώρα που λήφθηκε το dump. Σημαντικό εύρημα ήταν το **Mozilla Thunderbird** (είναι email client) με process id (αναγνωριστικό διεργασίας) 188. Οι υπόλοιπες ήταν κατά κύριο λόγο διεργασίες των Windows XP.

Στις **09:40** με την εντολές *cmdline*, *cmdscan*, *consoles* ελέγχουμε την δραστηριότητα μέσω τερματικού. Αξιοσημείωτη είναι η εντολή *mdd_1.3.exe -o z:lcharlie-2009-12-11.ram* η οποία εκτελέστηκε από τους technical experts με τερματικό το οποίο ξεκίνησαν οι ίδιοι, για να πάρουν το dump της μνήμης στον τόπο του εγκλήματος.

Στις **10:00** τρέχουμε τις εντολές *sockets*, *connscan* για να δούμε τις ανοιχτές συνδέσεις που υπήρχαν εκείνη την ώρα, ή και συνδέσεις που άνοιξαν αλλά τερμάτισαν. Βρίσκουμε διάφορες IP διευθύνσεις για την διεργασία 188 (Thunderbird), οι οποίες δεν ανήκουν στο εύρος διευθύνσεων (address space) της εταιρείας M57Biz. Σημειώνονται οι ip διευθύνσεις: 63.245.209.10, 198.189.255.73, 192.168.1.1, 208.97.132.223, 63.245.221.11.

Στις **10:20** εκτελούμε την εντολή *hashdump* για να βρούμε τα NTLM Hashes των κωδικών πρόσβασης των χρηστών του μηχανήματος.

Στις **10:30** εκτελούμε την εντολή *filescan* για να βρούμε αρχεία τα οποία ήταν φορτωμένα στην μνήμη, από το file system (σύστημα αρχείων σκληρού δίσκου). Βασικά ευρήματα ήταν τα αρχεία *Inbox.msf*, *Sent.msf*, *Trash.msf* και *Unsent Messages.msf*, τα οποία είναι όλα αρχεία που περιέχουν emails από την εφαρμογή Thunderbird. Παίρνουμε dump των αρχείων αυτών (δηλαδή τα εξάγουμε από το image αρχείο της μνήμης) και τα αποθηκεύουμε για ανάλυση.

4.2 Ανάλυση περιεχομένων δίσκου H/Y Laptop

Σε αυτό το σημείο διερευνάται ο δίσκος του Laptop που ανήκει στον πιθανό δράστη(ώρα **11:00**). Δίνεται απάντηση σε όλα τα απαραίτητα για το case ερωτήματα όπως ορίζουν οι προβλεπόμενες πρακτικές. Από την ανάλυση δίνεται απάντηση στις εξής θεματικές περιοχές:

- 1) Χαρακτηριστικά του Υπολογιστή και Δομή των Partitions. Η ανάλυση των partitions)έδειξε ότι ο υπολογιστής είχε ένα κύριο partition, όπου ήταν εγκατεστημένο το λειτουργικό σύστημα. Ταυτοποιήθηκαν τα hash values για όλες τις εικόνες (MD5 & SHA-1), παρέχοντας μια βάση για την εξασφάλιση της ακεραιότητας των δεδομένων κατά την διάρκεια της έρευνας. Επιπλέον, επαληθεύτηκε ότι οι κατακερματισμοί απόκτησης και επαλήθευσης συμφωνούσαν.
- 2) Λειτουργικό Σύστημα και Δικτύωση. Το εγκατεστημένο λειτουργικό σύστημα ήταν Windows XP, με ημερομηνία και ώρα εγκατάστασης στις 2009-11-08 17:25:47. Ο καταχωρημένος ιδιοκτήτης επιβεβαιώθηκε ότι ήταν ο βασικός ύποπτος Charlie. Η ζώνη ώρας ήταν Pacific Daylight Time. Το όνομα του υπολογιστή ήταν M57-Charlie. Η πληροφορία των δικτύων περιλάμβανε ένα δίκτυο με διεύθυνση IP που είχε ανατεθεί από DHCP.
- 3) Λογαριασμοί Χρήστη και Δραστηριότητα Συστήματος. Οι λογαριασμοί χρήστη που βρέθηκαν περιλάμβαναν τον Administrator, τον Charlie και το Help Assistant με τον Charlie να είναι ο τελευταίος που συνδέθηκε στο PC. Η τελευταία καταγεγραμμένη διακοπή (shutdown) ήταν στις 2009-12-11 09:09:57. Οι εφαρμογές που είχαν εγκατασταθεί μετά την εγκατάσταση του λειτουργικού περιλάμβαναν δημοφιλή προγράμματα όπως τα Mozilla, Thunderbird, Invisible Secrets...
- 4) Πληροφορίες σχετικά με τους Web Browsers και τις Αναζητήσεις και επικοινωνίες μέσω e-mail.
- 5) Εξωτερικές Συσκευές: Ανιχνεύθηκαν εξωτερικές συσκευές, όπως USB sticks, που συνδέθηκαν στον υπολογιστή.

Οι λεπτομέρειες της έρευνας για τον δίσκο βρίσκονται στο [Παράρτημα E](#).

Email

Αρχικά, δεδομένης της γνώσης του case, ξεκινήσαμε να διαβάζουμε τα email του Charlie. Το εργαλείο Autopsy τα εμφανίζει σε ειδική κατηγορία. Στην φάση αυτή τα ευρήματα είναι πολλά και **σημαντικά**. Παρατηρείται ότι το εταιρικό του email (charlie@m57.biz) το χρησιμοποιούσε για να επικοινωνεί και με προσωπικές του επαφές. Παρατίθενται συνοπτικά με χρονολογική σειρά:

2009-11-16, 11:02:37: ο Pat καλωσορίζει τον Charlie στην εταιρεία

2009-11-17, 10:33:39: ο Pat κλείνει συμβόλαιο με την εταιρεία Nitroba, με τον CEO της Alex, για έρευνα σε δύο πατέντες. Ο Charlie αναλαμβάνει την πατέντα των χρονομηχανών (time machines) και ο Ιο της τηλεμεταφοράς (teleportation).

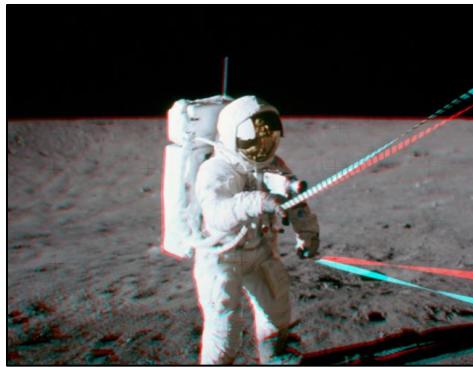
2009-11-17, 10:54:17: ο Charlie στέλνει email στον Ιο σχολιάζοντας την συμπεριφορά του Pat (την επόμενη ημέρα, στις 2009-11-18 10:01:50, ο Ιο απαντάει και συμφωνεί).

2009-11-30, 08:54:27: ο Ιο στέλνει email στον Charlie, με επισυναπτόμενο ένα pdf αρχείο το οποίο είναι πατέντα για την έρευνα της τηλεμεταφοράς, ρωτώντας τον Charlie πώς του φαίνεται αυτή η πατέντα.

2009-12-01, 13:02:34: Ο Charlie στέλνει email σε προσωπική του επαφή (alix.pery@yahoo.com), με θέμα «Pack your bags», λέγοντας ότι θα μπορέσουν να πάνε διακοπές, και ότι θα αγοράσει ένα αυτοκίνητο.

2009-12-02, 13:04:29: Ο Charlie στέλνει email στην διεύθυνση jaimie@project2400.com η οποία ανήκει στην εταιρεία **project2400** (ανταγωνίστρια της Nitroba), λέγοντας ότι «έχει κάπι που τους ενδιαφέρει», «αφορά ανταγωνιστή», «γνωρίζουν την **τιμή του**», και «να διαγράψουν αυτό το email». Αμέσως μετά του στάλθηκε αυτοματοποιημένο email από το domain της project2400, για αποτυχία παράδοσης email στην διεύθυνση jaimie@project2400.com. Στις κεφαλίδες του email βρέθηκε η ip διεύθυνση 208.97.132.222 (email server της project2400), η οποία βρέθηκε στις ανοικτές συνδέσεις στην ανάλυση μνήμης (βλ. [4.1 Ανάλυση περιεχομένων μνήμης Η/Y Laptop](#)). Αργότερα ξαναέστειλε το ίδιο email στην διεύθυνση jaimie@project2400.com.

2009-12-03, 09:51:33: Ο Jamie από την project2400 απαντάει λέγοντας ότι «θα του δώσουν 50χιλ.», «θα βάλουν 10χιλ. για αρχή, και τα υπόλοιπα όταν δουν το υλικό». Την ίδια μέρα ο Charlie απαντάει με μία επισυναπτόμενη εικόνα, λέγοντας «οι **οδηγίες για το άνοιγα, μόλις δει και την επόμενη κατάθεση**».



Εικόνα 11α Εύρημα Αλληλογραφίας (astronaut1.jpg)

2009-12-04, 09:41:47: Ο Charlie **απειλεί** τον Andy από την swexpert (andy@swexpert.com) ότι «θα δημοσιεύσει πληροφορία η οποία θα ακυρώσει την τρέχουσα πατέντα τους (Immortality)». Ζητάει 100χιλ., και να «μην ανακατεύσουν την αστυνομία αλλιώς θα πλήξει την επιχείρηση δημοσιεύοντας τα αρχεία». Επισυνάπτει ένα **κρυπτογραφημένο** συμπιεσμένο αρχείο (01.zip), προστατευμένο με **κωδικό**.

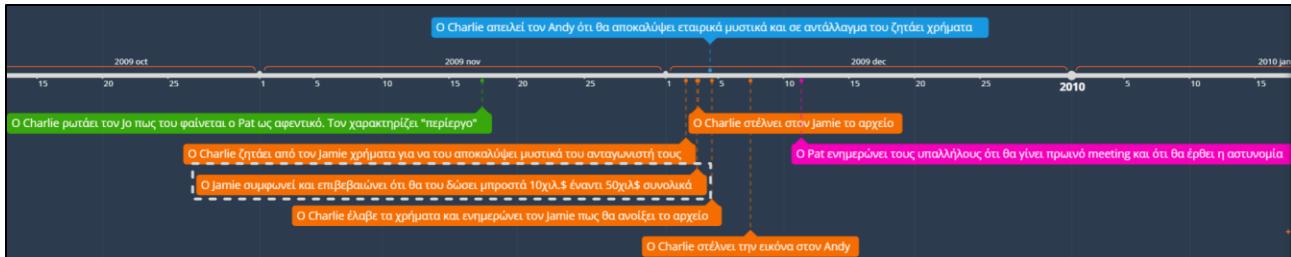
Στις 13:06:23 την ίδια ημέρα, ξαναστέλνει email στον Jamie από την **project2400**, αναφέροντας ότι «έλαβε την κατάθεση», «να χρησιμοποιήσει το steg πρόγραμμα, για το οποίο μιλήσανε, με κωδικό **nitro**», και «να διαγράψει αυτά τα email».

2009-12-07, 11:44:18: Ο Charlie στέλνει μία εικόνα που «είχε υποσχεθεί» στον Andy.



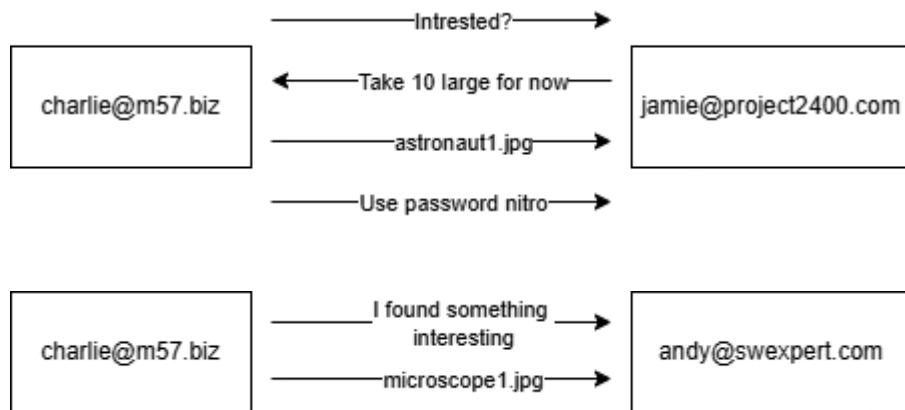
Εικόνα 12β Εύρημα Αλληλογραφίας (microscope1.jpg)

2009-12-11, 08:55:53: Ο Pat ενημερώνει του Charlie, Jo και Terry ότι πρέπει να έχουν ένα meeting, διότι έλαβε τηλεφώνημα από την αστυνομία.



Εικόνα 13 Timeline Αλληλογραφίας

Συνοπτικά, στις επόμενες εικόνες βλέπουμε την επικοινωνία με τις project2400 και SWEXPERT:



File System

ΣΤΙΣ **13:00** ξεκινάμε να ερευνούμε το file system (σύστημα αρχείων) του δίσκου. Πρόκειται για ένα τυπικό Windows XP file system. Ξεκινάμε με τον φάκελο του χρήστη Charlie.

Κατάλογος /img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Desktop: βρίσκουμε τον φάκελο web, ο οποίος περιέχει μέσα το αρχείο patentauto.py και 7 .txt αρχεία. Το python αρχείο πρόκειται για πρόγραμμα το οποίο με αυτοματοποιημένο τρόπο αναζητά πληροφορία στον browser Mozilla Firefox. Συγκριμένα, τις ώρες:

- 09:00-10:00, 13:00-14:00 και 16:00-17:00 έψαχνε περιεχόμενο από το αρχείο urls_personal.txt, το οποίο περιέχει συνδέσμους με αυτοκίνητα, εφημερίδες, σελίδες για αναζήτηση πατέντων κ.ά.
- 10:00-12:00 και 14:00-16:00 έψαχνε online περιεχόμενο από το αρχείο patentterms.txt.

Κατάλογος /img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/**Start Menu/Programs**: βρίσκουμε έναν φάκελο από ένα πρόγραμμα Hex Editor (Cygnus Hex Editor).

Κατάλογος Κατάλογος /img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/**My Documents**: σε αυτόν τον κατάλογο βρίσκουμε τα εξής αρχεία:

- 6 pdf σχετικά με τις έρευνες του Charlie
- Τις εικόνες *astronaut.jpg* και ***astronaut1.jpg***. Η *astronaut1.jpg* είναι η ίδια η οποία στάλθηκε με email, όπως αναφέρθηκε παραπάνω (επαλήθευση μέσω MD5 και SHA1 hash).
- Τις εικόνες *microscope.jpg* και ***microscope1.jpg***. Η *microscope1.jpg* είναι η ίδια η οποία στάλθηκε με email, όπως αναφέρθηκε παραπάνω (επαλήθευση μέσω MD5 και SHA1 hash).
- Το αρχείο ***01.zip*** το οποίο είναι το ίδιο με αυτό το οποίο στάλθηκε στην project2400 με email, όπως αναφέρθηκε παραπάνω (επαλήθευση μέσω MD5 και SHA1 hash). Ήταν κρυπτογραφημένο και προστατευμένο με κωδικό πρόσβασης. Βλέπουμε ότι το αρχείο αυτό περιέχει έναν φάκελο με όνομα *Immortality*, και μέσα εκεί τα αρχεία *Thumbs.db*, *us005026637-001.tif*, *us006982168-001.tif*.

Επιπρόσθετα βρίσκουμε τους καταλόγους:

- /Downloads: περιέχει διάφορα αρχεία εγκατάστασης προγραμμάτων, csv αρχεία με δεδομένα, εκτελέσιμα, και 2 pdf
- /Nitroba: περιέχει το αρχείο “Nitroba work.odt” στο οποίο είναι σημειώσεις για πατέντες/ευρήματα για την έρευνα της Nitroba περί της χρονομηχανής.
- /Patents: περιέχει τα Method_of_real_time_machine_path_plannin.pdf και Time_machine_time_puzzle.pdf τα οποία είναι υπάρχουσες πατέντες για χρονομηχανές.
- /Quantum Cryptography: φάκελος για έρευνα της εταιρείας περί Κβαντικής Κρυπτογραφίας.

Κάδος Ανακύκλωσης / Recycler

Στις **14:00** αναλύουμε τον κάδο ανακύκλωσης.

Στον κατάλογο /img_charlie-2009-12-11.E01/vol_vol2/**RECYCLER**/ υπάρχει το περιεχόμενο του κάδου ανακύκλωσης για διαγεγραμμένα αρχεία. Βλέπουμε τον φάκελο S-1-5-21-682003330-329068152-1644491937-1003 (το SID του Charlie, βλ. [Παράρτημα Ε](#), ερώτημα 6). Μέσα σε αυτόν τον φάκελο βρίσκουμε το αρχείο INFO2 περιέχει δύο φορές την καταχώρηση C:\Documents and Settings\Charlie\My Documents\Immortality,

και τον φάκελο *Dc1*, ο οποίος περιέχει το *us006982168-001.tif* (ίδιο όνομα αρχείο που υπάρχει στο *01.zip*).

Άρα, στον κατάλογο */img_charlie-2009-12-11.E01/vol_vo12/Documents and Settings/Charlie/My Documents* υπήρχε ένας φάκελος με όνομα *Immortality* και δύο αρχεία.

Εκτυπώσεις / Print Spooler Artifacts

ΣΤΙΣ **14:30** ελέγχουμε για τυχόν εκτυπώσεις.

Για αυτό κοιτάζουμε τον κατάλογο */img_charlie-2009-12-11.E01/vol_vo12/WINDOWS/system32/spool/PRINTERS*, αλλά ο φάκελος είναι κενός.

Στοιχεία Φυλλομετρητών / Internet Artifacts

ΣΤΙΣ **14:40** ελέγχουμε την δραστηριότητα μέσω Internet.

Μέχρι τις 2009-11-12 το laptop είχε μόνο Internet Explorer εγκατεστημένο. Έπειτα εγκαταστάθηκε o Mozilla Firefox.

Ιστορικό περιήγησης: Συνοπτικά βρήκαμε αναζητήσεις για:

- Εγκατάσταση του Mozilla Thunderbird
- PATENTSCOPE
- Google Patents (γενικά διάφορες σελίδες για αναζήτηση πατεντών)
- Σελίδες από τουριστικά γραφεία (διακοπές στα Fiji)
- **Στεγανογραφία και εργαλεία (tools) για εκτέλεση τεχνικών στεγανογραφίας (InvisibleSecrets2)**
- Εργαλείο για την προβολή .tiff αρχείων(AlternaTIFF)
- Εταιρεία πώλησης αεροσκαφών(Gulfair)
- Wipo.int
- Πωλήσεις οχημάτων πολυτελείας
- Ιστοσελίδα τουριστικού θέρετρου στα Fiji Islands
- Εγκατάσταση του 7-zip
- Εργαλείο Hex-Editor
- Πατέντες σχετικές με το project Immortality

Σελιδοδείκτες / Bookmarks

Internet Explorer: οι προεπιλεγμένοι (default) της εγκατάστασης.

Mozilla Firefox: οι προεπιλεγμένοι (default), κάποιοι που αφορούν ιστοσελίδες με πατέντες, και ένας σελιδοδείκτης σε ιστοσελίδα με αυτοκίνητα.

Εγκατεστημένα Προγράμματα

Αναφορικά, βρέθηκαν:

- Mozilla Firefox
- Mozilla Thunderbird
- Πρόγραμμα εκτυπωτή Brother HL-2170W v1.00
- 7-zip v4.65
- Invisible Secrets 2.1
- Python 2.6.4
- OpenOffice 3.1
- Internet Explorer
- AVG

Ανάλυση ευρημάτων email

Στις 15:00 με χρήση εργαλείων αναλύθηκαν τα microscope1.jpg, astronaut1.jpg, 01.zip. Οι τεχνικές λεπτομέρειες βρίσκονται στο [Παράρτημα E](#). Από την ανάλυση προέκυψε ότι:

1. Το αρχείο astronaut1.jpg που στάλθηκε στην project2400 με τεχνική στεγανογραφίας, περιείχε μέσα του ένα άλλο αρχείο, το “Nitroba work.odt”, το οποίο έχει αναφερθεί παραπάνω στην ενότητα αυτή.
2. Το αρχείο 01.zip ήταν κρυπτογραφημένο και κλειδωμένο με κωδικό πρόσβασης. Ο κωδικός πρόσβασης αυτός υπάρχει κρυμμένος μέσα στο αρχείο microscope1.jpg και είναι η λέξη “immortal”. Με αυτόν τον κωδικό ξεκλειδώνουμε το 01.zip και βλέπουμε ότι μέσα στο zip αρχείο υπάρχουν δύο .tif αρχεία

4.3 Ανάλυση περιεχομένων USB

Έχοντας αναλύσει τη μνήμη και τον σκληρό δίσκο με το Autopsy, ξεκινάμε και την ανάλυση του USB(ώρα 16:30). Το USB αν και έχει πολύ λιγότερο όγκο πληροφορίας σε σχέση με το δίσκο και τη μνήμη, σε καμία περίπτωση δεν πρέπει να παραλειφθεί από την έρευνα, καθώς μπορεί σε αυτό να περιλαμβάνονται ουσιαστικά πειστήρια για την επιτυχημένη διερεύνηση του εγκλήματος.

File System

Στις 16:40 ξεκινάμε την ανάλυση διερευνώντας το File System του USB. Το File System είναι τύπου NTFS. Αρχικά παίρνουμε πληροφορίες για τα partitions της μνήμης του USB. Βλέπουμε ότι το USB είναι χωρισμένο σε δύο volumes(vol1, vol2), τα οποία καταλαμβάνουν τα sectors 0-0 και 1-2068479 αντίστοιχα. Το πρώτο partition πιθανόν να είναι built-in στο USB από τον κατασκευαστή. Στο δεύτερο partition περιέχεται όλη η πληροφορία που μας ενδιαφέρει.

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol₁_vol2/**Email**:

Το μεγαλύτερο μέρος της δεσμευμένης μνήμης του USB αποτελείται από τα emails του ύποπτου. Πιο συγκεκριμένα, ο ύποπτος έχει κρατήσει αρχείο όλων των συνομιλιών μεταξύ των συναδέλφων καθώς και των αντιπροσώπων των εταιρειών που φαίνεται να επιχειρεί να διαρρεύσει τα δεδομένα. Αυτό συμβάλλει στην επιβεβαίωση της ενοχής του ως έναν βαθμό, διότι απορρίπτεται το ενδεχόμενο κάποιος τρίτος να έχει στείλει τα email από τον υπολογιστή του. Ακόμη βλέπουμε και τις ηλεκτρονικές διευθύνσεις ταχυδρομείου με τις οποίες έχει έρθει σε επαφή ο ύποπτος. Μαζί με τα emails υπάρχουν τα pdfs από τις έρευνες που έχει φαίνεται να έχει σκοπό να δώσει στους ανταγωνιστές της εταιρείας.

Πρέπει ακόμα να αναφερθεί ότι βρίσκονται και τα ονόματα κάποιων αρχείων που έχουν διαγραφεί από τον χρήστη, τα ονόματα των οποίων είναι Charlie_2009-11-20_1303_Sent.txt, Charlie_2009-11-20_1305_Received_Part1.2. Καταλαβαίνουμε ότι αυτά είναι πιθανά emails τα οποία για κάποιο λόγο ο ύποπτος έχει επιλέξει να διαγράψει.

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol_vo2/**01.zip**:

Ενδιαφέρον έχουν ακόμα, τα zipped αρχεία που περιέχει το USB. Ο ύποπτος έχει σε συμπιεσμένη μορφή και κωδικοποιημένο τον φάκελο Immortality που περιέχει δύο αρχεία .tif . Ωστόσο, ο φάκελος είναι διαθέσιμος σε άλλο path κάνοντας εφικτό να δούμε τα αρχεία που φαίνεται να είναι αυτά που ήθελε να διαρρεύσει. Ο ύποπτος διατηρεί λοιπόν αρχείο με τα απόρρητα δεδομένα τόσο σε συμπιεσμένη όσο και κανονική μορφή.

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol_vo2/**Nitroba work.odt**:

Περιέχει τις σημειώσεις για πατέντες/ευρήματα για την έρευνα της Nitroba περί της χρονομηχανής.

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol_vo2/**Immortality**:

Σε αυτό το φάκελο περιέχονται τα papers της έρευνας της εταιρείας σε όχι καθαρή μορφή, χωρίς να ζητείται κάποιος κωδικός πρόσβασης ή να είναι σε συμπιεσμένη μορφή.

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol_vo2/**\$Extend**, /Charlie-work-usb-2009-12-11.E01/vol_vo2/**\$Unalloc**,/Charlie-work-usb-2009-12-11.E01/vol_vo2/\$ 11.E01/vol_vo2/**\$OrphanFiles**:

Αυτοί οι φάκελοι είναι built-in κρυφοί του usb και περιέχουν logs για πληροφορίες της συσκευής και της δραστηριότητας του χρήστη σε μορφή όμως μη αναγνώσιμη.

Κατάλογοι /Charlie-work-usb-2009-12-11.E01/vol_vo2/**\$Unalloc**

Φαίνεται ότι είναι κάποιο διαγραμμένο αρχείο. Δεν παίρνουμε πολλές σημαντικές πληροφορίες. Να αναφερθεί ότι το αρχείο είχε δεσμεύσει μεγάλο χώρο μνήμης(Size:10210304000 Bytes).

Κατάλογος /Charlie-work-usb-2009-12-11.E01/vol_vo2/**invsecr2.exe**:

Τέλος, βρίσκουμε και ένα εκτελέσιμο αρχείο με όνομα `invsecr2.exe` το οποίο το αφού το εξάγουμε και το τρέχουμε τοπικά στον υπολογιστή μας. Διαπιστώνουμε ότι είναι ένα εργαλείο το οποίο δίνει τη δυνατότητα να κωδικοποίησης μιας φωτογραφίας. Μαζί με το εκτελέσιμο είναι και κάποιες περίεργες φωτογραφίες, οι οποίες περιέχονται και στον σκληρό δίσκο και είναι πιθανόν αυτές που αντάλλαξε ο ύποπτος με τους jamie@project2400.com, andy@swexpert.

Analysis Results

Το Autopsy μας παρέχει κάποια εργαλεία ανάλυσης που μας βοηθάνε στην έρευνα, καθώς αναλύουν αρχεία τα οποία είναι δύσκολο για εμάς στην ανάγνωση. Με αυτόν τον τρόπο μας παρέχεται επιπλέον πληροφορία. Στην περίπτωση του USB μας επιστρέφεται μια λίστα όλων των emails που ο ύποπτος έχει αλληλεπιδράσει.

Οι λεπτομέρειες της έρευνας για το USB βρίσκονται στο [Παράρτημα ΣΤ](#).

5. Παρουσίαση

Εισαγωγή

Στις **11/12/2009** η ομάδα “Crime Seen” ανέλαβε από την εταιρεία M57 το έργο της αναζήτησης ψηφιακών πειστηρίων για την παράνομη πράξη που εκτελέστηκε από υπάλληλο της. Ο CEO της εταιρίας M57Biz, ο Pat, ήταν εκείνος ο οποίος ενημέρωσε για το έγκλημα.

Ο σκοπός του έργου είναι να διαπιστωθεί αν ο ύποπτος (Charlie) αποκάλυψε εταιρικά μυστικά ή/και έλαβε χρήματα για αυτά. Για να επιτευχθεί αυτό η ομάδα μετέβη στα γραφεία της εταιρείας M57, πραγματοποίησε συνεντεύξεις με τους παρευρισκόμενους(CISO, IT Admin, Charlie), έλαβε όλα τα ψηφιακά πειστήρια που ήταν διαθέσιμα εκείνη τη στιγμή και την ίδια ημέρα κατάσχεσε κάποιες συσκευές/εξαρτήματα για περαιτέρω ανάλυση.

Η δομή (format) των ημερομηνιών είναι **ηη/μμ/έτος**.

Από τις **12/12/2009** έως και τις **18/12/2009** αναλύθηκαν τα δεδομένα και παρακάτω παρουσιάζονται τα αποτελέσματα ανά κατηγορία.

Πληροφορίες έρευνας:

Όνομα case	<i>Charlie</i>
Αριθμός case	103972641
Ημερομηνία καταχώρησης	12/11/2009 09:30:05 PST
Ημερομηνία έναρξης	12/11/2009 09:30:05 PST
Ημερομηνία τερματισμού	18/11/2009 09:30:05 PST
Examiner	Crime Seen
Οργανισμός	Athens University of Economics and Business
Επικοινωνία	nik.argyriou@aueb.gr e.gkinis@aueb.gr el.georgiadis@aueb.gr

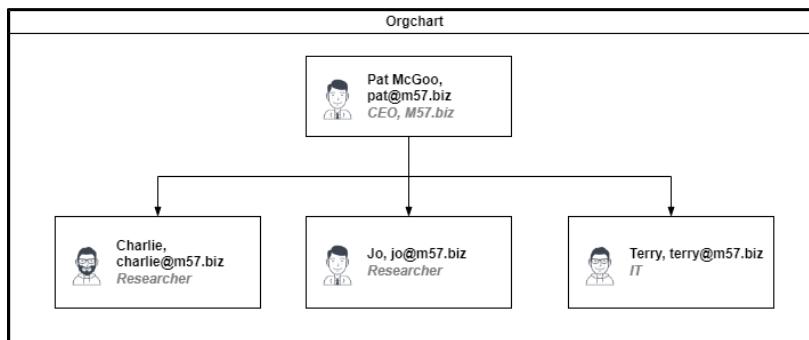
Πίνακας 6 Πληροφορίες Έρευνας

Στοιχεία εταιρείας – θύματος:

Θύμα	M57Biz
Τοποθεσία	M57Biz HQ, Πατησίων 97, 1 ^{ος} όροφος
ΑΦΜ	9996899199
CEO	Pat

Πίνακας 7 Στοιχεία εταιρείας

Η εταιρεία M57Biz έχει ως δραστηριότητα την αναζήτηση patents για πελάτες της. Ο Pat McGoo είναι ο CEO της εταιρείας ενώ οι Charlie, Jo και Terry είναι υπάλληλοι της. Συγκεκριμένα οι Charlie και Jo συμμετέχουν στην αναζήτηση patents ενώ ο Terry είναι IT Admin της εταιρείας.



Εικόνα 14 Οργανόγραμμα Εταιρείας

Περιγραφή Αποδείξεων (Evidence)

Τα στοιχεία τα οποία βρέθηκαν είναι τα εξής

Ποσότητα	Είδος	Αρίθμηση
1	Laptop	001
1	USB	001a
1	HDD	001b
1	Μπαταρία	001c

Πίνακας 8 Πίνακας 10 Evidence

Τα παραπάνω είναι όλες οι πηγές πειστηρίων. Το Laptop του Charlie βρέθηκε ανοιχτό, και το USB αποσυνδεδεμένο, πάνω στο γραφείο του, δίπλα από το laptop.

Οι παρευρισκόμενοι ήταν ο CISO, ο IT Admin (Terry) και ο Charlie.

Όνοματεπώνυμο	Ρόλος	Σχέση με το συμβάν
Terry	IT Admin	Υπό διερεύνηση (αρχικά δεν υπήρχαν κατηγορίες εναντίον του)
Charlie	Εργαζόμενος ερευνητής/υπάλληλος	Κατηγορούμενος για το έγκλημα
-	CISO	Υπό διερεύνηση (αρχικά δεν υπήρχαν κατηγορίες εναντίον του)

Πίνακας 9 Λίστα Παρευρισκόμενων

Η σκηνή του εγκλήματος ήταν στον 1^ο όροφο της εταιρείας. Πρόκειται για έναν οποίος είναι διαμορφωμένος ως open-space χώρος εργασίας, δηλαδή κάθε υπάλληλος επιλέγει σε ποιο γραφείο θα καθίσει να εργαστεί (δεν υπάρχει προκαθορισμένη θέση για τον κάθε ένα ξεχωριστά). Ο Charlie καθόταν στην δεξιά γωνία του χώρου (ένδειξη κόκκινου κύκλου στην εικόνα παρακάτω).

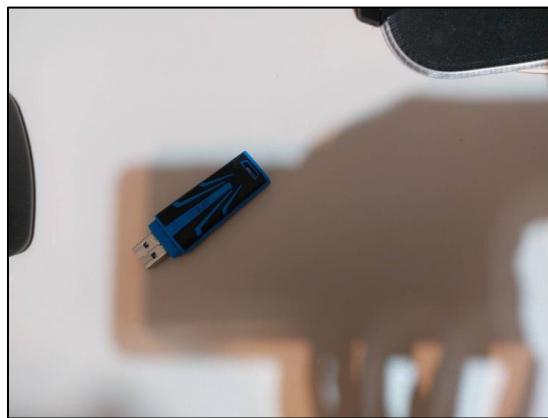


Εικόνα 15 Κάτοψη χώρου εταιρείας M57

Φωτογραφήθηκαν τα στοιχεία (οι πηγές πειστηρίων) στο γραφείο του Charlie.



Εικόνα 16 Οθόνη στο laptop του Charlie, όπως αυτή βρέθηκε



Εικόνα 17 USB δίπλα από το laptop του Charlie, όπως αυτό βρέθηκε

Πειστήριο	Όνομα	SHA1 hash MD5 hash
Μνήμη	charlie-2001-12-11.mddramimage	40B0CF7ADE174B36D508180F38C5271DD4EA289A
		A70415FC1321E5C5CC145B32F9B871D6
Δίσκος	charlie-2001-12-11.E01	EE1D5FEBB63DEF90C2900B6984D21A6A137F00CE
		A459F1AA45941AD4FA22D5CB9D35F7FC
USB	charlie-work-usb-2001-12-11.E01	E49BF6048856570CC3D49B1485D6D87AAAB6AB0A
		8C23941655B3313F4A31A1A66085BE86

Πίνακας 10 Πειστήρια & Hash values

Στοιχείο	Λεπτομέρειες			Σημειώσεις
Laptop (PC)	HW	Type	Physical Machine	HP Pavilion Model 15
		CPU	Intel Duo Core	
		RAM	2 GB	
		HDD Size	60 GB	
		File System	NTFS/exFAT	
		IP Address	192.168.1.104	
	SW (OS)	Operating System	Microsoft Windows XP 5.1	English (32 bits)
USB / Removable Media #1 (RM#1)	HW	Type	USB removable storage device	
		Mfg.	Patriot	
		Model	Exporter USB 3.0	
		Serial No.	5a45ca52-76e3-4eda-8c3a-ad7c0b4fa6a8	Unique serial number
		Size	4 GB	
		File System	NTFS	
		Volume label	F	

Πίνακας 11 Λεπτομέρειες Πειστηρίων

Περιγραφή ανάλυσης evidence

Η έρευνα πραγματοποιήθηκε σύμφωνα με την διεθνή μεθοδολογία ACPO. Κατά τη διάρκεια όλου του έργου εφαρμοστήκαν όλες οι βέλτιστες πρακτικές, τηρήθηκαν όλες οι διαδικασίες που ορίζονται για την σήμανση και την τεκμηρίωση των πειστηρίων ώστε να είναι **αποδεκτά, αυθεντικά, αξιόπιστα, πλήρη και ξεκάθαρα**. Συνοπτικά, παρουσιάζονται μερικές πρακτικές κλειδιά:

- **Ανίχνευση και εντοπισμός**
 - Αφήνουμε τους εκτυπωτές να τελειώσουν με τις εκτυπώσεις τους
 - Δεν ενεργοποιούμε κανένα μηχάνημα
 - Για κλειστά μηχανήματα: σιγουρεύουμε ότι είναι κλειστά, για laptop προσέχουμε ότι μπορεί να ενεργοποιείται εάν ανοίξει το καπάκι
 - Για ανοιχτά μηχανήματα: λαμβάνουμε πειστήρια μνήμης ή/και άλλη πληροφορία που θα χαθεί μόλις κλείσει ο υπολογιστής
 - Ψάχνουμε τον χώρο για επιπρόσθετα στοιχεία (π.χ. σημειωματάρια)
 - Καταγράφουμε λεπτομερώς κάθε κίνηση
- **Διαφύλαξη**
 - Χρησιμοποιούμε μόνο αυθεντικό λογισμικό, και παίρνουμε διπλά τα πιστά αντίγραφα

- Μόνο έμπειρο προσωπικό αποσυναρμολογεί τα μηχανήματα με ειδικό εξοπλισμό
- Κατά την μεταφορά, αποφεύγουμε καταστάσεις στις οποίες τα στοιχεία μπορεί να υποστούν φυσική βλάβη (π.χ., απομακρύνουμε τους σκληρούς δίσκους από θερμαινόμενα καθίσματα, μαγνήτες κλπ., δεν τοποθετούμε laptop δίπλα από το παράθυρο του αυτοκινήτου κλπ.)
- Ο εξοπλισμός φυλάσσεται ασφαλώς στο εργαστήριο

- **Ανάλυση**

- Η ανάλυση γίνεται με μεθοδικό τρόπο, πρώτα συλλέγονται όλα τα αποδεικτικά στοιχεία
- Έπειτα ελέγχονται τα στοιχεία για την ορθότητά τους. Ελέγχονται και κρυμμένα ή παραπομένα αρχεία
- Τα παραπάνω βήμα διεξάγονται πάντα σύμφωνα με την ισχύουσα νομοθεσία

Τα εργαλεία που χρησιμοποιήθηκαν ήταν τα εξής:

Όνομα	Έκδοση	Περιγραφή	Τόπος Χρήσης
Access Data FTK Imager	4.7.1.2	Λήψη πειστηρίων/λήψη πιστών αντιγράφων μνήμης και δίσκου ενός υπολογιστή	Στον τόπο εγκλήματος για λήψη πειστηρίων (live acquisition σε ανοιχτά μηχανήματα) ή στο εργαστήριο για λήψη πειστηρίων από κλειστά μηχανήματα
mdd_1.3	1.3	Λήψη πειστηρίου μνήμης ενός υπολογιστή	Στον τόπο εγκλήματος για λήψη πειστηρίου μνήμης από ανοιχτά μηχανήματα
Volatility Framework	2.6.1	Ανάλυση μνήμης (π.χ., εμφάνιση ενεργών προγραμμάτων για ένα πλέον κλειστό μηχάνημα)	Στο εργαστήριο
Autopsy	4.21.0	Ανάλυση δίσκου ενός υπολογιστή (π.χ., ανάγνωση αποθηκευμένων αρχείων)	Στο εργαστήριο

Πίνακας 12 Εργαλεία

Περιγραφή ανάλυσης evidence

Όπως προαναφέρθηκε, τα στοιχεία η-εγκλήματος είναι ένα laptop και ένα USB. Παρουσιάζονται συνοπτικά στοιχεία υψηλού επιπέδου για κατανόηση της μεγάλης εικόνας.

Στοιχείο laptop	Λεπτομέρειες
Λειτουργικό σύστημα	Windows XP 5.1
#Σκληρών Δίσκων / Χωρητικότητα	1 / 60 GB
# Χρηστών	2 / Administrator & Charlie
#Εγκατεστημένων Προγραμμάτων	113
Δομή Συστήματος Αρχείων (File System)	

Πίνακας 13 Στοιχεία

Λίστα με σημαντικά αρχεία και φακέλους στον δίσκο (εάν έχει κατάληξη, π.χ. .exe, είναι αρχείο, εάν είναι υπογραμμισμένο, είναι φάκελος):

Όνομα	Πλήρες μονοπάτι	Σύντομη Περιγραφή	MD5 τιμή
<u>My Documents</u>	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/My Documents	Περιλαμβάνει διάφορα αρχεία του Charlie σχετικά με τις έρευνες των πελατών της M57Biz.	
01.zip	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/My Documents/01.zip	Συμπιεσμένο κρυπτογραφημένο, προστατευμένο με κωδικό. Περιλαμβάνει τα δεδομένα τα οποία διέρρευσαν	4fa239c22e5fb7b93 4a1bf68e4e0e2e7

microscope1.j pg	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/My Documents/microscope1.jpg	Η ίδια εικόνα με το μικροσκόπιο, μέσα στην οποία είναι κρυμμένος ο κωδικός πρόσβασης για το αρχείο 01.zip (με την τεχνική στεγανογραφίας)	4be2c4abb48c4389 ca798e6c21736ea1
<u>My Documents/Patents</u>	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/My Documents/Patents	Περιέχει τα αρχεία τα οποία διέρρευσαν μέσω του email του Charlie	
<u>Desktop/web</u>	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Desktop/web /	Φάκελος στο Desktop μέσα στον οποίο βρέθηκαν URLs σχετικά με την αναζήτηση πατέντων στο διαδίκτυο	
patentauto.py	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Desktop/web /patentauto.py	Πρόγραμμα python το οποίο αναζητούσε αυτόματα υλικό στο διαδίκτυο από δύο λίστες, την urls_personal.txt και patentterms.txt	865bf7033814cd91 a9bb074e4e52e847
<u>Local Folders</u>	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders	Περιέχει όλο το υλικό για τα email (αποσταλμένα, εισερχόμενα, διαγραμμένα, πρόχειρα)	

Πίνακας 14 Λίστα σημαντικών αρχείων/φακέλων

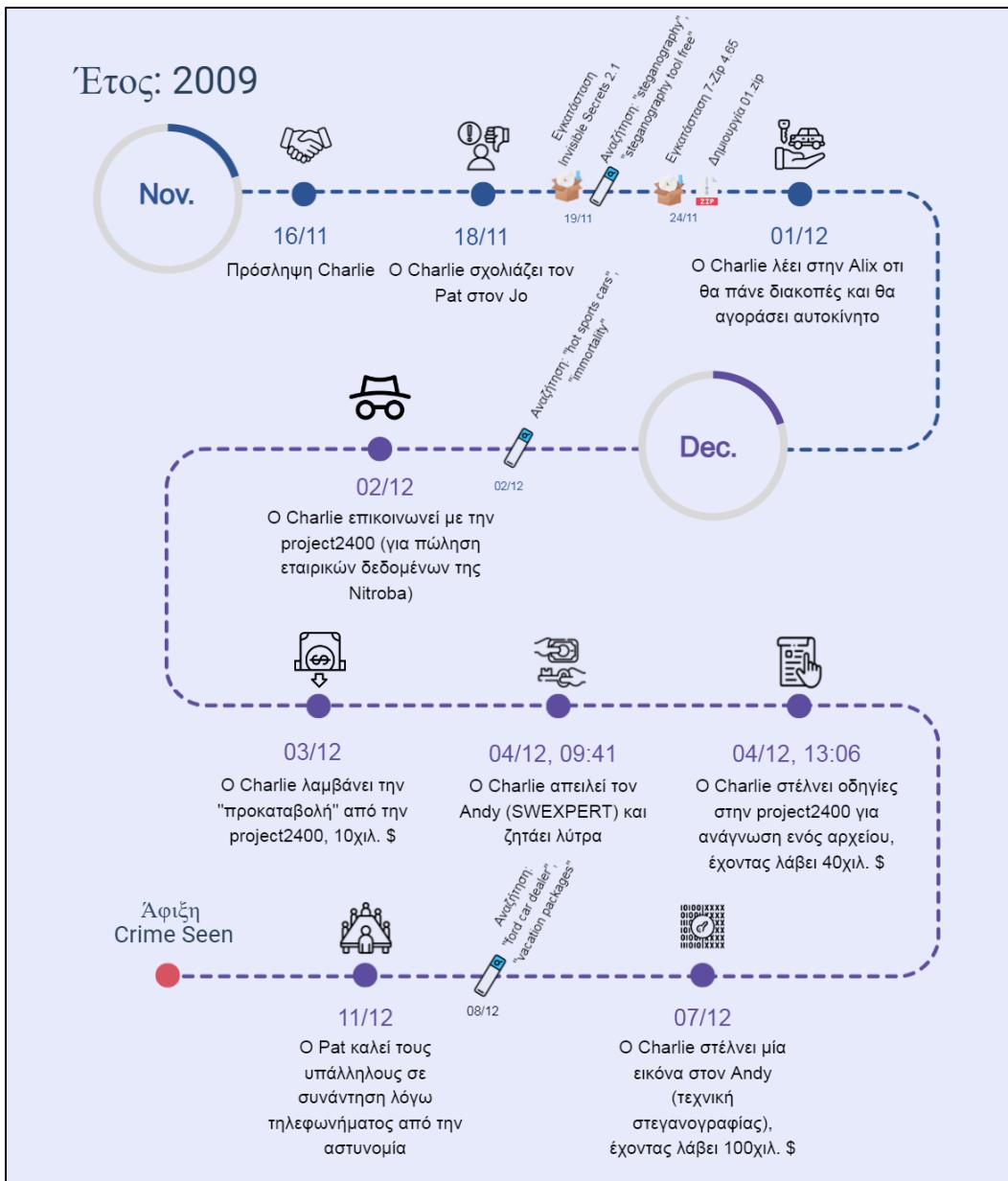
Λίστα με **σημαντικά αρχεία** και φακέλους στο **USB** (εάν έχει κατάληξη, π.χ. .exe, είναι αρχείο, εάν είναι υπογραμμισμένο, είναι φάκελος):

Όνομα	Πλήρες μονοπάτι	Σύντομη Περιγραφή	MD5 τιμή
0.1.zip	/img_charlie-work-usb-2009-12-11.E01/vol_vol2/01.zip/	Συμπιεσμένο αρχείο κρυπτογραφημένο , και προστατευμένο με κωδικό . Περιλαμβάνει τα δεδομένα τα οποία διέρρευσαν (το ίδιο με αυτό στον δίσκο)	Not calculated

<u>Immortality</u>	/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Immortality	Φάκελος που περιέχει τα αρχεία του 0.1.zip μη-κρυπτογραφημένα, μη-προστατευμένα	
<u>Email</u>	/img_charlie-work-usb-2009-12-11.E01/vol_vol2>Email	Φάκελος που περιέχει τα αρχεία του 0.1.zip μη-κρυπτογραφημένα, μη-προστατευμένα	
invsecr2.exe	/img_charlie-work-usb-2009-12-11.E01/vol_vol2/invsecr2.exe	Αρχείο εγκατάστασης για πρόγραμμα το οποίο κρυπτογραφεί/αποκρυπτογραφεί αρχεία, και κρύβει πληροφορία με την τεχνική στεγανογραφίας (και την αποκαλύπτει)	83150daa46ccfe62 a4aeb6c4898905a8

Πίνακας 15 Λίστα σημαντικών αρχείων/φακέλων στο USB

Χρονολογική ταξινόμηση σημαντικών γεγονότων

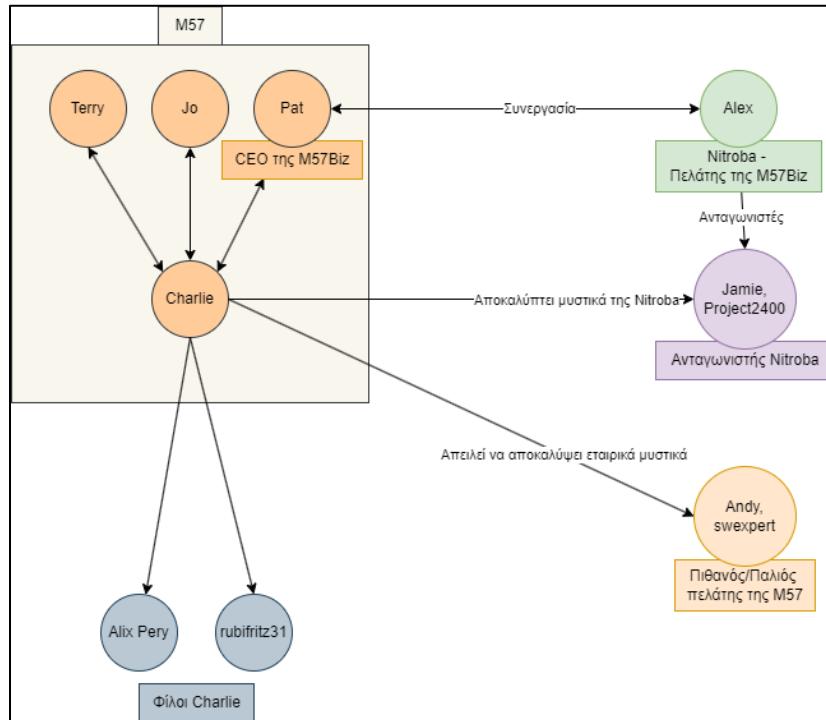


Εικόνα 18 Timeline σημαντικών γεγονότων

Ηλεκτρονική αλληλογραφία του Charlie: Κατόπιν ανάλυσης των αρχείων της αλληλογραφίας φάνηκε ότι ο Charlie εκτός από τις ενδοεταιρικές επικοινωνίες είχε έρθει σε επαφή με φιλικά του πρόσωπα καθώς και με τα δύο (2) θύματα που φαίνεται ότι εκβίαζε:

- 1. Jamie, Project2400:** Ο Charlie απαιτούσε χρήματα από την εν-λόγω εταιρεία ώστε να τους αποστείλει μυστικά για την Nitroba(Ανταγωνίστρια εταιρεία της Project2400)

2. **Andy, swexpert**: Ο Charlie απαιτούσε χρήματα από την εν-λόγω εταιρεία για να μην αποκαλύψει δημόσια κάποια μυστικά της.
3. **Pat, M57**: το αφεντικό του Charlie



Εικόνα 19 Ηλεκτρονική Αλληλογραφία του Charlie

Συμπεράσματα

Εν κατακλείδι, παρουσιάστηκαν τα στοιχεία τα οποία βρέθηκαν και η μεθοδολογία που ακολουθήθηκε για να έρθει η παρούσα έρευνα εις πέρας με αντικειμενικό τρόπο. Η μεθοδολογία του οργανισμού ACPO είναι διεθνώς αποδεκτή και έχει αποδειχθεί η αξία της.

Το υλικό το οποίο κατασχέθηκε και αναλύθηκε, αποδεικνύει πληθώρα ενοχοποιητικών στοιχείων για τον Charlie. Η επικοινωνία μέσω email σε συνδυασμό με την κρυπτογράφηση των δεδομένων στον φορητό του υπολογιστή του αποδίδουν μεγάλο μερίδιο ευθύνης. Ακόμη η επικοινωνία με τους ανταγωνιστές πελατών της εταιρείας M57Biz, εγείρει και άλλες υποψίες.

Τα πειστήρια τα οποία κατατίθενται από την Crime Seen είναι όλα αυθεντικά, αξιόπιστα, πλήρη και ξεκάθαρα. Τον τελικό λόγο τον έχει πάντα το δικαστήριο. Ευθύνη της ομάδας είναι να υπηρετεί την δικαιοσύνη, πάντα, αντικειμενικά.

Παράρτημα Α – Αρχική Συνομιλία

(Με Ρ συμβολίζουμε τον Pat και Ε τον Expert Witness):

(Ε): Καλησπέρα σας, τι έχει συμβεί;

(Ρ): Καλησπέρα, λάβαμε μια ειδοποίηση από την αστυνομία ότι πρόκειται να έρθει σύντομα το πρωί στα γραφεία μας για μια υπόθεση εκβιασμού. Θα ήθελα να είστε παρόντες και εσείς με την ομάδα σας προκειμένου να διερευνήσετε το περιστατικό.

(Ε): Πείτε μου μερικές βασικές πληροφορίες για την υπόθεση του εκβιασμού.

(Ρ): Απ' ότι φαίνεται ένας υπάλληλος της εταιρείας ζητάει χρήματα από παλιό μας πελάτη.

(Ε): Που βρίσκεται τώρα ο υπάλληλος; Στο γραφείο;

(Ρ): Ναι. Δουλεύει στο γραφείο με εταιρικό laptop, και όποτε χρειάζεται το παίρνει και εκτός εταιρείας.

(Ε): Υπάρχει και άλλος κόσμος στην σκηνή που εντοπίστηκε το ηλεκτρονικό έγκλημα;

(Ρ): Ναι, υπάρχουν κάποιοι άλλοι υπάλληλοι.

(Ε): Ωραία, μην πειράξετε τίποτα. Θα σας προωθήσω τη σύμβαση εργασίας για να υπογράψετε και θα έρθουμε από εκεί για να ξεκινήσουμε την έρευνα. Μέχρι να έρθουμε, απομονώστε το γραφείο, μην αφήσετε κανέναν να πλησιάσει καθώς μπορεί να επηρεάσει τη σκηνή του εγκλήματος.

Παράρτημα Β – Συνέντεύξεις

Συνέντευξη με τον Υπεύθυνο ασφάλειας (CISO) της εταιρείας

(TW): Καλησπέρα, είμαι ο Βαγγέλης Γκίνης και είμαι μέλος της ομάδας διερεύνησης του συμβάντος. Αρχικά να σε ενημερώσω ότι η συνομιλία πρόκειται να καταγραφεί. Θα ήθελα να μου αναφέρεις την θέση και τους ρόλους σου στην εταιρεία.

(CISO): Εγώ είμαι ο CISO και οι αρμοδιότητες μου είναι η στρατηγική σχεδίαση της ασφάλειας των πληροφοριακών συστημάτων της εταιρείας M57Biz. Επίσης είμαι υπεύθυνος για την προστασία των δεδομένων της εταιρείας από εξωτερικές και εσωτερικές απειλές και βοηθάω στην γενικότερη συμμόρφωση των νομικών απαιτήσεων.

(TW): Τι πιστεύεις ότι έχει συμβεί;

(CISO): Υπάρχουν υποψίες ότι ο Charlie έχει επικοινωνία με ανταγωνιστή ενός πελάτη μας ζητώντας χρήματα για να του πουλήσει πατέντα μας.

(TW): Είχε προηγηθεί κάποια περίεργη συμπεριφορά από τον ύποπτο;

(CISO): Δεν έχουμε παρατηρήσει περίεργη συμπεριφορά. Μερικές φορές μόνο μας δείχνει πως του αρέσει η καλή ζωή.

(TW): Τι δικαιώματα πρόσβασης έχουν οι εργαζόμενοι στα δεδομένα της εταιρείας;

(CISO): Εφαρμόζουμε least privilege principle. Ο καθένας έχει τον υπολογιστή του, και έχει πρόσβαση σε αυτά. Μετά, υπάρχουν ειδικές άδειες για ορισμένα δεδομένα, π.χ., πρόσβαση σε remote drives μέσα στο LAN της εταιρείας.

(TW): Τι πολιτική εφαρμόζετε για τους κωδικούς πρόσβασης σε νέους υπαλλήλους που τους δίδεται εταιρικό λάππο; Πρέπει να αλλάξει o default κωδικός πρόσβασης εντός ορισμένου χρονικού πλαισίου;

(CISO): Ναι, έχουμε default κωδικούς πρόσβασης και τους λέμε ότι εντός ενός μήνα πρέπει να έχουν αλλάξει τον κωδικό με βάση κάποια πολιτική, π.χ., να έχει τουλάχιστον 7 χαρακτήρες κλπ.

(TW): Τι συστήματα ασφαλείας φυσικού χώρου έχετε;

(CISO): Κάμερες και access card system. Διατηρούμε υλικό από κάμερες και logs για τις τελευταίες 15 ημέρες.

(TW): Αυτά θα τα χρειαστούμε. Που κάθεται ο ύποπτος;

(CISO): Στο γραφείο στην γωνία.

(TW): Χρησιμοποιείτε κάποιο μέθοδο κρυπτογράφησης των δίσκων τύπου BitLocker;

(CISO): Όχι

(TW): Πείραξε κάποιος το λάππο του Charlie πριν έρθουμε;

(CISO): Όχι, ο χώρος απομονώθηκε όσο είναι δυνατόν. Επίσης, δεν επιτρέψαμε σε κανέναν να εισέλθει στον χώρο.

Συνέντευξη με τον IT Administrator(Terry) της εταιρείας

(TW): Καλησπέρα, είμαι ο Βαγγέλης Γκίνης και είμαι μέλος της ομάδας διερεύνησης του συμβάντος. Αρχικά να σε ενημερώσω ότι η συνομιλία πρόκειται να καταγραφεί. Θα ήθελα να μου αναφέρεις την θέση και τους ρόλους σου στην εταιρεία.

(IT-Admin): Καλησπέρα σας, εργάζομαι ως διαχειριστής της εσωτερικής IT υποδομής στην εταιρεία. Οι αρμοδιότητες μου είναι διαχείριση και συντήρηση των υπολογιστών και του δικτύου, εγκατάσταση, ρύθμιση, και ενημέρωση λογισμικών και εφαρμογών, παρακολούθηση ορθής λειτουργίας της υποδομής και παροχή υποστήριξης στους χρήστες

(TW): Πείτε μας παρακαλώ τι ακριβώς συνέβη κατά την εκτίμηση σας;

(IT-Admin): Απ' ότι έχω καταλάβει ο Charlie εκβίασε έναν ανταγωνιστή ενός πελάτη μας. Τους ζήτησε, μάλλον, χρήματα για να τους αποκαλύψει την πατέντα.

(TW): Είχε προηγηθεί κάποια περίεργη συμπεριφορά από τον ύποπτο;

(CISO): Προσωπικά δεν είχα παρατηρήσει κάτι περίεργο. Δεν γνωρίζω για τους άλλους συναδέλφους.

(TW): Σε ποιον cloud provider φιλοξενούνται τα εταιρικά Emails;

(IT-Admin): Στη Microsoft

(TW): Έχεις πρόσβαση σε message traces και logs;

(IT-Admin): Ναι

(TW): Ωραία. Υπάρχει εσωτερικό τοπικό domain; Υπάρχει επίσης κάποιο Active Directory για τους χρήστες;

(IT-Admin): Ναι υπάρχει domain και active directory

(TW): Ο ύποπτος τι είδους χρήστης είναι; Σε ποια file shares έχει πρόσβαση;

(IT-Admin): Είναι general purpose χρήστης. Έχει πρόσβαση στα βασικά δεδομένα, δηλαδή έχει κάποια στο laptop του και έχει πρόσβαση σε έναν shared drive εντός LAN. Έπειτα από αυτό, λόγω δουλειάς μπορεί να του στέλνονται στο email αρχεία τα οποία βρίσκονται στο laptop του.

(TW): Θα χρειαστούμε τα logs από τις ενέργειες του συγκεκριμένου χρήστη όπως επίσης και το γενικότερο network diagram της εταιρείας.

Συνέντευξη με τον πιθανό δράστη (Charlie)

(TW): Είσαι ο Charlie;

(Ch): Ναι, εγώ είμαι.

(TW): Εγώ είμαι ο Βαγγέλης Γκίνης και είμαι μέλος της ομάδας διερεύνησης του συμβάντος. Για το τυπικό να σε ενημερώσω ότι έχεις το δικαίωμα να προσλάβεις δικηγόρο. Ότι πεις μπορεί να χρησιμοποιηθεί ενάντια σου στο δικαστήριο. Επίσης από εδώ και στο εξής η συνομιλία μας θα καταγράφεται. Είσαι εντάξει με αυτό;

(Ch): Ναι.

(TW): Ποιος είναι ο ρόλος σου στην εταιρεία;

(Ch): Είμαι ερευνητής στην εταιρεία.

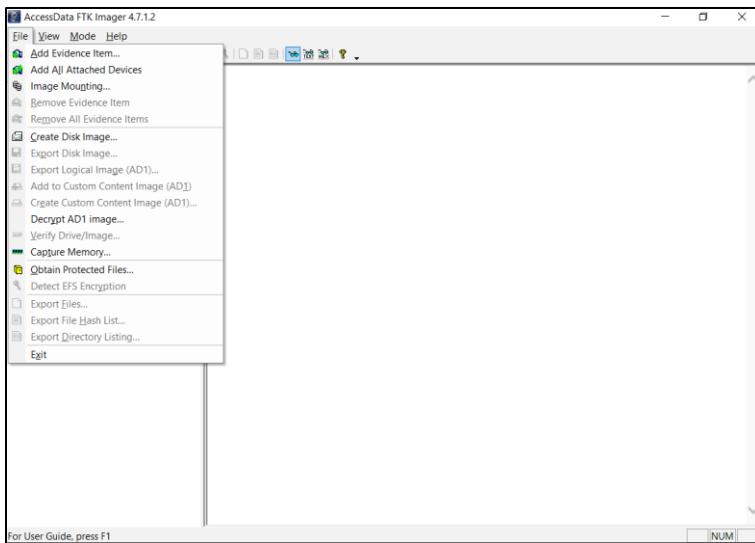
- (TW): Πόσο καιρό δουλεύεις εδώ;
- (Ch): Περίπου έναν μήνα.
- (TW): Είσαι ικανοποιημένος από τις συνθήκες εργασίας σου;
- (Ch): Ναι, μια χαρά είμαι.
- (TW): Τι μισθό παίρνεις;
- (Ch): Πρέπει να απαντήσω;
- (TW): Δεν είσαι υποχρεωμένος.
- (Ch): Ωραία, δεν θέλω να πω.
- (TW): Γνωρίζει κάποιος άλλος πέραν από εσένα τον κωδικό του laptop σου;
- (Ch): Όχι, μόνο εγώ.
- (TW): Έχεις καταλάβει, γιατί κατηγορείσαι;
- (Ch): Ναι και θα σας πω ότι είπα και σε αυτούς, δεν έχω κάνω κάτι.
- (TW): Οι συνάδελφοι σου επιμένουν ότι ζήτησες χρήματα από παλιό πελάτη σας και απείλησες με δημοσίευση πατέντας. Τι έχεις να πεις για αυτό;
- (Ch): Το laptop είναι ανοιχτό συνέχεια στο γραφείο μου, κάποιος μπορεί να το χρησιμοποιήσε.
- (TW): Μάλιστα.

Παράρτημα Γ – Διαφύλαξη πειστηρίων

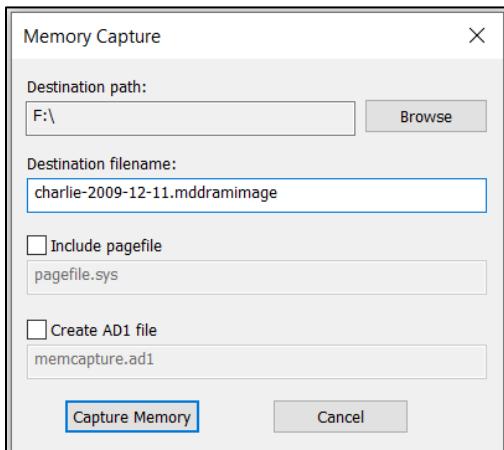
Στο παρόν παράρτημα αποτυπώνονται όλες οι τεχνικές λεπτομέρειες για την διαφύλαξη των πειστηρίων όπου λήφθηκαν από τον τόπο του εγκλήματος. Λαμβάνουμε διπλά αντίγραφα μνήμης.

Διαφύλαξη μνήμης: FTK Imager

Επιλέγουμε στον κατάλογο File > Capture Memory.



Εισάγουμε τις λεπτομέρειες για το dump αρχείο, όπως όνομα και destination path.



Κάνουμε κλικ στο “Capture Memory” και μόλις η διαδικασία τελειώσει έχουμε το πειστήριο της μνήμης.

Διαφύλαξη μνήμης: mdd_1.3

```
C:\>mdd_1.3.exe -o 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 1023.48 MB of physical memory to file 'charlie-2009-12-11.ram'.

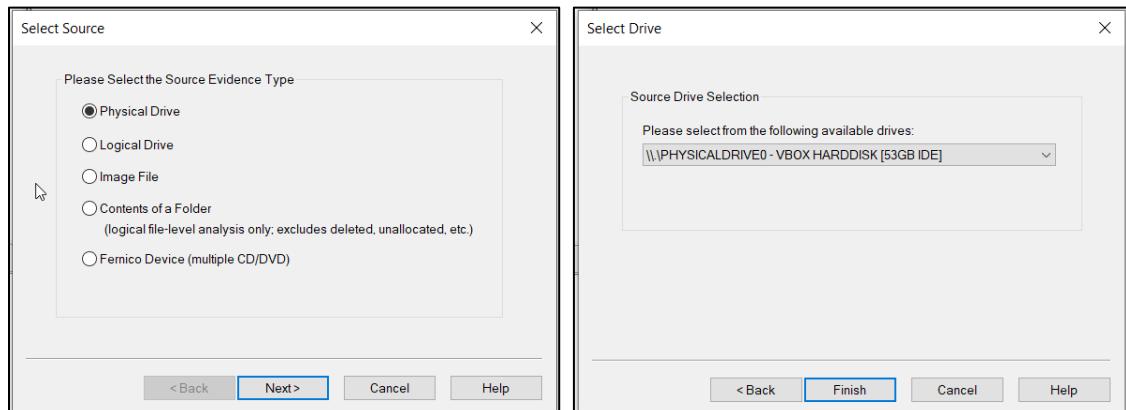
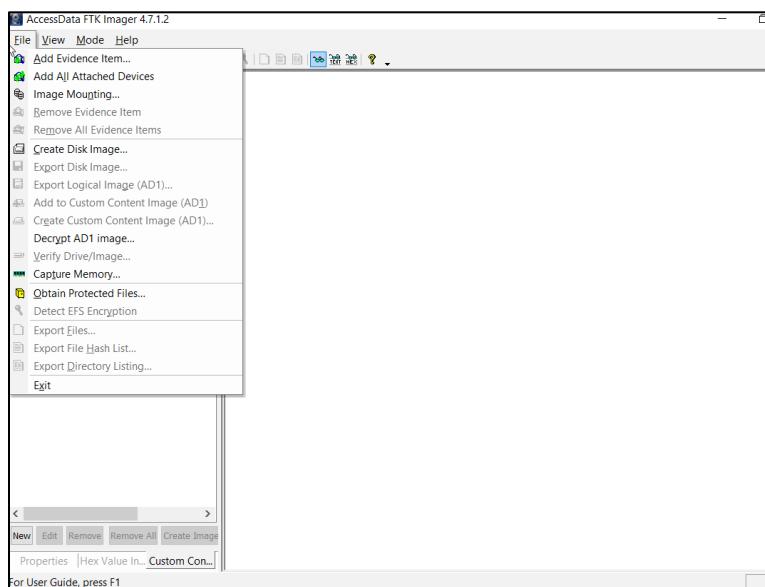
262012 map operations succeeded <1.00>
0 map operations failed

took 27 seconds to write
MD5 is: fceef6f301eef8adad6f583e3766457c

```

Διαφύλαξη δίσκου: FTK Imager

Στον κατάλογο επιλέγουμε File > Create Disk Image > Physical Drive (PHYSICALDRIVE0) > Finish.



Εμφανίζεται το επόμενο παράθυρο, επιλέγουμε Add > E01 > Next > Εισάγουμε τις πληροφορίες για το συγκεκριμένο έγκλημα > Next > Εισάγουμε πληροφορίες για το αρχείο > Finish > Start:

Create Image

Image Source
\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

Add Overflow Location

Verify images after they are created Precalculate Progress Statistics
 Create directory listings of all files in the image after they are created

Start Cancel

Evidence Item Information

Case Number: 103972641

Evidence Number: 001

Unique Description: Disk

Examiner: Georgiadis Eleftherios

Notes:

< Back Next > Cancel Help

Select Image Destination

Image Destination Folder
F:\

Image Filename (Excluding Extension)
charlie-2009-12-11.E01

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption

< Back Finish Cancel Help

Create Image

Image Source
\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

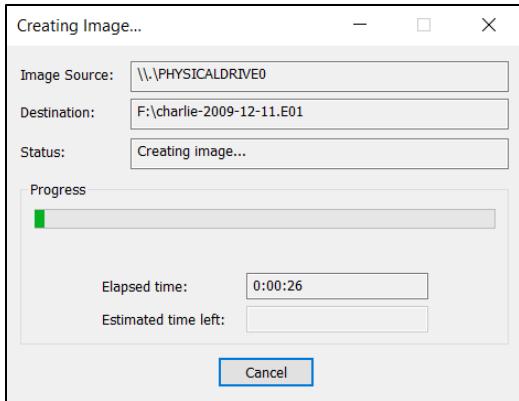
Image Destination(s)
F:\\charlie-2009-12-11.E01 [E01]

Add... Edit... Remove

Add Overflow Location

Verify images after they are created Precalculate Progress Statistics
 Create directory listings of all files in the image after they are created

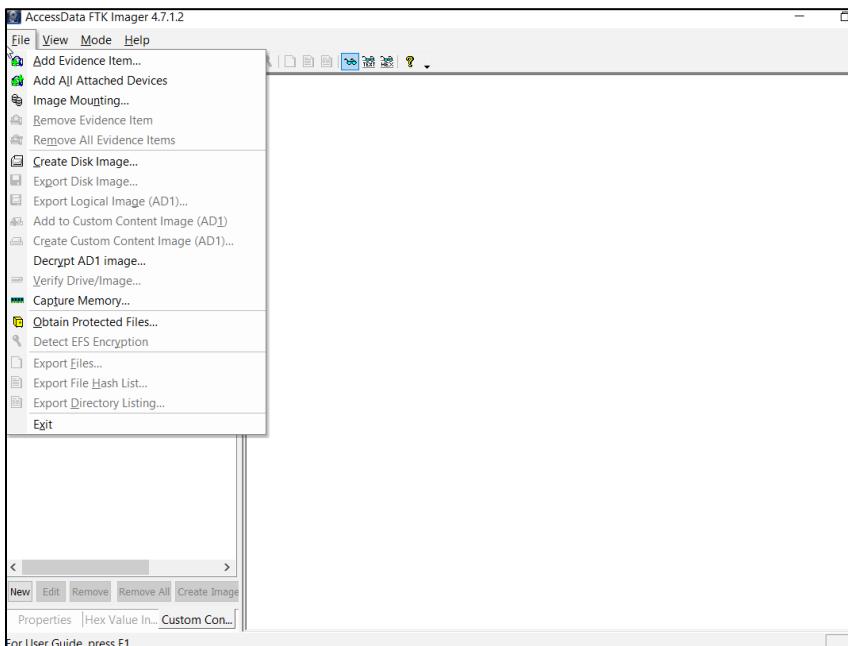
Start Cancel

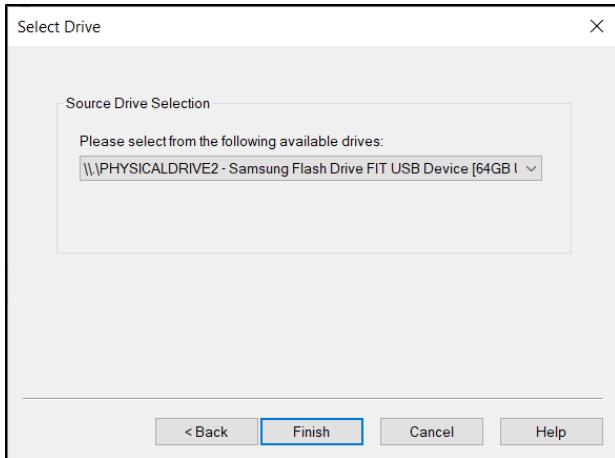


Μόλις τελειώσει η διαδικασία θα πρέπει να έχουμε το αρχείο στο directory που επιλέξαμε.

Διαφύλαξη USB: FTK Imager

Στον κατάλογο επιλέγουμε File > Create Disk Image > Physical Drive (PHYSICALDRIVE2) > Finish.





Εμφανίζεται το επόμενο παράθυρο, επιλέγουμε Add > E01 > Next > Εισάγουμε τις πληροφορίες για το συγκεκριμένο έγκλημα > Next > Εισάγουμε πληροφορίες για το αρχείο > Finish > Start:

Create Image

Image Source: \\.\PHYSICALDRIVE

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

Add Overflow Location

Verify images after they are created Precalculate Progress Statistics

Create directory listings of all files in the image after they are created

Start Cancel

Evidence Item Information

Case Number: 103972641

Evidence Number: 002

Unique Description: USB

Examiner: Georgiadis Eleftherios

Notes:

< Back Next > Cancel Help

Select Image Destination

Image Destination Folder: F:\

Image Filename (Excluding Extension): charlie-work-usb-2009-12-11.E01

Image Fragment Size (MB): 1500

For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption

< Back Finish Cancel Help

Create Image

Image Source: \\.\PHYSICALDRIVE

Starting Evidence Number: 1

Image Destination(s): F:\charlie-work-usb-2009-12-11.E01 [E01]

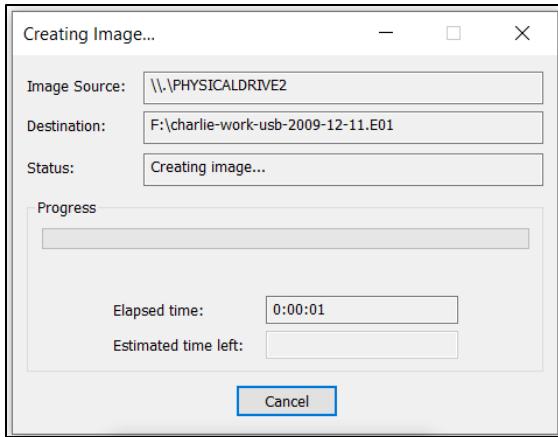
Add... Edit... Remove

Add Overflow Location

Verify images after they are created Precalculate Progress Statistics

Create directory listings of all files in the image after they are created

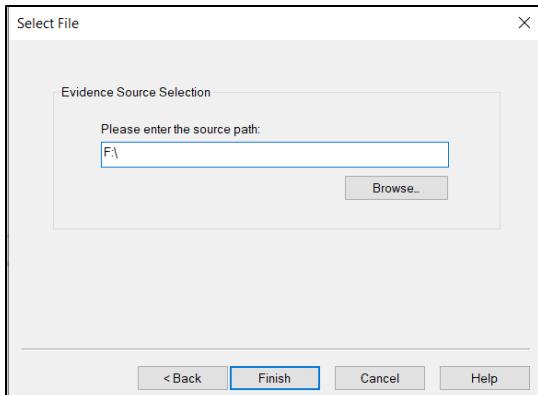
Start Cancel



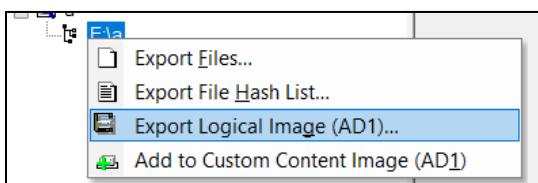
Μόλις τελειώσει η διαδικασία θα πρέπει να έχουμε το αρχείο στο directory που επιλέξαμε.

Παραγωγή SHA1 και MD5 τιμών:

Μέσω του FTK Imager στο μενού επιλέγουμε File > Add Evidence Item > Contents of a Folder > Next > Επιλέγουμε το path στο οποίο αποθηκεύσαμε τα τρία παραπάνω αρχεία > Finish.



Με δεξί κλικ στο κλαδί του δέντρου > Export File Hash List παίρνουμε τα hash values για όλα αυτά τα τρία αρχεία στο directory. Επιλέγουμε που επιθυμούμε να αποθηκεύσουμε τα αποτελέσματα και ξεκινάει η διαδικασία του hashing.



Παράρτημα Δ – Ανάλυση μνήμης H/Y Laptop

Με τη βοήθεια του volatility απαντάμε στα παρακάτω ερωτήματα. Επιπρόσθετα, επισυνάπτεται αρχείο με τις ακριβείς εντολές οι οποίες εκτελέστηκαν και παρήγαγαν τα παρακάτω αποτελέσματα (charlie-2009-12-11_volatility_analysis.bat), όπως και το ακριβές αποτέλεσμα (σε .txt αρχεία) το οποίο παρήγαγε το volatility για κάθε εντολή.

1) Ποιες διεργασίες τρέχανε όταν λήφθηκε το Dump της μνήμης;

Possible Answer	Process name	PID	PPID	Th ds	Start at
System	4	0	64	2009-12-11 16:53:21 PST	
smss.exe	876	4	3	2009-12-11 16:53:21 PST	
csrss.exe	924	876	11	2009-12-11 16:53:22 PST	
winlogon.exe	948	876	17	2009-12-11 16:53:23 PST	
services.exe	992	948	15	2009-12-11 16:53:23 PST	
lsass.exe	1004	948	22	2009-12-11 16:53:23 PST	
svchost.exe	1180	992	17	2009-12-11 16:53:23 PST	
svchost.exe	1268	992	10	2009-12-11 16:53:24 PST	
svchost.exe	1392	992	74	2009-12-11 16:53:24 PST	
svchost.exe	1532	992	5	2009-12-11 16:53:24 PST	
svchost.exe	1644	992	11	2009-12-11 16:53:24 PST	
spoolsv.exe	1908	992	10	2009-12-11 16:53:26 PST	
svchost.exe	1796	992	4	2009-12-11 16:53:40 PST	
avgwdsvc.exe	1728	992	25	2009-12-11 16:53:40 PST	
jqs.exe	320	992	5	2009-12-11 16:53:42 PST	
explorer.exe	1348	1304	13	2009-12-11 16:53:46 PST	
hkcmd.exe	2684	1348	2	2009-12-11 16:53:51 PST	
jusched.exe	2804	1348	2	2009-12-11 16:53:51 PST	
ctfmon.exe	2832	1348	1	2009-12-11 16:53:52 PST	
alg.exe	2956	992	6	2009-12-11 16:53:52 PST	
soffice.exe	3048	3000	1	2009-12-11 16:53:52 PST	
soffice.bin	3088	3048	7	2009-12-11 16:53:53 PST	
avgfws9.exe	3939	992	25	2009-12-11 16:54:05 PST	
thunderbird.exe	188	1348	10	2009-12-11 08:54:43 PST	
cmd.exe	3296	1348	1	2009-12-11 08:59:32 PST	
mdd_1.3.exe	1768	3296	1	2009-12-11 08:59:51 PST	

Πίνακας 16 Διεργασίες

- Διεργασίες συστήματος, οι οποίες ξεκινάνε αυτόματα με την έναρξη του λειτουργικού συστήματος
- Διεργασίες επιπέδου χρήστη, οι οποίες ξεκίνησαν αυτόματα (άρα όχι από τον χρήστη χειροκίνητα)
- Διεργασίες επιπέδου χρήστη, οι οποίες ξεκίνησαν από τον ίδιο τον χρήστη χειροκίνητα

2) Ποια connections υπήρχαν όταν λήφθηκε το Dump της μνήμης

Possible Answer	Local Address	Remote Address	PID
	192.168.1.104:1311	192.168.1.1:139	4
	192.168.1.104:1303	63.245.209.10:80	188
	192.168.1.104:1208	198.189.255.73:80	2804

	192.168.1.104:1310	192.168.1.1:445	4
	127.0.0.1:1301	127.0.0.1:1302	188
	192.168.1.104:1304	208.97.132.223:995	188
	127.0.0.1:1302	127.0.0.1:1301	188
	192.168.1.104:1307	208.97.132.223:995	188
	127.0.0.1:1300	127.0.0.1:1299	188
	127.0.0.1:1299	127.0.0.1:1300	188
	192.168.1.104:1305	63.245.221.11:80	188

Πίνακας 17 Connections

3) Ποια sockets είναι ανοιχτά;

Possible Answer	PID	Port	Proto	Protocol	Address	Create Time
2804	1208	6	TCP	0.0.0.0	2009-12-11 03:42:16 PST	
4	138	17	UDP	192.168.1.104	2009-12-11 16:53:26 PST	
4	0	47	GRE	0.0.0.0	2009-12-11 16:58:52 PST	
188	1299	6	TCP	127.0.0.1	2009-12-11 08:54:45 PST	
1004	500	17	UDP	0.0.0.0	2009-12-11 16:53:43 PST	
1392	123	17	UDP	192.168.1.104	2009-12-11 16:53:46 PST	
4	445	6	TCP	0.0.0.0	2009-12-11 16:53:06 PST	
1268	135	6	TCP	0.0.0.0	2009-12-11 16:53:24 PST	
188	1302	6	TCP	0.0.0.0	2009-12-11 08:54:51 PST	
4	1310	6	TCP	0.0.0.0	2009-12-11 08:59:28 PST	
1392	123	17	UDP	127.0.0.1	2009-12-11 16:53:46 PST	
1004	0	255	Reserved	0.0.0.0	2009-12-11 16:53:43 PST	
1644	1900	17	UDP	192.168.1.104	2009-12-11 16:53:52 PST	
4	139	6	TCP	192.168.1.104	2009-12-11 16:53:26 PST	
188	1301	6	TCP	127.0.0.1	2009-12-11 08:54:51 PST	
2956	1034	6	TCP	127.0.0.1	2009-12-11 16:53:54 PST	
188	1300	6	TCP	0.0.0.0	2009-12-11 08:54:45 PST	
4	137	17	UDP	192.168.1.104	2009-12-11 16:53:26 PST	
1644	1900	17	UDP	127.0.0.1	2009-12-11 16:53:52 PST	
1004	4500	17	UDP	0.0.0.0	2009-12-11 16:53:43 PST	
320	5152	6	TCP	127.0.0.1	2009-12-11 16:53:43 PST	
4	445	17	UDP	0.0.0.0	2009-12-11 16:53:06 PST	
4	1045	6	TCP	0.0.0.0	2009-12-11 16:58:52 PST	

Πίνακας 18 Sockets

4) Ποιο είναι το αποτέλεσμα του hashdump;

Possible Answer	Hash
	Administrator:500:f0d412bd764ffe81aad3b435b51404ee;209c6174da490caeb422f3fa5a7ae634:::
	Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
	HelpAssistant:1000:c84fa92b5e90e68cdf2b9bc99a6ddf59:fc20a40d2ee88511f2093e88e4e90d03:::
	SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:a92937cd0574859facc0017cd2e8bdb:::
	Charlie:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Πίνακας 19 Hashdump

5) Ποιο είναι το αποτέλεσμα του imageinfo;

Imageinfo
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/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 : 0xffffd0000L
KPCR for CPU 1 : 0xf7717000L
KUSER_SHARED_DATA : 0xffffd00000
Image date and time : 2009-12-11 16:59:52 UTC+0000
Image local date and time : 2009-12-11 08:59:52 -0800

6) Ποιο είναι το ιστορικό του cmd;

CMD-History
System pid: 4
smss.exe pid: 876 Command line : \SystemRoot\System32\smss.exe
csrss.exe pid: 924
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
winlogon.exe pid: 948 Command line : winlogon.exe
services.exe pid: 992 Command line : C:\WINDOWS\system32\services.exe
lsass.exe pid: 1004 Command line : C:\WINDOWS\system32\lsass.exe
svchost.exe pid: 1180 Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
svchost.exe pid: 1268 Command line : C:\WINDOWS\system32\svchost -k rpcss
svchost.exe pid: 1392 Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
svchost.exe pid: 1532 Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
svchost.exe pid: 1644 Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
spoolsv.exe pid: 1908 Command line : C:\WINDOWS\system32\spoolsv.exe
svchost.exe pid: 1796 Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
avgwdsvc.exe pid: 1728 Command line : "C:\Program Files\AVG\AVG9\avgwdsvc.exe"
jqs.exe pid: 320 Command line : "C:\Program Files\Java\jre6\bin\jqs.exe" -service -config "C:\Program Files\Java\jre6\lib\deploy\jqs\jqs.conf"
explorer.exe pid: 1348 Command line : C:\WINDOWS\Explorer.EXE
hkcmd.exe pid: 2684 Command line : "C:\WINDOWS\system32\hkcmd.exe"
jusched.exe pid: 2804 Command line : "C:\Program Files\Java\jre6\bin\jusched.exe"
ctfmon.exe pid: 2832 Command line : "C:\WINDOWS\system32\ctfmon.exe"
alg.exe pid: 2956 Command line : C:\WINDOWS\System32\alg.exe
soffice.exe pid: 3048 Command line : "C:\Program Files\OpenOffice.org 3\program\soffice.exe" -quickstart
soffice.bin pid: 3088 Command line : "C:\Program Files\OpenOffice.org 3\program\soffice.exe" "-quickstart" "-env:OOO_CWD=2C:\Program Files\OpenOffice.org 3\program"
avgfws9.exe pid: 3936 Command line : "C:\Program Files\AVG\AVG9\avgfws9.exe"
thunderbird.exe pid: 188 Command line : "C:\Program Files\Mozilla Thunderbird\thunderbird.exe"
cmd.exe pid: 3296 Command line : "C:\WINDOWS\system32\cmd.exe"
mdd_1.3.exe pid: 1768 Command line : z:\mdd_1.3.exe -o z:\charlie-2009-12-11.ram

Παράρτημα Ε – Ανάλυση δίσκου H/Y Laptop

- 1) What are the hash values (MD5 & SHA-1) of all images? Does the acquisition and verification hash value match?

Possible Answer	Class	Hash Algo.	Hash value
charlie-2009-12-11.mddramimage	MD5	38067CC457546B3156975D9A52D4229F	
	SHA1	15C1AE5E2AC3DA7A9CDAAA9A162AA9AC9DDE3D9D	
charlie-2009-12-11.E01	MD5	A459F1AA45941AD4FA22D5CB9D35F7FC	
	SHA1	EE1D5FEBB63DEF90C2900B6984D21A6A137F00CE	
charlie-work-usb-2009-12-11.E01	MD5	8C23941655B3313F4A31A1A66085BE86	
	SHA1	E49BF6048856570CC3D49B1485D6D87AAAB6AB0A	
Considerations	Windows 10 Powershell: Get-FileHash -Algorithm MD5 .\charlie-2009-12-11.mddramimage Get-FileHash -Algorithm SHA1 .\charlie-2009-12-11.mddramimage Get-FileHash -Algorithm MD5 .\charlie-2009-12-11.E01		

Πίνακας 20 Hash values						
-------------------------------	--	--	--	--	--	--

2) Identify the partition information of PC image.

Possible Answer	No.	Bootable	File system	Start Sector	Total Sectors	Size
	vol1	Όχι	Unallocated	0	62	-
	vol2	Ναι	NTFS/exFAT	63	19.968.731	10.223.958.528B
	vol3	Όχι	Unallocated	19.968.795	30.932	-
Evidence Location						

Πίνακας 21 HDD Partitions

3) Explain installed OS information in detail. (OS name, install date, registered owner...)

Possible Answer	OS Name	Microsoft Windows XP
	Version	5.1
	Build Number	1.511.1
	Registered Owner	Charlie
	System Root	C:\WINDOWS
	Install Date	2009-11-08 17:25:47 PST

Evidence Location	/img_charlie-2009-12-11.E01/vol_vol2/WINDOWS/system32/config/software \Microsoft\Windows NT\CurrentVersion																																																															
<table border="1"> <thead> <tr> <th colspan="3">Values</th> </tr> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>SubVersionNumber</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>CurrentBuild</td> <td>REG_SZ</td> <td>1.511.1.0 (Obsolete data - do not use)</td> </tr> <tr> <td>InstallDate</td> <td>REG_DWORD</td> <td>0x4af7f9fb (1257729947)</td> </tr> <tr> <td>ProductName</td> <td>REG_SZ</td> <td>Microsoft Windows XP</td> </tr> <tr> <td>RegDone</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>RegisteredOrganization</td> <td>REG_SZ</td> <td>M57.biz</td> </tr> <tr> <td>RegisteredOwner</td> <td>REG_SZ</td> <td>Charlie</td> </tr> <tr> <td>SoftwareType</td> <td>REG_SZ</td> <td>SYSTEM</td> </tr> <tr> <td>CurrentVersion</td> <td>REG_SZ</td> <td>5.1</td> </tr> <tr> <td>CurrentBuildNumber</td> <td>REG_SZ</td> <td>2600</td> </tr> <tr> <td>BuildLab</td> <td>REG_SZ</td> <td>2600xpsp_sp3_gdr.090804-1435</td> </tr> <tr> <td>CurrentType</td> <td>REG_SZ</td> <td>Multiprocessor Free</td> </tr> <tr> <td>CSDVersion</td> <td>REG_SZ</td> <td>Service Pack 3</td> </tr> <tr> <td>SystemRoot</td> <td>REG_SZ</td> <td>C:\WINDOWS</td> </tr> <tr> <td>SourcePath</td> <td>REG_SZ</td> <td>D:\ISB</td> </tr> <tr> <td>PathName</td> <td>REG_SZ</td> <td>C:\WINDOWS</td> </tr> <tr> <td>Productid</td> <td>REG_SZ</td> <td>76487-027-5250835-22765</td> </tr> <tr> <td>DigitalProductId</td> <td>REG_BIN</td> <td>A4 00 00 00 03 00 00 00 37 36 34 38 37 2D 30 32...</td> </tr> <tr> <td>LicensesInfo</td> <td>REG_BIN</td> <td>E7 77 18 13 57 BE 58 50 F3 DB BD 78 35 D6 FD D4...</td> </tr> </tbody> </table>		Values			Name	Type	Value	SubVersionNumber	REG_SZ	(value not set)	CurrentBuild	REG_SZ	1.511.1.0 (Obsolete data - do not use)	InstallDate	REG_DWORD	0x4af7f9fb (1257729947)	ProductName	REG_SZ	Microsoft Windows XP	RegDone	REG_SZ	(value not set)	RegisteredOrganization	REG_SZ	M57.biz	RegisteredOwner	REG_SZ	Charlie	SoftwareType	REG_SZ	SYSTEM	CurrentVersion	REG_SZ	5.1	CurrentBuildNumber	REG_SZ	2600	BuildLab	REG_SZ	2600xpsp_sp3_gdr.090804-1435	CurrentType	REG_SZ	Multiprocessor Free	CSDVersion	REG_SZ	Service Pack 3	SystemRoot	REG_SZ	C:\WINDOWS	SourcePath	REG_SZ	D:\ISB	PathName	REG_SZ	C:\WINDOWS	Productid	REG_SZ	76487-027-5250835-22765	DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 37 36 34 38 37 2D 30 32...	LicensesInfo	REG_BIN	E7 77 18 13 57 BE 58 50 F3 DB BD 78 35 D6 FD D4...
Values																																																																
Name	Type	Value																																																														
SubVersionNumber	REG_SZ	(value not set)																																																														
CurrentBuild	REG_SZ	1.511.1.0 (Obsolete data - do not use)																																																														
InstallDate	REG_DWORD	0x4af7f9fb (1257729947)																																																														
ProductName	REG_SZ	Microsoft Windows XP																																																														
RegDone	REG_SZ	(value not set)																																																														
RegisteredOrganization	REG_SZ	M57.biz																																																														
RegisteredOwner	REG_SZ	Charlie																																																														
SoftwareType	REG_SZ	SYSTEM																																																														
CurrentVersion	REG_SZ	5.1																																																														
CurrentBuildNumber	REG_SZ	2600																																																														
BuildLab	REG_SZ	2600xpsp_sp3_gdr.090804-1435																																																														
CurrentType	REG_SZ	Multiprocessor Free																																																														
CSDVersion	REG_SZ	Service Pack 3																																																														
SystemRoot	REG_SZ	C:\WINDOWS																																																														
SourcePath	REG_SZ	D:\ISB																																																														
PathName	REG_SZ	C:\WINDOWS																																																														
Productid	REG_SZ	76487-027-5250835-22765																																																														
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 37 36 34 38 37 2D 30 32...																																																														
LicensesInfo	REG_BIN	E7 77 18 13 57 BE 58 50 F3 DB BD 78 35 D6 FD D4...																																																														

Πίνακας 22 OS Details

4) What is the time zone setting?

Possible Answer	Timezone	Pacific Daylight Time																														
	Daylight Time Bias	-60 mins																														
Evidence Location	<table border="1"> <thead> <tr> <th colspan="3">Values</th> </tr> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Bias</td> <td>REG_DWORD</td> <td>0x000001e0 (480)</td> </tr> <tr> <td>StandardName</td> <td>REG_SZ</td> <td>Pacific Standard Time</td> </tr> <tr> <td>StandardBias</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>StandardStart</td> <td>REG_BIN</td> <td>00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00</td> </tr> <tr> <td>DaylightName</td> <td>REG_SZ</td> <td>Pacific Daylight Time</td> </tr> <tr> <td>DaylightBias</td> <td>REG_DWORD</td> <td>0xfffffc4 (4294967236)</td> </tr> <tr> <td>DaylightStart</td> <td>REG_BIN</td> <td>00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00</td> </tr> <tr> <td>ActiveTimeBias</td> <td>REG_DWORD</td> <td>0x000001e0 (480)</td> </tr> </tbody> </table>		Values			Name	Type	Value	Bias	REG_DWORD	0x000001e0 (480)	StandardName	REG_SZ	Pacific Standard Time	StandardBias	REG_DWORD	0x00000000 (0)	StandardStart	REG_BIN	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00	DaylightName	REG_SZ	Pacific Daylight Time	DaylightBias	REG_DWORD	0xfffffc4 (4294967236)	DaylightStart	REG_BIN	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00	ActiveTimeBias	REG_DWORD	0x000001e0 (480)
Values																																
Name	Type	Value																														
Bias	REG_DWORD	0x000001e0 (480)																														
StandardName	REG_SZ	Pacific Standard Time																														
StandardBias	REG_DWORD	0x00000000 (0)																														
StandardStart	REG_BIN	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00 00																														
DaylightName	REG_SZ	Pacific Daylight Time																														
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)																														
DaylightStart	REG_BIN	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00																														
ActiveTimeBias	REG_DWORD	0x000001e0 (480)																														

Πίνακας 23 Timezone setting

5) What is the computer name?

Possible Answer	M57-CHARLIE									
Evidence Location	/img_charlie-2009-12-11.E01/vol_vol2/Windows/System32/config/system \CurrentControlSet\Control\ComputerName\ComputerName									
<table border="1"> <thead> <tr> <th colspan="3">Values</th> </tr> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>ComputerName</td> <td>REG_SZ</td> <td>M57-CHARLIE</td> </tr> </tbody> </table>		Values			Name	Type	Value	ComputerName	REG_SZ	M57-CHARLIE
Values										
Name	Type	Value								
ComputerName	REG_SZ	M57-CHARLIE								

Πίνακας 24 Computer Name

- 6) List all accounts in OS except the system accounts: *Administrator, Guest, systemprofile, LocalService, NetworkService*. (Account name, login count, last logon)

Possible Answer <small>(Timezone is applied)</small>	Account	SID	NT Hash	Status	Login Count	Account Created Time	Last Login Time	Login Failure Time																																																																																										
	Administrator	S-1-5-21-682003330-329068152-1644491937-500	f0d412bd764ffe81aad3b435b51404ee	Enabled	5	2009-11-08 09:05:58 PST	2009-11-09 17:19:53 PST	2009-11-10 11:12:39 PST																																																																																										
	Charlie	S-1-5-21-682003330-329068152-1644491937-1003	aad3b435b51404eeaad3b435b51404ee	Enabled	51	2009-11-10 11:13:30 PST	2009-12-10 16:53:26 PST	-																																																																																										
	SYSTEM	S-1-5-18			-	-	-	-																																																																																										
	LOCAL SERVICE	S-1-5-19			-	-	-	-																																																																																										
	NT Service Virtual Account	S-1-5-80-324959683-3395802011-921526492-919036580-1730255754			-	-	-	-																																																																																										
	NETWORK SERVICE	S-1-5-20			-	-	-	-																																																																																										
	HelpAssistant	S-1-5-21-682003330-329068152-1644491937-1000	c84fa92b5e90e68cdf2b9bc99a6ddf59	Disabled	0	2009-11-08 17:19:34 PST	-	-																																																																																										
Evidence Location	<table border="1"> <thead> <tr> <th>△ Name</th> <th>S</th> <th>C</th> <th>O</th> <th>Login Name</th> <th>Host</th> <th>Scope</th> <th>Realm Name</th> <th>Creation Time</th> </tr> </thead> <tbody> <tr> <td>█ S-1-5-18</td> <td></td> <td></td> <td></td> <td>SYSTEM</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td>NT AUTHORITY</td> <td></td> </tr> <tr> <td>█ S-1-5-19</td> <td></td> <td></td> <td></td> <td>LOCAL SERVICE</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td>NT AUTHORITY</td> <td></td> </tr> <tr> <td>█ S-1-5-20</td> <td></td> <td></td> <td></td> <td>NETWORK SERVICE</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td>NT AUTHORITY</td> <td></td> </tr> <tr> <td>█ S-1-5-21-682003330-329068152-1644491937-1000</td> <td>0</td> <td></td> <td></td> <td>HelpAssistant</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td></td> <td>2009-11-08 17:19:34 PST</td> </tr> <tr> <td>█ S-1-5-21-682003330-329068152-1644491937-1002</td> <td>0</td> <td></td> <td></td> <td>SUPPORT_388945a0</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td></td> <td>2009-11-08 17:22:05 PST</td> </tr> <tr> <td>█ S-1-5-21-682003330-329068152-1644491937-1003</td> <td>0</td> <td></td> <td></td> <td>Charlie</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td></td> <td>2009-11-10 11:13:30 PST</td> </tr> <tr> <td>█ S-1-5-21-682003330-329068152-1644491937-500</td> <td>0</td> <td></td> <td></td> <td>Administrator</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td></td> <td>2009-11-08 09:05:58 PST</td> </tr> <tr> <td>█ S-1-5-21-682003330-329068152-1644491937-501</td> <td>0</td> <td></td> <td></td> <td>Guest</td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td></td> <td>2009-11-08 09:05:58 PST</td> </tr> <tr> <td>█ S-1-5-80-324959683-3395802011-921526492-919036</td> <td>0</td> <td></td> <td></td> <td></td> <td>charlie-2009-12-11.E01_1 Host</td> <td>Local</td> <td>NT SERVICE</td> <td></td> </tr> </tbody> </table>								△ Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time	█ S-1-5-18				SYSTEM	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY		█ S-1-5-19				LOCAL SERVICE	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY		█ S-1-5-20				NETWORK SERVICE	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY		█ S-1-5-21-682003330-329068152-1644491937-1000	0			HelpAssistant	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 17:19:34 PST	█ S-1-5-21-682003330-329068152-1644491937-1002	0			SUPPORT_388945a0	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 17:22:05 PST	█ S-1-5-21-682003330-329068152-1644491937-1003	0			Charlie	charlie-2009-12-11.E01_1 Host	Local		2009-11-10 11:13:30 PST	█ S-1-5-21-682003330-329068152-1644491937-500	0			Administrator	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 09:05:58 PST	█ S-1-5-21-682003330-329068152-1644491937-501	0			Guest	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 09:05:58 PST	█ S-1-5-80-324959683-3395802011-921526492-919036	0				charlie-2009-12-11.E01_1 Host	Local	NT SERVICE	
△ Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time																																																																																										
█ S-1-5-18				SYSTEM	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY																																																																																											
█ S-1-5-19				LOCAL SERVICE	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY																																																																																											
█ S-1-5-20				NETWORK SERVICE	charlie-2009-12-11.E01_1 Host	Local	NT AUTHORITY																																																																																											
█ S-1-5-21-682003330-329068152-1644491937-1000	0			HelpAssistant	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 17:19:34 PST																																																																																										
█ S-1-5-21-682003330-329068152-1644491937-1002	0			SUPPORT_388945a0	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 17:22:05 PST																																																																																										
█ S-1-5-21-682003330-329068152-1644491937-1003	0			Charlie	charlie-2009-12-11.E01_1 Host	Local		2009-11-10 11:13:30 PST																																																																																										
█ S-1-5-21-682003330-329068152-1644491937-500	0			Administrator	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 09:05:58 PST																																																																																										
█ S-1-5-21-682003330-329068152-1644491937-501	0			Guest	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 09:05:58 PST																																																																																										
█ S-1-5-80-324959683-3395802011-921526492-919036	0				charlie-2009-12-11.E01_1 Host	Local	NT SERVICE																																																																																											
	Hashdump (NTLM, βλ. Παράρτημα Γ):																																																																																																	
	Administrator: 500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::																																																																																																	
	Guest: 501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::																																																																																																	
	HelpAssistant: 1000:c84fa92b5e90e68cdf2b9bc99a6ddf59:fc20a40d2ee88511f2093e88e4e90d03:::																																																																																																	
	SUPPORT_388945a0: 1002:aad3b435b51404eeaad3b435b51404ee:a92937cd0574859facc0017cd2e8bdb:::																																																																																																	
	Charlie: 1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::																																																																																																	

Πίνακας 25 OS Accounts

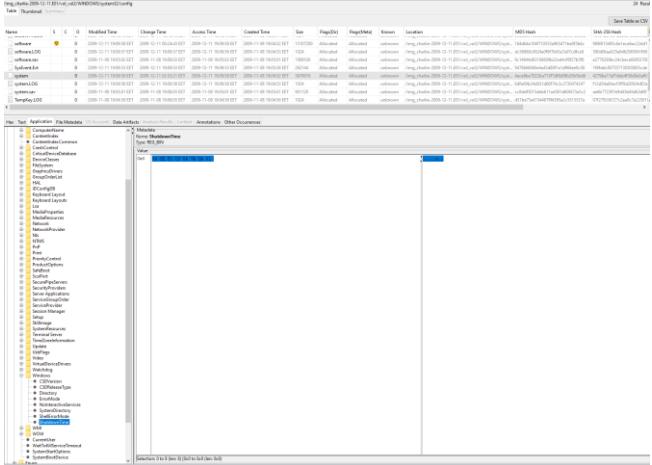
- 7) Who was the last user to logon into PC?

Possible Answer	Charlie - 2009-12-10 16:53:26 PST
Evidence Location	OS Accounts

Πίνακας 26 Last Logon

- 8) When was the last recorded shutdown date/time?

Possible Answer	2009-12-11 09:09:57.5156228
-----------------	-----------------------------

Evidence Location	
-------------------	--

Πίνακας 27 Last shutdown

- 9) Explain the information of network interface(s) with an IP address assigned by DHCP.

Possible Answer	Device Name	Intel(R) PRO/1000 MT Network Connection
	IP Address	192.168.1.104
	Subnet Mask	255.255.255.0
	Name Server	
	Domain	
	Default Gateway	192.168.1.1
	DHCP Usage	
	DHCP Server	192.168.1.1
Evidence Location	/img_charlie-2009-12-11.E01/vol_vol2/WINDOWS/system32/config/system/ControlSet001/Services/Tcpip/Parameters/Interfaces	

Πίνακας 28 Network settings

- 10) What applications were installed by the suspect after installing OS?

Possible Answer <u>(Timezone is applied)</u>	Name	Installation Date	Version	Manufacturer	Installation Path
	IDNMitigationAPIs	2009-11-09 14:40:00 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	ie7	2009-11-09 14:40:00 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Windows Internet Explorer 8 v.20090308.1 40743	2009-11-09 14:40:00 PST		Microsoft	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	NLSDownlevelMapping	2009-11-09 14:40:00 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	OpenOffice.org 3.1 v.3.1.9420	2009-11-09 15:04:29 PST		OpenOffice	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	{26A24AE4-039D-4CA4-87B4-2F83216017FB}	2009-11-09 15:27:10 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/

	Java(TM) 6 Update 17 v.6.0.170	2009-11-09 15:27:39 PST		Oracle	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	MPlayer2	2009-11-10 15:58:33 PST		MPlayer team	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	WebFldrs XP v.9.50.7523	2009-11-10 15:58:41 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Mozilla Firefox (3.5.5) v.3.5.5 (en-US)	2009-11-12 15:48:03 PST		Mozilla Corporation	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Mozilla Thunderbird (2.0.0.23) v.2.0.0.23 (en-US)	2009-11-12 15:52:43 PST		Mozilla Corporation	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Python 2.6.4 v.2.6.4150	2009-11-12 15:57:04 PST		Python Software Foundation	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Foxit Reader v.3.1.3.1030	2009-11-17 11:50:44 PST			/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Adobe Flash Player 10 Plugin v.10.0.32.18	2009-11-18 11:04:30 PST		Adobe Inc	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Invisible Secrets 2.1	2009-11-19 08:43:32 PST		East-Tec	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Apple Software Update v.2.1.1.116	2009-11-19 11:10:16 PST		Apple	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Apple Application Support v.1.1.0	2009-11-19 11:10:36 PST		Apple	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	QuickTime v.7.65.17.80	2009-11-19 11:11:26 PST		Apple	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	7-Zip 4.65	2009-11-24 11:19:52 PST		OpenSource – Igor Pavlov	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Cygnus Hex Editor FREE EDITION 1.00 v.1.00	2009-11-24 12:01:10 PST		SoftCircuits	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
	Brother HL-2170W v.1.00	2009-11-30 07:11:15 PST		Brother-USA	/img_charlie-2009-12-11.E01/vol_vol2/Program Files/
Evidence Location	<ul style="list-style-type: none"> - Data Artifacts/Installed Programs - /img_charlie-2009-12-11.E01/vol_vol2/Program Files 				

Πίνακας 29 Installed Applications

11) What web browsers were used?

Possible Answer	FireFox,, Internet Explorer
-----------------	-----------------------------

Evidence Location	FireFox Analyzer Internet Explorer Analyzer
-------------------	--

Πίνακας 30 Browsers

12) Identify directory/file paths related to the web browser history.

Possible Answer	MS IE (9 or lower)	
	MS IE 11	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Application Data/Microsoft/Internet Explorer/.
	Mozilla	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles
Evidence Location	- History, Cache, Cookies, Bookmarks	

Πίνακας 31 Browser files

13) What websites were the suspect accessing? (Timestamp, URL...)

Possible Answer	Timestamp	URL	Browser
	2009-11-16 13:19:38 PST	http://www.google.com/patents	FireFox Analyzer
	2009-11-16 13:29:37 PST	http://www.espacenet.com/index.en.htm	FireFox Analyzer
	2009-11-16 13:30:47 PST	http://pafft.uspto.gov/	FireFox Analyzer
	2009-11-16 13:31:14 PST	http://www.wipo.int/patentscope/search/en/search.jsf	FireFox Analyzer
	2009-11-16 13:44:49 PST	http://www.ft.com/home/us	FireFox Analyzer
(Some duplicated and meaningless items are excluded)	2009-11-18 08:47:15 PST	http://finance.yahoo.com/	FireFox Analyzer
	2009-12-07 12:56:21 PST	http://www.peertopatent.org/	FireFox Analyzer
	2009-11-20 13:12:03 PST	http://www.supercars.net/index.html	FireFox Analyzer
	2009-12-10 16:01:48 PST	bbc.co.uk	FireFox Analyzer
	2009-12-10 16:01:50 PST	http://www.google.com/patents/about?id=vVPJAAAAEBAJ&dq=time+travel	FireFox Analyzer
	2009-11-08 17:28:40 PST	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail	Internet Explorer Analyzer
(Timezone is applied)	2009-11-17 10:29:53 PST	http://www.controller.com/	FireFox Analyzer
	2009-11-17 13:34:34 PST	http://www.controller.com/drilldown/manufacturers.aspx?catID=9&setype=1&guid=3D26C16D5A224A41841BE9CD9314897E	FireFox Analyzer
	2009-11-18 13:04:19 PST	http://www.turtlefiji.com/#	FireFox Analyzer
	2009-11-19 10:39:24 PST	http://en.wikipedia.org/wiki/Steganography	FireFox Analyzer
	2009-11-19 10:40:55 PST	http://home.comcast.net/~ebm.md/stego/softwarewindows.html	FireFox Analyzer
	2009-11-19 10:41:48 PST	http://www.brothersoft.com/downloads/steganography-tool.html	FireFox Analyzer
	2009-11-19 10:42:17 PST	http://www.neobytesolutions.com/downloads/invsecr2.exe	FireFox Analyzer
	2009-11-19 13:20:30 PST	http://www.gulfstream.com/	FireFox Analyzer
	2009-11-20 13:11:27 PST	http://www.supercars.net/gallery/119513/2232/1.html	FireFox Analyzer
	2009-11-23 09:48:27 PST	http://www.us-cert.gov/control_systems/csvuls.html	FireFox Analyzer
	2009-11-24 13:19:32 PST	http://cdnetworks-us-2.dl.sourceforge.net/project/sevenzip/7-Zip/4.65/7z465.exe	FireFox Analyzer
	2009-12-07 13:39:56 PST	http://www.friendlyplanet.com/	FireFox Analyzer
	2009-12-08 13:15:09 PST	http://www.ferrari.com/English/Pages/Home.aspx	FireFox Analyzer
	2009-12-10 14:19:29 PST	http://www.wipo.int/pctdb/en/fetch.jsp?LANG=ENG&DB SELECT=PCT&SERVER_TYPE=19-00&SORT=11274962-KEY&TYPE_FIELD=256&IDB=0&IDOC=943845&C=0&ELEMENT_SET=BASICHTML-ENG&RESULT=1&TOTAL=31&START=1&DISP=25&FORM=SEP-0/HITNUM.B-ENG.DP,MC,AN,PA,ABSUM-ENG&SEARCH_IA=KR2008005670&QUERY=et%2fquantum+and+et%2fcryptography%0d%0a	
Evidence Location	- Data Artifacts/Web Bookmarks - Data Artifacts/Web Cookies		

	<ul style="list-style-type: none"> - Data Artifacts/Web Downloads - Data Artifacts/Web History - Data Artifacts/Web Search
--	---

Πίνακας 32 Browser History

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

Possible Answer	Timestamp	Keyword	Browser
<u>(Some duplicated and meaningless items are excluded)</u> <u>(Timezone is applied)</u>	2009-11-12 17:50:27 PST	mozrepl	FireFox Analyzer
	2009-11-12 17:51:43 PST	thunderbird email	FireFox Analyzer
	2009-11-12 17:54:56 PST	python	FireFox Analyzer
	2009-11-16 12:03:50 PST	monterey	FireFox Analyzer
	2009-11-19 08:48:47 PST	time machine	FireFox Analyzer
	2009-11-19 08:50:26 PST	time travel	FireFox Analyzer
	2009-11-19 08:51:19 PST	http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=%2Fnetahtm%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN%2F4974166	FireFox Analyzer
	2009-11-19 08:52:14 PST	http://www.uspto.gov/web/patents/classification/uspc700/defs700.htm	FireFox Analyzer
	2009-11-19 10:41:37 PST	steganography	FireFox Analyzer
	2009-11-19 10:41:43 PST	steganography tool free	FireFox Analyzer
	2009-11-24 13:04:19 PST	Immortality	FireFox Analyzer
	2009-11-24 13:19:22 PST	7zip	FireFox Analyzer
	2009-11-24 13:57:05 PST	hex editor	FireFox Analyzer
	2009-11-24 13:57:33 PST	open source hex editor	FireFox Analyzer
	2009-12-02 08:55:58 PST	hot sports cars	FireFox Analyzer
	2009-12-03 13:04:06 PST	General Electric	FireFox Analyzer
	2009-12-03 13:09:00 PST	2009 Shelby	FireFox Analyzer
	2009-12-04 12:27:45 PST	fox news	FireFox Analyzer
	2009-12-08 12:58:16 PST	vacation packages	FireFox Analyzer
	2009-12-08 13:01:37 PST	mediterranean vacation packages	FireFox Analyzer
	2009-12-08 13:01:46 PST	http://www.expedia.com/pubs/spec/scripts/eap.asp?goto=daily&ssemcid=13172-1&page=/packages/default.asp&cpaid=13172-1&%7Bcreative%7D=&kend=1&keyword=vacation+packages!p.24314717.%7Bifsearch:1%7D%7Bifcontent:0%7D.%7Bcreative%7D.%7Bkeyword%7D.%7Bplacement%7D.vacation+packagesXxXx24683600%7C%7Bifsearch:1%7D%7Bifcontent:0%7D%7C%7Bcreative%7D%7C%7Bkeyword%7D%7C%7Bplacement%7D	FireFox Analyzer
	2009-12-08 13:01:51 PST	http://www.ncl.com/nclweb/cruiser/cmsPages.html?pageId=EuropeCruises&utm_source=Google&utm_medium=ppc&utm_campaign=Europe&s_kwcid=TC 9931 mediterranean%20vacation S p 4024611241	FireFox Analyzer
	2009-12-08 14:17:01 PST	exotic car dealer	FireFox Analyzer
	2009-12-08 14:17:34 PST	ford car dealer	FireFox Analyzer
Considerations	- Web browser logs		

Πίνακας 33 Searched keywords

15) List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)

Possible Answer	Timestamp (Timezone is applied)	Search Keyword
Considerations		

Πίνακας 34 Keywords searched in Windows Explorer

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

Possible Answer	Mozilla Thunderbird
Evidence Location	HKLM\SOFTWARE\Classes\mailto\shell\open\command (→ Mozilla Thunderbird) HKLM\SOFTWARE\Clients\Mail Default (→ Mozilla Thunderbird)

Πίνακας 35 Email Client

17) Where is the e-mail file located?

Possible Answer	/img_charlie-2009-12-11.E01/vol_vol2/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/
Considerations	- Mozilla Thunderbird

Πίνακας 36 Email File Location

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

Possible Answer	charlie@m57.biz
Considerations	-

Πίνακας 37 Email Account

19) List all e-mails of the suspect. If possible, identify deleted e-mails.

Possible Answer <u>(Timezone is applied)</u>	Timestamp	E-Mail Communication								
	Tue, 17 Nov 2009 10:54:17	<table border="1"> <tr> <td>Source</td> <td>[Sent Items]</td> </tr> <tr> <td>From → To</td> <td>charlie@m57.biz → jo@m57.biz</td> </tr> <tr> <td>Subject</td> <td>What's wrong with Pat</td> </tr> <tr> <td>Body</td> <td> <p>Hey Jo,</p> <p>Don't you think Pat is a weird boss? I think there is something funny about him. What do you think?</p> <p>Charlie</p> </td> </tr> </table>	Source	[Sent Items]	From → To	charlie@m57.biz → jo@m57.biz	Subject	What's wrong with Pat	Body	<p>Hey Jo,</p> <p>Don't you think Pat is a weird boss? I think there is something funny about him. What do you think?</p> <p>Charlie</p>
Source	[Sent Items]									
From → To	charlie@m57.biz → jo@m57.biz									
Subject	What's wrong with Pat									
Body	<p>Hey Jo,</p> <p>Don't you think Pat is a weird boss? I think there is something funny about him. What do you think?</p> <p>Charlie</p>									
	Wed, 02 Dec 2009 13:25:45	<table border="1"> <tr> <td>Source</td> <td>[Sent Items]</td> </tr> <tr> <td>From → To</td> <td>charlie@m57.biz → jamie@project2400.com</td> </tr> <tr> <td>Subject</td> <td>Interested?</td> </tr> <tr> <td>Body</td> <td> <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> </td> </tr> </table>	Source	[Sent Items]	From → To	charlie@m57.biz → jamie@project2400.com	Subject	Interested?	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>
Source	[Sent Items]									
From → To	charlie@m57.biz → jamie@project2400.com									
Subject	Interested?									
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>									
	Thu, 3 Dec 2009 09:51:33	<table border="1"> <tr> <td>Source</td> <td>[Inbox Items]</td> </tr> <tr> <td>From → To</td> <td>jamie@project2400.com → charlie@m57.biz</td> </tr> <tr> <td>Subject</td> <td>Re: Interested?</td> </tr> <tr> <td>Body</td> <td> <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> </td> </tr> </table>	Source	[Inbox Items]	From → To	jamie@project2400.com → charlie@m57.biz	Subject	Re: Interested?	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>
Source	[Inbox Items]									
From → To	jamie@project2400.com → charlie@m57.biz									
Subject	Re: Interested?									
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>									

		J
Thu, 3 Dec 2009 12:16:52	Source	[Sent Items]
	From → To	charlie@m57.biz→ jamie@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>
Fri, 4 Dec 2009 09:41:47	Source	[Sent Items]
	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</p>
Fri, 4 Dec 2009 13:06:23	Source	[Sent Items]
	From → To	charlie@m57.biz→ jamie@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>
Mon, 7 Dec 2009 11:44:18	Source	[Sent Items]
	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</p>
Fri, 11 Dec 2009 08:55:53	Source	[Sent Items]
	From → To	pat@m57.biz→ charlie@m57.biz , jo@m57.biz , terry@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>
Evidence Location	Data Artifacts/Email messages	

Πίνακας 38 Essential Emails

20) List external storage devices attached to PC.

Possible Answer	Device Name	Volume Name	Serial No.	First Connected Time	Connected Time After Reboot
	USB 2.0 Flash Disk USB Device				
	SanDisk Cruzer USB Device				
	LaCie Rugged FW/USB USB Device				
	Kingston DataTraveler 2.0 USB Device				
Considerations	HKLM\SYSTEM\MountedDevices\ HKLM\SYSTEM\ControlSet##\Enum\USBSTOR\				

Πίνακας 39 External Storage Devices

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

Possible Answer	192.168.1.1
Considerations	Data Artifacts/Remote Drive

Πίνακας 40 Network Drive IP

22) List all directories that were traversed in 'RM#1'.

Possible Answer (Timezone is applied)	Timestamp	Directory Path	Source
	2009-11-17 10:57:11 PST	F:\	Recent Documents
	2009-12-10 14:28:05 PST	F:\Email\other	Recent Documents
	2009-11-24 13:56:35 PST	F:\microscope.jpg	Recent Documents
	2009-11-24 14:05:29 PST	F:\Copy of microscope.jpg	Recent Documents
Considerations	<ul style="list-style-type: none"> - 'Timestamp' may not be accurate. - F:\ - Recent Documents 		

Πίνακας 41 Directories traversed in RM1

23) List all files that were opened in 'RM#1'.

Possible Answer (Timezone is applied)	Timestamp	Directory Path	Source
	2009-11-17 10:57:11 PST	F:\M57biz.jpg	Recent Documents
	2009-11-24 13:56:35 PST	F:\microscope.jpg	JumpList
	2009-12-10 14:28:05 PST	F:\Email\other	ShellBag (created)

	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	
	2009-12-10 14:28:05 PST	F:\Email\other\QC Project.eml	
	2009-11-17 10:57:11 PST	F:\	
	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	
	2009-11-24 13:56:35 PST	F:\	
	2009-11-24 14:05:29 PST	F:\Copy of microscope.jpg	
Considerations	<ul style="list-style-type: none"> - 'Timestamp' may not be accurate. - F:\ - Recent Documents 		

Πίνακας 42 Files opened in RM1

24) List all directories that were traversed in the company's network drive.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	-	\Z:\	ShellBag
	2009-12-11 07:06:27 PST	\Z:\windd	ShellBag
Considerations	<ul style="list-style-type: none"> - 'Timestamp' may not be accurate. - Z:\ is mapped on \\192.168.1.1 		

Πίνακας 43 Directories traversed in network drive

25) List all files that were opened in the company's network drive.

Possible Answer	Timestamp	Directory Path	Source
	2009-12-11 07:06:31 PST	\\\Z:\windd\32bits_i386	
Considerations	- 'Timestamp' may not be accurate. - Z:\ is mapped on \\192.168.1.1		

Πίνακας 44 Files opened in network drive

26) Find traces related to cloud services on PC.(Service name, log files...)

Δεν υπάρχουν σχετικά traces

27) What files were deleted from Google Drive?

Δεν υπάρχουν σχετικά traces

Κατόπιν περαιτέρω αναζήτησης στο File System βρήκαμε τα εξής:

1. /img_charlie-2009-12-11.E01/vol_vo12/Documents and Settings/Charlie/My Documents/

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
[parent folder]				2009-12-11 08:59:51 PST	2009-12-11 08:59:51 PST	2009-12-11 08:59:53 PST	2009-11-10 17:57:47 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Quantum Cryptography				2009-12-10 14:23:30 PST	2009-12-10 14:23:38 PST	2009-12-10 14:23:38 PST	2009-12-04 13:53:27 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
[current folder]				2009-12-04 13:53:27 PST	2009-12-04 13:53:27 PST	2009-12-10 14:23:38 PST	2009-11-10 17:59:19 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Nitroba				2009-11-30 08:48:14 PST	2009-11-30 08:48:14 PST	2009-12-10 14:20:27 PST	2009-11-19 13:27:33 PST	280	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
microscope1.jpg	V	1		2009-11-24 14:19:41 PST	2009-11-24 14:18:36 PST	2009-11-24 13:40:30 PST	2009-11-24 13:40:30 PST	136274	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Downloads				2009-11-24 13:38:39 PST	2009-11-24 13:38:39 PST	2009-12-10 14:19:44 PST	2009-11-12 17:55:55 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
astronaut1.jpg	1			2009-11-24 13:43:42 PST	2009-11-24 13:44:00 PST	2009-12-10 14:18:36 PST	2009-11-24 13:43:42 PST	722717	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
astronaut.jpg	1			2009-11-24 13:33:53 PST	2009-11-24 13:41:55 PST	2009-12-10 14:18:36 PST	2009-11-24 13:40:28 PST	713418	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
astronaut.jpgZone.Identifier	1			2009-11-24 13:33:53 PST	2009-11-24 13:41:55 PST	2009-12-10 14:18:36 PST	2009-11-24 13:40:28 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
microscope.jpg	V	0		2009-11-24 13:27:51 PST	2009-11-24 14:04:53 PST	2009-12-10 14:18:35 PST	2009-11-24 13:40:30 PST	162274	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
microscope.jpgZone.Identifier	V	0		2009-11-24 13:27:51 PST	2009-11-24 14:04:53 PST	2009-12-10 14:18:35 PST	2009-11-24 13:40:30 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
01.zip	!	1		2009-11-24 13:09:44 PST	2009-12-04 09:41:44 PST	2009-12-04 09:41:47 PST	2009-12-04 09:41:47 PST	108438	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
95253 SCSI.Mathew+Malizia.pdf	!	1		2009-11-20 13:06:49 PST	2009-12-07 11:51:59 PST	2009-12-10 14:20:58 PST	2009-11-20 13:06:48 PST	7390	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
99202 Complexity Theory.Louis+Fleet.pdf	!	1		2009-11-20 13:06:49 PST	2009-12-07 08:39:30 PST	2009-12-08 09:39:30 PST	2009-11-20 13:06:49 PST	59565	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
97315 ScatterGather.OJulie+Molock.pdf	!	1		2009-11-20 13:06:48 PST	2009-11-20 13:06:48 PST	2009-11-30 08:46:45 PST	2009-11-20 13:06:48 PST	64343	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
98521 WANs+Greg+Hiller.pdf	!	1		2009-11-20 13:06:47 PST	2009-12-08 09:39:04 PST	2009-12-09 08:39:03 PST	2009-11-20 13:06:47 PST	99483	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Patents				2009-11-19 08:50:46 PST	2009-12-10 14:20:27 PST	2009-11-19 08:49:08 PST	2009-11-19 08:49:08 PST	592	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
AC7640A9d1.pdf	!	1		2009-11-17 13:54:02 PST	2009-12-07 11:51:59 PST	2009-12-07 16:34:37 PST	2009-11-17 13:54:32 PST	48006	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
23EE12E5d01.pdf	!	1		2009-11-17 13:54:02 PST	2009-12-07 11:51:58 PST	2009-12-09 08:39:31 PST	2009-11-17 13:54:16 PST	768724	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
My Music				2009-11-10 17:58:41 PST	2009-11-11 14:11:01 PST	2009-12-10 14:52:53 PST	2009-11-10 17:58:21 PST	384	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
My Pictures				2009-11-10 17:58:41 PST	2009-11-11 14:11:01 PST	2009-12-10 14:52:53 PST	2009-11-10 17:58:21 PST	384	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
desktop.ini	0			2009-11-10 17:58:41 PST	2009-12-10 17:58:41 PST	2009-12-10 14:52:53 PST	2009-11-10 17:58:21 PST	78	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	

Εικόνα 20 Documents

2. /img_charlie-2009-12-11.E01/vol_vo12/Documents and Settings/Charlie/My Documents/Downloads/

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
[parent folder]				2009-12-04 13:53:32 PST	2009-12-04 13:53:32 PST	2009-12-11 08:59:19 PST	2009-11-10 17:57:47 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
[current folder]				2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-12-10 14:19:44 PST	2009-11-12 17:55:55 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
cygnus.zip	1			2009-11-24 13:58:39 PST	700828								
cygnus.zipZone.Identifier	1			2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
7z465.exe	1			2009-11-24 13:19:39 PST	2009-12-07 11:51:59 PST	2009-12-09 08:39:36 PST	2009-11-24 13:19:39 PST	399956	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
7z465.exeZone.Identifier	1			2009-11-24 13:19:39 PST	2009-12-07 11:51:59 PST	2009-12-09 08:39:36 PST	2009-11-24 13:19:39 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
060402_rpts_torn.csv	0			2009-11-20 13:45:18 PST	2009-11-20 13:45:18 PST	2009-12-09 08:39:48 PST	2009-11-20 09:04:09 PST	9982	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
060402_rpts_torn.csvZone.Identifier	1			2009-11-20 13:45:18 PST	2009-11-20 13:45:18 PST	2009-12-09 08:39:48 PST	2009-11-20 09:04:09 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
alternatif_1.1.exe	V	1		2009-11-19 13:17:15 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-19 13:17:14 PST	484640	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
alternatif_1.1.exeZone.Identifier	1			2009-11-19 13:17:15 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-19 13:17:14 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
PNEUMATIC_BOILING_GLOVE.pdf	1			2009-11-19 08:47:39 PST	2009-11-19 08:47:39 PST	2009-12-09 08:39:38 PST	2009-11-19 08:47:38 PST	295250	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
PNEUMATIC_BOILING_GLOVE.pdfZone.Identifier	1			2009-11-19 08:47:39 PST	2009-11-19 08:47:39 PST	2009-12-09 08:39:38 PST	2009-11-19 08:47:38 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
lightning-0.9-bw.vni.xpi	0			2009-11-18 13:01:14 PST	2009-11-18 13:01:14 PST	2009-12-09 08:39:47 PST	2009-11-18 13:01:13 PST	214261	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
lightning-0.9-bw.vni.xpiZone.Identifier	1			2009-11-18 13:01:14 PST	2009-11-18 13:01:14 PST	2009-12-09 08:39:47 PST	2009-11-18 13:01:13 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
MKspreadsheetTagged.csv	V	1		2009-11-17 16:44:42 PST	2009-11-17 16:44:42 PST	2009-12-09 08:39:44 PST	2009-11-17 16:44:41 PST	128298	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
MKspreadsheetTagged.csvZone.Identifier	1			2009-11-17 16:44:42 PST	2009-11-17 16:44:42 PST	2009-12-09 08:39:44 PST	2009-11-17 16:44:41 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
FoxItReader31_enu_Setup_1030.exe	V	1		2009-11-17 13:30:02 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-17 13:49:59 PST	5313992	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
FoxItReader31_enu_Setup_1030.exeZone.Identifier	1			2009-11-17 13:30:02 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-17 13:49:59 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
python-2.6.ansi	1			2009-11-12 17:55:59 PST	2009-11-10 17:55:59 PST	2009-11-12 17:55:52 PST	2009-11-12 17:55:51 PST	1490496	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
python-2.6.ansiZone.Identifier	1			2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	2009-11-12 17:55:52 PST	2009-11-12 17:55:51 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Thunderbird Setup 2.0.0.23.exe	V	1		2009-11-12 17:52:08 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-12 17:55:51 PST	6873872	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	
Thunderbird Setup 2.0.0.23.exeZone.Identifier	1			2009-11-12 17:52:08 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-12 17:55:51 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol_vo12/Documents and...	

Εικόνα 21 Downloads

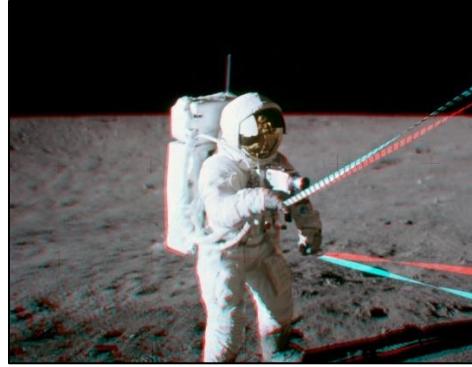
3. /img_charlie-2009-12-11.E01/vol₂/Documents and Settings/Charlie/Desktop/web

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash
[parent folder]				2009-12-04 13:53:32 PST	2009-12-04 13:53:32 PST	2009-11-10 08:59:19 PST	2009-11-10 17:57:47 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	
[current folder]				2009-12-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-12-10 08:59:44 PST	2009-11-12 17:51:55 PST	56	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	
cygnause.zip	1			2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	290828	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7ca54fbefbe61686fe0db4a6d1323
cygnause.zip.Zone.Identifier	1			2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	2009-11-24 13:58:39 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
7z465.exe	1			2009-11-24 13:19:39 PST	2009-12-10 14:19:44 PST	2009-12-09 08:59:36 PST	2009-11-24 13:19:39 PST	539956	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	fcd1b1472302c7c831474d471f1403
7z465.exe.Zone.Identifier	1			2009-11-24 13:19:39 PST	2009-12-10 14:19:44 PST	2009-12-09 08:59:36 PST	2009-11-24 13:19:39 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
066402_rptz_tom.csv	0			2009-11-20 13:45:18 PST	2009-11-20 13:45:18 PST	2009-12-09 08:59:48 PST	2009-11-20 09:41:09 PST	9982	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	809e92696607350c679388d3cf113
066402_rptz_tom.csv.Zone.Identifier	1			2009-11-20 13:45:18 PST	2009-11-20 13:45:18 PST	2009-12-09 08:59:48 PST	2009-11-20 09:41:09 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
alternatif_1.9.exe	▼			2009-11-19 13:17:15 PST	2009-12-10 14:19:44 PST	2009-12-09 08:59:36 PST	2009-11-19 13:17:14 PST	484640	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	48b12783eaab9462e450c2e450c3d7008
alternatif_1.9.exe.Zone.Identifier	1			2009-11-19 13:17:15 PST	2009-12-10 14:19:44 PST	2009-12-09 08:59:36 PST	2009-11-19 13:17:14 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
PNEUMATIC_BOXING_GLOVE.pdf	1			2009-11-19 08:47:39 PST	2009-11-19 08:47:39 PST	2009-12-09 08:39:38 PST	2009-11-19 08:47:36 PST	295250	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	52c44124ea1a2ea1f104f2be62a
PNEUMATIC_BOXING_GLOVE.pdf.Zone.Identifier	1			2009-11-19 08:47:39 PST	2009-11-19 08:47:39 PST	2009-12-09 08:39:38 PST	2009-11-19 08:47:36 PST	295250	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
lightning-0.9-tb-win.vpi	0			2009-11-18 13:01:14 PST	2009-11-18 13:01:14 PST	2009-12-09 08:59:47 PST	2009-11-18 13:01:13 PST	2144261	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	70ebba7c1237e3db99536c991b6
lightning-0.9-tb-win.vpi.Zone.Identifier	1			2009-11-18 13:01:14 PST	2009-11-18 13:01:14 PST	2009-12-09 08:59:47 PST	2009-11-18 13:01:13 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
M1KspreadsheetTagged.csv	▼			2009-11-17 16:44:42 PST	2009-11-17 16:44:42 PST	2009-12-09 08:59:44 PST	2009-11-17 16:44:41 PST	1282920	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	fca894bd212635220f44294a4cd
M1KspreadsheetTagged.csv.Zone.Identifier	1			2009-11-17 16:44:42 PST	2009-11-17 16:44:42 PST	2009-12-09 08:59:44 PST	2009-11-17 16:44:41 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
FoxitReader31_enu_Setup_1030.exe.Zone.Identifier	1			2009-11-17 13:50:02 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-17 13:49:59 PST	5313992	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	c92ea1d1526bd78cfa579597ec
FoxitReader31_enu_Setup_1030.exe.Zone.Identifier	1			2009-11-17 13:50:02 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-17 13:49:59 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942
python-2.6.4.msi	1			2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	14890496	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	2e2bf60ae73e99d343a7fe9ed9f7
python-2.6.4.msi.Zone.Identifier	1			2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	2009-11-12 17:55:59 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7dd1764b6fdefeef1f66698e9942
Thunderbird Setup 2.0.23.exe	▼			2009-11-12 17:52:08 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-12 17:51:55 PST	6873872	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	aed5155377647ec207bf355a
Thunderbird Setup 2.0.23.exe.Zone.Identifier	1			2009-11-12 17:52:08 PST	2009-12-10 14:19:44 PST	2009-12-09 08:39:36 PST	2009-11-12 17:51:55 PST	46	Allocated	Allocated	unknown	/img_charlie-2009-12-11.E01/vol ₂ /Documents and...	7da764b6fdefeef1f66698e9942

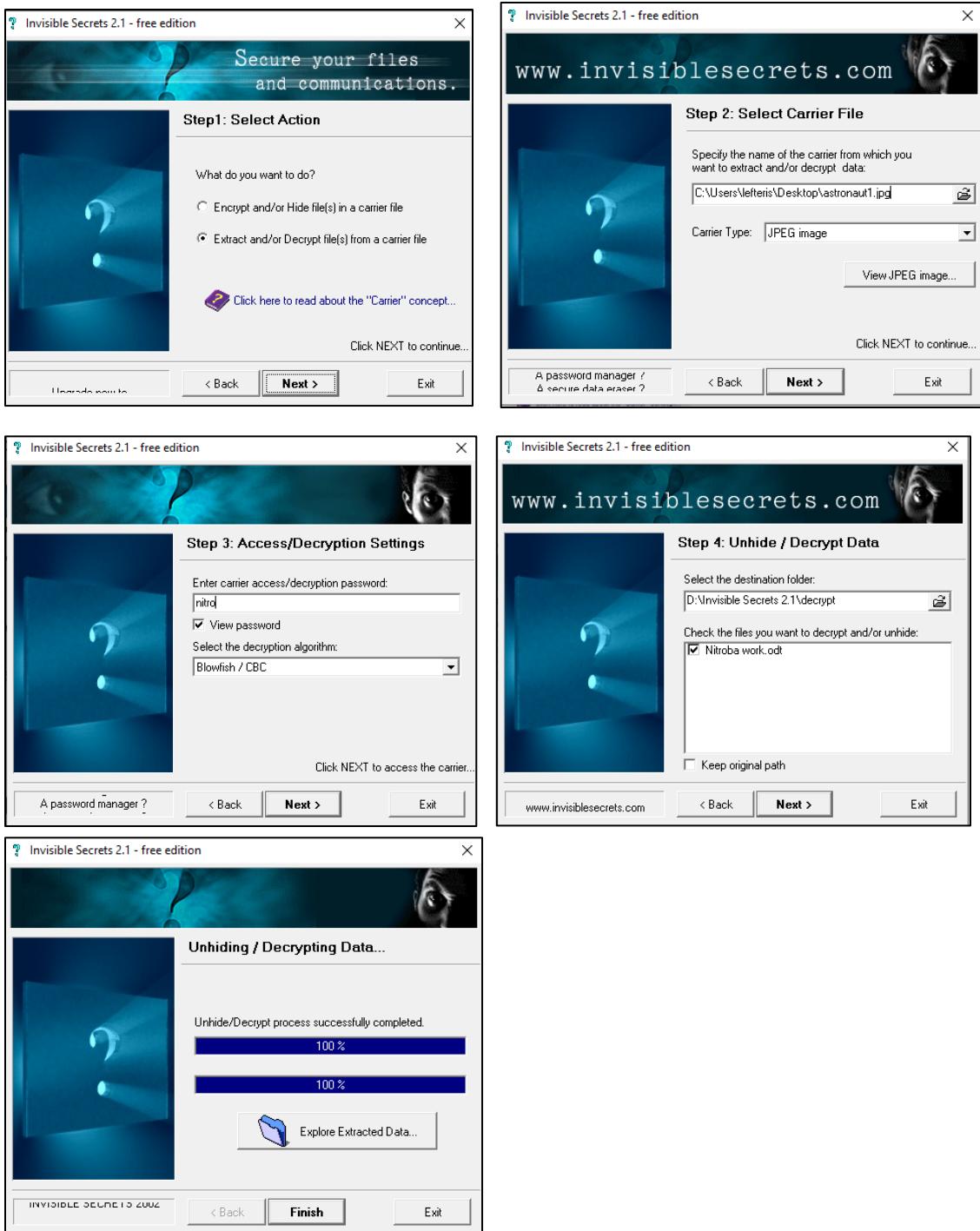
Εικόνα 22 Desktop/web

Ανάλυση κρυπτογραφημένων αρχείων και αρχείων με κρυμμένη πληροφορία (τεχνική στεγανογραφίας).

Αρχικά αναλύεται το **astronaut1.jpg** το οποίο στάλθηκε στην project2400, ανταγωνίστρια εταιρεία της Nitroba.



Στο email αναγραφόταν ότι «πρέπει να χρησιμοποιηθεί το πρόγραμμα steg με κωδικό nitro». Οπότε με χρήση του Invisible Secrets2.1 αντιστρέφουμε την στεγανογραφία για το αρχείο **astronaut1.jpg**.



Επιτυχώς, με τον κωδικό nitro καταφέραμε να εξάγουμε το αρχείο “Nitroba work.odt”, το οποίο είναι το **ίδιο** με αυτό που βρέθηκε στο home directory του Charlie στο file system του laptop. Τρέχουμε τις παρακάτω εντολές για να βρούμε τα MD5, SHA1 hash:

- Get-FileHash -Algorithm MD5 .\Nitroba work.odt
- Get-FileHash -Algorithm SHA1 .\Nitroba work.odt

- Get-FileHash -Algorithm SHA256 .\Nitroba work.odt

Όνομα αρχείου	Nitroba work.odt
SHA1	1837FD381A6A5D462CCF3E381761834F3E389B28
MD5	56FD56FC40B7C6D7B7572711F863BC8D
SHA256	10D6EF8C863C2165F2D846FD68B48C0B9C73E7F579D25080DA89D493AF067F04

Σύγκριση με Autopsy:

MD5:	56fd56fc40b7c6d7b7572711f863bc8d
SHA-256:	10d6ef8c863c2165f2d846fd68b48c0b9c73e7f579d25080da89d493af067f04

Περιεχόμενα αρχείου:

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

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

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

PriorityData:

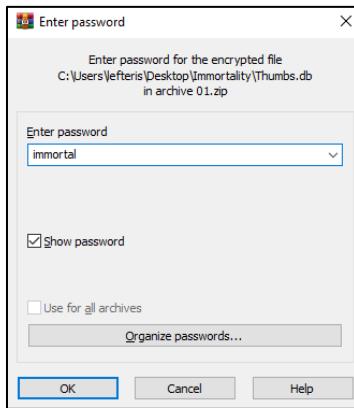
11/700,015 31.01.2007 US

Title: SIMULATION SYSTEM IMPLEMENTING REAL-TIME MACHINE DATA

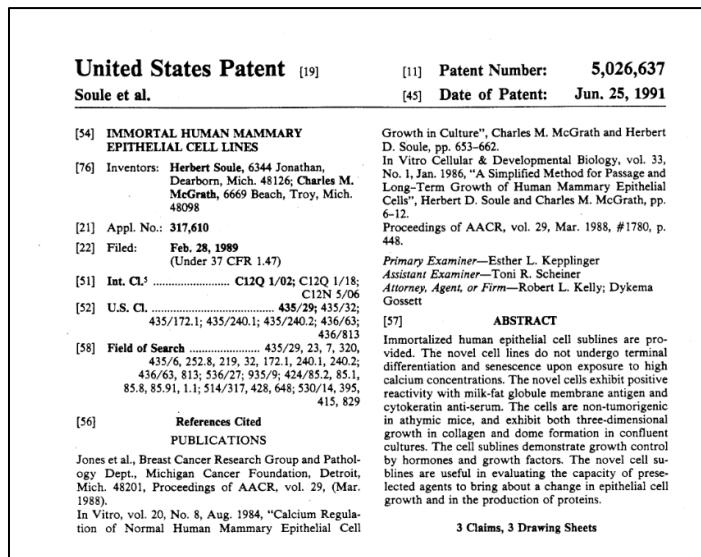
Έπειτα αναλύουμε τα **01.zip** και **microscope1.jpg**. Ανοίγουμε με έναν hex editor το αρχείο microscope1.jpg. Βλέπουμε το εξής:

Decoded text
JFIF.....
.....ÿÛ.C.....
.....
.....
.....
.....
.....ÿÛ.C...
.....
.....
.....
password=immorta
l.....ÿÀ
....e.s..".....
..ÿÀ.....
.....

Υπάρχει το κείμενο “password=immortal”. Δοκιμάζουμε να αποσυμπιέσουμε το 01.zip με τον κωδικό “immortal”:



Πλέον τα αρχεία εμφανίζονται, και βρίσκουμε τα us005026637-001.tif και us006982168-001.tif. Τα περιεχόμενά τους αντίστοιχα φαίνονται στις εικόνες:



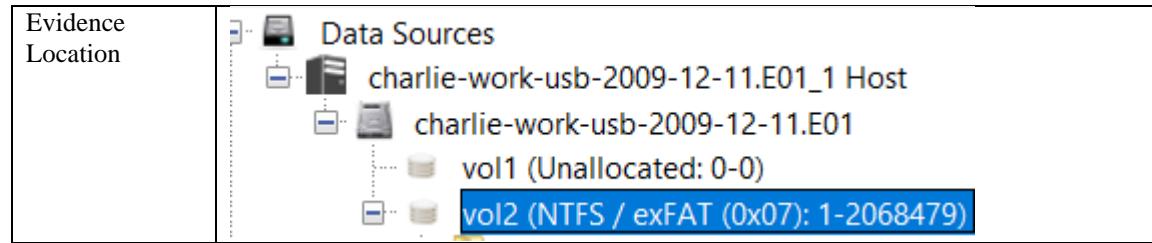
 United States Patent Topalian et al.		(10) Patent No.: US 6,982,168 B1 (45) Date of Patent: Jan. 3, 2006
<p>(54) IMMORTAL HUMAN PROSTATE EPITHELIAL CELL LINES AND CLONES AND THEIR APPLICATIONS IN THE RESEARCH AND THERAPY OF PROSTATE CANCER</p> <p>(75) Inventors: Suzanne L. Topalian, Brookville, MD (US); W. Marston Linehan, Rockville, MD (US); Robert K. Bright, Portland, OR (US); Cathy B. Vocke, Germantown, MD (US)</p> <p>(73) Assignee: The United States of America as represented by the Department of Health and Human Services, Washington, DC (US)</p> <p>(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.</p> <p>(21) Appl. No.: 08/913,770</p> <p>(22) PCT Filed: Jan. 30, 1997</p> <p>(86) PCT No.: PCT/US97/01430</p> <p>§ 371 (c)(1), (2), (4) Date: Sep. 22, 1997</p> <p>(87) PCT Pub. No.: WO97/28255</p> <p>PCT Pub. Date: Aug. 7, 1997</p> <p>Related U.S. Application Data</p> <p>(60) Provisional application No. 60/011,042, filed on Feb. 2, 1996.</p> <p>(51) Int. Cl. C12N 15/85 (2006.01)</p> <p>(52) U.S. CL 435/325; 435/366; 435/371; 435/384; 435/385; 435/386</p> <p>(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.</p> <p>(56) References Cited</p> <p>U.S. PATENT DOCUMENTS</p> <p>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 Chepen 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</p> <p>FOREIGN PATENT DOCUMENTS</p> <p>WO WO 92/16645 10/1992 WO WO 95/29990 11/1995 WO WO 95/29994 11/1995</p>		
<p>OTHER PUBLICATIONS</p> <p>Chiarello, E. <i>Oncogene</i> 16: 541-545, 1998.* Kekemir, <i>Genes Chromosomes Cancer</i> 11:195-198, 1994.* Drexler, <i>Leukemia & Lymphoma</i> 9:1-25, 1993.* Embleton, <i>Immunol. Ser.</i> 23:181-207, 1984.* Hea, In: <i>Tissue Culture Meth. & Applications</i>, Kruse & Patterson, Eds., p. 764, 1973.* Mustafa O. <i>Int. J. Oncol.</i> 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" <i>Cancer Genet. Cytogenet.</i> vol. 96, pp. 123-128, 1997.* Freshney, <i>Culture of Animal Cells. A manual of basic technique</i> chapter 13, p. 130, 1983.* Smith, R. T. "Cancer and the immune system" <i>Clinical Immunology</i>, vol. 41 No. 4, pp. 841-850, Aug. 1994.* McNamee J. M et al. <i>Gene Therapy</i> 7(8): 653-63, 2000.* Panda et al., "Neoplastic Transformation of a Human Prostate Epithelial Cell Line by the v-Ki-ras Oncogene", <i>The Prostate</i> 23:91-98 (1993). Hayward et al., "Establishment and Characterization of an Immortalized But Non-Transformed Human Prostate Epithelial Cell Line: BPH-1", <i>In Vitro Cell Dev. Biol.</i> 31A:14-24, Jun. 1995. Castagnetti et al., "Prostate Long-Term Epithelial Cell Lines", <i>Annals of The New York Academy of Sciences</i>, vol. 595, pp. 149-164, 1990. Bouidou et al., "Distinct Androgen 5α-Reduction Pathways in Cultured Fibroblasts and Immortalized Epithelial Cells From Normal Human Adult Prostate", <i>The Journal of Urology</i>, vol. 152, 226-231, Jul. 1994. Narayan et al., "Establishment and Characterization of a Human Primary Prostatic Adenocarcinoma Cell Line (ND-1)", <i>The Journal of Urology</i>, vol. 148, 1600-1604, Nov. 1992. Rham et al., "Stepwise immortalization and transformation of adult human prostate epithelial cells by a combination of HPV-18 and v-Ki-ras", <i>Proc. Natl. Acad. Sci. USA</i>, vol. 91, pp. 11874-11878, Dec. 1994.</p> <p style="text-align: center;">(Continued)</p> <p><i>Primary Examiner</i>—Susan Ungar <i>Assistant Examiner</i>—Miah-Tam Davis (74) Attorney, Agent, or Firm—Leydig, Voit & Mayer, Ltd.</p>		
<p>(57) ABSTRACT</p> <p>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.</p> <p style="text-align: center;">21 Claims, 6 Drawing Sheets</p>		

Παράτημα ΣΤ – Ανάλυση USB

Από την ανάλυση του USB στο Autopsy βλέπουμε πολλές χρήσιμες πληροφορίες για το case. Ο ύποπτος έχει αντιγράψει σε αυτό αρχεία τα οποία μπορούν να υποστηρίξουν την ενοχή του.

1) Identify the partition information of USB image

Possible Answer	No.	Bootable	File system	Start Sector	Total Sectors	Size
	1		Unknown	0	0	512 B
	2	*	NTFS	1	2068479	132.382.208B



Πίνακας 45 USB Partition details

2) Listing all the essential emails

Possible Answer <u>(Timezone is applied)</u>	Timestamp	E-Mail Communication								
	Wed, 02 Dec 2009 13:25:45	<table border="1"> <tr> <td>Source</td><td>[Sent Items]</td></tr> <tr> <td>From → To</td><td>charlie@m57.biz → jamie@project2400.com</td></tr> <tr> <td>Subject</td><td>Interested?</td></tr> <tr> <td>Body</td><td> <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> </td></tr> </table>	Source	[Sent Items]	From → To	charlie@m57.biz → jamie@project2400.com	Subject	Interested?	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>
Source	[Sent Items]									
From → To	charlie@m57.biz → jamie@project2400.com									
Subject	Interested?									
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>									
	Thu, 3 Dec 2009 09:51:33	<table border="1"> <tr> <td>Source</td><td>[Inbox Items]</td></tr> <tr> <td>From → To</td><td>jamie@project2400.com → charlie@m57.biz</td></tr> <tr> <td>Subject</td><td>Re: Interested?</td></tr> <tr> <td>Body</td><td> <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> </td></tr> </table>	Source	[Inbox Items]	From → To	jamie@project2400.com → charlie@m57.biz	Subject	Re: Interested?	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>
Source	[Inbox Items]									
From → To	jamie@project2400.com → charlie@m57.biz									
Subject	Re: Interested?									
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>									
	Thu, 3 Dec 2009 12:16:52	<table border="1"> <tr> <td>Source</td><td>[Sent Items]</td></tr> <tr> <td>From → To</td><td>charlie@m57.biz → jamie@project2400.com</td></tr> <tr> <td>Subject</td><td></td></tr> <tr> <td>Body</td><td> <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> </td></tr> </table>	Source	[Sent Items]	From → To	charlie@m57.biz → jamie@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>
Source	[Sent Items]									
From → To	charlie@m57.biz → jamie@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>									
	Fri, 4 Dec 2009 09:41:47	<table border="1"> <tr> <td>Source</td><td>[Sent Items]</td></tr> <tr> <td>From → To</td><td>charlie@m57.biz → andy@swexpert.com</td></tr> <tr> <td>Subject</td><td>I Found Something</td></tr> <tr> <td>Body</td><td> <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> </td></tr> </table>	Source	[Sent Items]	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>
Source	[Sent Items]									
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>									

		C
	Fri, 4 Dec 2009 13:06:23	<p>Source [Sent Items]</p> <p>From → To charlie@m57.biz → jamie@project2400.com</p> <p>Subject Instructions</p> <p>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</p>
	Mon, 7 Dec 2009 11:44:18	<p>Source [Sent Items]</p> <p>From → To charlie@m57.biz → andy@swexpert.com</p> <p>Subject Picture</p> <p>Body Andy, Here's the picture I promised... Make sure you delete this. C</p>
	Fri, 11 Dec 2009 08:55:53	<p>Source [Sent Items]</p> <p>From → To pat@m57.biz → charlie@m57.biz, jo@m57.biz, terry@m57.biz</p> <p>Subject Important Meeting</p> <p>Body Team, 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. Pat</p>
Evidence Location	Data Artifacts/Email messages	

Πίνακας 46 USB Essential Emails

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

Possible Answer	charlie@m57.biz
Considerations	Data Artifacts/Communication Accounts/Email

Πίνακας 47 USB Email account

4) *What was the e-mail account the suspect had communicated?*

Possible Answer	jaime@project2400.com
Considerations	Data Artifacts/Communication Accounts/Email

Πίνακας 48 USB Email account communication

7) Which are the email addresses the suspect had communication:

Emails	jaime@project2400.com ,
	4B16D65D.4060604@m57.biz
	alix.pery@yahoo.com
	charlie@m57.biz
	jaspermcraehelvick@yahoo.com
	jo@m57.biz
	pat@m57.biz
	andy@swexpert.com
	z31@mail.com
	Bfritz31@mail.com
	rubinfritz31@mail.com

	terry@m57.biz
--	--

6) *Where are the deleted files?*

Possible Answer	Charlie_2009-11-20_1303_Sent.txt, Charlie_2009-12-02_1305_Received_Part 1.2
Evidence Location	File Views/Deleted Files/File System

Πίνακας 49 USB Deleted Files

7) Are there any exe files?

Possible Answer	Invsecr2.exe
Description	Εφαρμογή για κρυπτογράφηση/αποκρυπτογράφηση εικόνων. Πιθανώς έχει χρησιμοποιηθεί από τον χρήστη.
Evidence Location	img_charlie-work-usb-2009-12-11.E01/vol_vol2

Πίνακας 50 USB exe files

6) Are there any zip files?

Possible Answer	3 zip αρχεία, τα 2 από αυτά απαιτούν κωδικό για να γίνουν εξαγωγή
Description	Το μοναδικό αρχείο που είναι zip και μπορεί να γίνει εξαγωγή είναι το Charlie_Email το οποίο περιλαμβάνει όλη την αλληλογραφία του υπόπτου. Στα άλλα 2 αρχεία απαιτείται κωδικός για να γίνουν εξαγωγή. Αν πατήσει κάποιος πάνω τους μπορεί να δει έναν φάκελο με όνομα Immortality που περιέχει 2 αρχεία .tif. Ωστόσο, ο φάκελος Immortality μαζί με τα περιεχόμενα του είναι προσβάσιμος από το Directory path του USB, χωρίς να απαιτείται κάποιος κωδικός πρόσβασης.
Evidence Location	img_charlie-work-usb-2009-12-11.E01/vol_vol2/01.zip/Immortality

Πίνακας 51 USB zip files

Παράρτημα Ζ – Εξοπλισμός Εργαστηρίου

Hardware Εξοπλισμός

1. Ηλεκτρονικός Υπολογιστής / Desktop Workstation ερευνητών



Εικόνα 23 Desktop Workstation (Windows 10 dual boot Ubuntu)

2. Φορητοί Υπολογιστές / Laptop Workstations



Εικόνα 24 Laptop Workstations (2 Windows 7, 1Linux Mint)

3. Σκληροί Δίσκοι για αποθήκευση προγραμμάτων και backup



Εικόνα 25 HDDs για αποθήκευση λογισμικού και backup

4. DVR



Εικόνα 26 DVR για αποθήκευση video footage

5. Κάμερες παρακολούθησης



Εικόνα 27 Κάμερες παρακολούθησης LAB

6. Συσκευές ανάγνωσης εξωτερικών components (CD/DVD, σκληροί δίσκοι)



Εικόνα 28 CD/DVD external reader



Eικόνα 29 HDD/SSD external reader (SATA connection)



Eικόνα 30 Write blocker

7. Bootable σκληροί δίσκοι και Live USBs με ειδικά λειτουργικά συστήματα



Eικόνα 31 Qubes OS SSD and CAINE OS USB

8. Smartphones και Tablet Android



Εικόνα 32 Android smartphones (version 7, 9, 13)



Εικόνα 33 Android 4 tablet

9. Ειδικοί αντάπτορες για ανάγνωση από εξωτερικές πηγές



Εικόνα 34 USB Type A to Type C, SD card readers

10. Λοιπός καλωδιακός εξοπλισμός (ρεύματος, μεταφοράς δεδομένων, δικτύου κλπ.)



Εικόνα 35 Connectivity cables

11. Φωτογραφική μηχανή



Εικόνα 36 Φωτογραφική Μηχανή

12. Smartphone Repair Tool Kit



Εικόνα 37 Smart Phone Tool Kit

13. Access Card System



Εικόνα 38 Access Card System για ελεγχόμενη πρόσβαση στο LAB

Software Εξοπλισμός

To software αυτό είναι εγκατεστημένο στα workstations, καθώς και σε εφεδρικούς HDD.

Memory & Disk Imaging and Live Acquisition
FTK Imager
DD
EnCase
Live Response Collection
Memory Analysis
Volatility Framework 2.6
Volatility Framework 3
'Ετοιμα custom scripts για data acquisition
Disk Analysis

Autopsy 4.21
FEX Imager
Network Analysis
GNS 3
Network Miner 2.8.1
Operating Systems
Windows 10
Ubuntu Linux 22.04
Linux Mint 21.3
Caine OS 13
Qubes OS 4.2.1
Kali Linux 2019.1

Παράρτημα Η – RACI Matrix

	Expert Witness (Αργυρίου Νικόλαος)	Technical Witness A (Γκίνης Ευάγγελος)	Technical Witness B (Γεωργιάδης Ελευθέριος)
1. Προετοιμασία			
1.1 Προετοιμασία των απαιτούμενων ενταλμάτων και εξουσιοδοτήσεων έρευνας / συμβάσεις	A, R	I	I
1.2 Επικοινωνία με τους υπεύθυνους της εταιρείας	A, R	I	I
1.3 Οργάνωση της ομάδας ερευνητών και ανάθεση ρόλων	A, R	I	I
1.4 Επιλογή κατάλληλων εργαλείων που πρόκειται να χρησιμοποιηθούν (jump bags)	A, C	R	I
1.5 Ενημέρωση σχετικά με την ισχύουσα νομοθεσία	A, R	I	I
1.6 Σχεδιάζεται – αποφασίζεται η διαδικασία βάσει της οποίας θα πραγματοποιηθεί η έρευνα με στόχο τη συλλογή του μέγιστου αριθμού των αποδείξεων στον ελάχιστο δυνατό χρόνο, ελαχιστοποιώντας τις επιπτώσεις στο θύμα.	A	I	R
2. Εντοπισμός & Ανίχνευση			
2.1 Αποκλεισμός σκηνής η-εγκλήματος	A	R	I
2.2 Διαρκής αναλυτική καταγραφή σε ειδικές φόρμες (π.χ., Chain of Custody)	A	I	R
2.3 Καταγραφή των παρευρισκομένων	A	R	I
2.4 Συνέντευξη με τους παρευρισκόμενους	A, C	R	I
2.5 Σχεδιάγραμμα τοπολογίας δικτύου	A	I	R
2.6 Ερωτηματολόγια στους παρόντες στο χώρο (IT)	A	R	I
2.7 Ερωτηματολόγια στους παρόντες στο χώρο (RnD department)	A	I	R
2.8 Φωτογράφιση χώρου	A, C	R	I
2.9 Σχεδιάγραμμα χώρου	A	I	R
2.10 Αναλυτική Καταγραφή του εξοπλισμού – πηγών ψηφιακών πειστριών (Μοντέλο, serial number, καταγραφή τυχόν βλάβης)	A	I, C	R
2.10.1 Καταγραφή της κατάστασης του εξοπλισμού (ενεργοί, μη ενεργοί Ή/Ν, συνδεδεμένοι στο δίκτυο) ΠΡΟΣΟΧΗ: όλες οι συσκευές θα πρέπει να παραμείνουν ως έχουν και οι εκτυπωτές πρέπει να τελειώσουν τις τρέχουσες εκτυπώσεις τους	A, C	I	R

2.11 Έλεγχος των συνδεδεμένων συσκευών μέσω ασύρματου δικτύου (με wireless signal detector)	A	R	I, C
2.12 Αναζήτηση για σημειωματάρια και σημαντικά έγγραφα που μπορεί να περιέχουν κωδικούς πρόσβασης, στοιχεία επικοινωνίας κ.ά.	A	R	I
2.13 Έλεγχος τήρησης των παραπάνω ενεργειών	A, R	I	I
3. Διαφύλαξη			
3.1 Συλλογή πειστηρίων από ενεργές συσκευές	A	R	I, C
3.2 Συλλογή πειστηρίων από κάμερες ασφαλείας και access control συστήματα	A	I, C	R
3.3 Τοποθέτηση αποδεικτικής ταινίας (evidence tape) στις θύρες των συσκευών (power button, usb ports, cd/dvd drives)	A	R	I, C
3.3 Τοποθέτηση αναγνωριστικών ετικετών σε συσκευές, καλώδια, και άλλα αποδεικτικά στοιχεία	A, C	I	R
3.4 Πακετάρισμα συσκευών σε χάρτινες κούτες και ειδικές σακούλες (αδιάβροχες, αντιστατικές)	A, C	R	R
3.5 Ασφαλής μεταφορά στον εργαστηριακό χώρο (ενημέρωση Chain of Custody φόρμας)	A	I	R
3.6 Έλεγχος τήρησης των παραπάνω ενεργειών	A, R	I	I
4. Ανάλυση			
4.1 Καταχώρηση στοιχείων η-εγκλήματος	A	R	I
4.2 Λήψη backup σε off-site σημεία (π.χ., cloud)	A	I	R
4.3 Μελέτη μνήμης	A	R	I, C
4.4 Μελέτη δίσκου	A	I, C	R
4.5 Μελέτη εξωτερικών πηγών (π.χ., USB)	A	R	I, C
4.6 Συγκέντρωση αποδεικτικών στοιχείων	A, C	R	R
5. Παρουσίαση			
5.1 Εξαγωγή τελικού πορίσματος	A, R	I	I
5.2 Προετοιμασία υλικού για δικαστήριο	A, R	I	I

Εικόνα 39 RACI Matrix

Παράτημα Θ – Chain of Custody Φόρμα

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: **103972641** Offense: Data leakage (11122009)

Submitting Officer: (Name/ID#) **Evangelos Gkinis(2)**

Victim: **M57Biz.**

Suspect: **Charlie**

Date/Time Seized: **11/12/2009 10:10:05 PST** Location of Seizure: **M57's Office**

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
001	1	Laptop (Used by Charlie)
001a	1	USB Flash (Charlie's USB Flash)
001b	1	HDD (Charlie's Laptop)
001c	1	Battery(Charlie's Laptop)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
001	11/12/2009, 14:00:00	Terry(IT Admin)	Evangelos Gkinis(2)	M57's Office/Charlie Office
001a	11/12/2009, 14:00:00	Terry(IT Admin)	Evangelos Gkinis(2)	M57's Office/Charlie Office
001b	11/12/2009, 14:00:00	Terry(IT Admin)	Evangelos Gkinis(2)	M57's Office/Charlie Office
001c	11/12/2009, 14:00:00	Terry(IT Admin)	Evangelos Gkinis(2)	M57's Office/Charlie Office
001	11/12/2009, 15:10:00	Evangelos Gkinis(2)	Georgiadis Eleftherios (1)	Lab (Ευελπίδων 47)
001a	11/12/2009, 15:10:00	Evangelos Gkinis(2)	Georgiadis Eleftherios (1)	Lab (Ευελπίδων 47)

001b	11/12/2009, 15:10:00	Evangelos Gkinis(2)	Georgiadis Eleftherios (1)	Lab (Ευελπίδων 47)
001c	11/12/2009, 15:10:00	Evangelos Gkinis(2)	Georgiadis Eleftherios (1)	Lab (Ευελπίδων 47)

Παράρτημα I – Νομοθεσία

Στη φάση της προετοιμασίας, είναι απαραίτητο να διασφαλίσουμε ότι όλα τα μέλη της ομάδας που θα διερευνήσει το συμβάν κατανοούν και σέβονται τους νόμους που ορίζονται και τις διαδικασίες που πρέπει να ακολουθήσουν. Συγκεκριμένα πρέπει να γνωρίζουν για:

- Το νόμο 4624/2019 περί Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).
- Νόμιμη Εξουσιοδότηση: Πριν από οποιαδήποτε έρευνα, πρέπει να υπάρχει κατάλληλη εξουσιοδότηση. Αυτό μπορεί να περιλαμβάνει εντάλματα έρευνας ή εταιρική εξουσιοδότηση, ειδικά όταν η έρευνα περιλαμβάνει την εξέταση εταιρικών συσκευών ή λογαριασμών.
- Chain of Custody: Για να διασφαλιστεί η αξιοπιστία των αποδεικτικών στοιχείων στο δικαστήριο, πρέπει να τηρείται μια σαφής αλυσίδα κύριας ευθύνης που καταγράφει ποιος έχει πρόσβαση στα δεδομένα, πότε, και για ποιο σκοπό.
- Το άρθρο 292Α του ποινικού κώδικα περί εγκλημάτων κατά της ασφάλειας τηλεφωνικών επικοινωνιών.
- Το άρθρο 292Β του Ποινικού κώδικα περί Παρακώλυσης λειτουργίας πληροφοριακών συστημάτων.
- Το άρθρο 292Γ του Ποινικού κώδικα περί μέσων και εργαλείων εκμετάλλευσης για την διάπραξη των εγκλημάτων που ορίζονται στο άρθρο 292Β.
- Το άρθρο 348Β του Ποινικού κώδικα περί προσέλκυσης παιδιών για γενετήσιους λόγους.
- Το άρθρο 370Β του Ποινικού κώδικα περί παράνομης πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα.
- Το άρθρο 370Γ του Ποινικού κώδικα περί Παράνομης πρόσβασης σε πληροφοριακό σύστημα.
- Το άρθρο 370Δ του Ποινικού κώδικα περί χρήσης τεχνικών μέσων για την παρακολούθηση ή αποτύπωσης σε υλικό φορέα μη δημόσιων διαβιβάσεων δεδομένων από, προς ή εντός πληροφοριακού συστήματος.
- Το άρθρο 370Ε του Ποινικού κώδικα περί αγοράς, παραγωγής, παροχής, πώλησης συσκευών ή προγραμμάτων υπολογιστή σχεδιασμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β,370Γ.

- Το άρθρο 379 του Ποινικού κώδικα περί Φθοράς ψηφιακών δεδομένων.
- Το άρθρο 379Α του Ποινικού κώδικα περί Φθοράς ψηφιακών δεδομένων σε διακεκριμένες περιπτώσεις στο πλαίσιο εγκληματικής οργάνωσης.
- Το άρθρο 381Α του Ποινικού κώδικα περί Φθοράς ηλεκτρονικών δεδομένων.
- Το άρθρο 381Β του Ποινικού κώδικα περί αγοράς, παραγωγής, παροχής, πώλησης συσκευών ή προγραμμάτων υπολογιστή σχεδιασμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α.
- Το άρθρο 386Α του Ποινικού κώδικα περί απάτης με υπολογιστή.

Παράρτημα ΙΑ – Σύμβαση

ΣΥΜΒΑΣΗ ΕΡΓΑΣΙΑΣ

Ανάμεσα στην M75Biz με έδρα τη Λ. Ευέλπιδων 47,Αθήνα , και την ομάδα ανάλυσης ψηφιακών πειστηρίων, αναφερόμενη ως "Crime Seen", αποτελούμενη από τους Αργυρίου Νικόλαο, Γκίνης Ευάγγελο και Γεωργιάδη Ελευθέριο έχει συμφωνηθεί η παρακάτω σύμβαση εργασίας:

Άρθρο 1: Αντικείμενο

1.1 Η M75Biz αναθέτει στα μέλη της "Crime Seen" τη διερεύνηση και ανάλυση ενός πιθανού ηλεκτρονικού εγκλήματος που διαπράχθηκε στην έδρα της εταιρείας.

1.2 Τα καθήκοντα των μελών της ομάδας περιλαμβάνουν, αλλά δεν περιορίζονται στην ανάλυση των ψηφιακών αποδεικτικών στοιχείων, την εκπόνηση τεχνικών εκθέσεων, τη συλλογή δεδομένων και οποιαδήποτε άλλη ενέργεια απαιτείται για την ολοκλήρωση της διερεύνησης.

Άρθρο 2: Διάρκεια

2.1 Η σύμβαση αυτή ισχύει για τη διάρκεια της διερεύνησης και ανάλυσης του εγκλήματος, μέχρι την παρουσίαση των τελικών εκθέσεων στο δικαστήριο.

Άρθρο 3: Αμοιβή

3.1 Η M75Biz δεσμεύεται να καταβάλει το ποσό των 7000\$ στην ομάδα "Crime Seen", το οποίο θα χρηματοδοτηθεί ανάλογα με το πρόγραμμα πληρωμής που θα συμφωνηθεί μεταξύ των μερών.

Άρθρο 4: Ευθύνη

4.1 Τα μέλη της "Crime Seen" αναλαμβάνουν την ευθύνη για την εκτέλεση των καθηκόντων τους με επαγγελματισμό και σύμφωνα με τις βέλτιστες πρακτικές.

Άρθρο 5: Εμπιστευτικότητα

5.1 Οι Εργαζόμενοι δεσμεύονται να διατηρήσουν απόλυτη εμπιστευτικότητα & εχεμύθεια σχετικά με τα δεδομένα και τις πληροφορίες που θα έλθουν στην κατοχή τους κατά την διάρκεια της εκτέλεσης των καθηκόντων τους.

Αυτή η σύμβαση εργασίας αποτελεί νομικά δεσμευτικό έγγραφο και τίθεται υπό την ισχύ των νόμων της Ελλάδας/Αττικής.

Για τον Εργοδότη:

[Υπογραφή]

[Όνομα και Θέση]

Για την ομάδα:

[Υπογραφή]

[Όνομα και Θέση]

Παράρτημα IB – Καταγραφή φόρμας σκληρού δίσκου

Φόρμα στοιχείων σκληρού δίσκου

Τεχνικές Προδιαγραφές Σκληρού δίσκου

Case ID	103972641
Κατασκευαστής	SEAGATE
S/N	890000107102
Κύλινδροι	40,000
Κεφαλές	2
Δίσκοι	(1)
Χωρητικότητα	10239860736 Bytes

Λεπτομέρειες κατάσχεσης σκληρού δίσκου

Ηταν προσαρτημένος ο δίσκος;	ΝΑΙ
Ηταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;	ΝΑΙ
Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε;	Αφαιρέθηκε η εξωτερική πηγή ενέργειας και κατόπιν η μπαταρία. Έπειτα ο Technical witness άνοιξε το laptop από την κάτω πλευρά, αποσύνδεσε τον δίσκο και τον τοποθέτησε σε αντιστατική σακούλα με προορισμό το εργαστήριο.
Ηταν ο δίσκος προστατευμένος με κωδικό πρόσβασης;	ΟΧΙ

Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι;

Δημιουργία αντιγράφου

Εφαρμογή δημιουργίας αντιγράφου	Access Data FTK Imager	'Έκδοση	4.7.1.2
Τόπος λήψης πιστού αντιγράφου	M57 office		
Ημερομηνία λήψης πιστού αντιγράφου	11/12/2009		
hashes	<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. Try the new cross-platform PowerShell https://aka.ms/pscore6 PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm SHA1 .\charlie-2009-12-11.mddramimage Algorithm Hash ----- --- SHA1 15C1AE5E2AC3DA7A9CDAAA9A162AA9AC9DDE3D9D Ασφάλεια Πληροφ... PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm MD5 .\charlie-2009-12-11.mddramimage Algorithm Hash ----- --- MD5 38067CC457546B3156975D9A52D4229F Ασφάλεια Πληροφ... PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm MD5 .\charlie-2009-12-11.E01 Algorithm Hash ----- --- MD5 A459F1AA45941AD4FA22D5CB9D35F7FC PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm SHA1 .\charlie-2009-12-11.E01 Algorithm Hash ----- --- SHA1 EE1D5FEBB63DEF90C2900B6984D21A6A137F00CE PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm MD5 .\charlie-work-usb-2009-12-11.E01 Algorithm Hash ----- --- MD5 8C23941655B3313F4A31A1A66085BE86 PS D:\Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων ΟΠΑ\Β' Εξάμηνο\Ψηφιακά Πληροφορία > Get-FileHash -Algorithm SHA1 .\charlie-work-usb-2009-12-11.E01 Algorithm Hash ----- --- SHA1 E49BF6048856570CC3D49B1485D6D87AAAB6AB0A</pre>		

Εγκληματολόγος ερευνητής που έκανε την κατάσχεση

Όνοματεπώνυμο	Ελευθέριος Γεωργιάδης	Τίτλος	Technical Witness
Τηλέφωνο		Τμήμα	Technical Dpt
Υπογραφή		Ημ/νια	11/12/2009

Παράρτημα ΙΓ – Εικόνες

Εικόνα 1 Βήματα Διαδικασίας.....	10
Εικόνα 2 Κάτοψη χώρου εταιρείας M57	12
Εικόνα 3 Τοπολογία δικτύου της εταιρείας	13
Εικόνα 4 Οθόνη στο laptop του Charlie, όπως αυτή βρέθηκε	14
Εικόνα 5 USB δίπλα από το laptop του Charlie, όπως αυτό βρέθηκε	14
Εικόνα 6 Charlie's Laptop.....	18
Εικόνα 7 Charlie's USB	18
Εικόνα 8 Charlie's Laptop SSD	19
Εικόνα 9 Charlie's Laptop Power Supply Unit	19
Εικόνα 10 Charlie's Laptop Battery	19
Εικόνα 11α Εύρημα Αλληλογραφίας (astronaut1.jpg)	24
Εικόνα 12β Εύρημα Αλληλογραφίας (microscope1.jpg)	24
Εικόνα 13 Timeline Αλληλογραφίας	25
Εικόνα 14 Οργανόγραμμα Εταιρείας	32
Εικόνα 15 Κάτοψη χώρου εταιρείας M57	33
Εικόνα 16 Οθόνη στο laptop του Charlie, όπως αυτή βρέθηκε	34
Εικόνα 17 USB δίπλα από το laptop του Charlie, όπως αυτό βρέθηκε	34
Εικόνα 18 Timeline σημαντικών γεγονότων	40
Εικόνα 19 Ηλεκτρονική Αλληλογραφία του Charlie	41
Εικόνα 20 Documents	66
Εικόνα 21 Downloads.....	66
Εικόνα 22 Desktop/web.....	67
Εικόνα 23 Desktop Workstation (Windows 10 dual boot Ubuntu)	75
Εικόνα 24 Laptop Workstations (2 Windows 7, 1Linux Mint).....	75
Εικόνα 25 HDDs για αποθήκευση λογισμικού και backup	75
Εικόνα 26 DVR για αποθήκευση video footage.....	76
Εικόνα 27 Κάμερες παρακολούθησης LAB	76
Εικόνα 28 CD/DVD external reader.....	76
Εικόνα 29 HDD/SSD external reader (SATA connection)	77
Εικόνα 30 Write blocker.....	77
Εικόνα 31 Qubes OS SSD and CAINE OS USB	77
Εικόνα 32 Android smartphones (version 7, 9, 13).....	78
Εικόνα 33 Android 4 tablet	78
Εικόνα 34 USB Type A to Type C, SD card readers	79
Εικόνα 35 Connectivity cables.....	79
Εικόνα 36 Φωτογραφική Μηχανή	79

Εικόνα 37 Smart Phone Tool Kit	80
Εικόνα 38 Access Card System για ελεγχόμενη πρόσβαση στο LAB	80
Εικόνα 39 RACI Matrix	83

Παράρτημα ΙΔ – Πίνακες

Πίνακας 1 Πηγές Πειστηρίων	14
Πίνακας 2 Λεπτομέρειες Πειστηρίων	35
Πίνακας 3 Forensics Team USB Flash.....	16
Πίνακας 4 RAM Details	17
Πίνακας 5 HDD Details.....	17
Πίνακας 6 USB Details	17
Πίνακας 7 Πληροφορίες Έρευνας.....	31
Πίνακας 8 Στοιχεία εταιρείας.....	32
Πίνακας 9 Πίνακας 10 Evidence	32
Πίνακας 10 Λίστα Παρευρισκόμενων	33
Πίνακας 11 Πειστήρια & Hash values	34
Πίνακας 12 Εργαλεία.....	36
Πίνακας 13 Στοιχεία.....	37
Πίνακας 14 Λίστα σημαντικών αρχείων/φακέλων	38
Πίνακας 15 Λίστα σημαντικών αρχείων/φακέλων στο USB	39
Πίνακας 16 Διεργασίες	52
Πίνακας 17 Connections	53
Πίνακας 18 Sockets.....	53
Πίνακας 19 Hashdump	53
Πίνακας 20 Hash values.....	55
Πίνακας 21 HDD Partitions.....	55
Πίνακας 22 OS Details	56
Πίνακας 23 Timezone setting	56
Πίνακας 24 Computer Name	56
Πίνακας 25 OS Accounts.....	57
Πίνακας 26 Last Logon.....	57
Πίνακας 27 Last shutdown	58
Πίνακας 28 Network settings	58
Πίνακας 29 Installed Applications.....	59
Πίνακας 30 Browsers	60
Πίνακας 31 Browser files	60
Πίνακας 32 Browser History	61

Πίνακας 33 Searched keywords	61
Πίνακας 34 Keywords searched in Windows Explorer	62
Πίνακας 35 Email Client	62
Πίνακας 36 Email File Location	62
Πίνακας 37 Email Account	62
Πίνακας 38 Essential Emails	63
Πίνακας 39 External Storage Devices	64
Πίνακας 41 Network Drive IP.....	64
Πίνακας 42 Directories traversed in RM1	64
Πίνακας 43 Files opened in RM1.....	65
Πίνακας 44 Directories traversed in network drive	65
Πίνακας 45 Files opened in network drive.....	66
Πίνακας 46 USB Partition details.....	72
Πίνακας 47 USB Essential Emails.....	73
Πίνακας 48 USB Email account.....	73
Πίνακας 49 USB Email account communication.....	73
Πίνακας 50 USB Deleted Files	74
Πίνακας 51 USB exe files	74
Πίνακας 52 USB zip files	74

Λεξικό Όρων

- Hash: Αποτέλεσμα συνάρτησης κατακερματισμού
- File System: Ο τρόπος όπου ένα Λειτουργικό σύστημα αναπαριστά τα αρχεία του
- IP address: 32/64 bit αναγνωριστικό όπου έχει κάθε device σε ένα δίκτυο
- HDD: Hard Drive Disk
- GDPR: General Data Protection Regulation
- Expert Witness: Ο επικεφαλής της ομάδας, υπόλογος σε όλες τις διαδικασίες που λαμβάνουν χώρα κατά τη διάρκεια της έρευνας. Λογοδοτεί στο δικαστήριο.
- Technical Witness: Εξετάζει και αναλύει όλα τα ψηφιακά πειστήρια που του αναθέτει ένας Expert Witness κάνοντας χρήση βέλτιστων πρακτικών, μεθοδολογιών και εργαλείων.
- Zip: συμπιεσμένο αρχείο
- Στεγανογραφία/Steganography: τεχνική με την οποία κρύβονται πληροφορίες (κείμενο), μέσα σε ένα αρχείο, χωρίς να παρατηρείται σημαντική αλλαγή στο ίδιο το αρχείο με γυμνό μάτι.

- Κρυπτογραφία: μετατροπή μίας πληροφορίας από απλό κατανοητό κείμενο σε μία σειρά από μη-κατανοητή πληροφορία, με την χρήση ενός κλειδιού κρυπτογράφησης.
- Partitions: διαμερίσεις ενός σκληρού δίσκου (λογικός διαχωρισμός)

Βιβλιογραφία

1. ACPO. Good Practice Guide for Computer-Based Electronic Evidence Official Release Version 4.0.
2. Egnyte. (n.d.). *35387.pdf on Egnyte*. [online] Available at: <https://sansorg.egnyte.com/dl/2I1YaePBo3>.