

**ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ**



ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

ΜΑΘΗΜΑ: Ψηφιακά Πειστήρια

Διδάσκων: ΘΕΟΔΩΡΟΣ ΝΤΟΥΣΚΑΣ

Αργυρόπουλος Χρήστος Δουραχαλής Φίλιππος Λαπάκης Γεράσιμος Μπότσος Βασίλης

Digital Forensics Investigation on M57 Biz Charlie

Εαρινό εξάμηνο 2022-2023

Table of Contents

0. Προετοιμασία	3
1. Εντοπισμός – Ανίχνευση	4
2. Συλλογή – Διαφύλαξη Πειστηρίων	7
2.1 Συλλογή και διαφύλαξη μνήμης πειστηρίου Laptop (0001)	8
2.2 Συλλογή και διαφύλαξη δίσκου πειστηρίου Laptop (0001)	10
2.3 Συλλογή και διαφύλαξη πειστηρίων USB (0002)	11
2.4 Υπολογισμός hash values για διασφάλιση της αυθεντικότητας	13
2.5 Κατάσχεση πειστηρίων	14
2.6 Αποθήκευση πειστηρίων σε ασφαλή τοποθεσία	14
3. Εξέταση – Ανάλυση	15
3.1 Εξέταση πιστού αντιγράφου δίσκου ενεργούς συσκευής - Laptop	15
3.2 Εξέταση πιστού αντιγράφου μνήμης ενεργούς συσκευής - Laptop	17
3.3 Εξέταση πιστού αντιγράφου μη ενεργούς συσκευής - USB	19
3.4 Ανάλυση ευρημάτων κι εξαγωγή πορίσματος	19
4. Παρουσίαση	27
4.1 Παρουσίαση και επεξήγηση των συμπερασμάτων της έρευνας	27
Παράρτημα Α – Συνεντεύξεις	30
Pat (CEO):	30
Terry (IT Admin):	30
Jo (Υπάλληλος M57):	31
Charlie (Υποπτος):	31
Παράρτημα Β – Ανάλυση μνήμης Laptop	32
Παράρτημα Γ – Ανάλυση δίσκου Laptop	36
Παράρτημα Δ – Φόρμες καταγραφής	64
Παράρτημα Ε – Φόρμες κατάσχεσης	66
Παράρτημα ΣΤ – Εξοπλισμός εργαστηρίου	68
Παράρτημα Ζ – Γλωσσάρι	68

0. Προετοιμασία

Κληθήκαμε στις 11/12/2009 από τον κ. Pat McGoo εκ μέρους της εταιρίας «M57 biz», για την διερεύνηση ενός περιστατικού εκβιασμού πρώην συνεργάτη της εταιρίας. Πιο συγκεκριμένα, ο κ. Andy, υπάλληλος της εταιρίας SWExpert ανέφερε την λήψη εκβιαστικού μηνύματος ηλεκτρονικής αλληλογραφίας από τον κ. Charlie, υπάλληλο της «M57 biz» (εφεξής θα αναφέρεται και ως «ύποπτος»).

Η επιστημονική ομάδα AUEB InfoSec Ltd αποτελείται από έναν (1) expert witness, τον Αργυρόπουλο Χρήστο, και τρεις (3) technical witnesses, τους Δουραχαλή Φίλιππο, Λαπάκη Γεράσιμο και Μπότσο Βασίλειο.

Στις 10/12/2009 ώρα 13:00 ο expert witness, X. Αργυρόπουλος, ως υπεύθυνος της ομάδας, έλαβε email από τον Pat McGoo, CEO της «M57 biz», στο οποίο ο Pat ζητούσε την συνδρομή της επιστημονικής ομάδας ώστε να εξακριβωθεί αν αληθεύουν όσα ισχυρίζεται ένας πρώην συνεργάτης περί εκβιασμού. Πιο συγκεκριμένα, ο κ. Andy της SWExpert (και πρώην συνεργάτης με τον κ. Pat) ισχυρίστηκε πως έλαβε εκβιαστικό email από τον κ. Charlie της «M57 biz». Από φόβο να μην εμπλακεί η αστυνομία επικοινωνήσε με τον προϊστάμενο του υπόπτου, δηλαδή τον κ. Pat, ο οποίος επικοινωνήσε με την AUEB InfoSec Ltd για να διαλευκάνει την υπόθεση.

Την ίδια μέρα στις 19:00 πραγματοποιήθηκε συνάντηση του κ. McGoo με την ομάδα στο γραφείο μας, όπου αποφασίσαμε να αποδεχθούμε την πρόταση, συνάπτοντας το σχετικό συμφωνητικό εχεμύθειας και καθορίζοντας την ημέρα και ώρα δράσης της ομάδας. Επιπλέον, ορίστηκε το πεδίο ορισμού της έρευνας να είναι το open space office του πρώτου ορόφου του κτιρίου. Η επεξεργασία των προσωπικών δεδομένων των προσώπων που αφορά η έρευνα έγινε σύμφωνα με όσα ορίζει ο νόμος Ν.2472/97. Τότε, ο X. Αργυρόπουλος ανέθεσε αρμοδιότητες στα παρακάτω μέλη κι εξασφάλισε την παροχή των απαιτούμενων εργαλείων για την ολοκλήρωση αυτών (Παράρτημα [ΣΤ]).

Παρουσίαση μελών ομάδας:

Expert Witness - Χρήστος Αργυρόπουλος: Διαθέτει πολυετή εμπειρία στην διερεύνηση υποθέσεων ψηφιακής εγκληματολογίας καθώς και στην διαχείριση ομάδων που αναλαμβάνουν έργα αυτής της φύσης. Είναι εξοικειωμένος με τις διαφορετικές μεθοδολογίες digital forensics και τις βέλτιστες πρακτικές που πρέπει να ακολουθούνται σε μια έρευνα και διαθέτει εκτενείς γνώσεις πάνω στην νομοθεσία περί ηλεκτρονικού εγκλήματος. Είναι εγγεγραμμένος στο μητρώο πραγματογνωμόνων της Cerpel για digital forensics και είναι μέλος του οργανισμού ISFCE.

Technical Witness #1 – Φίλιππος Δουραχαλής: Ειδικεύεται στην ανάλυση ηλεκτρονικών υπολογιστών και είναι άριστος γνώστης του λειτουργικού συστήματος Windows. Γνωρίζει όλες τις απαραίτητες διαδικασίες και τις πρακτικές για την συλλογή και διαφύλαξη πειστηρίων από ενεργές συσκευές. Διαθέτει βαθιά γνώση των συστημάτων υπολογιστών, των λειτουργικών συστημάτων και της αποθήκευσης δεδομένων. Έχει μεγάλη εμπειρία στην χρήση εργαλείων για την διαφύλαξη της αυθεντικότητας των πειστηρίων και την ανάλυσή τους, όπως τα EnCase, AccessData Forensic Toolkit (FTK), Autopsy και Volatility, ενώ είναι πιστοποιημένος κατά GCFE (GIAC Certified Forensic Examiner).

Technical Witness #2 – Γεράσιμος Λαπάκης: Επικεντρώνεται στην εγκληματολογία δικτύων και διαθέτει γνώσεις αποκώμισης πειστηρίων από δικτυακές πηγές. Έχει παρακολουθήσει

σεμινάρια επικοινωνίας, καταφέροντας έτσι να θέσει τις ερωτήσεις συνοδευόμενες από την κατάλληλη στάση σώματος που να φαίνεται προσιτός στους ερωτηθέντες και να εκμαιεύει απαντήσεις. Γνωρίζει καλά την διαδικασία συλλογής πειστηρίων από φορητά μέσα αποθήκευσης, καθώς διαθέτει την πιστοποίηση ACE (AccessData Certified Examiner), για χρήση του FTK Imager. Έχει, επίσης, εμπειρία στην εξέταση πειστηρίων με το εργαλείο Volatility.

Technical Witness #3 –Βασίλης Μπότσος: Είναι ειδικός στην κατάσχεση και διαφύλαξη πειστηρίων έχοντας εμπειρία πολλών υποθέσεων στην καταγραφή τους κι έχει αναπτύξει την ικανότητα να αντιλαμβάνεται την κατάσταση στην οποία βρίσκονται και τι διαχείριση απαιτεί αυτή. Γνωρίζει καλά την μεθοδολογία ACPO και κατέχει επαγγελματικό δίπλωμα αυτοκινήτου ώστε να μεταφέρει τα πειστήρια σε ασφαλή τοποθεσία μετά την κατάσχεσή τους. Τέλος, έχει εμπειρία στην χρήση εργαλείων όπως το Autopsy για την ανάλυση κι εξέταση πειστηρίων.

Ανάθεση ρόλων ομάδας:

Ο πρώτος technical witness, Φ. Δουραχαλής, ορίστηκε υπεύθυνος να αποκλείσει και να χαρτογραφήσει τον χώρο του εγκλήματος, για το οποίο χρειάστηκε ειδική ταινία, μια φωτογραφική κάμερα, και γραφικές ύλες για τον σχεδιασμό του χώρου. Στη συνέχεια, θα έπρεπε να αναλάβει την συλλογή πειστηρίων από τις ενεργές συσκευές που θα εντοπίζονταν στην σκηνή του εγκλήματος, και για αυτόν τον λόγο εφοδιάστηκε με ένα USB stick φορτωμένο με την έκδοση 4.7.1.2 του FTK Imager, την έκδοση 2.2.1 του FEX Imager και την έκδοση 13.0 (Warp) του Caine. Τέλος, θα έπρεπε να αναλύσει και να εξετάσει τα συλλεγμένα πειστήρια από αποθηκευτικά μέσα ενεργών συσκευών χρησιμοποιώντας την 4.20.0 έκδοση του Autopsy.

Ο δεύτερος technical witness, ο Γ. Λαπάκης, ορίστηκε υπεύθυνος να πάρει συνεντεύξεις από τους παρευρισκόμενους στην σκηνή του εγκλήματος, για τις οποίες ετοίμασε και κατάλληλες ερωτήσεις και να εξετάσει αν υπάρχουν ασύρματα σήματα στον χώρο, χρησιμοποιώντας wireless signal detector. Στη συνέχεια, θα έπρεπε να συλλέξει πειστήρια από μη ενεργές συσκευές στον χώρο του εγκλήματος με χρήση ενός USB stick εφοδιασμένου με την προαναφερθείσα έκδοση του FTK Imager και του FEX Imager και να εξετάσει την συλλεγμένη μνήμη από τις ενεργές συσκευές με την έκδοση 2.6 του Volatility.

Τέλος, ο τρίτος technical witness, Β. Μπότσος, επιφορτίστηκε με την καταγραφή του εξοπλισμού που μπορεί να αποτελέσει πιθανά πειστήρια και την κατάσταση στην οποία βρίσκονται, συμπληρώνοντας την Φόρμα Κατάσχεσης. Στη συνέχεια, θα έπρεπε να αναλάβει την κατάσχεση των πειστηρίων και την αποθήκευση τους σε ασφαλή τοποθεσία, συμπληρώνοντας την φόρμα Chain of Custody. Για όλα τα παραπάνω εφοδιάστηκε με ειδικά γάντια και αντιστατικές σακούλες. Τέλος, ορίστηκε υπεύθυνος να εξετάσει τα συλλεγμένα πειστήρια από μη ενεργές συσκευές.

Επιπλέον, η ομάδα πήρε μαζί της τα εγχειρίδια χρήσης των εργαλείων που θα χρησιμοποιούσε, μαζί με μερικά επιπλέον αποθηκευτικά μέσα για την διαφύλαξη των πειστηρίων.

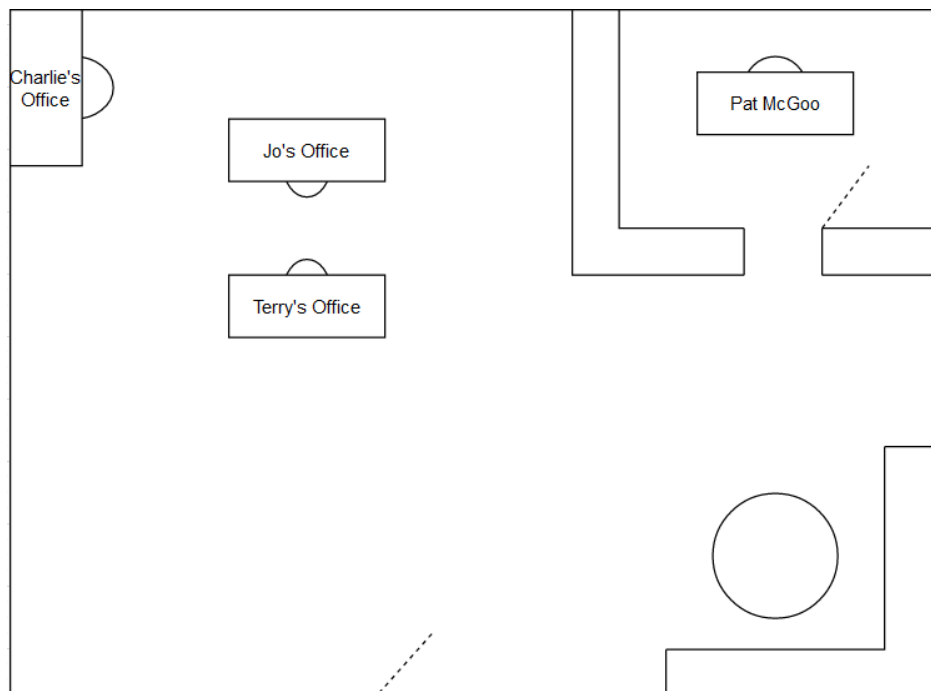
1. Εντοπισμός – Ανίχνευση

Στις 11/12/2009 και ώρα 10:00 η επιστημονική ομάδα έφτασε στο σημείο του εγκλήματος, όπου τους περίμενε ο κ. McGoo. Ο Φ. Δουραχαλής αμέσως απέκλεισε τον ανοιχτό χώρο του φερόμενου εγκλήματος που συμπεριλάμβανε την δεξιά γωνία του open-space γραφείου, στον 1^ο όροφο της εταιρίας, ενώ λίγα λεπτά αργότερα άρχισε να τον καταγράφει, φωτογραφίζοντας

και βιντεοσκοπώντας εξ ολοκλήρου την σκηνή και καταγράφοντας σχηματικά στο τετράδιό του την κάτοψη αυτής. Οι φωτογραφίες που τράβηξε και η κάτοψη που σχεδίασε ήταν οι εξής:



Φωτογραφία 1.1: Σκηνή Εγκλήματος.



Φωτογραφία 1.1: Κάτοψη Open Space Γραφείου.

Στις 10:15 ο Γ. Λαπάκης ξεκίνησε να παίρνει συνεντεύξεις από τους παρευρισκόμενους, χρησιμοποιώντας τις προετοιμασμένες ερωτήσεις. Οι ερωτηθέντες ήταν ο κ. Pat McGoo, ο CEO της εταιρείας «M57 Biz», ο κ. Terry ως ο IT Admin, και ο κ. Jo ως συνάδελφος του υπόπτου. Τέλος, ερωτήθηκε και ο κ. Charlie, όντας ο ύποπτος της υπόθεσης (Παράρτημα [Α]). Μετά την ολοκλήρωση των συνεντεύξεων, στις 10:25 χρησιμοποίησε τον ανιχνευτή ασύρματων σημάτων ώστε να εντοπίσει περαιτέρω πειστήρια, χωρίς όμως να καταφέρει να βρει κάτι.

Στις 10:30 ο Β. Μπότσος άρχισε την καταγραφή των πειστηρίων και την κατάσταση στην οποία αυτά βρίσκονταν, συμπληρώνοντας την Φόρμα Κατάσχεσης (Παράρτημα [Ε]). Πιο συγκεκριμένα, εντοπίστηκε ένα ενεργό laptop (Φωτογραφία 1.3) πάνω στο γραφείο του κ. Charlie, κατασκευασμένο από την εταιρεία DELL, με μέγεθος οθόνης 15.6" μαύρου χρώματος, με κατεβασμένο το καπάκι, βρισκόμενο σε καλή κατάσταση. Το εν λόγω laptop δεν είχε συνδεδεμένο πάνω του καμία εξωτερική συσκευή ή καλώδιο, ενώ δεν είχε ούτε παροχή ρεύματος. Για αυτόν τον λόγο, ο Β. Μπότσος, αφού ήλεγξε πως δεν υπήρχε κίνδυνος, τοποθέτησε ταινία στις θύρες και το disk tray του laptop. Επιπλέον, πάνω στο γραφείο του κ. Charlie εντοπίστηκε ένα USB stick (Φωτογραφία 1.2) μη προσαρτημένο στο προαναφερθέν laptop, κατασκευασμένο από την εταιρεία Kingston με σειριακό αριθμό 2007110203195377 και συνολική χωρητικότητα 1.05 GB.



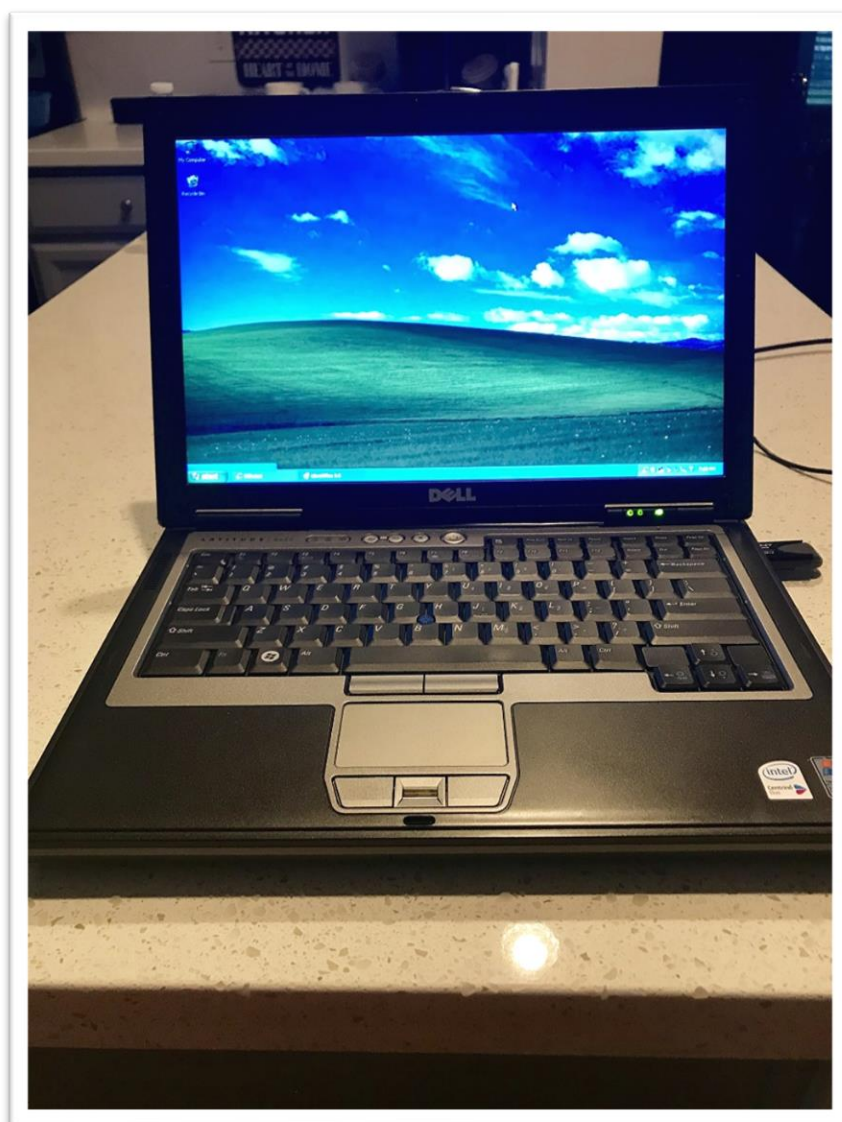
Φωτογραφία 1.2: Dell Laptop κ. Charlie.



Φωτογραφία 1.3: Kingston USB stick κ Charlie.

2. Συλλογή – Διαφύλαξη Πειστηρίων

Στις 10:40 ο Φ. Δουραχαλής παρατηρώντας ότι τα ενδεικτικά φώτα LED του DELL laptop ήταν ενεργοποιημένα, άνοιξε με προσεκτικές κινήσεις το καπάκι προκειμένου να ενεργοποιηθεί η οθόνη, ενώ παράλληλα ο Χ. Αργυρόπουλος ξεκίνησε την βιντεοσκόπηση της διαδικασίας. Το laptop δεν προστατευόταν με κάποιον κωδικό. Μόλις σήκωσε την οθόνη, κούνησε με απαλές κινήσεις το ποντίκι χωρίς να πατήσει το πληκτρολόγιο με σκοπό την απενεργοποίηση του screen saver, όπου και διαπιστώθηκε ότι υπήρχαν ενεργά προγράμματα που χρησιμοποιούσε ο χρήστης προηγουμένως. Εκείνη την στιγμή ζητήθηκε η γνώμη του expert witness, ο οποίος αποφάνθηκε ότι πρέπει να γίνει live acquisition των δεδομένων που υπήρχαν στο laptop εκείνη την στιγμή (όπως τα περιεχόμενα μνήμης, cache, registry).



Φωτογραφία 2.1: Dell Laptop κ. Charlie.

2.1 Συλλογή και διαφύλαξη μνήμης πειστηρίου Laptop (0001)

Στις 10:43 συνδέσαμε στον υπολογιστή ένα κατάλληλα διαμορφωμένο USB (Παράρτημα [ΣΤ]) και ξεκινήσαμε την διαδικασία λήψης πιστών αντιγράφων της μνήμης χρησιμοποιώντας τα εργαλεία MDD και DumpIt, για την λήψη ενός κύριου αντιγράφου, κι ενός backup, διασφαλίζοντας με αυτόν τον τρόπο την ακεραιότητα των πειστηρίων.

Στις 10:58 ολοκληρώθηκε η εκτέλεση των εργαλείων, με τα αποτελέσματα να γράφονται στο USB μας.


```

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

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

-> Dumping 2045.98 MB of physical memory to file 'z:\charlie-2009-12-11.raw'.
C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.mddramimage MD5
MD5 hash of charlie-2009-12-11.mddramimage:
38067cc457546b3156975d9a52d4229f
CertUtil: -hashfile command completed successfully.

C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.mddramimage MD5 > charlie-2009-12-11-md5.txt

C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.mddramimage SHA256
SHA256 hash of charlie-2009-12-11.mddramimage:
e0c72dc7bc9aa7e15f17f1b5acc460e66dd72f09dd999b00840b15a194665e4d
CertUtil: -hashfile command completed successfully.

C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.mddramimage SHA256 > charlie-2009-12-11-sha256.txt

```

Φωτογραφία 2.2: Λήψη πρώτου πιστού αντιγράφου μνήμης πειστηρίου (laptop ID) και υπολογισμός hash value

```

C:\Documents and Settings\Charlie\DumpIt.exe

DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      17686331392 bytes ( 16867 Mb)
Free space size:         18134863872 bytes ( 17294 Mb)

* Destination = \\?\C:\Documents and Settings\Charlie\PHILIP-LAPTOP-20230604-144658.raw

--> Are you sure you want to continue? [y/n]

C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.raw MD5
MD5 hash of charlie-2009-12-11.raw:
b9ce3a15ae32fbf769154008a7036e18
CertUtil: -hashfile command completed successfully.

C:\Documents and Settings\Charlie>certutil -hashfile charlie-2009-12-11.raw SHA256
SHA256 hash of charlie-2009-12-11.raw:
cf609d0b4d8e80d1ddab87991e4ae0e82e2d80892226ce8d943e327722743eeb
CertUtil: -hashfile command completed successfully.

```

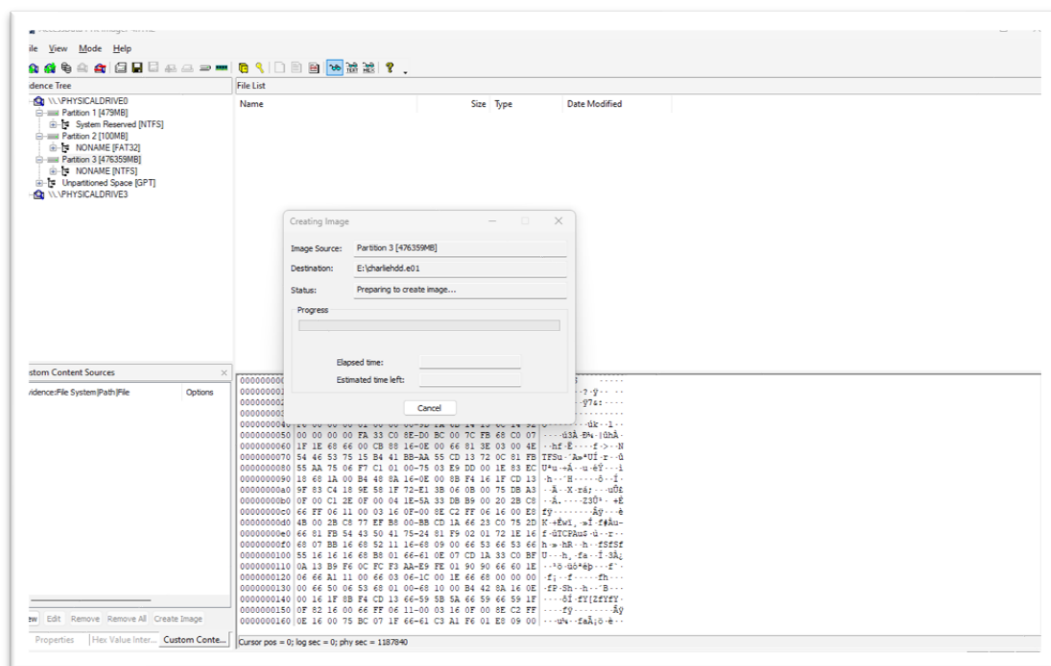
Φωτογραφία 2.3: Λήψη δεύτερου πιστού αντιγράφου μνήμης πειστηρίου (laptop ID) και υπολογισμός hash value

1 ^ο πιστό αντίγραφο μνήμης	
Εργαλείο λήψης αντιγράφου	MDD 1.3
Πειστήριο	Dell Studio 15 (0001)
Ημ/νια διαφύλαξης	11/12/2009 10:44:12π.μ.
Παραγόμενο αρχείο	charlie-2009-12-11.mddramimage charlie-2009-12-11-md5.txt charlie-2009-12-11-sha256.txt
MD5 hash	38067cc457546b3156975d9a52d4229f
SHA256 hash	e0c72dc7bc9aa7e15f17f1b5acc460e66dd72f09dd999b00840b15a194665e4d
Χρησιμοποιούμενες εντολές	mdd_1.3.exe -o z:\charlie-2009-12-11.mddramimage certutil -hashfile Charlie-2009-12-11.mddramimage md5 certutil -hashfile Charlie-2009-12-11.mddramimage sha256

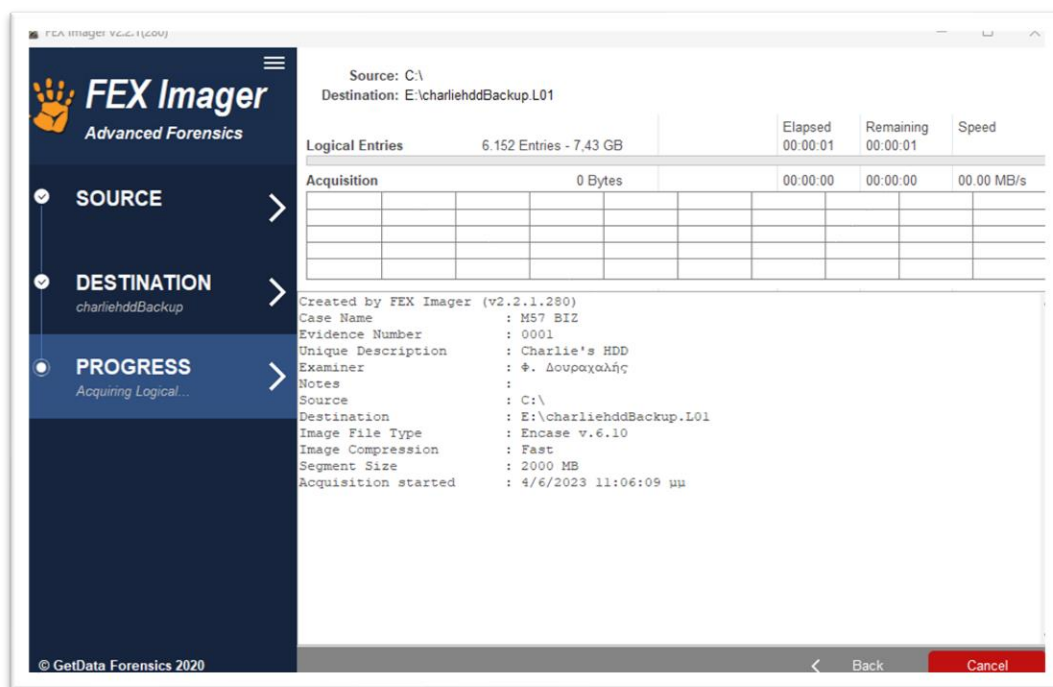
2 ^ο πιστό αντίγραφο μνήμης	
Εργαλείο λήψης αντιγράφου	DumpIt
Πειστήριο	Dell Studio 15 (0001)
Ημ/νια διαφύλαξης	11/12/2009 10:54:03π.μ.
Παραγόμενο αρχείο	charlie-2009-12-11.mddramimage charlie-2009-12-11-dumpit-md5.txt charlie-2009-12-11-dumpit-sha256.txt
MD5 hash	b9ce3a15ae32fbf769154008a7036e18
SHA256 hash	cf609d0b4d8e80d1ddab87991e4ae0e82e2d80892226ce8d943e327722743eeb
Χρησιμοποιούμενες εντολές	Run DumpIt.exe. Type 'y' to dump RAM image to disk certutil -hashfile Charlie-2009-12-11.raw md5 certutil -hashfile Charlie-2009-12-11.raw sha256

2.2 Συλλογή και διαφύλαξη δίσκου πειστηρίου Laptop (0001)

Στις 11:07 ξεκίνησε η διαφύλαξη των πειστηρίων του δίσκου με χρήση των εργαλείων FTK Imager και FEX Imager για την λήψη του πρώτου και του δεύτερου αντιγράφου αντίστοιχα.



Φωτογραφία 2.4: Λήψη 1ου πιστού αντιγράφου με το FTK Imager



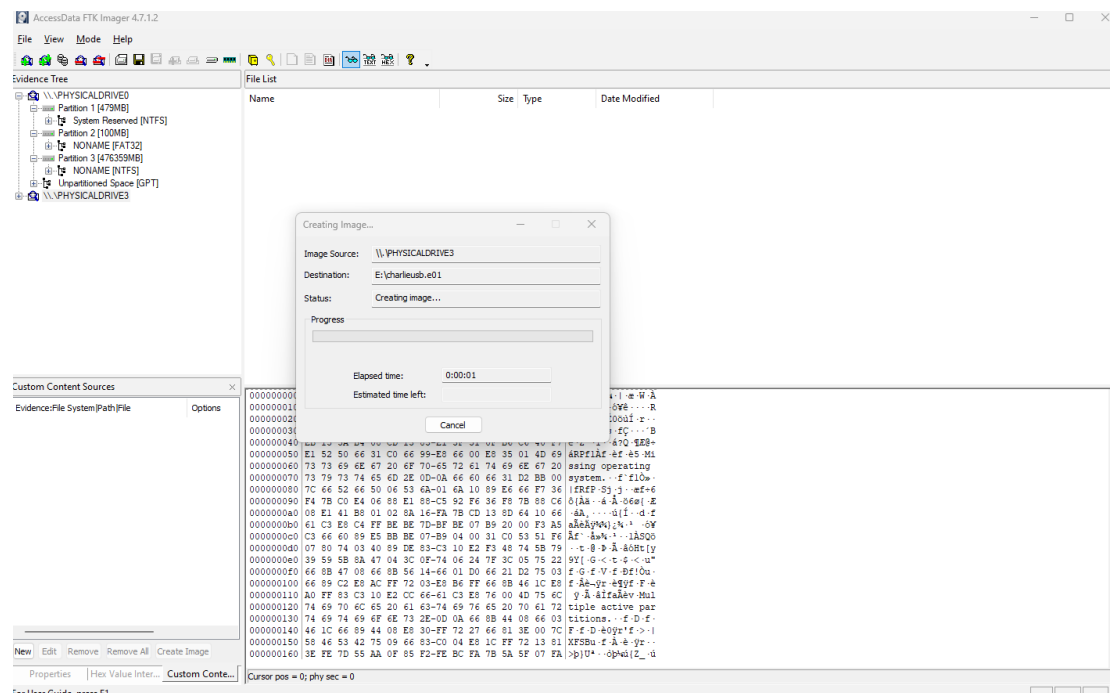
Φωτογραφία 2.5: Λήψη backup πιστού αντιγράφου με το FEX Imager

1 ^ο πιστό αντίγραφο δίσκου	
Εργαλείο λήψης αντιγράφου	FTK Imager 4.7.12
Πειστήριο	Dell Studio 15 (0001)
Ημ/νια διαφύλαξης	11/12/2009 11:07:03π.μ.
Παραγόμενο αρχείο	charlie-2009-12-11.E01
MD5 hash	0377b3d41bbbc295a1c9f00aa07ee174

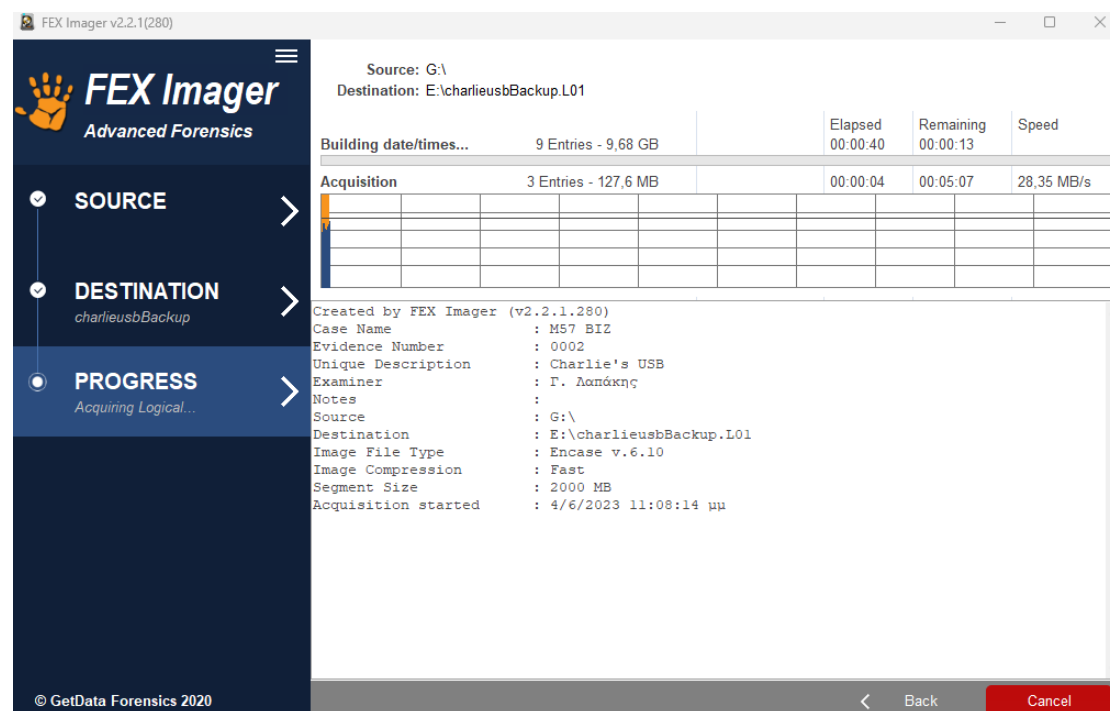
2 ^ο πιστό αντίγραφο δίσκου	
Εργαλείο λήψης αντιγράφου	FEX Imager 2.2.1
Πειστήριο	Dell Studio 15 (0001)
Ημ/νια διαφύλαξης	11/12/2009 11:17: 01π.μ.
Παραγόμενο αρχείο	charlie-2009-12-11.E01
MD5 hash	0377b3d41bbbc295a1c9f00aa07ee174

2.3 Συλλογή και διαφύλαξη πειστηρίων USB (0002)

Στις 10:53 ο Γ. Λαπάκης ξεκίνησε την λήψη αντιγράφου του Kingston DataTraveler 2.0 USB, το οποίο δεν ήταν συνδεδεμένο στο Laptop. Στη συνέχεια, το τοποθέτησε στο laptop του και με την βοήθεια του εργαλείου AccessData FTK Imager έκανε λήψη του πρώτου πιστού αντιγράφου. Ακόμη, πάρθηκε ένα δεύτερο πιστό αντίγραφο για λόγους ασφαλείας (backup) μέσω ενός διαφορετικού εργαλείου, του FEX Imager, ενώ και στις δυο περιπτώσεις έγινε χρήση της μεθόδους Bit-stream disk-to-image file. Τα images του USB αποθηκεύτηκαν με ασφάλεια στον εξωτερικό σκληρό δίσκο της ομάδας.



Φωτογραφία 2.6: Λήψη 1ου πιστού αντιγράφου με το FTK Imager



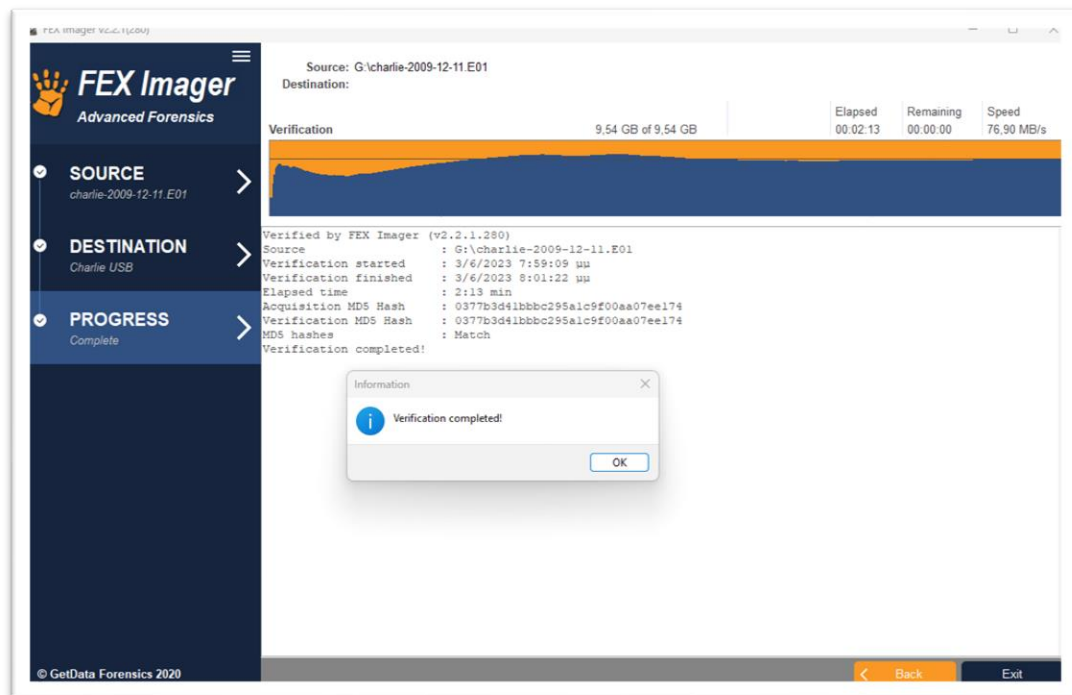
Φωτογραφία 2.7: Λήψη 2ου πιστού αντιγράφου με το FEX Imager

1 ^ο πιστό αντίγραφο USB	
Εργαλείο λήψης αντιγράφου	FTK Imager 4.7.1.2
Πειστήριο	Kingston DataTraveler 2.0 (0002)
Ημ/νια διαφύλαξης	11/12/2009 10:53:12π.μ.
Παραγόμενο αρχείο	charlie-work-usb-2009-12-11.E01
MD5 hash	9c0de6c8532d7a66ddcf01861dfb6535

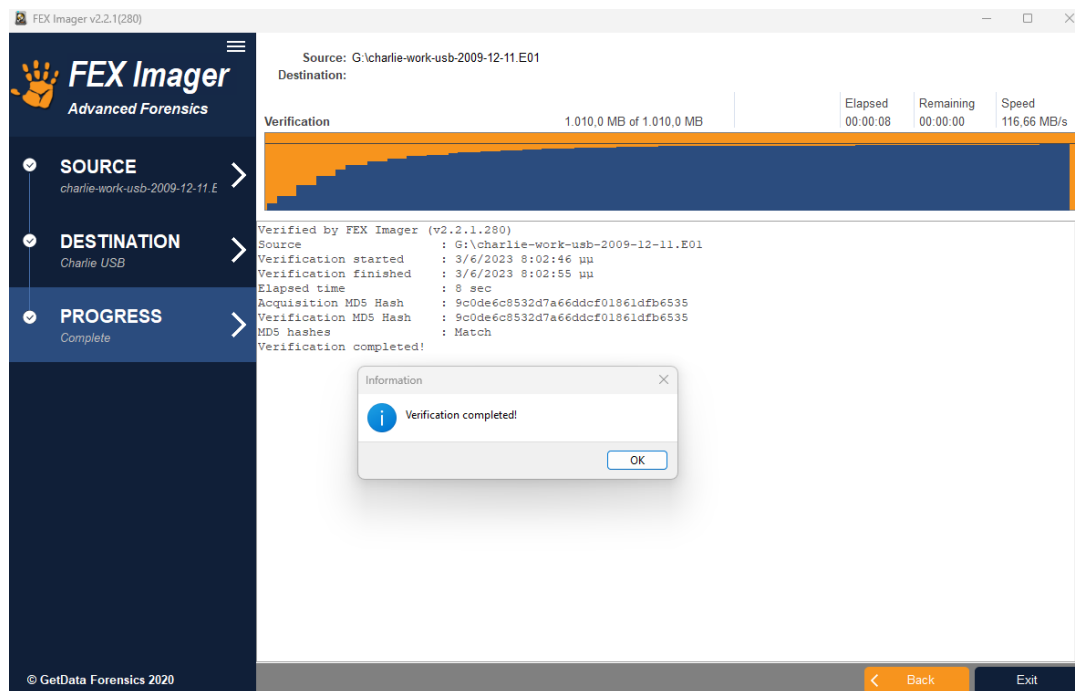
2 ^ο πιστό αντίγραφο USB	
Εργαλείο λήψης αντιγράφου	FEX Imager 2.2.1
Πειστήριο	Kingston DataTraveler 2.0 (0002)
Ημ/νια διαφύλαξης	11/12/2009 11:03:38π.μ.
Παραγόμενο αρχείο	charlie-work-usb-2009-12-11.E01
MD5 hash	9c0de6c8532d7a66ddcf01861dfb6535

2.4 Υπολογισμός hash values για διασφάλιση της αυθεντικότητας

Στις 11:27 ο Γ. Λαπάκης υπολόγισε τα MD5 hash values για να διασφαλιστεί η αυθεντικότητα κι η ακεραιότητα των δεδομένων του USB και ο Φ. Δουραχαλής υπολόγισε τα hash values του σκληρού δίσκου του Laptop. Για τον σκοπό αυτό, και στις δύο περιπτώσεις χρησιμοποιήθηκε το εργαλείο FEX Imager.



Φωτογραφία 2.8: Λήψη MD5 hash FEX Imager HDD



Φωτογραφία 2.9: Λήψη MD5 hash FEX Imager USB

2.5 Κατάσχεση πειστηρίων

Στις 11:36, και αφού είχε ολοκληρωθεί η διαδικασία του live acquisition της ενεργούς συσκευής, ο B. Μπότσος αφαίρεσε προσεκτικά τη μπαταρία της για την ακαριαία απενεργοποίησή του laptop. Κατόπιν έλεγξε το disk tray, όπου δεν βρήκε κάποιο οπτικό μέσο, αφαίρεσε το σκληρό δίσκο και τον τοποθέτησε σε αντιστατική σακούλα. Έπειτα κάλυψε όλες τις θύρες καθώς και το κουμπί ενεργοποίησης με ειδική ταινία και τοποθέτησε τις κατάλληλες ετικέτες στο USB, στο Laptop και στα περιφερειακά του εξαρτήματα. Στη συνέχεια το Laptop τοποθετήθηκε σε ειδικά διαμορφωμένο κλωβό Faraday και το USB σε αντιστατική σακούλα για την ασφαλή μετακίνησή τους στο εργαστήριο. Επίσης, συλλέχθηκε ο φορτιστής του Laptop και τοποθετήθηκε σε κατάλληλη τσάντα.

2.6 Αποθήκευση πειστηρίων σε ασφαλή τοποθεσία

Στις 11:41 το chain of custody υπογράφηκε από τον B. Μπότσο και για τα δυο πειστήρια, πριν την μεταφορά τους στο εργαστήριο. Για την μεταφορά τους στο εργαστήριο έγιναν οι κατάλληλες ενέργειες ώστε να αποφευχθεί η πιθανή τους έκθεση σε μαγνητικά πεδία τα οποία μπορεί να προκληθούν από ραδιοπομπούς, μαγνήτες από ηχεία και θερμές πηγές οι οποίες μπορούν να προκαλέσουν στατικό ηλεκτρισμό. Στο όχημα μεταφοράς έγινε προσεκτική ρύθμιση της θερμοκρασίας και των επιπέδων υγρασίας. Τα πειστήρια επιπλέον τοποθετήθηκαν προσεκτικά σε ειδικά διαμορφωμένο σημείο στο όχημα, ώστε να αποφευχθούν ζημιές από αναταράξεις και δονήσεις που μπορεί να προκύπτουν κατά την μεταφορά τους.

Στις 12:03 κατά την άφιξη των πειστηρίων στο εργαστήριο, ο Β.Μπότσος διασφάλισε την αποθήκευση τους σε τοποθεσία ελεγχόμενης θερμοκρασίας και υγρασίας. Τέλος, κρατήθηκαν μακριά από τυχόν δονήσεις, σκόνη και άλλες πιθανές απειλές οι οποίες θα ήταν υπεύθυνες για την καταστροφή τους ή για την πρόκληση ζημίας.

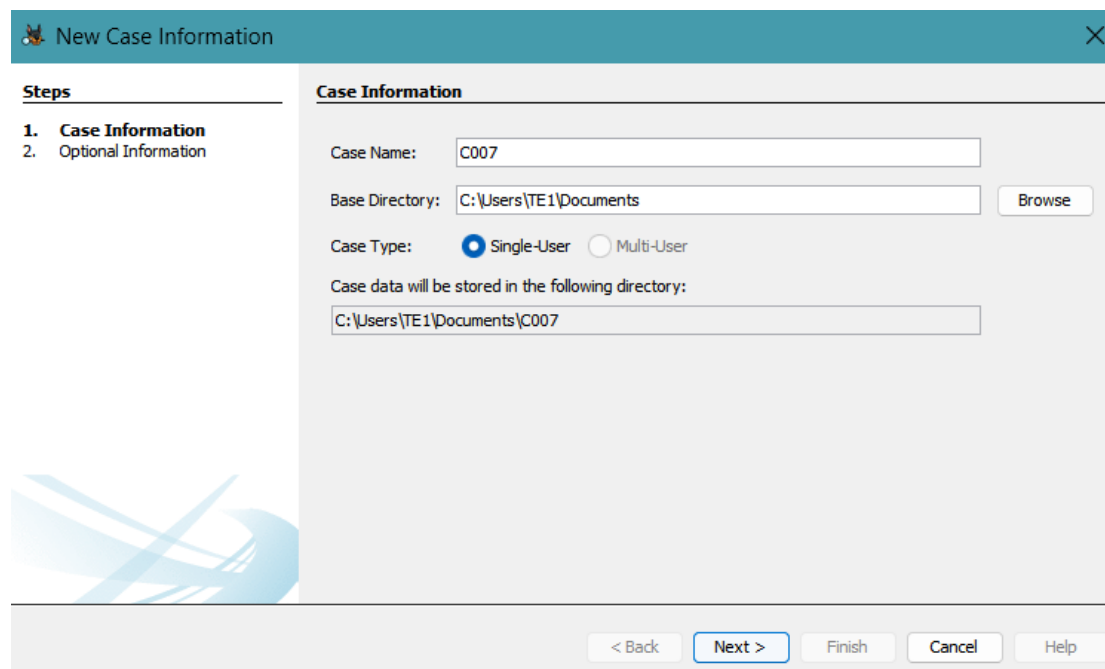
3. Εξέταση – Ανάλυση

Η εξέταση των πιστών αντιγράφων του σκληρού δίσκου και του USB έγινε με την χρήση του εργαλείου Autopsy, όπου χρησιμοποιήθηκαν τα αντίγραφα που δημιουργήσαμε μέσω του FTK Imager.

3.1 Εξέταση πιστού αντιγράφου δίσκου ενεργούς συσκευής - Laptop

Στις 12:09 ο Φ. Δουραχαλής σύλλεξε διάφορες πληροφορίες που αφορούσαν τον σκληρό δίσκο όπως για παράδειγμα τα αρχεία (επίσης διαγραμμένα και μετονομασμένα αρχεία), την registry, τα e-mails, τις συνδεδεμένες συσκευές και το ιστορικό πλοήγησης στο διαδίκτυο κ.α. Τα πορίσματα της ανάλυσης βρίσκονται στο Παράρτημα Γ.

Επιπλέον κατεβάσαμε ένα έτοιμο hash set με hashes αρχείων που έχουν εντοπιστεί σε προηγούμενες εγκληματολογικές έρευνες και το εισαγάγαμε στο Autopsy, προκειμένου να μας βοηθήσει στον εντοπισμό αρχείων στο αντίγραφο του δίσκου που έχουμε.



Φωτογραφία 3.1: Πληροφορίες case.

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: C007

Examiner

Name: Christos Argyropoulos

Phone: 6912345678

Email: ch.argyropoulos@auebdf.gr

Notes:

Organization

Organization analysis is being done for: Not Specified

< Back Next > Finish Cancel Help

Φωτογραφία 3.2: Στοιχεία expert witness.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\Philip\Downloads\charlie-2009-12-11.E01

☐ Ignore orphan files in FAT file systems

Time zone: GMT-8:00 PST

Sector size: Auto Detect

Hash Values (optional):

MD5:

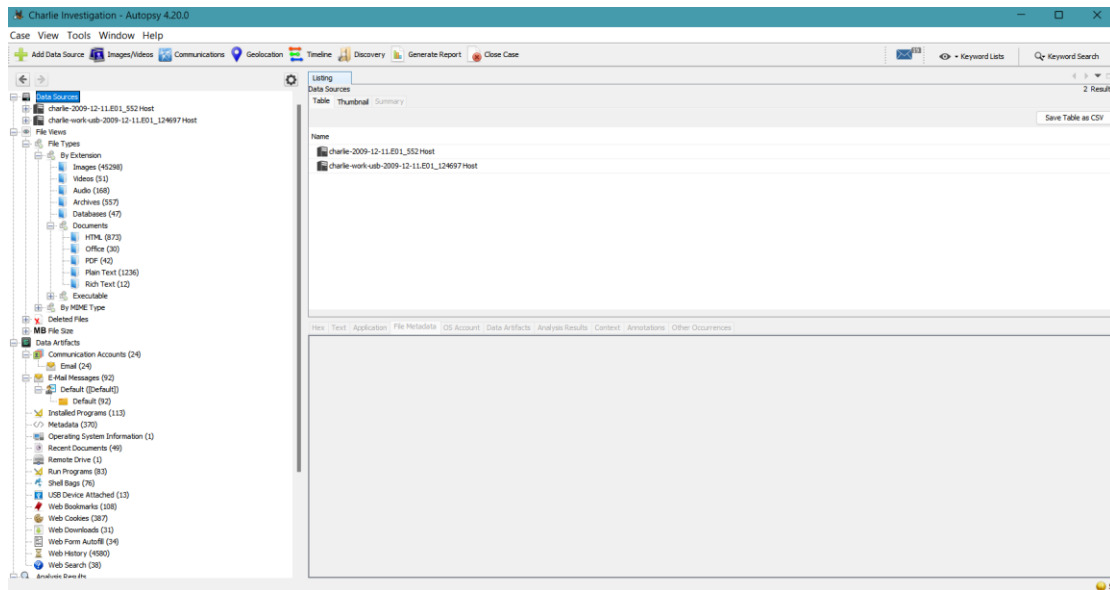
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

Φωτογραφία 3.3: Πηγή πειστηρίων.



Φωτογραφία 3.4: Ανάλυση πειστηρίων με Autopsy

3.2 Εξέταση πιστού αντιγράφου μνήμης ενεργούς συσκευής - Laptop

Στις 12:14 ο Γ. Λαπάκης χρησιμοποίησε το εργαλείο Volatility 2.6 για να πραγματοποιήσει την ανάλυση της μνήμης. Προτού μπορέσει να αναλύσει τα περιεχόμενα του πιστού αντιγράφου που είχε ληφθεί, χρειάστηκε να εξακριβωθεί το προφίλ του αντιγράφου της μνήμης και να βρεθεί το σωστό offset. Αυτό πραγματοποιήθηκε εκτελώντας τις ακόλουθες εντολές:

1. volatility_2.6_win64_standalone.exe -f charlie-2009-12-11.mddramimage imageinfo
2. volatility_2.6_win64_standalone.exe -f charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbgscan
3. volatility_2.6_win64_standalone.exe -f charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 --kdbg=0x805532e0

Έχοντας βρει το κατάλληλο προφίλ, προχώρησε στην συλλογή πληροφοριών σχετικά με τις διεργασίες που εκτελούνταν, τις ενεργές συνδέσεις, τις εικονικές διευθύνσεις των hives της registry, μέσω των οποίων εντοπίστηκαν τα volatile κλειδιά, και τις εντολές που είχε εκτελέσει ο χρήστης. Όλα τα αποτελέσματα καταγράφηκαν σε αρχεία κειμένου και κατόπιν λήφθηκε το MD5 hash των αρχείων αυτών με την εντολή των Windows:

certutil -hashfile [file] MD5

```
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile activeConnections.txt md5 > activeconnection_s_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile hardwareDump.txt md5 > hardwareDump_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile hashDump.txt md5 > hashDump_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile networkScan.txt md5 > networkScan_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile processes.txt md5 > processes_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile shellBags.txt md5 > shellBags_md5.txt
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>certutil -hashfile userCmd.txt md5 > userCmd_md5.txt
```

Φωτογραφία 3.5: Hashes.

Τα αναλυτικά αποτελέσματα βρίσκονται στο Παράρτημα [H].**Error! Reference source not found.**

Ευρήματα: Η ανάλυση των διεργασιών έγινε με βάση την μεθοδολογία που περιγράφεται από τον οργανισμό SANS¹, δηλαδή συγκρίνοντας τις παρατηρούμενες διεργασίες και συνδέσεις με κάποιο baseline διεργασιών που ορίζονται για ένα Windows Server 2008 R2 Μηχάνημα προκειμένου να ανιχνευθούν πιθανώς ύποπτες διεργασίες που έχουν εκκινηθεί από τον χρήστη ή δικτυακές συνδέσεις. Τα αποτελέσματα της ανάλυσης παρουσιάζονται στην συνέχεια:

Συστημικές διεργασίες			
Όνομα	PID	PPID	Owner
System	4	-	Local System
smss.exe	876	4	Local System
csrss.exe	924	876	Local System
winlogon.exe	948	876	Local System
services.exe	992	948	Local System
lsass.exe	1004	948	Local System
svchost.exe	1180	992	Local System
svchost.exe	1268	992	Local System
svchost.exe	1392	992	Local System
svchost.exe	1532	992	Local System
svchost.exe	1644	992	Local System
svchost.exe	1796	992	Local System

Πίνακας 1 Baseline συστημικών διεργασιών

PID	PPID	Process	Service	Local Network address	Foreign Network address
4	-	System	DELL OpenManage HTTPS	192.168.1.104:1311	192.168.1.1:139
			SMB	192.168.1.104:1310	192.168.1.1:445
2804	1348	jusched.exe	Java Update scheduler	192.168.1.104:1208	198.189.255.73:80
188	1348	thunderbird.exe	Mozilla Thunderbird	192.168.1.104:1303	63.245.209.10:80
				192.168.1.104:1304	208.97.132.223:995
				192.168.1.104:1307	208.97.132.223:996
				192.168.1.104:1305	63.245.221.11:80
1908	992	spoolsv.exe	Print Spooler Service	-	-
1348	1304	explorer.exe	File Explorer	-	-
3936	992	avgfws9.exe	AVG 9 Antivirus	-	-
3048	3000	soffice.exe	OpenOffice	-	-

Πίνακας 2 Διεργασίες χρήστη και ενεργές δικτυακές συνδέσεις

Με βάση τα παραπάνω ευρήματα συμπεραίνουμε ότι ο ύποπτος ήταν συνδεδεμένος στο μηχάνημά του, αφού παρατηρήσαμε διεργασίες που δημιουργούνται όταν ο χρήστης κάνει

¹ <https://www.sans.org/white-papers/35387/>

logon από ένα τερματικό (csrss.exe, winlogon.exe και explorer.exe). Παρότι δεν εντοπίστηκαν ύποπτες διεργασίες, αξιοσημείωτη είναι η ύπαρξη της διεργασίας thunderbird.exe, η οποία έχει ανοικτές δικτυακές συνδέσεις εκτός του οργανισμού και η οποία γνωρίζουμε ότι χρησιμοποιήθηκαν από τον ύποπτο για την αποστολή κακόβουλων e-mail

3.3 Εξέταση πιστού αντιγράφου μη ενεργούς συσκευής - USB

Στην συνέχεια ο B. Μπόττος προχώρησε με την ανάλυση του USB του υπόπτου και έγινε συλλογή και καταγραφή των πιο αξιοσημείωτων ευρημάτων που αφορούσαν το USB. Τα πορίσματα της ανάλυσης βρίσκονται στο Παράρτημα Γ.

3.4 Ανάλυση ευρημάτων κι εξαγωγή πορίσματος

Τέλος, οι τρεις technical witnesses συγκεντρώθηκαν υπό την επίβλεψη του expert witness για την ανάλυση των ευρημάτων. Αρχικά αναλύσαμε τα e-mails που είχε ανταλλάξει ο ύποπτος από το εταιρικό του email (charlie@m57.biz) μέσω του Thunderbird. Παρατηρήσαμε ότι ξεκίνησε να δουλεύει στην εταιρεία περίπου έναν μήνα, μαζί με τον Jo και τον Terry, όπως φαίνεται στο e-mail που στάλθηκε στις 2009-11-16 11:02:37 PST. Το περιεχόμενο των email υπέδειξε ορισμένα χλευαστικά σχόλια προς τον K. McGoo, τα οποία όπως φάνηκε αντάλλασσε με τους συναδέλφους του.

Εντοπίστηκε ένα email του οποίου το περιεχόμενο αφορούσε την αποκάλυψη εμπιστευτικής πληροφορίας της εταιρείας Nitroba, η οποία συνεργαζόταν με την εργοδότη εταιρία M57, έναντι χρηματικού αντιτίμου (2009-12-02 13:04:29 PST – Email 1). Ο παραλήπτης του ανωτέρου email ήταν ο Jaime της εταιρείας Project2400, ο οποίος συμφώνησε στην πρόταση του ύποπτου και προσέφερε 50.000 δολάρια, με προκαταβολή ύψους 10.000 δολαρίων (2009-12-03 09:51:33 PST – Email 2). Στην συνέχεια, ο ύποπτος απάντησε με ένα email (2009-12-03 12:16:52 PST – Email 3) το οποίο περιείχε ένα attachment με μια στεγανογραφημένη εικόνα ενός αστροναύτη (Attachment 1) και ανέφερε ότι θα αποστείλει τον κωδικό όταν θα παραλάβει και τα υπόλοιπα χρήματα. Όταν ολοκληρώθηκε η κατάθεση, απέστειλε τον κωδικό «nitro» για την αποστεγανογράφιση της εικόνας (2009-12-04 13:06:23 PST - Email 4) .

From: charlie@m57.biz;
To: jamie@project2400.com;
CC:
Subject: Interested?

Headers Text HTML RTF Attachments (0) Accounts

J,

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

C

E-mail 1

From: jamie@project2400.com;
To: charlie@m57.biz;
CC:
Subject: Re: Interested?

Headers Text HTML RTF Attachments (0) Accounts

C,

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.

J

> J,

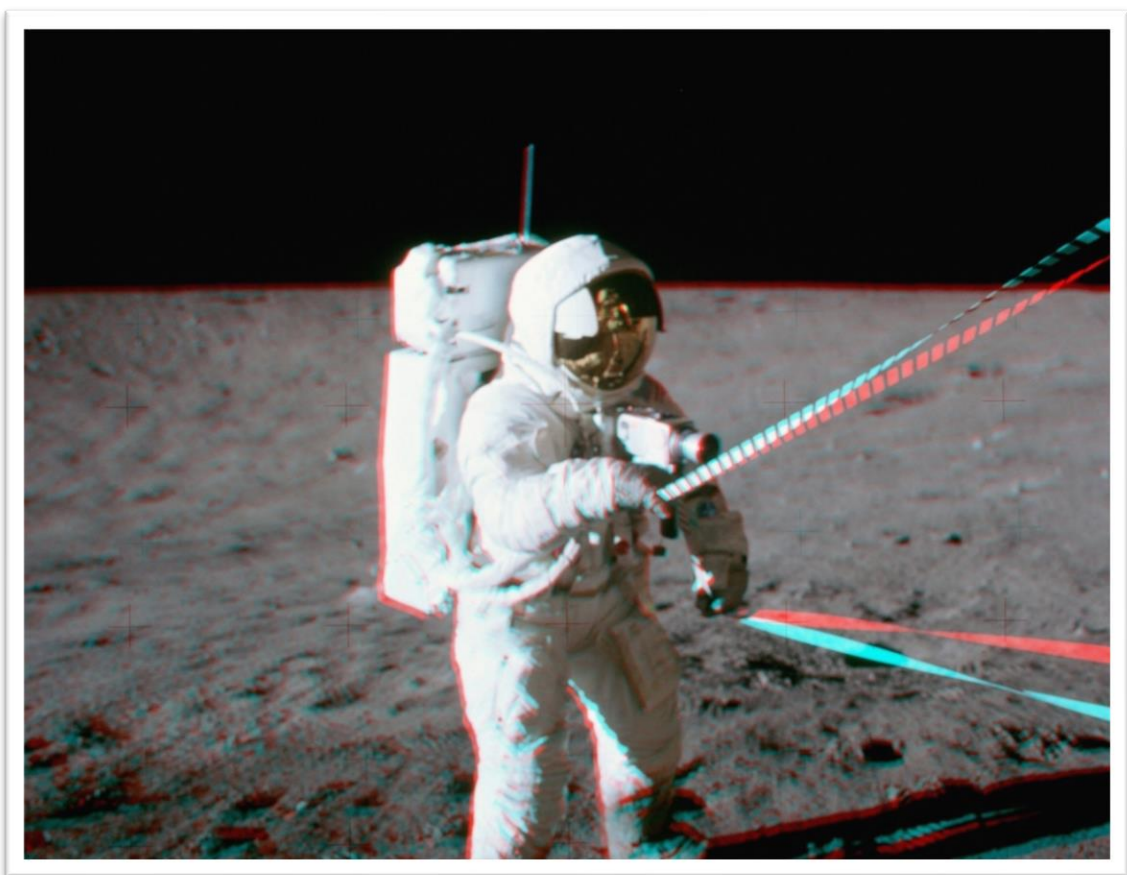
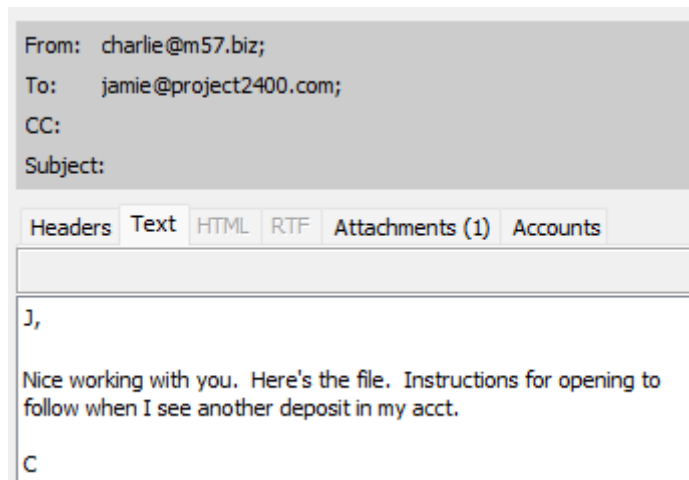
>

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

>

> C

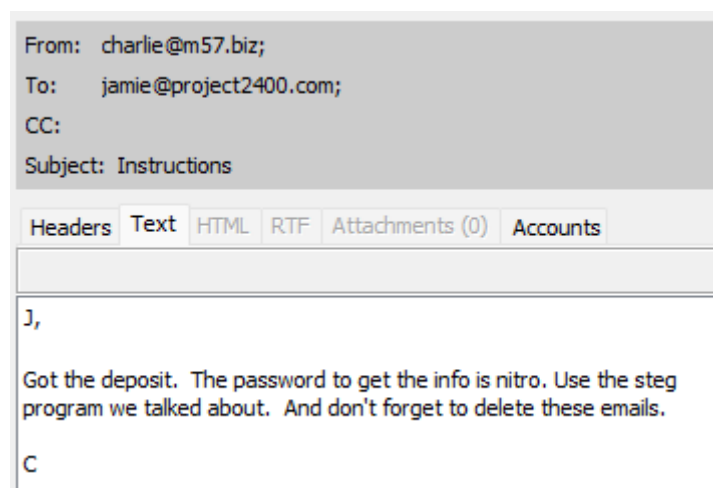
E-mail 2



Attachment 1

Path	C:/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Sent/astronaut1.jpg
MD5	45eade24b3a89b21fed303310ccbdc54
SHA-256	f57e2e43101088191f9929e1be088baeacb3ae4df18200701f4f814d6b551b32

E-mail 3



E-mail 4

Στο ίδιο χρονικό διάστημα εντοπίσαμε ένα email προς τον υπάλληλο Andy της εταιρείας SWExpert, όπου αναγραφόταν ότι ο Charlie είχε ανακαλύψει μία πατέντα η οποία θα ακύρωνε την πατέντα που αφορούσε την αθανασία της SWExpert (2009-12-04 09:41:47 PST - Email 5). Για να μην αποκαλύψει την εν' λόγω πληροφορία ζήτησε χρηματικό ποσό της τάξεως των 100.000 δολαρίων και απείλησε τον Andy να μην εμπλέξει την αστυνομία. Αυτό το email περιείχε ένα αρχείο zip (01.zip) με κωδικό, ο οποίος στάλθηκε στο επόμενο email (2009-12-07 11:44:18 PST - Email 6), μέσω μιας εικόνας (Attachment 2). Το ακόλουθο email περιείχε μια εικόνα με ένα μικροσκόπιο. Κατά την διάρκεια των ανωτέρω emails υπήρχε επικοινωνία του υπόπτου με δυο εξωτερικούς του φίλους, με τους οποίους συζητούσε για εξωτικά ταξίδια και πολυτελή αυτοκίνητα. Η πληροφορία αυτή διασταυρώθηκε όταν ανακτήθηκε στο ιστορικό αναζήτησής του.

From: charlie@m57.biz;
To: andy@swexpert.com;
CC:
Subject: I Found Something

Headers Text HTML RTF Attachments (1) Accounts

Andy,

Lucky for me, I just happened to stumble across this. I found a prior patent that will definitely invalidate your current immortality patent. You should have used my boss's prior art services, but, oh well, I'll just use your negligence to benefit me. I want 100k or I'll release this publicly. I don't need to tell you how much this will hurt your business if I go public with this. Don't involve the cops or this information will go public. See the attachment for details on what I found. I'll be in touch with my bank acct number. The password for the zip file will be hidden in the next picture I send you.

C

E-mail 5

From: charlie@m57.biz;
To: andy@swexpert.com;
CC:
Subject: Picture

Headers Text HTML RTF Attachments (1) Accounts

Andy,

Here's the picture I promised... Make sure you delete this.

C

E-mail 6



Attachment 2

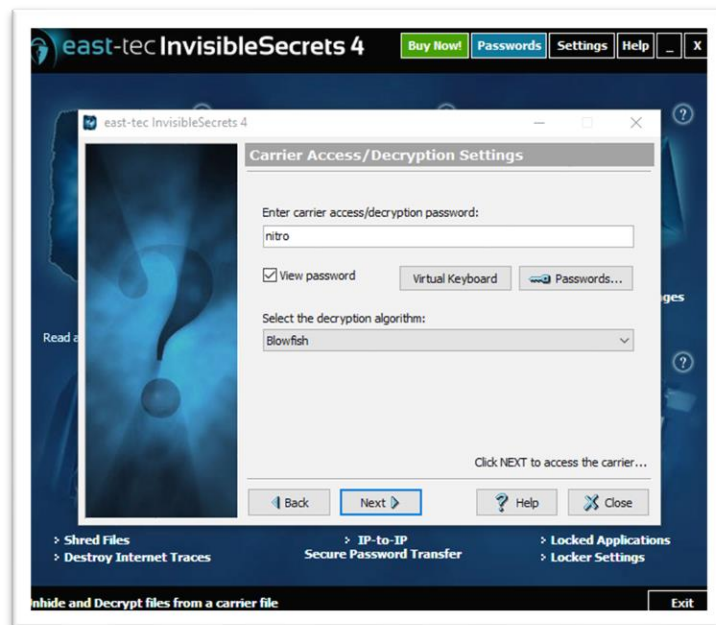
Path	C:/ Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Sent/microscope1.jpg
MD5	4be2c4abb48c4389ca798e6c21736ea1
SHA-256	99d057377f176c010166cde2c3e5ad517a7a3db7443810f048e38e4c32da0b29

Path	C:/ Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/Mail/Local Folders/Sent/01.zip
MD5	4fa239c22e5fb7b934a1bf68e4e0e2e7
SHA-256	07bf35fac76b6d068f3427dcc736142a99ca2b3643f147234e21a09650a41bc7

Ακόμη στο ιστορικό βρέθηκαν αναζητήσεις οι οποίες αφορούσαν εργαλεία στεγανογραφίας. Στον υπολογιστή του βρέθηκε το πρόγραμμα Cygnus Hex Editor 1.00, το οποίο χρησιμοποιείται για επεξεργασία HEX καθώς και το Invisible Secrets 2.1 για την στεγανογραφία. Στο USB το οποίο βρέθηκε στο γραφείο του περιέχονταν οι παραπάνω εικόνες και το αρχείο zip και τα e-mails.

Αναλύοντας τα παραπάνω ευρήματα μπορέσαμε να αποκρυπτογραφήσουμε τις εικόνες. Χρησιμοποιήσαμε το πρόγραμμα Invidible Secrets με τον κωδικό «nitro» και τον decryption algorithm BlowFish ώστε να αποστεγανογραφήσουμε την εικόνα του attachment 1

(astronaut.jpg) που είχε αποστείλει στον Jaime. Η εικόνα περιείχε το αρχείο «Nitroba work.odt», το οποίο έχουμε παραθέσει στην συνέχεια. Ανοίγοντας την 2^η εικόνα είτε με text editor (notepad) είτε κάνοντας dictionary attack μέσω του εργαλείου ArchPR, μπορέσαμε να βρούμε τον κωδικό «immortal», ο οποίος ξεκλειδώνει το αρχείο zip. Μέσα στο αρχείο zip περιέχονταν 2 εικόνες tif (us005026637-001.tif και us006982168-001.tif) οι οποίες αφορούσαν τις πατέντες υπ' αριθμόν «US 6,682,168 B1» και «5,026,637».



Εικόνα 1 Decrypt steganography file astronaut.jpg

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

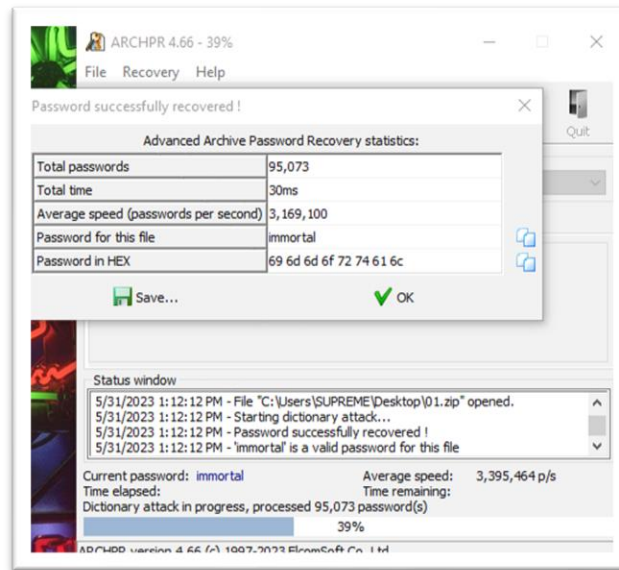
Pub. No.:	WO/2008/143237	International Application No.:	PCT/JP2008/059191
Publication Date:	27.11.2008	International Filing Date:	20.05.2008

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

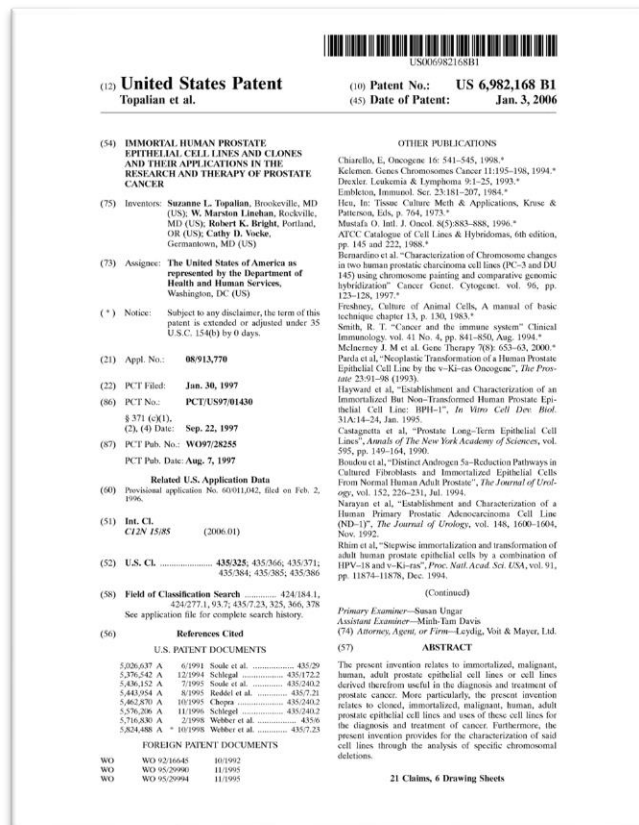
PriorityData:
11/700,015 31.01.2007 US

Title: SIMULATION SYSTEM IMPLEMENTING REAL-TIME MACHINE DATA

Εικόνα 2 Nitroba work.odt



Εικόνα 3 Dictionary attack retrieves file password



United States Patent [19]		[11] Patent Number: 5,026,637
Soule et al.		[45] Date of Patent: Jun. 25, 1991
[54] IMMORTAL HUMAN MAMMARY EPITHELIAL CELL LINES		Growth in Culture", Charles M. McGrath and Herbert D. Soule, pp. 653-662.
[76] Inventors: Herbert Soule, 6344 Jonathan, Dearborn, Mich. 48126; Charles M. McGrath, 6669 Beach, Troy, Mich. 48098		In Vitro Cellular & Developmental Biology, vol. 33, No. 1, Jan. 1986, "A Simplified Method for Passage and Long-Term Growth of Human Mammary Epithelial Cells", Herbert D. Soule and Charles M. McGrath, pp. 6-12.
[21] Appl. No.: 317,610		Proceedings of AACR, vol. 29, Mar. 1988, #1780, p. 448.
[22] Filed: Feb. 28, 1989 (Under 37 CFR 1.47)		Primary Examiner —Esther L. Kepplinger Assistant Examiner —Toni R. Scheiner Attorney, Agent, or Firm —Robert L. Kelly; Dykema Gossett
[51] Int. Cl. C12Q 1/02; C12Q 1/18; C12N 5/06		[57] ABSTRACT
[52] U.S. Cl. 435/29; 435/32; 435/172.1; 435/240.1; 435/240.2; 436/63; 436/813		Immortalized human epithelial cell sublines are provided. The novel cell lines do not undergo terminal differentiation and senescence upon exposure to high calcium concentrations. The novel cells exhibit positive reactivity with milk-fat globule membrane antigen and cytokeratin anti-serum. The cells are non-tumorigenic in athymic mice, and exhibit both three-dimensional growth in collagen and dome formation in confluent cultures. The cell sublines demonstrate growth control by hormones and growth factors. The novel cell sublines are useful in evaluating the capacity of preslected agents to bring about a change in epithelial cell growth and in the production of proteins.
[58] Field of Search 435/29, 23, 7, 320, 435/6, 252.8, 219, 32, 172.1, 240.1, 240.2; 436/63, 813; 536/27; 935/9; 424/85.2, 85.1, 85.8, 85.91, 1.1; 514/317, 428, 648; 530/14, 395, 415, 829		
[56] References Cited PUBLICATIONS Jones et al., Breast Cancer Research Group and Pathology Dept., Michigan Cancer Foundation, Detroit, Mich. 48201, Proceedings of AACR, vol. 29, (Mar. 1988). In Vitro, vol. 20, No. 8, Aug. 1984, "Calcium Regulation of Normal Human Mammary Epithelial Cell		3 Claims, 3 Drawing Sheets

Εικόνα 4 patents

4. Παρουσίαση

4.1 Παρουσίαση και επεξήγηση των συμπερασμάτων της έρευνας

Εισαγωγή

Στις 11/12/2009 ο Pat McGoo, CEO της νεοσύστατης M57-biz, επικοινωνήσε μέσω email με την ομάδα της AUEB InfoSec Ltd για την διερεύνηση ενός φερόμενου ηλεκτρονικού εκβιασμού που διαπράχθηκε στις 04/12/2009 από τον Charlie, εργαζόμενο στην M57-biz, προς τον Andy, εργαζόμενο της SWExperts. Πιο συγκεκριμένα, ο Andy ισχυρίστηκε πως ο Charlie βρήκε μια πατέντα η οποία, ούσα παλαιότερη, είναι ικανή να ακυρώσει μια κατοχυρωμένη πατέντα της SWExperts. Ο σκοπός της έρευνας ήταν να διαπιστωθεί εάν διαπράχθηκε ο εκβιασμός και τις λεπτομέρειες γύρω από αυτόν.

Περιγραφή Πειστηρίων

Στις 10/12/2009 η AUEB InfoSec Ltd επισκέφθηκε τα γραφεία της M57-biz με σκοπό την διερεύνηση του εγκλήματος. Εκεί τους περίμεναν οι Pat McGoo (CEO), Terry (IT Admin), Jo (εργαζόμενος, συνάδελφος του υπόπτου) και Charlie (εργαζόμενος, ύποπτος), από τους οποίους πάρθηκαν συνεντεύξεις (Παράρτημα Α). Στην σκηνή βρέθηκαν, ένα ενεργό laptop DELL κι ένα μη προσαρτημένο Kingston USB stick, και τα δύο πάνω στο γραφείο του Charlie. Η ομάδα της AUEB InfoSec Ltd πραγματοποίησε live acquisition στο ενεργό laptop, λαμβάνοντας πιστό αντίγραφο της μνήμης (με τα εργαλεία MDD και DumpIt) και του σκληρού δίσκου (με το εργαλείο AccessData FTK Imager 4.7.1.2 και FEX Imager 2.2.1), ενώ έλαβε και πιστό αντίγραφο του USB (ομοίως με τον δίσκο), καθώς και backup και hashes μέσω του εργαλείου FEX Imager v2.2.1. Τέλος, κατασχέθηκαν τα εν λόγω laptop (0001) και USB (0002), καθώς και ο φορτιστής του laptop.

Ανάλυση Πειστηρίων

Η ανάλυση των πειστηρίων έγινε σύμφωνα με την διεθνή μεθοδολογία ACPO, φροντίζοντας να αποφευχθεί η οποιαδήποτε αλλοίωση σε αυτά, όπως και να τηρηθούν οι διαδικασίες του chain of custody (Παράρτημα Ε). Πιο συγκεκριμένα, η ανάλυση του δίσκου του laptop και του USB πραγματοποιήθηκε με το εργαλείο Autopsy 4.20.0, ενώ για την μνήμη του laptop χρησιμοποιήθηκε το εργαλείο Volatility 2.6. Τα αποτελέσματα της ανάλυσης βρίσκονται στα Παραρτήματα Β και Γ της τεχνικής ανάλυσης.

Περιγραφή File System

ΑΝΑΛΥΣΗ ΣΚΛΗΡΟΥ ΔΙΣΚΟΥ LAPTOP	
Έναρξη	2009-12-10 16:53:26 PST
Πιστό Αντίγραφο	/img_charlie-2009-12-11.E01
Αρχεία	
Images	45287
Videos	51
Audio	168
Archives	553
Databases	46
HTML	873
Office	29
Pdf	30
Plain Text	1073
Rich Text	12
Exe	1423
Dll	5227
Bat	5
Cmd	2
Com	18
Deleted	3493 (1395 from File System)

ΑΝΑΛΥΣΗ USB	
Πιστό Αντίγραφο	/img_charlie-work-usb-2009-12-11.E01
Αρχεία	
Images	11
Videos	0
Audio	0
Archives	4
Databases	1
HTML	0
Office	1
Pdf	12
Plain Text	163
Rich Text	12
Exe	2
Dll	0
Bat	0

Cmd	0
Com	0
Deleted	2 (2 from File System)

Ευρήματα

Από τα συνολικά 36 ευρήματα, βρήκαμε 4 φωτογραφίες, από τις οποίες οι δυο ήταν στεγανογραφημένες, ενώ οι υπόλοιπες δυο περιέχονταν σε ένα προστατευμένο από κωδικό αρχείο zip. Τα προγράμματα που χρησιμοποιήθηκαν για την στεγανογραφία είναι το Cygnus HEX Editor και το Invisible Secrets. Επιπλέον βρέθηκαν 23 google searches τα οποία μεταξύ άλλων περιλάμβαναν αναζητήσεις για πατέντες, κατέβασμα ύποπτων προγραμμάτων, εξωτικά ταξίδια και πολυτελή αυτοκίνητα. Ακόμη, βρέθηκαν 6 emails από τα οποία τα 4 είχαν ανταλλαχθεί με τον κ. Jaime της εταιρείας Project2400, ενώ τα άλλα 2 με τον κ. Andy της εταιρείας SWExpert. Στα 2 emails που αφορούσαν τον κ. Andy βρέθηκαν στοιχεία εκβιασμού που θα ακύρωναν την πατέντα του. Τέλος, στα 4 emails που αφορούσαν τον κ. Jaime διαπιστώθηκε περιστατικό βιομηχανικής κατασκοπίας, με τον ύποπτο να προτείνει την ανταλλαγή εμπιστευτικών πληροφοριών για πατέντες που αφορούσαν την M57 Biz, έναντι χρηματικού αντιτίμου.

Αναλύοντας τα παραπάνω ευρήματα μπορέσαμε να αποκρυπτογραφήσουμε τις εικόνες. Χρησιμοποιήσαμε το πρόγραμμα Invidible Secrets με τον κωδικό «nitro» και τον decryption algorithm BlowFish ώστε να αποστεγανογραφήσουμε την εικόνα με τον αστροναύτη που είχε αποστείλει στον Jaime. Η εικόνα περιείχε το αρχείο «Nitroba work.odt», το οποίο αποτελεί στοιχείο βιομηχανικής κατασκοπίας. Ανοίγοντας την 2^η εικόνα είτε με text editor είτε κάνοντας dictionary attack μέσω του εργαλείου ArchPR, μπορέσαμε να βρούμε τον κωδικό «immortal», ο οποίος ξεκλειδώνει το αρχείο zip. Μέσα στο αρχείο zip περιέχονταν 2 εικόνες tif (us005026637-001.tif και us006982168-001.tif) οι οποίες αφορούσαν τις πατέντες υπ' αριθμόν «US 6,682,168 B1» και «5,026,637».

ΕΥΡΗΜΑΤΑ	ΑΡΙΘΜΟΣ
Φωτογραφίες	4
Archives	1
Ύποπτα Προγράμματα	2
Google searches	23
Emails	6
Σύνολο ευρημάτων	36

Συμπέρασμα

Από την ανάλυση των παραπάνω ευρημάτων διαπιστώσαμε ότι ο κ. Charlie πράγματι φαίνεται να εκβίασε τον κ. Andy με σκοπό το χρηματικό κέρδος. Ακόμη παρατηρήσαμε ότι ο ύποπτος εμπλέκεται σε περιστατικό βιομηχανικής κατασκοπίας μέσω παράνομης διαβίβασης εμπιστευτικών πληροφοριών, έναντι χρηματικού αντιτίμου.

Αθήνα, 9 Ιουνίου 2023

Υπογραφή Expert Witness

Χ. Αργυρόπουλος

Παράρτημα Α – Συνεντεύξεις

Pat (CEO):

- Ερώτηση:** Μπορείτε να μας μιλήσετε λίγο για τον λόγο που μας καλέσατε και συγκεκριμένα τι υποπτεύεστε;

Απάντηση: Πριν λίγες ημέρες έλαβα ένα email από τον κο Andy, εργαζόμενο της εταιρείας SWExpert, σύμφωνα με τον οποίο ο κος Charlie τον εκβίαζε έναντι χρηματικού αντιτίμου για να μην δημοσιεύσει πως η κατοχυρωμένη πατέντα της εταιρείας του σχετικά με την αθανασία μπορεί να ακυρωθεί.
- Ερώτηση:** Ποιά είναι η σχέση σας με τον κο Andy και την SWExpert;

Απάντηση: Ο κος Andy με είχε προσεγγίσει ώστε να τον συμβουλευσω για την κατοχύρωση της πατέντας της εταιρείας. Όμως, οι διαπραγματεύσεις δεν προχώρησαν και λίγες ημέρες μετά έπαψε η επικοινωνία μας.
- Ερώτηση:** Παρατηρήσατε κάτι ύποπτο την ημέρα του περιστατικού ή πριν από αυτό;

Απάντηση: Τις τελευταίες ημέρες ο Charlie είχε σταματήσει να έρχεται στο μεσημεριανό όπως συνηθίζαμε, κι έδειχνε να μην είναι συγκεντρωμένος στην δουλειά του.
- Ερώτηση:** Εμπιστεύεστε τον κο Charlie;

Απάντηση: Δεν έχω λόγο να μην τον εμπιστεύομαι, αν και πρέπει να σας υπενθυμίσω πως εργάζεται εδώ μονάχα έναν μήνα και δεν γνωρίζομαστε αρκετά.

Terry (IT Admin):

- Ερώτηση:** Είναι εταιρικά τα μηχανήματα, κι αν ναι, κρυπτογραφούνται;

Απάντηση: Ναι, τα μηχανήματα παρέχονται από την εταιρεία, αν και επιτρέπουμε στους υπαλλήλους μας να τα παίρνουν και σπίτι τους. Δεν κρυπτογραφούνται γιατί δεν το έχουμε κρίνει απαραίτητο.
- Ερώτηση:** Υπάρχει Active Directory;

Απάντηση: Όχι, αλλά έχουμε έναν shared network drive.
- Ερώτηση:** Υπάρχει VPN;

Απάντηση: Όχι.

4. **Ερώτηση:** Υπάρχει σύστημα ελέγχου πρόσβασης στον χώρο εργασίας;
Απάντηση: Ναι υπάρχει. Δυστυχώς όμως το Access Card System είναι εκτός λειτουργίας εδώ και δυο μήνες και δεν είναι αρμοδιότητά μας να το φτιάξουμε.
5. **Ερώτηση:** Μπορείς να φέρεις δικό σου USB;
Απάντηση: Οι εργαζόμενοι μας χρησιμοποιούν εταιρικά μηχανήματα και η σύνδεση προσωπικών τους συσκευών σε αυτά παραβιάζει τις πολιτικές ασφαλείας της εταιρίας μας. Ωστόσο, δεν έχουμε μηχανισμούς ελέγχου για το αν αυτές οι πολιτικές τηρούνται στην πράξη.
6. **Ερώτηση:** Πως γίνεται η αυθεντικοποίηση;
Απάντηση: Σύμφωνα με την πολιτική ασφαλείας, οι εργαζόμενοι πρέπει να ταυτοποιούνται με κωδικό πρόσβασης στις φορητές τους συσκευές, αν και, όπως σας είπα, δεν ελέγχουμε επαρκώς εάν και κατά πόσο αυτό εφαρμόζεται.
7. **Ερώτηση:** Μετά την αναφορά του περιστατικού. Πραγματοποιήσατε οποιαδήποτε ενέργεια στις συσκευές που βρίσκονταν στον χώρο (π.χ. λήψη αντιγράφων, απενεργοποίηση συσκευών κτλ);
Απάντηση: Όχι, με εντολή του Pat άφησα όλα τα μηχανήματα στην κατάσταση που ήταν μέχρι να έρθετε.

Jo (Υπάλληλος M57):

1. **Ερώτηση:** Ποια είναι η σχέση σας με τον Charlie;
Απάντηση: Ο Charlie ξεκίνησε στην εταιρεία να εργάζεται τον ίδιο καιρό μ' εμένα. Συνεργαζόμαστε χωρίς προβλήματα παρά τον λιγοστό χρόνο που δουλεύουμε μαζί.
2. **Ερώτηση:** Σε ποια project έχετε συνεργαστεί;
Απάντηση: Ο καθένας μας έχει το δικό του project, ωστόσο ανταλλάσσουμε πληροφορίες για τα project μας που μπορούν να βοηθήσουν τον άλλον.
3. **Ερώτηση:** Ποια είναι η άποψή του Charlie για τον Pat;
Απάντηση: Προσωπικά δεν έχω κάποιο πρόβλημα με τον Pat, αλλά ο Charlie τον θεωρούσε λίγο περίεργο αφεντικό.

Charlie (Υποπτος):

1. **Ερώτηση:** Είστε ικανοποιημένος από το περιβάλλον εργασίας σας;
Απάντηση: Ναι βεβαίως, δεν έχω κανένα πρόβλημα με τους συναδέλφους ή το αφεντικό μου.
2. **Ερώτηση:** Μπορείτε να μας πείτε σε ποια project της εταιρείας εργαζόσασταν, κι αν όχι μόνος σας τότε με ποιόν;
Απάντηση: Ο κος Pat μας ανέθεσε να βρούμε πατέντες σχετικά με διάφορα ζητήματα, σ' εμένα για την μηχανή του χρόνου και τον συνάδελφο μου, Jo, για την τηλεμεταφορά. Στη συνέχεια, μας ανέθεσε την κβαντική κρυπτογραφία την οποία ανέλαβα εγώ.

3. **Ερώτηση:** Ποιος ήταν ο σκοπός της συσκευής USB που βρέθηκε στο γραφείο σας;
Απάντηση: Προορίζεται για ίδια χρήση και μόνο.
4. **Ερώτηση:** Είχατε πρόσβαση σε εμπιστευτικές πληροφορίες στον εν λόγω φορητό υπολογιστή;
Απάντηση: Είχα πρόσβαση μόνο σε όσα δεδομένα χρειαζόνταν για να κάνω την δουλεία μου και τίποτα περισσότερο ή λιγότερο.
5. **Ερώτηση:** Χρησιμοποιείτε την εταιρική σας συσκευή για σκοπούς που δεν αφορούν την εργασία σας (π.χ. αποθήκευση αρχείων, πρόσβαση σε προσωπικούς λογαριασμούς, τήρηση προσωπικού προγράμματος κτλ);
Απάντηση: Όχι, χρησιμοποιώ το laptop που μου έχει δοθεί αποκλειστικά για την εκπλήρωση των καθηκόντων μου. Κάθε φορά που φεύγω από την εταιρία το κλείνω και το αφήνω πάνω στο γραφείο μου ώστε να το βρω την επόμενη φορά που θα έρθω.
6. **Ερώτηση:** Μπορείτε να παράσχετε οποιαδήποτε πληροφορία που θα μπορούσε να βοηθήσει στην έρευνα;
Απάντηση: Όχι, αλλά είμαι διαθέσιμος για όποια άλλη ερώτηση έχετε να μου θέσετε.

Παράρτημα Β – Ανάλυση μνήμης Laptop

Συστημικές διεργασίες		
Όνομα	PID	PPID
System	4	-
smss.exe	876	4
csrss.exe	924	876
winlogon.exe	948	876
services.exe	992	948
lsass.exe	1004	948
svchost.exe	1180	992
svchost.exe	1268	992
svchost.exe	1392	992
svchost.exe	1532	992
svchost.exe	1644	992
svchost.exe	1796	992

Πίνακας 3 Διεργασίες συστήματος που εντοπίστηκαν στο αντίγραφο της μνήμης

Διεργασίες χρήστη		
Όνομα	PID	PPID
spoolsv.exe	1908	992
jqsv.exe	320	992
explorer.exe	1348	1304
jusched.exe	2804	1348

ctfmon.exe	2832	1348
alg.exe	2956	992
soffice.exe	3048	3000
avgfws9.exe	3936	992
thunderbird.exe	188	1348

Πίνακας 4 Διεργασίες εκκινημένες από τον χρήστη που εντοπίστηκαν στο αντίγραφο της μνήμης

Δικτυακές συνδέσεις		
Local address	Foreign 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 5 Δικτυακές συνδέσεις που καταγράφηκαν με το Volatility

```
PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\charlie-2009-12-11.mddramimage imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone\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 : 0xfffff000L
      KPCR for CPU 1 : 0xf7717000L
      KUSER_SHARED_DATA : 0xfffff000L
      Image date and time : 2009-12-11 16:59:52 UTC+0000
      Image local date and time : 2009-12-11 08:59:52 -0800
```

Εικόνα 5 Πληροφορίες αντιγράφου μνήμης

```
PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbgscan
Volatility Foundation Volatility Framework 2.6
*****
Instantiating KDBG using: Kernel AS WinXPSP3x86 (5.1.0 32bit)
Offset (V) : 0x805532e0
Offset (P) : 0x5532e0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64 : 0x805532b8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab) : 2600.xpsp_sp3_gdr.090804-1435
PsActiveProcessHead : 0x80569658 (26 processes)
PsLoadedModuleList : 0x805634c0 (113 modules)
KernelBase : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader) : 5
Minor (OptionalHeader) : 1
KPCR : 0xfffff000 (CPU 0)
KPCR : 0xf7717000 (CPU 1)
```

Εικόνα 6 Προβολή πιθανών offsets

```

PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe
-f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbg=0x805532e0 shellbags
Volatility Foundation Volatility Framework 2.6
Scanning for registries...
Gathering shellbag items and building path tree...
*****
Registry: \Device\HarddiskVolume1\Documents and Settings\Charlie\NTUSER.DAT
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last updated: 2009-12-11 00:11:17 UTC+0000
Value      File Attr      File Name      Modified Date      Create Date      Access Date
-----
ItemPos1280x1024(1)  ARC          AVG900~1.LNK   2009-11-09 01:45:18 UTC+0000  2009-11-09 01:45:18 UTC+0000  2009-12-09 16:38:50 UTC+0000
ItemPos1280x1024(1)  ARC          FOXITR~1.LNK   2009-11-17 21:50:46 UTC+0000  2009-11-17 21:50:46 UTC+0000  2009-12-04 21:39:06 UTC+0000
ItemPos1280x1024(1)  ARC          MOZILL~1.LNK   2009-11-13 01:48:06 UTC+0000  2009-11-13 01:48:06 UTC+0000  2009-12-09 16:31:42 UTC+0000
ItemPos1280x1024(1)  ARC          MOZILL~2.LNK   2009-11-13 01:52:44 UTC+0000  2009-11-13 01:52:44 UTC+0000  2009-12-09 16:31:42 UTC+0000
ItemPos1280x1024(1)  ARC          OPENOF~1.LNK   2009-11-10 01:04:22 UTC+0000  2009-11-10 01:04:22 UTC+0000  2009-12-04 21:39:06 UTC+0000
ItemPos1280x1024(1)  DIR          web            2009-12-10 00:29:34 UTC+0000  2009-11-17 22:01:28 UTC+0000  2009-12-10 00:29:34 UTC+0000

```

```

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

```

Εικόνα 7 Φάκελοι και αρχεία που προσελάστηκαν από τον χρήστη

```

PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe
-f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbg=0x805532e0 consoles
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: csrss.exe Pid: 924
Console: 0x4f27c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: mdd - 70.66% complete
AttachedProcess: mdd_1.3.exe Pid: 1768 Handle: 0x718
AttachedProcess: cmd.exe Pid: 3296 Handle: 0x678
----
CommandHistory: 0x12b33f8 Application: mdd_1.3.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x718
----
CommandHistory: 0x4f5098 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x678
Cmd #0 at 0x12b32d8: z:\mdd_1.3.exe -o z:\charlie-2009-12-11.ram
----
Screen 0x4f2ea0 X:80 Y:300
Dump:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

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

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

```

Εικόνα 8 Λήψη των εντολών που εκτέλεσε ο χρήστης

```
PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbg=0x805532e0 connections
Volatility Foundation Volatility Framework 2.6
Offset(V) Local Address Remote Address Pid
-----
0x897e5008 127.0.0.1:1301 127.0.0.1:1302 188
0x898e4788 127.0.0.1:1302 127.0.0.1:1301 188
0x8979b730 192.168.1.104:1310 192.168.1.1:445 4
0x8946bbe8 192.168.1.104:1208 198.189.255.73:80 2804
0x8997f690 127.0.0.1:1300 127.0.0.1:1299 188
0x899b2cb0 127.0.0.1:1299 127.0.0.1:1300 188
```

Εικόνα 6 Ανίχνευση ενεργών συνδέσεων

```
PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbg=0x805532e0 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x092c3938 192.168.1.104:1311 192.168.1.1:139 4
0x093ea788 192.168.1.104:1303 63.245.209.10:80 188
0x0946bbe8 192.168.1.104:1208 198.189.255.73:80 2804
0x0979b730 192.168.1.104:1310 192.168.1.1:445 4
0x097e5008 127.0.0.1:1301 127.0.0.1:1302 188
0x0988ac88 192.168.1.104:1304 208.97.132.223:995 188
0x098e4788 127.0.0.1:1302 127.0.0.1:1301 188
0x0997a2c0 192.168.1.104:1307 208.97.132.223:995 188
0x0997f690 127.0.0.1:1300 127.0.0.1:1299 188
0x099b2cb0 127.0.0.1:1299 127.0.0.1:1300 188
0x09a9f2c0 192.168.1.104:1305 63.245.221.11:80 188
```

Εικόνα 7 Εντοπισμός όλων των συνδέσεων

```
PS C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\charlie-2009-12-11.mddramimage --profile=WinXPSP3x86 kdbg=0x805532e0 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0x89bfb9c8 System 4 0 64 512 ----- 0
0x89af0460 smss.exe 876 4 3 19 ----- 0 2009-12-11 00:53:21 UTC+0000
0x899fd970 csrss.exe 924 876 11 417 0 0 2009-12-11 00:53:22 UTC+0000
0x89b0b818 winlogon.exe 948 876 17 572 0 0 2009-12-11 00:53:22 UTC+0000
0x89afb5d0 services.exe 992 948 15 265 0 0 2009-12-11 00:53:23 UTC+0000
0x896e01e0 lsass.exe 1004 948 22 354 0 0 2009-12-11 00:53:23 UTC+0000
0x89afa608 svchost.exe 1180 992 17 194 0 0 2009-12-11 00:53:23 UTC+0000
0x89887a78 svchost.exe 1268 992 10 272 0 0 2009-12-11 00:53:24 UTC+0000
0x89387978 svchost.exe 1392 992 74 1523 0 0 2009-12-11 00:53:24 UTC+0000
0x89476da0 svchost.exe 1532 992 5 81 0 0 2009-12-11 00:53:24 UTC+0000
0x8988cc18 svchost.exe 1644 992 11 166 0 0 2009-12-11 00:53:24 UTC+0000
0x893a2ca8 spoolsv.exe 1908 992 10 114 0 0 2009-12-11 00:53:26 UTC+0000
0x8944d9e0 svchost.exe 1796 992 4 108 0 0 2009-12-11 00:53:40 UTC+0000
0x897899e0 avgwdsvc.exe 1728 992 25 962 0 0 2009-12-11 00:53:40 UTC+0000
0x89398160 jqs.exe 320 992 5 117 0 0 2009-12-11 00:53:42 UTC+0000
0x89395800 explorer.exe 1348 1304 13 481 0 0 2009-12-11 00:53:46 UTC+0000
0x892ccbc0 hkcmd.exe 2684 1348 2 104 0 0 2009-12-11 00:53:51 UTC+0000
0x892d6948 jusched.exe 2804 1348 2 152 0 0 2009-12-11 00:53:51 UTC+0000
0x8990ebe0 ctfdmon.exe 2832 1348 1 71 0 0 2009-12-11 00:53:52 UTC+0000
0x89292308 alg.exe 2956 992 6 107 0 0 2009-12-11 00:53:52 UTC+0000
0x892a29e0 soffice.exe 3048 3000 1 20 0 0 2009-12-11 00:53:52 UTC+0000
0x89281da0 soffice.bin 3088 3048 7 216 0 0 2009-12-11 00:53:53 UTC+0000
0x89482718 avgfws9.exe 3936 992 25 762 0 0 2009-12-11 00:54:05 UTC+0000
0x892e57b0 thunderbird.exe 188 1348 10 203 0 0 2009-12-11 16:54:43 UTC+0000
0x899a7020 cmd.exe 3296 1348 1 33 0 0 2009-12-11 16:59:32 UTC+0000
0x8938cb28 mdd_1.3.exe 1768 3296 1 24 0 0 2009-12-11 16:59:51 UTC+0000
```

Εικόνα 9 Διεργασίες μηχανήματος


```
C:\Users\Philip\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f charlie-2009-12-11.mddra
mimage --profile=WinXPSP3x86 --kdbg=0x805532e0 hivedump -o 0xe1390b60
Volatility Foundation Volatility Framework 2.6
Last Written      Key
2009-12-11 00:52:48 UTC+0000 \HARDWARE
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\DSDT
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\DSDT\DELL
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\DSDT\DELL\dt_ex
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\DSDT\DELL\dt_ex\00001000
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\FACS
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\FADT
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\FADT\DELL__
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\FADT\DELL__\GX270__
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\FADT\DELL__\GX270__\00000008
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\RSDT
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\RSDT\DELL__
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\RSDT\DELL__\GX270__
2009-12-11 00:52:48 UTC+0000 \HARDWARE\ACPI\RSDT\DELL__\GX270__\00000008
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\CentralProcessor
2009-12-11 00:52:54 UTC+0000 \HARDWARE\DESCRIPTION\System\CentralProcessor\0
2009-12-11 00:52:54 UTC+0000 \HARDWARE\DESCRIPTION\System\CentralProcessor\1
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\FloatingPointProcessor
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\FloatingPointProcessor\0
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\FloatingPointProcessor\1
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\MultifunctionAdapter
2009-12-11 00:52:48 UTC+0000 \HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0
```

Εικόνα 10 Volatility hivedump

Παράρτημα Γ – Ανάλυση δίσκου Laptop

Disclaimer: The registry can be found in “Charlie-2009-12-11.E01/vol2/WINDOWS/system32/config”

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
	PC	MD5	0377b3d41bbbc295a1c9f00aa07ee174
		SHA-1	Not calculated
	RM#2	MD5	9c0de6c8532d7a66ddcf01861dfb6535
		SHA-1	Not calculated
Evidence Location	N/A		

Listing
Keyword search 1 - Control
X

charlie-2009-12-11.E01_1 Host

Table
Thumbnail
Summary

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
charlie-2009-12-11.E01	Image	10239860736	512	Europe/Athens	8db75e97-919c-4bd4-afe5-7203ebc11549

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

Metadata

Name: /img_charlie-2009-12-11.E01
Type: E01
Size: 10239860736
MD5: 0377b3d41bbbc295a1c9f00aa07ee174
SHA1: Not calculated
SHA-256: Not calculated
Sector Size: 512
Time Zone: Europe/Athens
Acquisition Details: Acquired Date: Thu Jan 13 06:49:15 2011
: System Date: Thu Jan 13 06:49:15 2011
: Acquire Operating System: Linux
: Acquire Software Version: 20100226
Device ID: 8db75e97-919c-4bd4-afe5-7203ebc11549
Internal ID: 1
Local Path: D:\Lessons\Post\SecondSemester\Ψηφιακό Ποινικό\ProjectFiles\digital forensics\Project Files\charlie-2009-12-11.E01

2) Identify the partition information of PC image.

Possible Answer	No.	Bootable	File system	Start Sector	Total Sectors	Size
	1	False	Unallocated	0	63	32.256 B
	2	True	NTFS	63	19968732	10.223.988.736 B
	3	False	Unallocated	19968795	30933	15.837.696 B
Evidence Location	N/A					

charlie-2009-12-11.E01_1 Host
 charlie-2009-12-11.E01
 -- vol1 (Unallocated: 0-62)
 -- vol2 (NTFS / exFAT (0x07): 63-19968794)
 -- vol3 (Unallocated: 19968795-19999727)
 Views
 File Types
 Deleted Files
 File Size
 a Artifacts
 Installed Programs (113)
 Metadata (1)
 Operating System Information (1)
 Recent Documents (49)
 Remote Drive (1)
 Run Programs (83)
 Shell Bags (76)
 USB Device Attached (13)
 Web Bookmarks (108)
 Web Cookies (267)
 Web Downloads (28)
 Web Form Autofill (34)
 Web History (4580)
 Web Search (38)
 Ysis Results

Table	Thumbnail	Summary
Types	User Activity	Analysis Recent Files Past Cases Geolocation Timeline Ingest History Container
Display Name:	charlie-2009-12-11.E01	
Name:	charlie-2009-12-11.E01	
Device ID:	8db75e97-919c-4bd4-afe5-7203ebc11549	
Time Zone:	Europe/Athens	
Acquisition Details:	Acquired Date: Thu Jan 13 06:49:15 2011 System Date: Thu Jan 13 06:49:15 2011 Acquiry Operating System: Linux Acquiry Software Version: 20100226	
Image Type:	E01	
Size:	10,24 GB (10239860736 bytes)	
Unallocated Space:	1,22 GB (1221761024 bytes)	
Sector Size:	512 bytes	
MD5:	037b3d41bbbc295a1c9f00aa07ee174	
SHA1:		
SHA256:		
File Paths:	C:\Users\Jerry\Desktop\charlie-2009-12-11.E01	

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

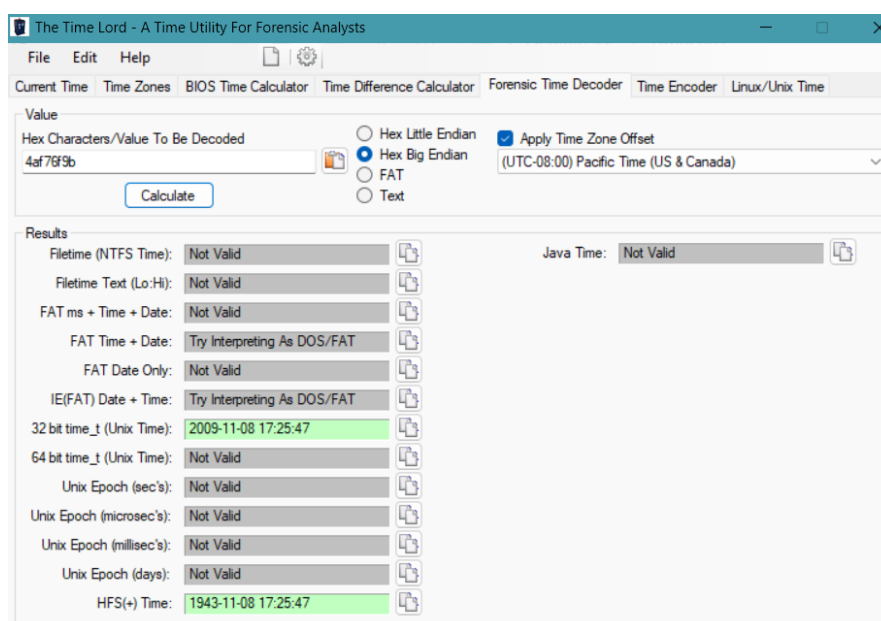
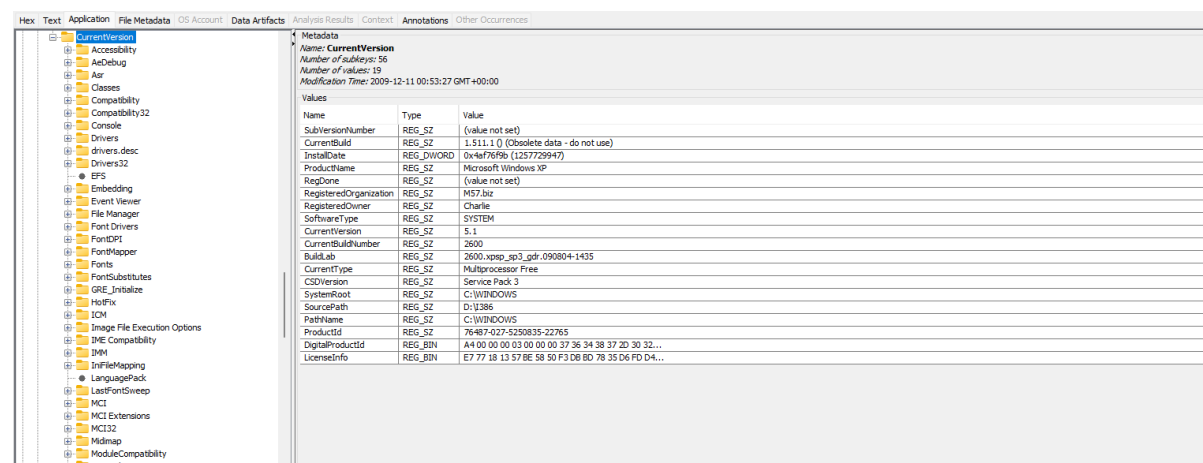
Annotations

Other Occurrences

3) Explain installed OS information in detail.

(OS name, install date, registered owner...)

Possible Answer	OS Name	Microsoft Windows XP Service Pack 3
	Version	5.1
	Build Number	1.511.1 ()
	Registered Owner	Charlie
	System Root	C:/WINDOWS
	Install Date	Monday, November 8, 2009 5:25:47 PM PST (1257729947 Linux Epoch)
Evidence Location	HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/ProductName HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/CSDVersion HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/CurrentBuild HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/RegisteredOwner HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/SystemRoot HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/InstallDate	



Χρησιμοποιήσαμε το <https://www.epochconverter.com/> για την μετατροπή από UNIX Timestamp και έπειτα το μετατρέψαμε σε PST μέσω του timelord.

4) What is the timezone setting?

Possible Answer	Timezone	Pacific Standard Time
	Daylight Time Bias	-60 minutes = -1hour 0xfffffc4 (Linux Epoch 4294967236)
Evidence Location	HKLM/SYSTEM/ControlSet###/Control/TimeZoneInformation/StandardName	
	HKLM/SYSTEM/ControlSet###/Control/TimeZoneInformation/DaylightBias	

DaylightBias
REG_DWORD

For example, this value might contain -60 (0xfffffc4), which indicates that one hour must be subtracted from the Bias.

Flag that indicates if the system should automatically adjust the clock for DST.

The user can configure this option under the time zone

<https://social.msdn.microsoft.com/Forums/en-US/2c4ae933-c67c-4036-b02a-d72e684154a7/daylight-savings-and-ewffbwf?forum=quebeccefs>

5) *What is the computer name?*

Possible Answer	M57-CHARLIE
Evidence Location	HKLM/SYSTEM/ControlSet###/Control/ComputerName/ComputerName/ComputerName

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

Possible Answer (Timezone is applied)	Account	SID	NT Hash	Login Count	Account Created Time	Last Login Time
	Charlie	1003	A	51	2009-11-10 11:13:30 PST	2009-12-10 16:53:26 PST
	HelpAssistan t	1000	B	0	2009-11-08 09:05:58 PST	-
Evidence Location	HKLM/SAM/SAM/Domains/Account/Users HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/ProfileList A) aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 B) c84fa92b5e90e68cdf2b9bc99a6ddf59:fc20a40d2ee88511f2093e88e4e90d03					

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
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-1-5-21-682003330-329068152-1644491937-1003			0	Charlie	charlie-2009-12-11.E01_1 Host	Local		2009-11-10 11:13:30 PST
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-1-5-80-324959683-3395802011-921526492-9190365			0		charlie-2009-12-11.E01_1 Host	Local	NT SERVICE	
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-1-5-21-682003330-329068152-1644491937-501			0	Guest	charlie-2009-12-11.E01_1 Host	Local		2009-11-08 09:05:58 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

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

Basic Properties
Login: Charlie
Full Name: Charlie
Address: S-1-5-21-682003330-329068152-1644491937-1003
Type:
Creation Date: 2009-11-10 11:13:30 PST
Object ID: 3014

charlie-2009-12-11.E01_1 Host Details
Last Login: 2009-12-11 02:53:26 EET
Login Count: 51
Administrator: True
Password Settings: Password does not expire
Flag: Normal user account
Home Directory: /Documents and Settings/Charlie

Realm Properties
Name: Unknown
Address: S-1-5-21-682003330-329068152-1644491937
Scope: Local
Confidence: Inferred

This user information is maintained in the F value located in the following path:

SAM\SAM\Domains\Account\Users\{RID}

The (RID), or Relative Identifier, is the portion of a Security Identifier (SID) that identifies a user or group in relation to the authority that issued the SID. Besides providing quite a bit of information about how SIDs are created, Microsoft also provides a list of RIDs (<http://support.microsoft.com/kb/157234>) for well-known users and groups as well as well-known aliases (seen in the SAM\SAM\Domains\BuiltIn\Aliases key).

The F value within the key is a binary data type and must be parsed appropriately (see the sam.h file, part of the source code for Peter's utility) to extract all the information. Some important dates are available in the contents of the binary data for the F value—specifically, several time/date stamps represented as 64-bit FILETIME objects. Those values and their locations are as follows:

- Bytes 8-15 represent the last login date for the account.
- Bytes 24-31 represent the date that the password was last reset (if the password hasn't been reset or changed, this date will correlate to the account creation date).
- Bytes 32-39 represent the account expiration date.
- Bytes 40-47 represent the date of the last failed login attempt (because the account name has to be correct for the date to be changed on a specific account, this date can also be referred to as the date of the last incorrect password usage).

Tools such as AccessData's Registry Viewer will decode this information for you automatically, as Figure 4.18 illustrates.

Figure 4.18 Portion of AccessData's Registry Viewer Showing Decode of a User's F Value

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

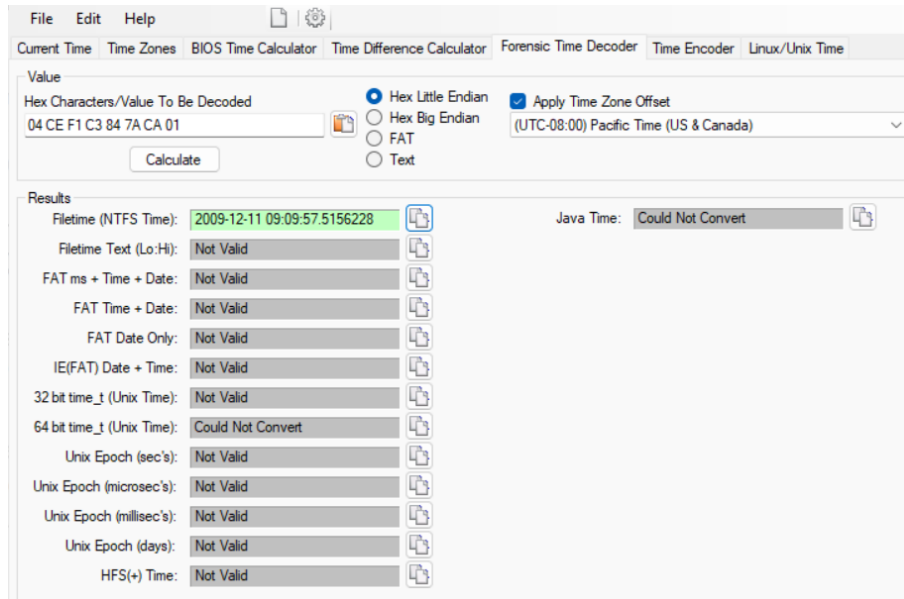
Possible Answer	Charlie
Evidence	HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Default UserName

Location	
----------	--

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

Possible Answer	Fri Dec 11 09:09:57 2009 PST (04 CE F1 C3 84 7A CA 01)
Evidence Location	HKLM/SYSTEM/ControlSet###/Control/Windows/ShutdownTime

Χρησιμοποιήσαμε ένα script για μετατροπή της REG_BIN value σε date που βρήκαμε στο ακόλουθο [link](#) και το μετατρέψαμε με το timelord.



```

from __future__ import division
import struct
import sys
from binascii import unhexlify
from datetime import datetime, timedelta

nt_timestamp = struct.unpack("<Q", unhexlify("04CEF1C3847ACA01"))[0]
epoch = datetime(1601, 1, 1, 0, 0, 0)
nt_datetime = epoch + timedelta(microseconds=nt_timestamp / 10)

print(nt_datetime.strftime("%c"))

Fri Dec 11 17:09:57 2009

```

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

Possible	Device Name	Intel(R) PRO/1000 MT Network Connection
	IP Address	192.168.1.104
	Subnet Mask	255.255.0.0

Answer	Name Server	192.168.1.1
	Domain	m57.biz
	Default Gateway	192.168.1.1
	DHCP Usage	YES
	DHCP Server	192.168.1.1
Evidence Location	GUID={B15FB27D-C44F-4540-AB9C-7C789450051B} HKLM/SOFTWARE/Microsoft/WindowNT/CurrentVersion/NetworkCards/9 HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpIPAddress HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpSubnetMask HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpNameServer HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpDomain HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpDefaultGateway HKLM/SYSTEM/ControlSet###/Services/Tcpip/Parameters/Interfaces/GUID/DhcpServer	

Κάναμε την αντιστοίχιση του ServiceName με το Description για να βρούμε το Device Name.

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

Possible Answer	Installation Time	Name	Version	Manufacturer	Installation Path
(Timezone is applied)	2009-11-24 12:01:10 PST	Cygnus Hex Editor FREE EDITION	1.00	SoftCircuits	C:/Program Files/Cygnus FREE EDITION/
	2009-11-19 08:43:32 PST	Invisible Secrets	2.1	east-tec	C:/Program Files/Invisible Secrets 2.1
	2009-11-17 11:50:44 PST	Foxit Reader	3.1.3.1030	Foxit	C:/Program Files/Foxit Software/Foxit Reader
	2009-11-12 15:52:43 PST	Mozilla Thunderbird	2.0.0.23	Mozilla	C:/Program Files/Mozilla Thunderbird
	2009-11-09 15:04:29 PST	OpenOffice.org	3.1.9420	Apache	C:/Program Files/OpenOffice.org 3/program/soffice.exe
	2009-11-08 15:44:32 PST	AVG	9.0	AVG Technologies	C:/Program Files/AVG/AVG9

	2009-11-08 15:22:58 PST	DXM_Runtime			Not Found
	2009-11-08 15:20:56 PST	AddressBook			Not Found
	2009-11-08 15:20:56 PST	OutlookExpress			Not Found
	2009-11-08 15:20:51 PST	DirectDrawEx			Not Found
	2009-11-08 15:20:51 PST	Fontcore			Not Found
	2009-11-08 15:20:51 PST	IE40			Not Found
	2009-11-08 15:20:51 PST	IE4Data			Not Found
	2009-11-08 15:20:51 PST	IE5BAKEX			Not Found
	2009-11-08 15:20:51 PST	IEData			Not Found
	2009-11-08 15:20:51 PST	MobileOptionPack			Not Found
Evidence Location	HKLM/SOFTWARE//Microsoft/Windows/CurrentVersion/Uninstall/~ C:/Program Files				

11) What web browsers were used?

Possible Answer	Windows Internet Explorer 8 (Updated from Windows Internet Explorer 7) 8.0.6001.18702 Mozilla Firefox (3.5.5)
Evidence Location	HKLM/SOFTWARE/Microsoft/InternetExplorer HKLM/SOFTWARE/Mozilla/Mozilla Firefox HKLM/SOFTWARE//Microsoft/Windows/CurrentVersion/Uninstall

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

Possible Answer	MS IE	index.dat
	Firefox	places.sqlite, cookies.sqlite, downloads.sqlite, favicons.sqlite, fomrhistory.sqlite

Evidence Location	C:/Documents and Settings/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default C:/Documents and Settings/Charlie/Local Settings/History/History.IE5/index.dat
-------------------	--

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

Possible Answer	Timestamp	URL	Browser
(Some duplicated and meaningless items are excluded) (Timezone is applied)	2009-11-12 15:47:08 PST	http://mozilla-mirror.3347.voxcdn.com/pub/mozilla.org/firefox/releases/3.5.5/win32/en-US/Firefox%20Setup%203.5.5.exe	IE
	2009-11-12 17:50:27 PST	http://hyperstruct.net/content/mozrepl	Firefox
	2009-11-18 12:57:14 PST	http://www.turtlefiji.com/	Firefox
	2009-11-19 10:42:17 PST	http://www.neobytesolutions.com/downloads/invsecr2.exe	Firefox
	2009-11-12 17:51:45 PST	http://www.mozillamessaging.com/en-US/thunderbird/	Firefox
	2009-11-12 17:54:56 PST	http://www.python.org/download/	Firefox
	2009-11-16 10:39:05 PST	http://webmail.m57.biz/src/login.php	Firefox
	2009-11-16 13:00:32 PST	http://en.wikipedia.org/wiki/Patent_research	Firefox
	2009-11-16 13:14:00 PST	http://en.wikipedia.org/wiki/Internet_as_a_source_of_prior_art	Firefox
	2009-12-10 14:19:34 PST	http://www.wipo.int/pctdb/en/fetch.jsp?SEARCH_I A=KR2006002671&DBSELECT=PCT&C=00&TO TAL=31&IDB=0&TYPE_FIELD=256&SERVER_T YPE=19-00&SORT=11274962- KEY&QUERY=et%2Fquantum+and+et%2Fcryptog raphy%0D%0A&START=1&ELEMENT_SET=BA SICHTML- ENG&RESULT=10&DISP=25&FORM=SEP- 0%2FHITNUM%2CB- ENG%2CDP%2CMC%2CAN%2CPA%2CABSUM - ENG&IDOC=929058&IA=KR2006002671&LANG =ENG&DISPLAY=NATIONAL	Firefox

	2009-12-10 09:59:34 PST	http://www.ferrari.com/English/Pages/Home.aspx	Firefox
	2009-12-10 09:56:45 PST	http://www.gulfstream.com/	Firefox
	2009-12-10 09:37:41 PST	http://www.friendlyplanet.com/	Firefox
	2009-12-10 09:30:59 PST	http://www.espacenet.com/	Firefox
	2009-12-10 09:20:18 PST	http://www.investorwords.com/	Firefox
	2009-12-08 17:31:12 PST	http://www.avg.com/us-en/upgrade-trial?lic=OUktQVNYTk4tWDRXR1ctTTBYRlItVDg0VlgtM1ZYMDI=	Firefox
	2009-12-08 14:17:34 PST	http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=kXT&q=ford+car+dealer&aq=f&oq=&aqi=g10	Firefox
	2009-12-08 14:17:01 PST	http://www.google.com/search?q=exotic+car+dealer&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a	Firefox
	2009-12-08 13:01:48 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 Sp 4024611241	Firefox
	2009-12-08 13:01:41 PST	http://www.expedia.com/daily/packages/default.asp?semcid=13172-1&eapid=13172-1&keyword=vacation%20packages!p.24314717.{ifsearch:1}{ifcontent:0}. {creative}. {keyword}. {placement}.vacation%20packagesXxXx24683600 {ifsearch:1}{ifcontent:0} {creative} {keyword} {placement}	Firefox
	2009-12-07 09:32:35 PST	http://www.us-cert.gov/control_systems/csvuls.html	Firefox
	2009-12-07 09:22:54 PST	http://afni.nimh.nih.gov/pub/dist/doc/program_help/3dsvm.html	Firefox
	2009-12-07 09:08:37 PST	http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/13845.html	Firefox
Evidence Location	C:/Documents and Settings/Charlie/Local Settings/History/History.IE5/index.dat C:/Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/		

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

Possible Answer	Timestamp	Keyword (URL)	Browser
(Some duplicated and meaningless items are excluded) (Timezone is applied)	2009-11-12 15:46:39 PST	firefox	IE
	2009-12-08 14:17:01 PST	Exotic car dealer	Firefox
	2009-11-19 08:49:43 PST	Time travel	Firefox
	2009-11-19 08:50:39 PST	Time machine -real	Firefox
	2009-11-19 08:52:00 PST	Time machine	Firefox
	2009-11-24 13:19:22 PST	7zip	Firefox
	2009-12-04 12:27:45 PST	Fox news	Firefox
	2009-11-24 13:57:05 PST	Hex editor	Firefox
	2009-12-02 08:55:58 PST	Hot sports cars	Firefox
	2009-12-08 13:01:37 PST	Mediterranean vacation packages	Firefox
	2009-11-12 17:50:27 PST	mozrepl	Firefox
	2009-11-12 17:54:56 PST	python	Firefox
	2009-11-19 10:39:24 PST	steganography	Firefox
	2009-11-18 13:00:37 PST	Thunderbird calendar	Firefox

	2009-11-12 17:51:43 PST	Thunderbird email	Firefox
	2009-12-08 12:58:16 PST	Vacation packages	Firefox
Evidence Location	Documents and Settings/Charlie/Local Settings/History/History.IE5/index.dat Documents and Settings/Charlie/Application Data/Mozilla/Firefox/Profiles/2usvf7i1.default/		

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

Possible Answer	Timestamp (Timezone is applied)	Search Keyword
		Not Found
Evidence Location	HKU/Software/Microsoft/Windows/CurrentVersion/Explorer/WordWheelQuery/ HKCU/Software/Microsoft/Search Assistant/ACMru	

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

Possible Answer	Mozilla Thunderbird 2.0
Evidence Location	C:/Program Files/Mozilla Thunderbird HKLM/SOFTWARE/Clients/Mail/Mozilla/shell/open/command HKLM/SOFTWARE/Clients/Mail/Mozilla Thunderbird

17) Where is the e-mail file located?

Possible Answer	C:/Users/Charlie/AppData/Thunderbird/Profiles/4zy34x9h.default/Mail/mail.m57.biz C:/Users/Charlie/AppData/Thunderbird/Profiles/4zy34x9h.default/Mail/mail.m57-1.biz /img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email
Evidence Location	C:/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/ /img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email

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

Possible Answer	charlie@m57.biz
Evidence Location	C:/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/ /img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email

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

(You can identify the following items: *Timestamp, From, To, Subject, Body, and Attachment*)

[Hint: just examine the OST file only.]

Possible Answer	Timestamp	E-Mail Communication	
		Source	[Inbox]

(Timezone is applied)	2009-11-16 11:02:37 PST	From → To	pat@m57.biz → charlie@m57.biz , jo@m57.biz , terry@m57.biz
		Subject	WELCOME TO THE COMPANY!
		Body	Dear Team, I am extremely excited to take this opportunity to welcome you all to the M57.biz family. It has been a dream of mine to open a business that provides an innovative service to companies, inventors, as well as investors. I look forward to all of your great work in your future assignments and I can't wait to get to know each of you a little more. Please feel free to send me any questions, concerns, or comments. Regards, Pat McGoo CEO, M57.biz pat@m57.biz 831-555-1234
	2009-11-16 13:26:16 PST	Source	[Sent]
		From → To	charlie@m57.biz → alix.pery@yahoo.com ; rubinfritz31@mail.com
		Subject	New email address
		Body	Hey everybody. I started working at the new company today. It's pretty slow going so far, we're just getting set up and figuring out where everything is. I got my new email set up, so you can send to me at this address. Charlie
	2009-11-17 10:30:59 PST	Source	[Inbox]
		From → To	pat@m57.biz → jo@m57.biz ; charlie@m57.biz
		Subject	Fw: M57.BIZ PRIOR ART INVESTIGATION SERVICES
		Body	----- Original Message ----- From: Alex Monroe To: Pat McGoo Sent: Tuesday, November 17, 2009 8:58 AM Subject: Re: M57.BIZ PRIOR ART INVESTIGATION SERVICES Dear Pat, Yes, we are very interested in using your prior art investigation services. Our R&D department is currently applying for patents in two key areas that we are counting on to gain market share over our major competitor, project2400.com . I am counting on you and

			<p>your firm to keep these research areas in strict confidentiality. We wouldn't want project2400 to know about our research interests.</p> <p>We will hire you to do prior art searches on these two areas:</p> <ul style="list-style-type: none"> ○ Time machines ○ Teleporters <p>Please send me a quote for these two investigations.</p> <p>Regards,</p> <p>Alex</p> <p>CEO - Nitroba.com</p> <p>On Nov 16, 2009, at 2:49 PM, Pat McGoo wrote:</p> <p>Alex,</p> <p>I enjoyed talking with you at the patent conference in San Francisco last week. I remember that you said that you would be interested in our prior art investigation services.</p> <p>If you are still interested in our services, then I can fax you over a service agreement right away. I hope to hear from you soon. Please do not hesistate to give me a call or email if you have any questions, concerns, or comments.</p> <p>Regards,</p> <p>Pat McGoo</p> <p>CEO, M57.biz</p> <p>pat@m57.biz</p> <p>831-555-1234</p>
	2009-11-17 10:33:39 PST	Source	[Inbox]
		From → To	pat@m57.biz → jo@m57.biz; charlie@m57.biz
		Subject	ASSIGNMENT OF NITROBA ACCOUNT
		Body	<p>Jo, Charlie:</p> <p>We have our first contract ! Nitroba wants us to do a prior art investigation in two key areas. Jo, you will be responsible for the teleporter patent search. Charlie, I want you to take the time machine patent search. This is our first real job, so let's make sure we do some quality research. Our reputation will depend on the time and effort that we put into this contract and on Nitroba's</p>

			<p>satisfaction with our results. Come by my office and we'll talk details.</p> <p>Pat</p>
2009-11-17 10:54:17 PST	Source	[Sent]	
	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>	
2009-11-18 09:29:57 PST	Source	[Inbox]	
	From → To	pat@m57.biz; → jo@m57.biz; charlie@m57.biz	
	Subject	Google patent	
	Body	<p>Jo, Charlie,</p> <p>I'm sure you already are using it, but check out google patent beta for searches... good stuff.</p> <p>Pat</p>	
2009-11-18 10:01:50 PST	Source	[Inbox]	
	From → To	jo@m57.biz → charlie@m57.biz	
	Subject	Re: What's wrong with Pat	
	Body	<p>yeah, he's weird. not sure what's wrong with him.</p> <p>----- Original Message ----- From: "Charlie" <charlie@m57.biz> To: <jo@m57.biz> Sent: Tuesday, November 17, 2009 10:54 AM Subject: What's wrong with Pat</p> <p>> Hey Jo, > > Don't you think Pat is a weird boss? I think there is something funny > about him. What do you think? > > Charlie</p>	
2009-11-18 12:53:59 PST	Source	[Sent]	
	From → To	charlie@m57.biz → pat@m57.biz	
	Subject	Re: Google patent	
	Body	<p>Pat McGoo wrote:</p> <p>> Jo, Charlie, > > I'm sure you already are using it, but check out google patent beta > for searches... good stuff. > > Pat Thanks! This looks like a great resource.</p>	

			Charlie
2009-11-18 12:59:55 PST	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com	
	Subject	Movie tonight???	
	Body	Wanna go see a flick tonight? I'll probably leave work at around 4:00pm. Pick you up at 5 for dinner first?	
		Charlie	
2009-11-19 09:42:11 PST	Source	[Inbox]	
	From → To	pat@m57.biz → terry@m57.biz ; jo@m57.biz ; charlie@m57.biz	
	Subject	ADDITIONAL GUIDANCE ON PATENT SEARCHING	
	Body	<p>Dear Team,</p> <p>please remember that if you want to do a full patent search, the USPTO ONLY has full text for patents issued from 1976 to the present. If we need to go back farther, you have to get the TIFF images for anything from 1790 on.</p> <p>Recently someone concluded there was no previous patent we were looking for (I won't name names!), having only searched from 1976 on, and luckily I caught it. Fiddlesticks by golly! But that's OK, we will continue to learn and get better !</p> <p>Pat</p>	
2009-11-20 09:57:49 PST	Source	[Inbox]	
	From → To	jo@m57.biz → charlie@m57.biz	
	Subject	Docs	
	Body	<p>Charlie,</p> <p>Here are some of those papers I was talking about the other day. They might help us in our searches. Let me know what you think.</p> <p>-Jo</p>	
2009-11-20 13:06:27 PST	Source	[Sent]	
	From → To	charlie@m57.biz → jo@m57.biz	
	Subject	Re: Docs	
	Body	<p>Jo Smith wrote:</p> <p>> Charlie,</p> <p>></p> <p>></p> <p>> Here are some of those papers I was talking about the other day. They</p> <p>> might help us in our searches. Let me know what you think.</p> <p>></p> <p>> -Jo</p> <p>Jo,</p>	

			<p>This is good stuff. Thanks for sending.....Just keep passing on stuff like this.</p> <p>Charlie</p>
2009-11-23 09:07:37 PST	Source	[Inbox]	
	From → To	pat@m57.biz → terry@m57.biz; charlie@m57.biz; jo@m57.biz	
	Subject	This week	
	Body	<p>Dear Team,</p> <p>we have a lot to accomplish this week, and it being a Holiday week we'll have to make sure we get the time in before Thursday if we want to take off for the Holiday. Let's plan on having an all people project status meeting tomorrow afternoon. By the end of the week I'd like to have something hard to start getting back to the customer.</p> <p>By the way, if anyone needs any good turkey recipes, let me know!</p> <p>Regards,</p> <p>Pat</p>	
2009-11-24 16:07:36 PST	Source	[Inbox]	
	From → To	pat@m57.biz → charlie@m57.biz; jo@m57.biz	
	Subject	New business	
	Body	<p>Charlie, Jo,</p> <p>great news - we got another contract. I need to have one (or both) of you start looking into quantum cryptography - anything and everything patented on the subject. If you get bored over the short vacation start having a look at it. This is with a new company, so let's impress them !</p> <p>Thanks</p> <p>Pat</p>	
2009-11-30 08:46:08 PST	Source	[Sent]	
	From → To	charlie@m57.biz → pat@m57.biz	
	Subject	Re: New business	
	Body	<p>Pat McGoo wrote:</p> <p>> Charlie, Jo,</p> <p>></p> <p>> great news - we got another contract. I need to have one (or both)</p> <p>> of you start looking into quantum cryptography - anything and</p> <p>> everything patented on the subject. If you get bored over the short</p> <p>> vacation start having a look at it. This is with a new company, so</p> <p>> let's impress them !</p> <p>></p>	

			> Thanks > Pat I'll start looking into this. Did everyone have a good weekend?
2009-11-30 08:54:27 PST	Source	[Inbox]	
	From → To	jo@m57.biz → charlie@m57.biz	
	Subject	teleporter	
	Body	Hey Charlie, Found this patent for teleportation. What do you think? - Jo	
2009-12-01 13:02:34 PST	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com	
	Subject	Pack your bags	
	Body	Alix, Pretty soon I'm going to be able to afford to take you on a nice vacation. Where would you want to go if you could name your destination? I'm getting a hot car too. Charlie	
2009-12-01 13:43:35 PST	Source	[Inbox]	
	From → To	alix.pery@yahoo.com → charlie@m57.biz	
	Subject	Re: Pack your bags	
	Body	Ooh! When will this happen?! I've always wanted to go on a Mediterranean cruise. Should I put a date on my calendar?	
			From: Charlie < charlie@m57.biz > To: Alix Pery < alix.pery@yahoo.com > Sent: Tue, December 1, 2009 1:02:34 PM Subject: Pack your bags Alix, Pretty soon I'm going to be able to afford to take you on a nice vacation. Where would you want to go if you could name your destination? I'm getting a hot car too. Charlie
2009-12-02 13:04:29 PST	Source	[Sent]	
	From → To	charlie@m57.biz → jamie@project2400.com	
	Subject	Interested?	
	Body	J, I have something that you'll definitely be interested in. It concerns your competitor. I'm doing a prior art search for them. Want to know what I've found? You know my price. I'll send you the goods after I	

			see half in my account. Make sure you delete this email. C
	2009-12-02 13:52:39 PST	Source	[Inbox]
		From → To	pat@m57.biz → charlie@m57.biz; jo@m57.biz
		Subject	New Project
		Body	Jo, Charlie, have you had a chance to start looking at that quantum cryptography project? I've found a few things so far - may be a harder nut to crack than I had originally thought. I want to wrap this one up before the end of the calendar year. One of you will need to take it, if not both, so let me know how your workload in going in general. Thanks Pat
	2009-12-03 08:51:14 PST	Source	[Inbox]
		From → To	jo@m57.biz → charlie@m57.biz;
		Subject	Re: New Project
		Body	Do you want this one? I was looking for that teleporter thing. - Jo ----- Original Message ----- From: Pat McGoo To: charlie@m57.biz ; jo@m57.biz Sent: Wednesday, December 02, 2009 1:52 PM Subject: New Project Jo, Charlie, have you had a chance to start looking at that quantum cryptography project? I've found a few things so far - may be a harder nut to crack than I had originally thought. I want to wrap this one up before the end of the calendar year. One of you will need to take it, if not both, so let me know how your workload in going in general. Thanks Pat
	2009-12-03 08:52:00 PST	Source	[Sent]
		From → To	charlie@m57.biz → pat@m57.biz
		Subject	Re: New Project
		Body	Pat McGoo wrote: > Jo, Charlie, >

			<p>> have you had a chance to start looking at that quantum</p> <p>> cryptography project? I've found a few things so far - may be a</p> <p>> harder nut to crack than I had originally thought.</p> <p>></p> <p>> I want to wrap this one up before the end of the calendar year.</p> <p>> One of you will need to take it, if not both, so let me know how your</p> <p>> workload in going in general.</p> <p>></p> <p>> Thanks</p> <p>> Pat</p> <p>I can start looking at it.</p> <p>Charlie</p>
2009-12-03 09:51:33 PST	Source	[Inbox]	
	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> <p>> J,</p> <p>></p> <p>> I have something that you'll definitely be interested in. It concerns</p> <p>> your competitor. I'm doing a prior art search for them. Want to know</p> <p>> what I've found? You know my price. I'll send you the goods after I</p> <p>> see half in my account. Make sure you delete this email.</p> <p>></p> <p>> C</p> <p>></p> <p>></p>	
2009-12-03 12:16:52 PST	Source	[Sent]	
	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>	
2009-12-03 13:02:33 PST	Source	[Sent]	
	From → To	charlie@m57.biz → alix.pery@yahoo.com	
	Subject	Re: Pack your bags	
	Body	Alix Pery wrote:	

			<p>> Ooh! When will this happen?! I've always wanted to go on a > Mediterranean cruise. Should I put a date on my calendar? > > ----- > ----- > *From:* Charlie <charlie@m57.biz> > *To:* Alix Pery <alix.pery@yahoo.com> > *Sent:* Tue, December 1, 2009 1:02:34 PM > *Subject:* Pack your bags > > Alix, > > Pretty soon I'm going to be able to afford to take you on a nice > vacation. Where would you want to go if you could name your > destination? I'm getting a hot car too. > > Charlie > I'll be seeing the money soon. How about we go over Christmas?</p>
	2009-12-03 13:16:14 PST	Source	[Sent]
		From → To	charlie@m57.biz → alix.pery@yahoo.com
		Subject	What do you think?
		Body	Alix - How do you like this car? Pretty sweet, huh! http://autos.yahoo.com/2010_ford_shelby_gt500/
	2009-12-04 09:22:27 PST	Source	[Inbox]
		From → To	terry@m57.biz → pat@m57.biz
		Subject	Re: Anti-virus
		Body	<p>Pat & Everyone Else,</p> <p>I need to change a setting on the anti-virus software. I will do that on Monday. You should all be safe and secure till Tuesday.</p> <p>Thanks, Terry</p> <p>----- Original Message ----- From: Pat McGoo To: terry@m57.biz Sent: Friday, December 04, 2009 9:14 AM Subject: Anti-virus</p> <p>Terry,</p> <p>is the anti-virus working? I think there is something wrong with mine...</p> <p>Pat</p>
	2009-12-04 09:41:47 PST	Source	[Sent]
		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.</p> <p>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>
	2009-12-04 13:06:23 PST	Source	[Sent]
		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>
	2009-12-07 11:44:18 PST	Source	[Sent]
		From → To	charlie@m57.biz → andy@swexpert.com
		Subject	Picture
		Body	<p>Andy,</p> <p>Here's the picture I promised... Make sure you delete this.</p> <p>C</p>
	2009-12-08 12:59:53 PST	Source	[Sent]
		From → To	charlie@m57.biz → pat@m57.biz
		Subject	Vacation time
		Body	<p>Hey boss,</p> <p>I'm planning a little vacation with a friend, so I was wondering about when would be a good time to take 2 weeks off? I was thinking of just extending my Christmas holiday a little bit. Are you OK with that?</p> <p>Charlie</p>
		Source	[Sent]

	2009-12-08 14:18:17 PST	From → To	charlie@m57.biz → rubinfritz31@mail.com
		Subject	Hey
		Body	Rub, You want to come test drive some cars with me later? I'm going to the ferrari dealer first, but I think I'm going with the Shelby. Charlie
	2009-12-10 09:37:52 PST	Source	[Inbox]
		From → To	rubinfritz31@mail.com → charlie@m57.biz
		Subject	When's it coming?
		Body	Charlie So when does the new car arrive? That sucks that the dealer didn't have the one you wanted in stock. I hope it isn't too long of a wait. Rub
	2009-12-10 14:18:21 PST	Source	[Sent]
		From → To	charlie@m57.biz → rubinfritz31@mail.com
		Subject	Re: When's it coming?
		Body	They said it should take about two weeks. Can't wait to take it for a ride. rubinfritz31@mail.com wrote: > Charlie > So when does the new car arrive? That sucks that the dealer didn't > have the one you wanted in stock. I hope it isn't too long of a wait. > > Rub
	2009-12-11 08:55:53 PST	Source	[Inbox]
		From → To	pat@m57.biz → terry@m57.biz ; jo@m57.biz ; charlie@m57.biz
		Subject	Important Meeting
		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
Evidence Location	C:/Documents and Settings/Charlie/Application Data/Thunderbird/Profiles/4zy34x9h.default/ /img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email		

20) List external storage devices attached to PC.

Possible Answer	Device Name	Volume Name (GUID)	Serial No.	First Connected Time	First Connected Time After Reboot
	Kingston DataTraveler 2.0 USB Device	fd7018a2-d5f8-11de-a023-000bdb4f6b10	2007110203195377	2009-11-20 09:20:21 PST	2009-12-11 12:26:02 PST
	LaCie Rugged FW/USB USB Device		00D04B881007C255	2009-11-16 16:25:20 PST	2009-11-17 2:25:20 PST
	Sandisk Cruzer USB Device	ee9b4db1-d3aa-11de-a020-000bdb4f6b10	43175107A4C24AD4	2009-11-17 13:09:09 PST	2009-11-17 23:09:18 PST
	USB 2.0 Flash Disk USB Device	ee9b4db0-d3aa-11de-a020-000bdb4f6b10	51491E64	2009-11-17 10:56:33 PST	2009-11-17 20:56:50 PST
Evidence Location	HKLM/SYSTEM/MountedDevices/ HKLM/SYSTEM/ControlSet###/Enum/USBSTOR/ HKLM/SYSTEM/CurrentControlSet/Enum/USB/ HKLM/SYSTEM/ControlSet###/Control/DeviceClasses/{a5dcbf10-6530-11d2-901f-00c04fb951ed}/ HKEY_LOCAL_MACHINE/SYSTEM/ControlSet###/Control/DeviceClasses/{53f5630d-b6bf-11d0-94f2-00a0c91efb8b} C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2 C:/Windows/setupapi.log				

21) Identify all traces related to 'renaming' of files in Windows Desktop.

(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)

[Hint: the parent directories of renamed files were deleted and their MFT entries were also overwritten. Therefore, you may not be able to find their full paths.]

Possible Answer	Timestamp	USN	Path (Of course, just file names are OK)	Event
(Timezone is applied)				Renamed Old
				Renamed New
Evidence Location	- NTFS journal file analysis (→ \$UsnJrnl) -/\$Extend/\$UsnJrnl:\$J (+ \$MFT for identifying full paths of files) - With NTFS journal file only, it may be hard to find full paths. - You can consider the Registry ShellBags for further information. - You can also consider the Windows Search database. (See Questions 46)			

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

Possible Answer	RemotePath://192.168.1.1/m57/ram UserName: m57admin
Evidence Location	C:/Documents and Settings/Charlie/NTUSER.DAT/Network/Z/RemotePath C:/Documents and Settings/Charlie/NTUSER.DAT/Network/Z/UserName

23) List all directories that were traversed in USB.

Possible Answer	Timestamp	Directory Path	Source
	2009-11-17 10:57:11 PST	F:/	Recent
	2009-11-20 09:38:09 PST???	F:/Email	Recent
	2009-12-10 14:28:05 PST	F:/Email/other	Recent
Evidence Location	C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/Shell/BagMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/Shell/Bags C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/ShellNoRoam/BagMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/ShellNoRoam/Bags C:/Documents and Settings/Charlie/Recent		

24) List all files that were opened in USB.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	2009-12-04 13:39:45 PS	F:/Email/Charlie_2009-11-20_0957_99202.ComplexityTheory.Louisa+Fleet.pdf	Recent
	2009-12-04 13:42:26 PST	F:/Email/Charlie_2009-11-30_0854_Received_US5041044.pdf	Recent
	2009-12-04 13:41:17	F:/Email/Charlie_2009-11-20_1055_Received_PETEFS.pdf	Recent

	PST		
	2009-11-24 13:56:35 PST	F:/microscope.jpg	Recent
	2009-11-24 14:05:29 PS	F:/Copy of microscope.jpg	Recent
	2009-12-10 14:29:37 PST	F:/Email/other/Picture_a1.jpg	Recent
	2009-12-10 14:28:05 PST	F:/Email/other/QC Project.eml	Recent
	2009-12-10 14:28:05 PST	F:/Email/other/Picture.eml	Recent
	2009-12-04 13:40:35 PST	F:/Email/Charlie_2009-11-20_0957_Received_98521.WANs.Greg+Hillier.pdf	Recent
	2009-12-04 13:40:28 PST	F:/Email/Charlie_2009-11-20_0957_Received_97315.ScatterGatherIO.Julio+Molock.pdf	Recent
	2009-11-17 10:57:11 PST	F:/M57biz.jpg	Recent
	2009-12-04 13:40:21 PST	F:/Email/Charlie_2009-11-20_0957_Received_95253.SCSI.Mathew+Malizia.pdf	Recent
	Evidence Location	C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/Shell/BagMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/Shell/Bags C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/ShellNoRoam/BagMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/ShellNoRoam/Bags	

	C:/Documents and Settings/Charlie/Recent
--	--

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

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	-	Desktop/My Computer/Z:/	Shell bags (Access)
	2009-12-11 06:55:38 PST	Desktop/My Computer/Z:/windd	Shell bags (Access)
	2009-12-11 06:55:38 PST	Desktop/My Computer/Z:/windd/32bits_i386	Shell bags (Access)
Evidence Location	C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/LastVisitedMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU C:/Documents and Settings/Charlie/NTUSER.DAT/Software/Microsoft/Windows/ShellNoRoam/BagMRU		

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

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)		Not files were opened	
Evidence Location	- Z: is mapped on//192.168.1.1		

29) Find traces related to cloud services on PC.

(Service name, log files...)

Possible Answer	Cloud Service	Type	Traces
		File/Dir	Not found
Evidence Location	C:/Program Files/		

30) *What files were deleted from Google Drive?*

Find the filename and modified timestamp of the file.

[Hint: Find a transaction log file of Google Drive.]

Possible Answer (Timezone is applied)	Timestamp	File name	Modified Time
		Not found	
Evidence Location	C:/Program Files/Google/Drive HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Installer/Folders/ HKLM/SOFTWARE/Google/Drive HKCU/NTUSER/Software/Microsoft/Windows/CurrentVersion/Run/GoogleDriveSync HKCU/NTUSER/Software/Classes		

43) *What kinds of data were stored in Windows Search database?*

Possible Answer	Not found
Evidence Location	HKCU/Software/Microsoft/Search Assistant/ACMr C:/ProgramData/Microsoft/Search/Data/Applications/Windows/Windows.edb

Παράρτημα Δ – Φόρμες καταγραφής

Φόρμα στοιχείων σκληρού δίσκου

Τεχνικές Προδιαγραφές Σκληρού δίσκου			
Case ID	C007		
Κατασκευαστής	Maxtor (51024H2)		
S/N	8db75e97-919c-4bd4-afe5-7203ebc11549 324b48315441434c2020202020202020202020202020202020		
Κύλινδροι	19,852		
Κεφαλές	16		
Δίσκοι	1		
Χωρητικότητα	10239860736 Bytes (10.2 GB)		
Λεπτομέρειες κατάσχεσης σκληρού δίσκου			
Ήταν προσαρτημένος ο δίσκος;		<input type="checkbox"/> OXI	<input checked="" type="checkbox"/> NAI
Ήταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;		<input type="checkbox"/> OXI	<input checked="" type="checkbox"/> NAI
Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε; TODO			
Ήταν ο δίσκος προστατευμένος με κωδικό πρόσβασης;		<input checked="" type="checkbox"/> OXI	<input type="checkbox"/> NAI
Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι;			
Δημιουργία αντιγράφου			
Εφαρμογή δημιουργίας αντιγράφου	AccessData FTK Imager	Έκδοση	3.0
Τόπος λήψης πιστού αντιγράφου		M57.biz Open-Space Office	
Ημερομηνία λήψης πιστού αντιγράφου		Wed Jan 12 20:49:15 2011	

Hashes		MD5: 0377b3d41bbbc295a1c9f00aa07ee17	
Εγκληματολόγος ερευνητής που έκανε την κατάσχεση			
Όνοματεπώνυμο	Αργυρόπουλος Χρήστος	Τίτλος	Ερευνητής / Αναλυτής
Τηλέφωνο	6942069420	Τμήμα	DF01
Υπογραφή	XA	Ημ/νια	Wed Jan 12 2011
Σχόλια	https://www.seagate.com/staticfiles/maxtor/en_us/documentation/quick_specs/diamondmax_plus_40_ultra_ata_100_quick_specs.pdf https://www.seagate.com/staticfiles/maxtor/en_us/documentation/manuals/dm_plus_40_ultra_ata_100_manual.pdf		

Φόρμα στοιχείων USB

Τεχνικές Προδιαγραφές USB			
Case ID	C007		
Κατασκευαστής	Kingston		
S/N	2007110203195377		
Κύλινδροι	-		
Κεφαλές	-		
Δίσκοι	-		
Χωρητικότητα	1059061760 Bytes (1.05 GB)		
Λεπτομέρειες κατάσχεσης USB			
Ήταν προσαρτημένο το USB;		<input checked="" type="checkbox"/> OXI	<input type="checkbox"/> NAI
Ήταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;		<input checked="" type="checkbox"/> OXI	<input type="checkbox"/> NAI
Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε;			
TODO			
Ήταν το USB προστατευμένο με κωδικό πρόσβασης;		<input checked="" type="checkbox"/> OXI	<input type="checkbox"/> NAI
Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι;			
Δημιουργία αντιγράφου			
Εφαρμογή δημιουργίας αντιγράφου	AccessData FTK Imager	Έκδοση	3.0
Τόπος λήψης πιστού αντιγράφου		M57.biz Open-Space Office	
Ημερομηνία λήψης πιστού αντιγράφου		Wed Jan 19 09:09:08 2011	
Hashes		MD5: 9c0de6c8532d7a66ddcf01861dfb6535	
Εγκληματολόγος ερευνητής που έκανε την κατάσχεση			
Όνοματεπώνυμο	Αργυρόπουλος Χρήστος	Τίτλος	Ερευνητής / Αναλυτής
Τηλέφωνο	6942069420	Τμήμα	DF01
Υπογραφή	XA	Ημ/νια	Wed Jan 19 2011

Σχόλια	
---------------	--

Παράρτημα Ε – Φόρμες κατάσχεσης

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: C007

Offense: Blackmailing & Industrial Espionage

Submitting Officer: (Name/ID#): Christos Argyropoulos (001)

Victim: M57

Suspect: Charlie

Date/Time Seized: Wed Jan 12 2011

Location of Seizure: Open Space M57 HQ, 1st Floor

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
0001	1	Dell Laptop (Dell Studio 15, 3007110203195377, Excellent Condition, No Marks, No Scratches)
0002	1	Usb Flash (Kingston DataTraveler 2.0, 2007110203195377, Excellent Condition, No Marks, No Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
0001	Wed Jan 12 20:49:15 2011	Pat McGoo (PM)	Christos Argyropoulos (CA)	Open Space M57 HQ
0002	Wed Jan 19 09:09:08 2011	Pat McGoo (PM)	Christos Argyropoulos (CA)	Open Space M57 HQ
0001	Wed Jan 12 2011	Christos Argyropoulos (CA)	Dourachalis Philip (DP)	AUEB InfoSec Ltd LAB
0002	Wed Jan 19 2011	Christos Argyropoulos (CA)	Dourachalis Philip (DP)	AUEB InfoSec Ltd LAB
0001	Wed Jan 22 2011	Dourachalis Philip (DP)	Christos Argyropoulos (CA)	AUEB InfoSec Ltd LAB
0002	Wed Jan 29 2011	Dourachalis Philip (DP)	Christos Argyropoulos (CA)	AUEB InfoSec Ltd LAB
0001	Wed Jan 22 2011	Christos Argyropoulos (CA)	Pat McGoo (PM)	Open Space M57 HQ
0002	Wed Jan 29 2011	Christos Argyropoulos (CA)	Pat McGoo (PM)	Open Space M57 HQ

Παράρτημα ΣΤ – Εξοπλισμός εργαστηρίου

Εξοπλισμός Forensics (Jump Bag)

Serial Numbers	Name
8T7B0D6X9Y, 4J9H2K5L7Q, 2D6F8G0M1N, 7P3R9S5T2W	x4 SanDisk USB stick 32GB (Caine, FTK Imager, FEX Imager, Volatility, MDD, DumpIt)
4U6V8W0X2Y, 1Z3A5B7C9D	x2 Samsung Portable SSD T7 USB 3.2 2.5"
6E8F0G2H4I	G319 Signal Detector Anti-eavesdropping GPS Anti-Location Scanner
3J5K7L9M1N	Sony Mirrorless Φωτογραφική Μηχανή ZV-E10 Crop Frame Kit (E PZ 16-50mm F3.5-5.6 OSS) Black
8O0P2Q4R6S	MSI Titan GT77HX 13VI-048PL 17.3" IPS UHD 144Hz (i9-13980HX/64GB/2TB SSD + 2TB SSD/GeForce RTX 4090/W11 Home) Core Black (US Keyboard)
-	Total THKTHP21476 Βαλίτσα με 147 Εργαλεία
-	Sawtooth EVIDENCE Tape
5T7U9V1W3X	Panasonic Βιντεοκάμερα Full HD (1080p) @ 50fps HC-V380 Αισθητήρας CMOS Αποθήκευση σε Κάρτα Μνήμης με Οθόνη Αφής 3" και HDMI / WiFi / USB 2.0
-	Walfront 100Pcs/Lot Anti Static Zip Lock Bags, ESD Shielding Static-Free Plastic Storage Bag for Electronic
1E5V7W9B3M	Veger Tank Lite Power Bank 50000mAh 20W (#1E5V7W9B3M)
-	Petzl Επαναφορτιζόμενος Φακός Κεφαλής Αδιάβροχος IP67 με Μέγιστη Φωτεινότητα 2800lm
5F7G9H1I3J	Ugreen CR113 USB 3.0 Hub (#5F7G9H1I3J)

Παράρτημα Ζ – Γλωσσάρι

- **Dynamic Host Configuration Protocol (DHCP):** Ένα σύνολο κανόνων που χρησιμοποιούνται από συσκευές επικοινωνιών, όπως υπολογιστές, δρομολογητές, ή προσαρμογείς δικτύου οι οποίοι επιτρέπουν στη συσκευή να ζητά και να λαμβάνει μια διεύθυνση IP από έναν διακομιστή που διαθέτει έναν κατάλογο διευθύνσεων.
- **IP:** Είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard για τη μεταξύ τους αναγνώριση και επικοινωνία.
- **Digital Evidence:** Πληροφορίες αποθηκευμένες σε δυαδική μορφή οι οποίες μπορούν να επικαλεστούν στο δικαστήριο.
- **Hash value:** Είναι μια αλφαριθμητική τιμή σταθερού μήκους που ταυτοποιεί μοναδικά τα δεδομένα.
- **Pacific Standard Time (PST):** Είναι μια κανονική ζώνη ώρας που χρησιμοποιείται από την πρώτη Κυριακή του Νοεμβρίου έως τη δεύτερη Κυριακή του Μαρτίου, όταν δεν ισχύει η θερινή ώρα
- **Browsers:** Ένας περιηγητής web ή φυλλομετρητής web είναι λογισμικό που επιτρέπει στον χρήστη του να προβάλλει και να αλληλεπιδρά με κείμενα, εικόνες, βίντεο, μουσική, παιχνίδια και άλλες πληροφορίες συνήθως αναρτημένες σε μια ιστοσελίδα ενός ιστότοπου στον Παγκόσμιο Ιστό ή σε ένα τοπικό δίκτυο.
- **URL:** Είναι η διεύθυνση ενός αρχείου ή μίας ιστοσελίδας μέσα στο Internet.
- **Live acquisition:** Στην ψηφιακή εγκληματολογία αναφέρεται στη διαδικασία συλλογής και διατήρησης volatile δεδομένων από ένα εν λειτουργία υπολογιστή ή ψηφιακή συσκευή.
- **Volatile:** Αναφέρεται στις πληροφορίες που βρίσκονται στην πτητική μνήμη (RAM) ή στον προσωρινό αποθηκευτικό χώρο ενός υπολογιστή και χάνονται όταν το σύστημα απενεργοποιείται ή επανεκκινείται.