

Έκθεση Συμπερασμάτων Υπόθεσης 001/AUEB

Expert Witness: Αλέξανδρος Καρράς

Technical Witness 1: Ελένη Τράμπαρη-Λάρδα

Technical Witness 2: Ιωάννης Σομός

Πίνακας Περιεχομένων

1. Εισαγωγή	3
2. Προετοιμασία.....	3
2.1 Προετοιμασία ενταλμάτων και εξουσιοδοτήσεων	3
2.2 Εξασφάλιση Εργαλείων και Τεχνικών	4
2.3 Καθορισμός Αρμοδιοτήτων	4
2.4 Σχεδιασμός Διαδικασίας και Έρευνας	4
3. Ανίχνευση & Εντοπισμός	4
3.1 Αποκλεισμός Σκηής η-Εγκλήματος	4
3.2 Καταγραφή Παρόντων στο Χώρο	5
3.3 Συνεντεύξεις.....	5
3.4 Φωτογράφιση Χώρου.....	5
3.5 Καταγραφή Πηγών Πειστηρίων.....	6
3.6 Φωτογράφιση Ενεργών Προγραμμάτων	7
3.7 Έλεγχος Δικτυακών Συνδέσεων.....	8
3.8 Καταγραφή Ειδικών Φορμών	8
4. Διαφύλαξη.....	8
4.1. Διαφύλαξη Μνήμης Πειστηρίου Laptop.....	8
4.2 Διαφύλαξη Δίσκου Πειστηρίου Laptop	9
4.3 Διαφύλαξη Πειστηρίου USB.....	9
4.4 Προετοιμασία και Μεταφορά Πειστηρίων στο Εργαστήριο	9
5. Ανάλυση.....	9
5.1 Ανάλυση Μνήμης Πειστηρίου Laptop.....	9
5.2 Ανάλυση Δίσκου Πειστηρίου Laptop	10
5.3 Ανάλυση Δίσκου Πειστηρίου USB.....	14
6. Παρουσίαση	15
Παράρτημα Α - RACI Matrix	18
Παράρτημα Β - Συνεντεύξεις.....	20
Παράρτημα Γ - Φόρμες κατάσχεσης, καταγραφής.....	24
Παράρτημα Δ - Πληροφορίες δίσκου & USB	27
Παράρτημα Ε - Ανάλυση δίσκου & USB.....	58
Παράρτημα ΣΤ - Αντίγραφο μνήμης	62
Παράρτημα Ζ - Screenshots forensics εργασιών ΑΕΓ	63

1. Εισαγωγή

Η ομάδα ΑΕΓ της εταιρίας Criminal Forensics Investigators έλαβε την ανάθεση έργου από την εταιρία M57.biz για την διερεύνηση ενός ηλεκτρονικού εγκλήματος το οποίο διαπράχθηκε (ή υπάρχει η υποψία ότι διαπράχθηκε) στην έδρα της τελευταίας την 11/12/2009 και ώρα 09:00.

Από την ανάθεση εξήχθησαν τα ακόλουθα: Πιθανή σκηνή του η-εγκλήματος το δεξί γωνιακό γραφείο στον 1ο όροφο των γραφείων της εταιρίας στο Monterey. Πιθανός δράστης η-εγκλήματος ο κύριος Jo Smith. Πιθανά μέσα η-εγκλήματος: 1) Εταιρικό Laptop (ενεργό), 2) USB flash drive (κατοχή υπό εξέταση). Ο χώρος παρακολουθείται από Access Card System. Παρόντες στη σκηνή του πιθανού η-εγκλήματος, ο Υπεύθυνος Ασφαλείας, ο IT Admin (κ. Terry Johnson) και ο Πιθανός Δράστης (κ. Jo Smith).

Η ομάδα ΑΕΓ έφτασε στον τόπο του πιθανού εγκλήματος την 11/12/2009 και ώρα 11:00.

2. Προετοιμασία

Η ομάδα ΑΕΓ είχε στη διάθεση της να προετοιμαστεί προ της άφιξής της στη σκηνή του πιθανού η-εγκλήματος. Αποφασίστηκε ότι ο κ. Καρράς θα έχει το ρόλο του Expert Witness αναλαμβάνοντας την ευθύνη του έργου και της ομάδας, η κ. Τράμπαρη-Λαρδα το ρόλο του Technical Witness 1 αναλαμβάνοντας τον αποκλεισμό της σκηνής του η-εγκλήματος, τη φωτογράφιση του χώρου και τη διασφάλιση του laptop και ο κ. Σομός το ρόλο του Technical Witness 2 αναλαμβάνοντας τις συνεντεύξεις των παρόντων στο χώρο, τη κατάσταση των πηγών πειστηρίων και τη διαφύλαξη του USB.

2.1 Προετοιμασία ενταλμάτων και εξουσιοδοτήσεων

Μας έχει δοθεί γραπτή εξουσιοδότηση από την εταιρία για την έρευνα του πιθανού η-εγκλήματος. Το laptop ως εταιρικό και με βάση τη πολιτική της εταιρίας μπορούσε να κατασχεθεί χωρίς να χρειαστεί άδεια από τον κ. Smith.

2.2 Εξασφάλιση Εργαλείων και Τεχνικών

Τα εργαλεία που χρησιμοποιήθηκαν για την συλλογή και ανάλυση των ψηφιακών πειστηρίων ήταν τα παρακάτω:

Εργαλείο	Έκδοση	Λειτουργία
FTK Imager	4.7.1.2	Αντίγραφο της μνήμης
Registry Viewer	2.0.0.7	Ανάλυση της registry
Autopsy	4.20.0	Ανάλυση του δίσκου
Volatility	2.6	Ανάλυση της μνήμης
NTFS Log Tracker	1.71	Ανάλυση του file system journal
undbx	0.21	Εξαγωγή των email
Digital Invisible Ink Toolkit	1.5	Στεγανάλυση αρχείων
TrueCrypt	7.2	Αποκρυπτογράφηση αρχείων

2.3 Καθορισμός Αρμοδιοτήτων

Για τον καθορισμό των αρμοδιοτήτων της ομάδας είναι υπεύθυνος ο Expert Witness (κ. Καρράς) και αναλύονται στο [Παράρτημα Α - RACI Matrix](#).

2.4 Σχεδιασμός Διαδικασίας και Έρευνας

Για το σχεδιασμό διαδικασίας και έρευνας είναι υπεύθυνος ο Expert Witness (κ. Καρράς) ο οποίος συντονίζει την ομάδα του με τέτοιο τρόπο ώστε να συλλεχθούν όσο περισσότερες αποδείξεις στον ελάχιστο δυνατό χρόνο.

3. Ανίχνευση & Εντοπισμός

Μετά την άφιξη στο χώρο εντοπίζουμε όλες τα δυνατές πηγές ψηφιακών πειστηρίων, αφού έχουμε διασφαλίσει ότι η σκηνή του η-εγκλήματος έχει απομονωθεί.

3.1 Αποκλεισμός Σκηνής η-Εγκλήματος

Στις 11:00 με την άφιξή μας στο χώρο της πιθανής τέλεσης η-εγκλήματος, ενημερώσαμε τους παρευρισκόμενους: τον Υπεύθυνο Ασφαλείας, τον IT Admin και τον πιθανό δράστη κ. Smith, πως ο χώρος περίξ του γραφείο προς διερεύνηση θα παραμείνει off-limits μέχρι το πέρας των ενεργειών μας.

3.2 Καταγραφή Παρόντων στο Χώρο

Στις 11:05 ο Technical Witness 2 κατέγραψε τους παρευρισκόμενους στο χώρο τέλεσης του πιθανού η-εγκλήματος και τους ενημέρωσε πως θα γίνουν ορισμένες ερωτήσεις σχετικά με το περιστατικό. Αυτοί ήταν:

- Υπεύθυνος Ασφαλείας,
- IT Admin
- Πιθανός Δράστης

Αφού του υποδείχθηκε σχετικός χώρος πλησίον του γραφείου, ενημέρωσε τους ανωτέρω πως θα εισέλθουν μεμονωμένα και ύστερα από δική του έκκληση.

3.3 Συνεντεύξεις

Στις 11:10 ξεκίνησε η συνέντευξη με τον Υπεύθυνο Ασφαλείας.

Στις 11:35 ξεκίνησε η συνέντευξη με τον IT Admin.

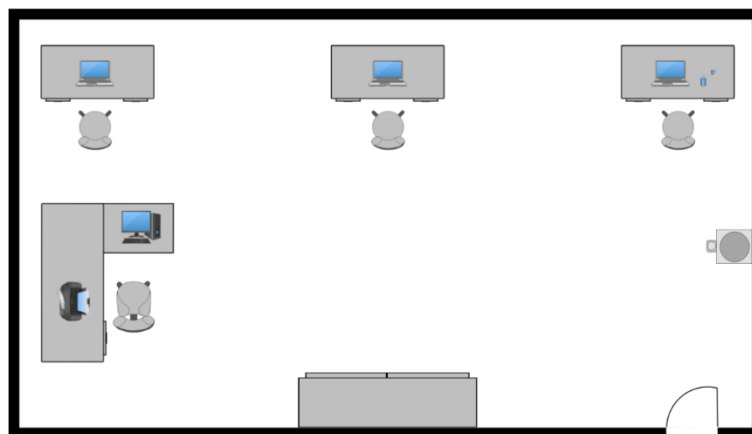
Στις 12:00 ξεκίνησε η συνέντευξη με τον Πιθανό Δράστη.

Οι ερωτήσεις και οι αντίστοιχες απαντήσεις παρουσιάζονται στο [Παράρτημα Β - Συνεντεύξεις](#).

3.4 Φωτογράφιση Χώρου

Στις 11:30 ξεκίνησε η καταγραφή του χώρου στον οποίο βρίσκονται 5 γραφεία “open-space”. Το γραφείο στη δεξιά γωνία ανήκει στον πιθανό δράστη (κ. Smith). Πάνω στο γραφείο του βρέθηκε ένα ενεργοποιημένο Laptop μάρκας Dell και δεξιά σε αυτό ένα USB χωρητικότητας 256MB.

Στις 11:35 ο Technical Witness 1 κατέγραψε με σχεδιάγραμμα και φωτογραφίες τον χώρο και τα πειστήρια.



3.5 Καταγραφή Πηγών Πειστηρίων

Στις 11:35 ο Technical Witness 2 ανέλαβε την καταγραφή πειστηρίων. Όσον αφορά το laptop, αφού αντιλήφθηκε ότι είναι ενεργοποιημένο, κουνηθεί το ποντίκι ώστε να ανοίξει η οθόνη (ακολουθώντας τις οδηγίες του ACPO) και φωτογραφήθηκε το περιεχόμενο της ανοιχτής οθόνης του.

Το USB που βρέθηκε στο γραφείο του πιθανού δράστη κατασχέθηκε για ανάλυση.

Φωτογραφίες από τα πειστήρια που βρέθηκαν στο γραφείο του Jo Smith:



¹ Laptop Dell - ενεργοποιημένο πάνω στο γραφείο του υπόπτου



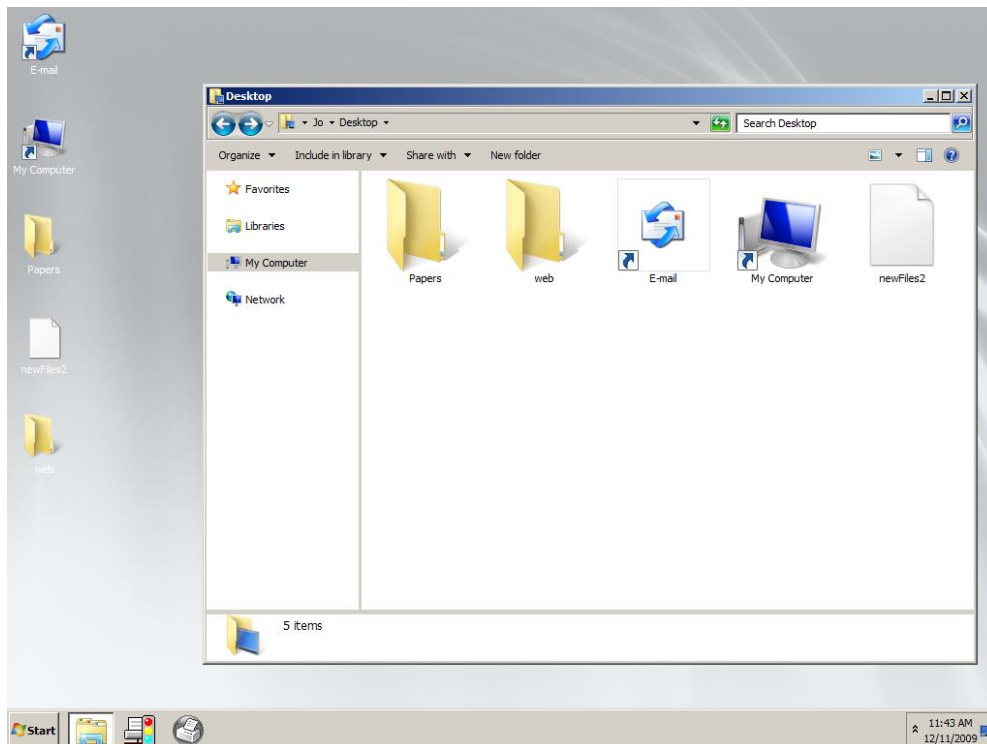
² Ο σκληρός δίσκος του laptop - αφαιρέθηκε μετά από την κατάλληλη διαδικασία ανάλυσης του laptop



3 USB - βρέθηκε στο γραφείο του υπόπτου δίπλα στο laptop του

3.6 Φωτογράφιση Ενεργών Προγραμμάτων

Στις 11:43 ο Technical Witness 1 φωτογράφησε την ανοιχτή οθόνη ώστε να φαίνονται τα ενεργά προγράμματα που είχε αφήσει ο κ. Smith.



Τα προγράμματα που ήταν ενεργά ήταν τα εξής:

Διεργασία	PID	Περιγραφή
explorer.exe	1324	Windows Explorer
BrStsWnd.exe	2772	Brother Printer Status
BRNIPMON.exe	3280	Brother IP Monitor

3.7 Έλεγχος Δικτυακών Συνδέσεων

Στις 11:48 έγινε έλεγχος των δικτυακών συνδέσεων μέσω του εργαλείου volatility από τον Technical Witness 1.

Τρέχοντας το plugin *connscan* εμφανίστηκαν δύο συνδέσεις στο τοπικό δίκτυο και μία σε εξωτερικό. Τρέχοντας το plugin *psslist* βρήκαμε τις διεργασίες processes στα οποία αντιστοιχούν. Δεν φαίνεται να υπάρχει κάποια ύποπτη σύνδεση.

Τοπική Διεύθυνση	Απομακρυσμένη Διεύθυνση	PID	Διεργασία	Πρωτόκολλο
192.168.1.106:1026	129.6.15.28:37	2040	AVGIDSAgent.exe	Time
192.168.1.106:1185	192.168.1.1:139	4	System	Samba
192.168.1.106:1184	192.168.1.1:445	4	System	Samba

3.8 Καταγραφή Ειδικών Φορμών

Στις 12:00 συμπληρώθηκαν οι φόρμες κατάσχεσης σκληρού δίσκου των ψηφιακών πειστηρίων (σκληρός δίσκος laptop και USB) βρίσκονται στο [Παράρτημα Γ - Φόρμες κατάσχεσης, καταγραφής](#), για τις οποίες είναι υπεύθυνοι οι Technical Witnesses.

4. Διαφύλαξη

Ο Expert Witness αποφάσισε να ληφθεί το πιστό αντίγραφο του laptop επί τόπου, καθώς μπορεί να χαθούν σημαντικά δεδομένα αν απενεργοποιηθεί. Το στάδιο της διαφύλαξης διήρκησε από της 12:10 έως της 12:30.

4.1. Διαφύλαξη Μνήμης Πειστηρίου Laptop

Καθώς το laptop ήταν ενεργοποιημένο έπρεπε να ακολουθήσουμε το ACPO Guidelines.

Ο Technical Witness 1 ακολούθησε τις παρακάτω κινήσεις:

1. Φωτογράφηση της σκηνής.
2. Επειδή στην οθόνη παρουσιάστηκε screen saver, αποφασίστηκε από τον Expert Witness να κουνηθεί το ποντίκι.
3. Φωτογραφήθηκε το περιεχόμενο της οθόνης.
4. Παρατηρήσαμε και σημειώσαμε τα processes που έτρεχαν εκείνη τη στιγμή και τα παράθυρα που ήταν ανοιχτά.
5. Πήραμε πιστό αντίγραφο της μνήμης του laptop με το εργαλείο FTK Imager που φαίνονται με λεπτομέρεια στο [Παράρτημα ΣΤ - Αντίγραφο μνήμης](#).

6. Αφαιρέσαμε το καλώδιο της παροχής ηλεκτρικού ρεύματος από το κομμάτι της που είναι συνδεδεμένο στην πρίζα (και όχι από τη θύρα του laptop).
7. Αφού το αφήσαμε να κρυώσει, τοποθετήσαμε labels και ξεκινήσαμε τη διαδικασία της ασφαλούς μετακίνησής του.

4.2 Διαφύλαξη Δίσκου Πειστηρίου Laptop

Ο Technical Witness 1 χρειάστηκε να ξεβιδώσει το laptop ώστε να απομονώσει το δίσκο του και έπειτα τον τοποθέτησε σε αντιστατική σακούλα ώστε να προστατευτεί από μαγνητικά πεδία και τον τοποθέτησε σε αεριζόμενες πλαστικές σακούλες.

4.3 Διαφύλαξη Πειστηρίου USB

Ο Technical Witness 2 τοποθέτησε το USB σε αντιστατική σακούλα ώστε να προστατευτεί από μαγνητικά πεδία, με προσοχή για να μην λυγίσει. Στο εργαστήριο λήφθηκε το αντίγραφο του με το εργαλείο FTK Imager.

4.4 Προετοιμασία και Μεταφορά Πειστηρίων στο Εργαστήριο

Αφού ο Expert Witness διασφάλισε την ακεραιότητα των ψηφιακών πειστηρίων μας και την τοποθέτησή τους σε κατάλληλες σακούλες, τα μετακίνησε στο εργαστήριο.

5. Ανάλυση

Στο εργαστήριο έγινε η ανάλυση της μνήμης από τον Expert Witness με το εργαλείο Volatility και ανάλυση του δίσκου ηλεκτρονικού υπολογιστή και USB flash drive με το εργαλείο Autopsy.

5.1 Ανάλυση Μνήμης Πειστηρίου Laptop

Αρχικά, αξιοποιήσαμε το plugin *imageinfo* για να λάβουμε πληροφορίες σχετικές με το αντίγραφο. Σύμφωνα με τις πληροφορίες που βρήκαμε, προσθέσαμε τις παραμέτρους `--profile=winXPSP3x86` και `--kdbg=0x8054cde0` για τα υπόλοιπα plugins. Στη συνέχεια, χρησιμοποιήσαμε τα plugins *connscan* (για την ανίχνευση των δικτυακών συνδέσεων), *filescan* (για την εύρεση των ανοιχτών αρχείων), *hashdump* (για την εμφάνιση των χρηστών και των LM & NT hashes τους), *hivelist* (για την εμφάνιση των registry hives), *hivedump* (για την εμφάνιση των περιεχομένων των registry hives), *printkey* (για την εμφάνιση

συγκεκριμένων registry keys), *shellbags* (για την ανάλυση των ShellBags), *windows* (για την εύρεση των ανοιχτών παραθύρων).

- Στις δικτυακές συνδέσεις δεν παρατηρήσαμε κάτι ύποπτο.
- Στα ανοιχτά αρχεία παρατηρήσαμε τον driver του TrueCrypt:
 - \Device\HarddiskVolume1\WINDOWS\system32\drivers\truecrypt.sys
- Από το hashdump είδαμε ότι ο Jo είναι ο μόνος χρήστης (εξαιρώντας τους χρήστες συστήματος). Επίσης, το NT hash του είναι “31d6cfe0d16ae931b73c59d7e0c089c0” που σημαίνει ότι ο κωδικός του είναι κενός.
- Σχετικά με τη registry, αναζητήσαμε στο HARDWARE hive (με offset 0xe1380690) το οποίο περιέχει στοιχεία που αφορούν τον σκληρό δίσκο του laptop. Περαιτέρω ανάλυση της registry έγινε με χρήση του Autopsy και του Registry Viewer.
- Αναφορικά με την ανάλυση των Shellbags από τα διάφορα ευρήματα ενδιαφέρον έχει η καταγραφή πρόσβασης στο E:\Pics\Hidden\ (14:43:51 10-12-2009).
- Στα ανοιχτά παράθυρα δεν παρατηρήσαμε κάτι ύποπτο.

5.2 Ανάλυση Δίσκου Πειστηρίου Laptop

Χρησιμοποιήσαμε το εργαλείο Autopsy για να έχουμε πρόσβαση στο δίσκο του laptop και την περαιτέρω ανάλυσή του. Ακολούθως, με το εργαλείο Registry Viewer, μπορέσαμε να αναλύσουμε σε βάθος τη registry των windows και ιδιαίτερα τα: NTUSER.DAT, SAM, software και system. Επιπλέον με το εργαλείο undbx είχαμε πρόσβαση στα email του υπόπτου. Τέλος με το εργαλείο NTFS Log Tracker αναλύσαμε τις ενέργειες των τελευταίων τριών ημερών που έχουν καταγραφεί στο δίσκο.

Αφότου είχαμε πρόσβαση με το εργαλείο Autopsy, κατευθυνθήκαμε εντός μνήμης και κάναμε εξαγωγή των registry NTUSER.DAT/χρήστης Jo, SAM, software και system. Στη συνέχεια για την εύρεση βασικών στοιχείων και πληροφοριών αξιοποιήσαμε το Registry Viewer όπου:

- Μετά από ανάλυση του software βρήκαμε (λεπτομέρειες [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):
 - a. Ότι ο υπολογιστής έτρεχε σε Windows XP SP3 2600 έκδοση, με ημερομηνία εγκατάστασης 17:54:50 UTC 20-11-2009.
 - b. Ως περιηγητές χρησιμοποιούσε Mozilla Firefox v3.3.5 & Microsoft Internet Explorer v8.6001.18702 .
 - c. Η εφαρμογή διαχείρισης email που χρησιμοποιούσε ήταν Outlook Express 6.0 με email account: jo@m57.biz .
- Μετά από ανάλυση του system βρήκαμε (λεπτομέρειες [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):
 - a. Ότι η ώρα ζώνης του υπολογιστή είχε οριστεί σε PST (UTC-08:00).
 - b. Το όνομα του Υπολογιστή ήταν M57-JO .
 - c. Ο τελευταίος τερματισμός λειτουργίας του υπολογιστή έγινε 11:58:13 από εμάς.
 - d. Η IP διεύθυνση του υπολογιστή ήταν 192.168.1.106, και ο Server άκουγε στο 192.168.1.1 .

- e. Τρεις διαφορετικές συσκευές (USB flash disk) είχαν συνδεθεί με τον υπολογιστή με serial numbers και ημερο-χρονολογία τελευταίας σύνδεσης: 51491E64 / 13:54:45 23-11-2009, 2B9ECCFF / 14:01:50 24-11-2009, AADA04411400000B / 14:41:17 10-12-2009 .
- Μετά από ανάλυση του SAM βρήκαμε (λεπτομέρειες [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):
 - a. Ότι τελευταίος χρήστης που έκανε είσοδο στον υπολογιστή ήταν ο χρήστης Jo
- Μετά από ανάλυση του NTUSER.DAT/χρήστης Jo (λεπτομέρειες [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):
 - a. Το webauto χρησιμοποιούντο ως μέρος της εργασίας του.
 - b. Το Outlook Express 6.0 με email account: jo@m57.biz χρησιμοποιούντο καθημερινώς.

Μέσω του εργαλείου Autopsy διενεργήσαμε ελέγχους και εξήγαμε τα ακόλουθα:

- Ο χρήστης Jo είχε SID:1003, έκανε είσοδο στο σύστημα 32 φορές και η τελευταία φορά ήταν 11:35:57 11-12-2009.
- Σύμφωνα με το ιστορικό εγκατάστασης προγραμμάτων, ανακαλύψαμε την εγκατάσταση κάποιων από το χρήστη Jo όπως (λεπτομέρειες στο [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):
 - a. Mozilla Firefox, με ημ/νια εγκατάστασης 11:34:59 20-11-2009
 - b. Apple Software Update, με ημ/νια εγκατάστασης 14:09:32 24-11-2009
 - c. QuickTime, με ημ/νια εγκατάστασης 14:11:29 24-11-2009
 - d. TrueCrypt, με ημ/νια εγκατάστασης 12:44:14 03-12-2009
- Σχετικά με τους περιηγητές που χρησιμοποιούσε, είχαμε πρόσβαση στο ιστορικό τους, cookies, cache, bookmarks, search όπου (λεπτομέρειες στα [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#) & [Παράρτημα Z - Screenshots forensics εργασιών ΑΕΓ](#)):
 - a. Διαπιστώσαμε την επίσκεψη στο <http://www.truecrypt.org/downloads> 12:43:24 03-12-2009
 - b. Διαπιστώσαμε την επίσκεψη στο <http://www.carmax.com/enUS/view-car> 08:57:52 10-12-2009
 - c. Διαπιστώσαμε την αναζήτηση σχετικά με quicktime 14:08:23 24-11-2009, car max 08:54:45 10-12-2009
- Αναφορικά με το configuration.xml στο C:\Documents and Settings\Jo\Application Data\TrueCrypt διαπιστώσαμε πως είχε ενεργό το WipeCacheOnAutoDismount και είχε δώσει σαν drive letter το E:.
- Προσφάτως είχε ανοίξει από τον φάκελο E:\Pics\Hidden\ τα ακόλουθα αρχεία:
 - a. patent01.JPG (03-12-2009 12:50:09)
 - b. patent03.JPG (10-12-2009 14:43:53).
- Αξιοποιώντας το PhotoRec module του Autopsy ανακτήσαμε κάποια διαγεγραμμένα αρχεία από τον δίσκο του laptop εκ των οποίων ορισμένα είναι από το διαγραμμένο φάκελο Pics. Δημιουργήσαμε MD5 hashset των κρυπτογραφημένων αρχείων και το περάσαμε στο Autopsy. Εκτελώντας το Hash Lookup module παρατηρήσαμε ότι κάποια από τα διαγεγραμμένα αρχεία είναι όντως ίδια με αυτά.

Με το εργαλείο undbx είχαμε πρόσβαση στα email του κ. Smith που έστειλε/έλαβε μέσω Outlook Express 6.0, είτε ήταν διαγεγραμμένα, είτε απεσταλμένα, είτε στο φάκελο εισερχομένων / αναγνωσμένων εκ των οποίων τα ακόλουθα κρίθηκαν ως κρίσιμα για την υπόθεση υπό έλεγχο (λεπτομέρειες στα [Παράρτημα Z - Screenshots forensics εργασιών ΑΕΓ & Παράρτημα Δ - Πληροφορίες δίσκου & USB](#)):

- (1) 20-11-2009 επικοινωνία μέσω email του Jo & Jordan σε 14:48 (απεσταλμένα-διαγεγραμμένα) & 14:51 (εισερχόμενα-διαγεγραμμένα)
- (2) 23-11-2009 επικοινωνία μέσω email του Jo & Jordan σε 10:07 (εισερχόμενα-διαγεγραμμένα) , 10:16 (διαγεγραμμένο εντελώς από το σύστημα- ανάκτηση από τα επόμενα στη σειρά), 10:24 (απεσταλμένα-διαγεγραμμένα), 10:26 (απεσταλμένα-διαγεγραμμένα)
- (3) 01-12-2009 επικοινωνία μέσω email του Jo προς Jordan σε 08:52 (απεσταλμένα-διαγεγραμμένα)
- (4) 03-12-2009 επικοινωνία μέσω email του Jo & Jordan σε 09:28 (εισερχόμενα-διαγεγραμμένα), 13:01 (απεσταλμένα-διαγεγραμμένα)
- (5) 10-12-2009 επικοινωνία μέσω email του Pat προς Terry με cc Jo σε 14:11 (εισερχόμενα)
- (6) 10-12-2009 επικοινωνία μέσω email του Jo & Jordan σε 14:15 (απεσταλμένα-διαγεγραμμένα), 14:20 (απεσταλμένα-διαγεγραμμένα)

Από τη χρήση του εργαλείου NTFS Log Tracker και την ανάλυση εγγραφών στο δίσκο τις τελευταίες τρεις ημέρες μέχρι και την άφιξή μας εξήγαμε χρήσιμα στοιχεία για την διαλεύκανση της υπόθεσης—σε κάποιες περιπτώσεις η ακριβής χρονική στιγμή καταγραφής διαφέρει από την αναμενόμενη καθώς η αποθήκευση γίνεται τμηματικά, ωστόσο η σειρά παρουσίας είναι η λογικά εξαγόμενη (λεπτομέρειες στα [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#) & [Παράρτημα Z - Screenshots forensics εργασιών ΑΕΓ](#)):

- Σχετικά με τις μετονομασίες και διαγραφές παρατηρήσαμε 2 ιδιαίτερες περιπτώσεις:
 - a. 08:41:12 11-12-2009
C:\Documents and Settings\Jo\Desktop\Pics διεγράφη
 - b. 08:41:12 11-12-2009
C:\Documents and Settings\Jo\Desktop\newFiles διεγράφη
- Πιο συγκεκριμένα σχετικά με την εξέταση του file system journal παρατηρήσαμε κινήσεις μη αναμενόμενες:
 - a. 08:37:01 11-12-2009 το πρόγραμμα TrueCrypt τρέχει.
 - b. 08:37:17-08:37:50 11-12-2009 ένα πλήθος αρχείων προσπελάστηκαν κατά την εκτέλεση κάποιας διεργασίας.
 - c. 08:38:20 11-12-2009 το πρόγραμμα TrueCrypt τερμάτισε μια εργασία.
 - d. 08:38:43 11-12-2009 δημιουργήθηκε ο φάκελος C:\Documents and Settings\Jo\Desktop\newFiles2 και έπειτα διεγράφη.
 - e. 08:38:46 11-12-2009 καταγράφηκε μια παραμετροποίηση στο πρόγραμμα TrueCrypt
 - f. 08:39:32 11-12-2009 προσπελάστηκε το αρχείο C:\Documents and Settings\Jo\Desktop\Papers\Papers10\12097.RPCs.Fernado+Loring.pdf

- g. 08:39:40 11-12-2009 δημιουργήθηκε το αρχείο C:\Documents and Settings\Jo\Desktop\newFiles2
- h. 08:41:12 11-12-2009 όλο το πλήθος αρχείων που προσπελάστηκαν στο b. διεγράφησαν.
- Τα MD5 hashes των αξιοσημείωτων αρχείων παραθέτονται στο [Παράρτημα Ε - Ανάλυση δίσκου & USB](#).

Συμπεράσματα Ανάλυσης Δίσκου

- Το πρόγραμμα TrueCrypt δε χρειαζόταν για τη δουλειά του όπως μάθαμε από τις συνεντεύξεις.
- Μέσω του ιστορικού των web browsers παρατηρήσαμε τα sites που επισκέφτηκε όπως το carmax για αναζήτηση αυτοκινήτων, αλλά με μια πρώτη ματιά δεν φαίνεται κάτι ύποπτο.
- Επιβεβαιώθηκε μέσω του ιστορικού η αναζήτηση για πατέντες σχετικά με το project για teleporters που δούλευε το οποίο μας ανέφερε στη συνέντευξη.
- Οι φωτογραφίες και τα βίντεο δεν φάνηκε να είχαν γίνει download και δεν τα έχει λάβει από κάποιον κατά το χρονικά διάστημα ελέγχου και πιθανότατα τα μετέφερε ο ίδιος από κάποιο δίσκο
- Όσον αφορά τα emails που έστειλε ο κ. Smith μέσω Outlook Express 6.0 τα εξάγαμε με το εργαλείο undbx, στα οποία εντοπίσαμε μια σχετική αντιπάθεια του κ. Smith προς το αφεντικό του κ. McGoo, καθώς φαίνεται ότι τον κορόιδευε με τους συνάδελφους του.
- Ακόμα, φαίνεται να υπάρχει μια συνομιλία με τον κ. Stanford ο οποίος δεν είναι υπάλληλος της εταιρίας.
- Σε συνομιλία με τον κ. Stanford φαίνεται να του προτείνει τη χρήση κάποιων εργαλείων (diit-1.5.jar, TrueCrypt) μετά από ένα ανήσυχο email του κ. Smith σχετικά με ένα παλιό του laptop, το οποίο περιείχε φωτογραφίες τις οποίες δεν ήθελε να δει ο κ. Johnson (που ήταν υπεύθυνος για τον καθαρισμό του laptop πριν το ξεφορτωθεί).
- Επιπρόσθετα, μάθαμε από την ανταλλαγή email με τον κ. Stanford ότι στο TrueCrypt μπορείς να χρησιμοποιήσεις ως κωδικό ένα αρχείο.
- Από τη registry στο αρχείο system παρατηρήσαμε ότι το USB που βρέθηκε στο γραφείο του ύποπτου (με σειριακό αριθμό: AADA04411400000B) έχει συνδεθεί στο laptop, επομένως το χρησιμοποίησε.
- Μέσω του εργαλείου NTFS Log Tracker ανακαλύψαμε τη χρήση του TrueCrypt και βρήκαμε το αρχείο που χρησιμοποιούσε ο ύποπτος ως κωδικό για τη κρυπτογράφηση αρχείων.
- Χρησιμοποιήσαμε αυτό το PDF ως κωδικό για την αποκρυπτογράφηση του αρχείου newFiles2 που είχε ο κ. Smith στο Desktop
- Με την αποκρυπτογράφησή του αποκαλύφθηκε ότι το newFiles2 περιείχε 3 φακέλους (Hidden, New Patents, Patents) και 3 αρχεία.
 - a. Τα αρχεία ήταν το diit-1.5.jar, test.png, testHide.bmp τα οποία του είχε στείλει ο κ. Stanford μέσω email.
 - b. Ο φάκελος New Patents ήταν κενός.

- c. Στο φάκελο Patents βρέθηκε ένα αρχείο με όνομα patent001.PNG που φαίνεται να είναι μια πατέντα για teleporters.
- d. Στο φάκελο Hidden βρέθηκαν 43 εικόνες .jpg με παράνομο περιεχόμενο τα οποία έχουν ως ονομασίες πατέντες (π.χ. patent01.jpg) και 2 ακόμα φακέλοι: HighQuality και Videos. Στο φάκελο HighQuality βρέθηκαν 82 εικόνες .jpg με ονόματα του στυλ hr_patent01 αντίστοιχες του φακέλου Hidden και στο φάκελο Videos βρέθηκαν 6 videos με παράνομο περιεχόμενο.

5.3 Ανάλυση Δίσκου Πειστηρίου USB

Με τη χρήση του Autopsy αναλύσαμε επίσης τα περιεχόμενα του USB. Εκεί βρήκαμε πολλά αρχεία PDF που περιέχουν διάφορες μελέτες. Επίσης παρατηρήσαμε ορισμένες εικόνες και video που έχουν διαγραφεί και δεν καταφέραμε να ανακτήσουμε, όπως ένας φάκελος με όνομα HighQuality που θα μπορούσε να συμπίπτει με τον φάκελο που βρήκαμε στο κρυπτογραφημένο αρχείο newFiles2 στο Desktop του laptop του υπόπτου.

6. Παρουσίαση

Η εταιρία κάλεσε την ομάδα συμβούλων διερεύνησης ψηφιακών πειστηρίων για τη διερεύνηση του ηλεκτρονικού εγκλήματος κατοχής παράνομων πληροφοριών από έναν υπάλληλό τους, τον κ. Jo Smith.

Σκοπός: Προσδιορισμός αν ο πιθανός δράστης Jo Smith κατείχε παράνομες πληροφορίες σχετικά και τι στοιχεία υπάρχουν που να τον συσχετίζουν με αυτή την κατηγορία.

Αδικήματα: Κατοχή παράνομου περιεχομένου

Εργαλεία που χρησιμοποιήθηκαν: FTK Imager, Registry Viewer, Autopsy, Volatility, NTFS Log Tracker, undbx, Digital Invisible Ink Toolkit, TrueCrypt

Προετοιμασία

Έχοντας στα χέρια μας την εξουσιοδότηση από την εταιρία και τα κατάλληλα εντάλματα για την έρευνα του η-εγκλήματος, ανεβήκαμε στον 1ο όροφο της εταιρίας, όπου βρίσκεται το γραφείο του πιθανού δράστη και αποκλείσαμε το χώρο.

Ανίχνευση και Εντοπισμός

Αφού αποκλείστηκε η σκηνή του πιθανού εγκλήματος, έγινε καταγραφή των παρόντων στο χώρο οι οποίοι ήταν ο υπεύθυνος ασφαλείας, ο IT Admin και ο πιθανός δράστης κ. Jo Smith. Από αυτούς λήφθηκαν συνεντεύξεις που φαίνονται στο [Παράρτημα Β - Συνεντεύξεις](#) και έπειτα έγινε η φωτογράφιση του χώρου όπου εντοπίσαμε ένα laptop μάρκας Dell και ένα USB μάρκας Imation πάνω στο γραφείο του κ. Smith.

Το laptop φάνηκε να είναι ενεργοποιημένο επομένως ακολουθώντας τις οδηγίες από το ACPO Guidelines κουνήσαμε το ποντίκι φωτογραφίσαμε τα ενεργά προγράμματα- διεργασίες που έτρεχαν τα οποία ήταν τα: *explorer.exe*, *BrStsWnd.exe* και *BRNIPMON.exe*. Τέλος, έγινε η κατάλληλη καταγραφή ειδικών φορμών κατάσχεσης για τα παραπάνω ψηφιακά πειστήρια, τα οποία φαίνονται στο [Παράρτημα Γ - Φόρμες κατάσχεσης, καταγραφής](#).

Διαφύλαξη

Για τη διαφύλαξη των ψηφιακών πειστηρίων, πραγματοποιήθηκε λήψη πιστού αντιγράφου της μνήμης του laptop στη σκηνή του εγκλήματος. Έπειτα, αφαιρέσαμε το καλώδιο της παροχής ηλεκτρικού ρεύματος από το σημείο που είναι συνδεδεμένο στην πρίζα και αφού αφήσαμε τη συσκευή να κρυώσει, την ξεβιδώσαμε και αφαιρέσαμε το σκληρό του δίσκο. Τέλος, για την ασφαλή μετακίνησή τους βάλαμε κατάλληλα labels και τα τοποθετήσαμε (laptop, δίσκος, USB) σε αντιστατικές σακούλες με προσοχή ώστε να μην λυγίσουν.

Ανάλυση (Analysis)

1. Περιγραφή Evidence

Στο γραφείο του υπόπτου, βρέθηκαν ένα ενεργοποιημένο laptop με λειτουργικό σύστημα Microsoft Windows XP Service Pack 3 και ένα USB Imation 256 MB τοποθετημένο δίπλα το οποίο φάνηκε από την ανάλυση ότι έχει χρησιμοποιηθεί στο laptop του. Αυτά αναλύθηκαν από τα αντίγραφα μνήμης και δίσκου που λήφθηκαν.

2. Περιγραφή ανάλυσης evidence

Για την ανάλυση της μνήμης του laptop χρησιμοποιήθηκε το εργαλείο Volatility και για την ανάλυση του δίσκου του laptop και για το USB χρησιμοποιήθηκαν τα εργαλεία Autopsy και FTK imager. Ύστερα, με το Registry Viewer αναλύσουμε σε βάθος τη registry των windows και ιδιαίτερα τα: NTUSER.DAT/Jo, SAM, software και system. Ακόμα, με το εργαλείο undbx μπορέσαμε να εξάγουμε τα email του πιθανού δράστη και με το NTFS Log Tracker αναλύσαμε τις ενέργειες του τις τελευταίες τρεις ημέρες.

Μέσω των εργαλείων αυτών καταφέραμε να εξάγουμε πληροφορίες όπως τα προγράμματα που εγκατέστησε, τις σελίδες που επισκέφθηκε, την επικοινωνία του μέσω mail και άλλα όπως φαίνονται και στα [Παράρτημα Δ - Πληροφορίες δίσκου & USB](#) και [Παράρτημα Ζ - Screenshots forensics εργασιών ΑΕΓ](#).

Από την Ανάλυση εντοπίσαμε τα εξής:

- Ανταλλαγή email με μη συνεργάτη της εταιρία με όνομα Jordan Stanford, ο οποίος σε πρώτο χρόνο του έστειλε το εκτελέσιμο αρχείο diit-1.5.jar για στεγανογραφία (23-11-2009). Ύστερα, και καθώς ο Jo Smith ανέφερε σε email του (1-12-2009) ότι το εργαλείο αυτό ήταν αργό, του προτάθηκε σε δεύτερο χρόνο (3-12-2009) να κατεβάσει προγράμματα κρυπτογράφησης (TrueCrypt) το οποίο και χρησιμοποίησε.
- Για να μπορέσουμε να έχουμε πρόσβαση στα κρυπτογραφημένα αρχεία εγκαταστήσαμε το Digital Invisible Ink Toolkit (diit) καθώς και το TrueCrypt.
- Μέσω του file system journal αναγνωρίσαμε ένα πλήθος μη αναμενόμενων ενεργειών την 11-12-2009 μεταξύ 08:37:01-08:41:12 που μας κατεύθυναν στο αρχείο newFiles2 στην επιφάνεια εργασίας. Από την ίδια ημερο-χρονολογία αποφανθήκαμε ότι το αρχείο Desktop\Papers\Papers10\12097.RPCs.Fernado+Loring.pdf είχε χρησιμοποιηθεί σε διεργασία του TrueCrypt.
- Αποκρυπτογραφήσαμε το αρχείο **newFiles2** μέσω του TrueCrypt, χρησιμοποιώντας ως keyfile το προαναφερθέν pdf και αμέσως εμφανίστηκε φάκελος με το όνομα pics και εντός 3 φάκελοι Hidden 43 εικόνες .jpg, HighQuality (82 εικόνες .jpg), Videos (6 video), New Patents (κενό), Patents (patent01.jpg) και 3 αρχεία diit-1.5.jar, test.png, testHide.bmp. Τα εν λόγω αρχεία είχαν προσπελαστεί στο προαναφερθέν χρονικό διάστημα.
- Προσφάτως είχε ανοίξει τα αρχεία patent01.JPG (3-12-2009) και patent03.JPG (10-12-2009) στο φάκελο Hidden. Ενώ όλα τα επίμαχα αρχεία που είχαν κρυπτογραφηθεί βρέθηκαν ως διεγραμμένα στον υπολογιστή.
- Το περιεχόμενο των εικόνων και βίντεο κρίνεται παράνομο.

Συμπεράσματα

Ο κ. Jo Smith φαίνεται να έχει εις γνώση του διαγράψει πλήθος στοιχείων που πιθανώς να τον ενοχοποιούσαν σε ενδεχόμενο έλεγχο, όπως την επικοινωνία του μέσω email με τον κ. Jordan Stanford, όλα τα αρχεία που βρέθηκαν στο κρυπτογραφημένο αρχείο newFiles2 η άλλως φάκελο Pics καθώς και άλλα. Χρησιμοποίησε εκτός πολιτικής εταιρίας δύο προγράμματα, τα diit-1.5. & TrueCrypt για προσωπική του χρήση όντας υπεύθυνος για την κατοχή, διάθεση και επεξεργασία τους. Οι ενέργειες του προ της αφίξεώς μας, δείχνουν μελετημένη δράση κι επίγνωση και δεν μπορούν να αποδοθούν στη τύχη ή την ευήθεια.

Παράρτημα Α - RACI Matrix

	Expert Witness	Technical Witness 1	Technical Witness 2
1 Προετοιμασία			
1.1 Προετοιμασία ενταλμάτων & εξουσιοδοτήσεων	R	I	I
1.2 Εξασφάλιση εργαλείων και τεχνικών	R	I	I
1.3 Καθορισμός Αρμοδιοτήτων	R/A	I	I
1.4 Σχεδιασμός Διαδικασίας-Έρευνας	R	I	I
2 Ανίχνευση & Εντοπισμός			
2.1 Αποκλεισμός Σκηνής η-Εγκλήματος	A	R	I
2.2 Καταγραφή Παρόντων στο Χώρο	I	I	R
2.3 Συνεντεύξεις	C	I	R
2.4 Φωτογράφιση Χώρου	I	R	I
2.5 Καταγραφή Πηγών Πειστηρίων (κατάστασης τους)	I	I	R
2.6 Φωτογράφιση Ενεργών Προγραμμάτων	I	R	I
2.7 Έλεγχος Δικτυακών Συνδέσεων	I	R	I
2.8 Καταγραφή σε ειδικές φόρμες	C	R	R
3 Διαφύλαξη			
3.1 Διαφύλαξη Μνήμης Πειστηρίου Laptop	I	R	I
3.2 Διαφύλαξη Δίσκου Πειστηρίου Laptop	I	R	I
3.3 Διαφύλαξη Πειστηρίου USB	I	I	R
3.4 Διαφύλαξη logs από το Access Card System	I	I	R
3.5 Προετοιμασία & Μεταφορά Πειστηρίων στο Εργαστήριο	R/A	I	I
4 Ανάλυση			
4.1 Ανάλυση Μνήμης Πειστηρίου Laptop	R/A	C	I
4.2 Ανάλυση Δίσκου Πειστηρίου Laptop	R/A	C	I
4.3 Ανάλυση Πειστηρίου USB	R/A	I	C

4.4 Ανάλυση Access Card Sytem Logs	R/A	I	C
------------------------------------	-----	---	---

5 Παρουσίαση

5.1 Καταγραφή Διαδικασίας	R	I	I
---------------------------	---	---	---

5.2 Παρουσίαση και Επεξήγηση Συμπερασμάτων	R	I	I
--	---	---	---

Παράρτημα Β - Συνεντεύξεις

Συνέντευξη του Υπεύθυνου Ασφαλείας στις 11:10

Ερώτηση: Ο Jo Smith έκανε υπερωρίες; Ερχόταν εκτός ωραρίου;

Απάντηση: Απ' όσο γνωρίζω δεν έκανε υπερωρίες αλλά αυτό μπορούμε να το επιβεβαιώσουμε από το σύστημα καρτών μας.

Ερώτηση: Ποιες είναι οι οι πολιτικές για τα εταιρικά laptop; Μπορείς να τα πάρεις και στο σπίτι σου;

Απάντηση: Μερικοί υπάλληλοι έχουν εταιρικά laptop καθώς χρειάζεται να δουλέψουν και εκτός γραφείου για παράδειγμα λόγω κάποιων συνεδριών. Εννοείται ότι μπορούν να τα πάρουν σπίτι τους και έχει χρειαστεί να δουλέψουν ή να ψάξουν για κάποια έρευνα και εκτός γραφείου και ωραρίου.

Ερώτηση: Υπάρχουν πολιτικές για τα passwords (password complexity); Αν ναι, πόσο αυστηρά είναι;

Απάντηση: Δεν υπάρχει κάποια συγκεκριμένη πολιτική

Ερώτηση: Τι πολιτικές υπάρχουν για την εγκατάσταση προγραμμάτων;

Απάντηση: Επιτρέπεται να κατεβάσουν ό,τι προγράμματα πιστεύουν οι υπάλληλοι ότι χρειάζονται για τη δουλειά τους. Υπάρχει σύστημα που μπορώ να ελέγξω τι κατεβάζουν.

Ερώτηση: Παρατηρήσατε στον Jo Smith κάποιο πρόγραμμα που δεν συνηθίζεται να υπάρχει στα laptops της εταιρίας;

Απάντηση: Όχι, αλλά δεν τα ελέγχω και τόσο συχνά

Ερώτηση: Δίνετε USB ως εταιρία; Τι πολιτική υπάρχουν για τα USB;

Απάντηση: Δεν δίνουμε αλλά δεν υπάρχει κάποια πολιτική.

Ερώτηση: Θα μπορούσατε να μου δώσετε τα Logs από το access control system;

Απάντηση: Όχι, δε μπορώ να το κάνω αυτό. Απαγορεύεται.

Ερώτηση: Τι σύστημα είναι ακριβώς το access control system; Καταγράφεται;

Απάντηση: Υπάρχει καταγραφή, γίνεται με χτύπημα της κάρτας των υπαλλήλων. Το καταγραφικό κρατάει για 1 βδομάδα και έπειτα σβήνεται αυτόματα.

Ερώτηση: Ποιοι άλλοι έχουν πρόσβαση στον 1^ο όροφο;

Απάντηση: Μπορώ να σας δώσω μια λίστα με τα στοιχεία των υπαλλήλων που δουλεύουν στον 1ο όροφο.

Ερώτηση: Υπήρξε περιστατικό κλοπής κάποιας κάρτας το τελευταίο διάστημα;

Απάντηση: Όχι, δεν υπήρξε κάποιο περιστατικό κλοπής access card

Ερώτηση: Ο Jo Smith τι ρυθμίσεις έχει στη κάρτα του; Σε τι ορόφους έχει πρόσβαση;

Απάντηση: Ο Jo έχει πρόσβαση μόνο στον 1ο όροφο

Ερώτηση: Ο Jo Smith έχει προκαλέσει κάποιο άλλο πρόβλημα ασφάλειας;

Απάντηση: Όχι από όσο γνωρίζω. Το μόνο που ξέρω είναι ότι πρόσφατα είχε ένα θέμα με το laptop του και χρειάστηκε να αλλάξει, καθώς ήταν corrupted.

Συνέντευξη του IT Admin στις 11:35

Ερώτηση: Ο Jo Smith έκανε υπερωρίες; Ερχόταν εκτός ωραρίου;

Απάντηση: Όχι απ'ότι ξέρω

Ερώτηση: Υπάρχει κάποιος file server που αποθηκεύει το τμήμα αυτό τα δεδομένα της;

Απάντηση: Υπάρχει ένα network drive

Ερώτηση: Υπάρχει συγκεκριμένος φάκελος για κάθε όροφο ή τμήμα ;

Απάντηση: Όχι

Ερώτηση: Είναι εσωτερικά του οργανισμού ή σε cloud;

Απάντηση: Είναι εσωτερικά του οργανισμού

Ερώτηση: Οι υπάλληλοι χρησιμοποιούν κάποιο πρόγραμμα για encryption από την εταιρία;

Απάντηση: Όχι, οι υπάλληλοι δεν χρειάζεται να χρησιμοποιήσουν κάποιο πρόγραμμα για την κρυπτογράφηση καθώς λειτουργούν σε ασφαλές δίκτυο

Ερώτηση: Ποιο είναι το domain name των εταιρικών email;

Απάντηση: m57.biz

Ερώτηση: Μου ανέφεραν ότι ο Jo Smith έχει αλλάξει laptop. υπάρχει ακόμα η παλιά του συσκευή;

Απάντηση: Όχι

Συνέντευξη του πιθανού δράστη στις 12:00

Ερώτηση: Ποιος είναι ο ρόλος σου στην εταιρία;

Απάντηση: Δουλεύω ως υπάλληλος του Pat Macgoo. Μου αναθέτει projects για πατέντες που ψάχνουμε ανάλογα με το τι ζητάνε οι εταιρίες.

Ερώτηση: Ασχολείσαι αυτή τη περίοδο με κάποιο συγκεκριμένο project; Αν ναι, μόνος σου ή ομαδικά. Αν ασχολείσαι ομαδικά, με ποιους άλλους συνεργάζεσαι;

Απάντηση: Ναι, ασχολούμαι με τα teleporters που μας ανέθεσε μια εταιρία. Το δουλεύω ατομικά

Ερώτηση: Υπήρχε ανταλλαγή πληροφοριών για αυτό το project με κάποιο συνάδελφό σου; Αν ναι, με τι μέσο επικοινωνίας γινόταν;

Απάντηση: Ο συνάδελφός μου ο Charlie με βοηθάει αν βρει κάποια μελέτη σχετικά με το θέμα μου όπως αντίστοιχα τον βοηθάω και εγώ. Η επικοινωνία μας είναι συνήθως μέσω email.

Ερώτηση: Το project αυτό ήταν confidential;

Απάντηση: Ναι, όπως και όλα τα projects που δουλεύουμε

Ερώτηση: Υπήρχε ανταλλαγή πληροφοριών για αυτό το project με κάποιον εκτός εταιρίας;

Απάντηση: Όχι, αφού τα projects είναι confidential

Ερώτηση: Υπήρχε κάποιο ανησυχητικό γεγονός την τελευταία περίοδο (τελευταίο μήνα;) που χρειάστηκε να αναφέρεις; Για παράδειγμα με το εταιρικό σου laptop ή την κάρτα εισόδου σου

Απάντηση: Όχι απ'όσο θυμάμαι

Ερώτηση: Μας έχουν ήδη αναφέρει ότι είχες κάποιο πρόβλημα με το παλιό σου laptop και για αυτό χρειάστηκε να σου δώσουν καινούριο. Ισχύει αυτό;

Απάντηση: Ναι ισχύει, το είχα ξεχάσει

Ερώτηση: Τι είχε πάθει ακριβώς το laptop σου και σε ποιον το ανέφερες;

Απάντηση: Ήταν αργό και το ανέφερα στον Terry τον IT Administrator ώστε να το ελέγξει

Ερώτηση: Ποιος ήταν υπεύθυνος για την παλιά σου συσκευή; Ξέρεις αν την έχετε ακόμα;

Απάντηση: Υπεύθυνος ήταν ο κ. Terry Johnson. Δεν γνωρίζω αν την έχουμε ακόμα.

Ερώτηση: Χρειάστηκε να κάνεις εσύ κάποια κίνηση στο παλιό σου laptop πριν σου αλλάξουν τη συσκευή;

Απάντηση: Όχι, εγώ απλώς το ανέφερα και παρέδωσα τη συσκευή στον Terry για έλεγχο. Το επόμενο που ξέρω είναι ότι μου έφεραν καινούρια συσκευή με το λόγο ότι η παλιά ήταν corrupted.

Ερώτηση: Τι ρυθμίσεις έχεις στη κάρτα του; Σε τι ορόφους έχεις πρόσβαση;

Απάντηση: Στον όροφο που είναι το γραφείο μου, τον 1ο και στον όροφο που είναι το αφεντικό του, τον 2ο. Πολλές φορές χρειάστηκε να κάνουμε meetings για τα projects οπότε ανέβαινα στον όροφό του

Ερώτηση: Το USB που βρέθηκε πάνω στο γραφείο σου ανήκει σε εσένα; Αν όχι ξέρεις σε ποιον μπορεί να ανήκει ή πως βρέθηκε στο γραφείο σου;

Απάντηση: Όχι δεν ανήκει σε εμένα. Δεν ξέρω ποιανού είναι

Ερώτηση: Έχεις καλές σχέσης με τον Pat;

Απάντηση: Ναι, πηγαίνουμε συχνά και για διάλειμμα και καφέ-φai μαζί

Ερώτηση: Είχε αναφέρει τίποτα ανησυχητικό τον τελευταίο καιρό σχετικά με διαρροή πληροφοριών;

Απάντηση: Όχι, δεν είχε αναφέρει κάτι σε εμένα.

Ερώτηση: Έχεις κάποια υποψία για συνάδελφό σου για διαρροή πληροφοριών;

Απάντηση: Όχι, δεν γνωρίζω κάτι

Ερώτηση: Ποιες είναι οι ώρες εργασίας σου;

Απάντηση: Όπως όλων 9:00-17:00

Ερώτηση: Έκανες υπερωρίες; Ερχόσουν εκτός ωραρίου;

Απάντηση: Όχι αλλά κάποιες φορές έκανα έρευνα από το σπίτι μου τα σαββατοκύριακα ή τις αργίες για κάποια projects

Ερώτηση: Αυτό στο είχε αναθέσει ο Pat ή το έκανες από μόνος σου

Απάντηση: Το έκανα από μόνος μου αλλά υπήρχαν φορές που ο ίδιος μας παρότρυνε αν έχουμε χρόνο να το κάνουμε

Ερώτηση: Γενικά είσαι ευχαριστημένος από αυτή την δουλειά;

Απάντηση: Ναι, όλα είναι μια χαρά

Παράρτημα Γ - Φόρμες κατάσχεσης, καταγραφής

Φόρμα στοιχείων σκληρού δίσκου Laptop

Τεχνικές Προδιαγραφές Σκληρού δίσκου			
Case ID	001		
Κατασκευαστής	Western Digital		
S/N	WD153BA		
Κύλινδροι	156250		
Κεφαλές	3		
Δίσκοι	1		
Χωρητικότητα	15.3GB		
Λεπτομέρειες κατάσχεσης σκληρού δίσκου			
Ήταν προσαρτημένος ο δίσκος;			NAI
Ήταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;			NAI
<p>Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε;</p> <p>Αφαιρέσαμε το καλώδιο της παροχής ηλεκτρικού ρεύματος από την μεριά της πρίζας για να απενεργοποιηθεί το Laptop και μετά αφαιρέσαμε τον σκληρό του δίσκο. Έπειτα τοποθετήσαμε το σκληρό δίσκο σε αντιστατική σακούλα για την ασφαλή μετακίνησή του.</p>			
Ήταν ο δίσκος προστατευμένος με κωδικό πρόσβασης;			OXI
Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι;			
Δημιουργία αντιγράφου			
Εφαρμογή δημιουργίας αντιγράφου	FTK Imager	Έκδοση	4.7.1
Τόπος λήψης πιστού αντιγράφου		Ευελπίδων 47	
Ημερομηνία λήψης πιστού αντιγράφου		11/12/2009	
MD5 hash		434332cdbdb1463606cbea2d7a625745	
Εγκληματολόγος ερευνητής που έκανε την κατάσχεση			
Ονοματεπώνυμο	Ελένη Τράμπαρη-Λάρδα	Τίτλος	Technical Witness 1
Τηλέφωνο		Τμήμα	Digital Forensics
Υπογραφή	E.T	Ημ/νια	11/12/2009

Σχόλια	Εταιρικό laptop
--------	-----------------

Φόρμα στοιχείων σκληρού δίσκου USB

Τεχνικές Προδιαγραφές Σκληρού δίσκου			
Case ID	001		
Κατασκευαστής	Imation Corp.		
S/N	AADA04411400000B		
Κύλινδροι	15620		
Κεφαλές	2		
Δίσκοι	1		
Χωρητικότητα	256MB		
Λεπτομέρειες κατάσχεσης σκληρού δίσκου			
Ήταν προσαρτημένος ο δίσκος;			OXI
Ήταν σε λειτουργία το σύστημα κατά την ώρα της κατάσχεσης;			OXI
Εάν ναι, πώς απενεργοποιήθηκε και διασφαλίστηκε;			
Ήταν ο δίσκος προστατευμένος με κωδικό πρόσβασης;			OXI
Ο κωδικός δόθηκε από τον ιδιοκτήτη; Αν ναι ποιος είναι;			
Δημιουργία αντιγράφου			
Εφαρμογή δημιουργίας αντιγράφου	Autopsy	Έκδοση	4.20.0
Τόπος λήψης πιστού αντιγράφου		Ευελπίδων 47	
Ημερομηνία λήψης πιστού αντιγράφου		11/12/2009	
MD5 hash		8f23279deb398c3245829a98bc8fc1bd	
Εγκληματολόγος ερευνητής που έκανε την κατάσχεση			
Ονοματεπώνυμο	Ιωάννης Σομός	Τίτλος	Technical Witness 2
Τηλέφωνο		Τμήμα	Digital Forensics

Υπογραφή	Ι.Σ.	Ημ/νια	11/12/2009
Σχόλια	Προσωπικό USB		

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 001
 Offense: Παράνομο περιεχόμενο
 Submitting Officer: (Name/ID#) Αλέξανδρος Καρράς/007
 Victim: M57.BIZ
 Suspect: Jo Smith
 Date/Time Seized: 11122009
 Location of Seizure: M57 1ος όροφος

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
001	1	Laptop Dell, ενεργό, χωρίς σημάδια, χωρίς γρατζουνιές
002	1	USB Imation Corp., μη ενεργό, AADA04411400000B, χωρίς σημάδια, χωρίς γρατζουνιές

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
001	11122009	Terry Johnson	Ελένη Τράμπαρη-Λάρδα	M57
002	11122009	Terry Johnson	Ιωάννης Σομός	M57
001	11122009	Ελένη Τράμπαρη-Λάρδα	Αλέξανδρος Καρράς	Lab
002	11122009	Ιωάννης Σομός	Αλέξανδρος Καρράς	Lab

Παράρτημα Δ - Πληροφορίες δίσκου & USB

What are the hash values (MD5) of all images?

Does the acquisition and verification hash value match?

Possible Answer	Class	Hash Algo.	Hash value
	Laptop	MD5 (A)	434332cdbdb1463606cbea2d7a625745
		MD5 (V)	434332cdbdb1463606cbea2d7a625745
	USB	MD5 (A)	8f23279deb398c3245829a98bc8fc1bd
		MD5 (V)	8f23279deb398c3245829a98bc8fc1bd
Considerations	N/A		

Identify the partition information of PC image.

Possible Answer	No.	Bootable	File system	Start Sector	Total Sectors	Size
	1		Unallocated	0	63	32KB
	2	*	NTFS	63	30025422	15GB
	3		Unallocated	30025485	17955	9MB
Considerations	N/A					

Explain installed OS information in detail.

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

Possible Answer	OS Name	Windows
	Version	XP SP3
	Build Number	2600
	Registered Owner	JO
	System Root	C:\WINDOWS
	Install Date	20-11-2009 17:54:50 UTC
Considerations	- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	

What is the timezone setting?

Possible Answer	Timezone	Pacific Standard Time (UTC-08:00)
	Daylight Time Bias	0
Considerations	- HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation	

What is the computer name?

Possible Answer	M57-JO
Considerations	- HKLM\SYSTEM\ControlSet001\Control\ComputerName\ComputerName

List all accounts in OS except the system accounts: Administrator, Guest, HelpAssistant, SUPPORT_388945a0. (Account name, login count, last logon date...)

Possible Answer	Account	SID	NT Hash	Status	Login Count	Account Created Time	Last Login Time	Login Failure Time
(Timezone is applied)	Jo	1003	(a)	Enabled	32	2009-11-20 11:35:57	2009-12-11 11:05:20	never
Considerations	(a) 31d6cfe0d16ae931b73c59d7e0c089c0 ⇒ password: (empty)							

Who was the last user to logon into PC?

Possible Answer	Jo
Considerations	- HKLM\SAM\Domains\Account\Users\000003EB (modification time)

When was the last recorded shutdown date/time?

Possible Answer	11 DEC 2009 19:58:13
Considerations	- HKLM\SYSTEM\ControlSet001\Control\Windows\ShutdownTime

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

Possible Answer	Device Name	Intel(R) PRO/1000 MT Network Connection
	IP Address	192.168.1.106
	Subnet Mask	255.255.255.0
	Name Server	192.168.1.1
	Domain	m57.biz
	Default Gateway	192.168.1.1
	DHCP Usage	Yes
	DHCP Server	192.168.1.1
Considerations	- HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9E731064-973F-49A6-B6F9-5EA61EED4E01} - HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\0008	

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 14:11:29	QuickTime	7.65.17.80	Apple Inc.	C:\Program Files\QuickTime
	2009-11-30 09:34:53	Brother HL-2170W	1.00	Brother	C:\Program Files\Brother\BRHL2170
	2009-11-24 14:09:32	Apple Software Update	2.1.1.116	Apple Inc.	C:\Program Files\Apple Software Update

	2009-11-30 08:51:34	Adobe Reader	9.2.0	Adobe Systems Incorporate	C:\Program Files\Adobe\ Reader 9.0\ Reader
	2009-11-23 10:23:53	Python	2.6	Python Software Foundation	C:\Python26
	2009-12-03 12:44:14	TrueCrypt	6.3a	TrueCrypt Foundation	C:\ProgramFi les\TrueCryp
	2009-11-20 11:34:59	Mozilla Firefox	3.5.5	Mozilla	C:\Program Files\Mozilla Firefox
Considerations	- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~				

What web browsers were used?

Possible Answer	- Microsoft Internet Explorer v8.0.6001.18702 - Mozilla Firefox v3.3.5
Considerations	- HKLM\SOFTWARE\Microsoft\Internet Explorer (value:Version) - HKLM\SOFTWARE\Mozilla\Mozilla Firefox (CurrentVersion)

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

Possible Answer	Microsoft Internet Explorer	- C:\Documents and Settings\Jo\Local Settings\History\History.IE5\ - C:\Documents and Settings\Jo\Application Data\Cookies\ - C:\Documents and Settings\Jo\Local Settings\Temporary Internet Files\Content.IE5\
	Mozilla Firefox	- C:\Documents and Settings\Jo\Application Data\Mozilla\Firefox\Profiles\11u6o5x2.default\places.sqlite - C:\Documents and Settings\Jo\Application Data\Mozilla\Firefox\Profiles\11u6o5x2.default\cookies.sqlite - C:\Documents and Settings\Jo\Application Data\Mozilla\Firefox\Profiles\11u6o5x2.default\search.sqlite - C:\Documents and Settings\Jo\Application Data\Mozilla\Firefox\Profiles\11u6o5x2.default\bookmarkbackups\
Considerations	- History, Cookies, Cache, Search, Bookmarks	

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

	Timestamp	URL	Browser
Possible Answer (Timezone is applied)	2009-11-23 16:02:28	http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetacgi%2FPTO%2Fsearch-bool.html&r=2333091.2241637241&f=G&l=50&col=AND&d=PTXT&s1=time&OS=time&RS=time	Firefox
	2009-11-30 08:46:59	http://www.freepatentsonline.com/5041044.pdf	Firefox
	2009-11-30 14:49:55	http://books.google.com/patents?id=xhQZAAAAEBAJ&printsec=abstract&zoom=4&source=gb&overview_r&cad=0#v=onepage&q=&f=false	Firefox

	2009-11-30 16:50:28	http://whois.domaintools.com/teleporter.com	Firefox
	2009-11-30 16:52:39	http://message.snopes.com/showthread.php?t=17243	Firefox
	2009-12-03 12:43:24	http://www.truecrypt.org/downloads	Firefox
	2009-12-04 09:06:33	http://fraudgallery.com/	Firefox
	2009-12-10 08:57:52	http://www.carmax.com/enUS/view-car/default.html?AVi=9&id=6228869&N=4294966921+4294965709&Ne=662&D=90&zip=93940&pD=0&pI=0&pT=400&pC=200&pB=0&No=0&Ep=homepage:hhomepage%20Type&Rp=R&PP=20&sV=List&CD=14+240+398+15+9&Q=4eb4c7eb-bb6f-4602-aee7-f798f6ea6bec	Firefox
Considerations	- History, Cache, Cookie...		

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

	Timestamp	Keyword (URL)	Browser
(Some duplicated and meaningless items are excluded) (Timezone is applied)	2009-11-20 09:33:57	firefox (http://www.google.com/search?hl=en&source=hp&q=firefox&aq=f&oq=&aqi=g10)	IE
	2009-11-23 10:17:55	mozrepl (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=mozrepl&btnG=Google+Search)	Firefox
	2009-11-23 10:20:00	python (http://www.google.com/search?q=python&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Firefox
	2009-11-23 10:22:31	cnn (http://www.google.com/search?q=cnn&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Firefox
	2009-11-24 14:08:23	quicktime (http://www.google.com/search?q=quicktime&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)	Firefox
	2009-11-30 08:46:49	teleporter patent (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=teleporter+patent&btnG=Google+Search)	Firefox
	2009-11-30 08:47:31	adobe pdf (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=adobe+pdf&btnG=Google+Search)	Firefox
	2009-11-30 14:51:00	google maps (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=google+maps&btnG=Google+Search)	Firefox

		US%3Aofficial&channel=s&hl=en&source=hp&q=google+maps&btnG=Google+Search)	
	2009-12-04 09:04:48	wikipedia (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=wikipedia&btnG=Google+Search))	Firefox
	2009-12-04 09:06:18	nigerian prince email scam (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=nigerian+prince+email+scam&btnG=Google+Search))	Firefox
	2009-12-10 08:54:45	car max (http://www.google.com/search?client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&channel=s&hl=en&source=hp&q=car+max&btnG=Google+Search))	Firefox
Considerations	- Web browser logs		

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

Possible Answer	Timestamp (Timezone is applied)	Search Keyword
	2009-11-23 13:51:21	webauto
Considerations	- HKCU\Software\Microsoft\Search Assistant\ACMr\5603 - 'Timestamp' can be inferred from a timestamp of the parent key ('5603'). - 'Timestamp' may not be accurate because it depends on the update mechanism of Windows Explorer.	

What application was used for e-mail communication?

Possible Answer	Outlook Express 6.0 Windows Live Hotmail
Considerations	- HKLM\SOFTWARE\Classes\mailto\shell\open\command (→ Outlook Express) - HKLM\SOFTWARE\Classes\Mail (→ Hotmail, Outlook Express) - HKCU\Software\Microsoft\Outlook Express\5.0

Where is the e-mail file located?

Possible Answer	C:\Users\Jo\Local Settings\Application Data\Identities\{BC112AB3-3F86-4D46-A9E4-73A00E67A426}\Microsoft\Outlook Express
Considerations	- Outlook Express 6.0 - Outlook DBX file format

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

Possible Answer	jo@m57.biz
Considerations	- See Question 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)

Possible Answer (Timezone is applied)	Timestamp	E-Mail Communication	
	2009-11-16	Source	[inbox]
	10:27	From → To	Jo@m57.biz --> Jo@m57.biz
		Subject	Test e-mail
		Body	This is test e-mail jo1
	2009-11-16 11:03	Source	[inbox]
		From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz , Terry@m57.biz
		Subject	WELCOME TO THE COMPANY!
		Body	T 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 11:23	Source	[Inbox]
		From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz , Terry@m57.biz
		Subject	Lunch
		Body	Dear Team,
			today's the first day - do what you need to do, getting your office set up or what not. But normally we will observe a common workday, with 12-1 PM being the designated lunch time. I do not see any

			<p>reason why anyone should deviate from this schedule in the future.</p> <p>I tried the place across the street recently, it's pretty good. Perhaps once a week or so we could all try to have lunch together.</p> <p>Regards,</p> <p>Pat</p>
2009-11-17	Source		[inbox]
10:31	From → To		Pat@m57.biz , --> Jo@m57.biz , Charlie@m57.biz
	Subject		Fw: M57.BIZ PRIOR ART INVESTIGATION SERVICES
	Body		<p>----- Original Message -----</p> <p>From: Alex Monroe</p> <p>To: Pat McGoo</p> <p>Sent: Tuesday, November 17, 2009 8:58 AM</p> <p>Subject: Re: M57.BIZ PRIOR ART INVESTIGATION SERVICES</p> <p>Dear Pat,</p> <p>Yes, we are very interested in using your prior art investigation services. Our R&D department is currently applying for patents in two key areas that we are counting on to gain market share over our major competitor, project2400.com. I am counting on you and your firm to keep these research areas in strict confidentiality. We wouldn't want project2400 to know about our research interests. 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 hesitate 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	Source		[inbox]
10:33	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 satisfaction with our results. Come by my office and we'll talk details.</p> <p>Pat</p> <p>-----</p> <p>From: Jo Sent: Tuesday, November 17, 2009 10:49 AM To: Pat Subject: RE: ASSIGNMENT OF NITROBA ACCOUNT</p> <p>I am on it boss.</p>

		Jo
		----- From: Pat Sent: Tuesday, November 18, 2009 14:06 PM To: Jo Subject: RE: ASSIGNMENT OF NITROBA ACCOUNT If you have time this afternoon let's get together on this - I have a few ideas that might help out.
2009-11-17	Source	[Inbox]
10:34	From → To	Charlie@m57.biz --> Jo@m57.biz
	Subject	What's wrong with Pat
	Body	Hey Jo, Don't you think Pat is a weird boss? I think there is something funny about him. What do you think? Charlie
2009-11-17 10:40	Source	[inbox]
	From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz
	Subject	Lunch
	Body	I'm thinking about that place over on the corner today - they have the best tuna salad - I'll be leaving around 12:05 if anyone cares to join me. Pat
2009-11-17	Source	[Inbox]
15:54	From → To	Pat@m57.biz --> Jo@m57.biz , Terry@m57.biz Charlie@m57.biz
	Subject	Great Job Folks!
	Body	All, I am very proud of you all for jumping in with both feet and starting us off on the right foot. Go ahead and take off an hour early. See you all in the morning. Pat

	2009-11-17 20:39	Source	[inbox]
		From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz
		Subject	Inventions / Patents
		Body	<p>Jo, Charlie,</p> <p>I have an idea for an invention that I am very enthusiastic about. If you get time from your other responsibilities here or there, please take a minute two start seeing if this has been done before with some searches.</p> <p>You know those little plastic golf balls filled with liquid that you freeze and use as ice cubes? I want to do jacks. You know, like jacks that little kids play with? And a ball to go with it. The thinking is, jacks have a lot more surface area than balls - imagine how quickly they would cool down a frosty drink ! And, here's the best part, the kids could play with them while they were not being used for the primary purpose.</p> <p>I think this shows a lot of promise - let me know if you find anything.</p> <p>Thanks</p> <p>Pat</p>
	2009-11-18	Source	[inbox]
	09:03	From → To	Pat@m57.biz , --> Jo@m57.biz , Charlie@m57.biz , Terry@m57.biz ,
		Subject	COFFEE
		Body	<p>Charlie, Terry,</p> <p>just checking up on your preferences for coffee - jo is going shopping tomorrow, let us know what you want.</p> <p>Jo, I like my coffee cinnamon apple flavor with just a whisper of cream - be sure to get the heavy whipping cream, NOT the half and half. See if they have any of those nice pumpkin muffins, too.</p> <p>Pat</p>

			<p>-----</p> <p>From: Terry Sent: Wednesday, November 18, 2009 09:39 AM To: Jo, Charlie Subject: RE: COFFEE</p> <p>Coffee Cinnamon Apple? Is there such a flavor? And what is a whisper of cream?</p> <p>I feel for you Jo. That sucks that you have to go and run such a ridiculous shopping errand.</p> <p>-Terry</p> <p>-----</p> <p>From: Terry Sent: Wednesday, November 18, 2009 09:40 AM To: Pat, Jo, Charlie Subject: RE: COFFEE</p> <p>Normal coffee works for me. Nothing special.</p> <p>Thanks, Terry</p>
2009-11-18	Source		[Inbox]
09:28	From → To		Pat@m57.biz --> Jo@m57.biz , Charlie@m57.biz
	Subject		pneumatic boxing glove
	Body		<p>Check this one out:</p> <p>http://www.google.com/patents/about?id=lnUBA-AAAEBAJ</p> <p>I should have thought of that one!</p> <p>(Attached a picture)</p>
2009-11-18	Source		[inbox]
09:30	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>

			Pat
	2009-11-18 10:12	Source	[inbox]
		From → To	Terry@m57.biz --> Jo@m57.biz
		Subject	DVD Drive Fixed
		Body	Jo, I fixed the DVD Drive issue you told me about last night. I went ahead and replaced the drive. Please let me know if you have any further issues. Thanks, Terry
	2009-11-18	Source	[inbox]
	10:27	From → To	Jo@m57.biz --> Terry@m57.biz
		Subject	computer problem
		Body	Terry, Can you come by and take a look at my computer? It's gotten really slow all of a sudden. Thanks. Jo ----- From: Terry Sent: Wednesday, November 18, 2009 10:28 AM To: Jo Subject: RE: computer problem Jo, I'll stop by to check out the issue in a few minutes. Thanks, Terry IT Administrator, M57.biz terry@m57.biz 831-233-2883 ----- From: Jo Sent: Friday, November 20, 2009 9:55 AM To: Terry Subject: RE: computer problem

		<p>Terry,</p> <p>Did you fix my computer yet? It is still running way slow. Thanks.</p> <p>- Jo</p> <p>-----</p> <p>From: Terry Johnson Sent: Friday, November 20, 2009 9:57 AM To: Jo Smith Subject: RE: computer problem</p> <p>Jo,</p> <p>I'm coming over to your office in a little bit with a new computer to swap out for your broken down computer. I'll diagnose the problems from my desk.</p> <p>Thanks,</p> <p>Terry IT Administrator, M57.biz terry@m57.biz 831-233-2883</p> <p>-----</p> <p>From: Terry Sent: Friday, November 20, 2009 14:27 AM To: Jo Subject: RE: computer problem</p> <p>> Terry, > > My computer is working now. I guess I missed it the first time, but did > you swap my computer or just fix it? > > - Jo</p> <p>Jo,</p> <p>Yeah, it was corrupted, so I swapped it out.</p> <p>Terry IT Administrator, M57.biz terry@m57.biz 831-233-2883</p>
2009-11-19	Source	[Inbox/deleted]

	09:06	From → To	js9999sj@yahoo.com --> Jo@m57.biz
		Subject	hey
		Body	<p>hey Jo\, how's the new job working out? - Jordan</p> <p>-----</p> <p>Source: [Inbox/deleted] From: Jordan Sent: Thursday, November 19, 2009, 09:37 To: Jo Subject: RE: hey</p> <p>not bad. sorry to hear about your boss - that sucks. i got some work to do, but we'll talk later. Jordan</p> <p>From: Jo Smith <jo@m57.biz> To: Jordan Stanford <js9999sj@yahoo.com>-----t: Thu, November 19, 2009 9:08:42 AM Subject: Re: hey</p> <p>it's ok. my boss is kind of weird. I had to go get coffee the other day and he made me get some fruity and specific kind. other than that, it's alright. how are things with you? Jo</p>
	2009-11-19	Source	[Inbox]
	09:08	From → To	Pat@m57.biz --> Jo@m57.biz , Terry@m57.biz Charlie@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>

		Pat
2009-11-19 09:33	Source	[inbox]
	From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz
	Subject	Searches
	Body	<p>Jo, Charlie,</p> <p>how are your projects coming? Let's try to schedule a meeting for this afternoon or tomorrow morning to go over your status.</p> <p>Thanks Pat</p> <p>-----</p> <p>From: Charlie Sent: Thursday, November 19, 2009, 08:38 To: Pat, cc Jo Subject: RE: Searches</p> <p>I've been searching through a lot of patents. How about tomorrow at 10am for the meeting?</p> <p>Charlie</p> <p>-----</p> <p>From: Pat Sent: Thursday, November 20, 2009, 08:49 To: Charlie, cc Jo Subject: RE: Searches</p> <p>That will work for me.</p>
2009-11-19 09:42	Source	[Inbox]
	From → To	Pat@m57.biz --> Jo@m57.biz , Terry@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>
2009-11-19	Source		[inbox]
09:57	From → To		Pat@m57.biz , --> Charlie@m57.biz , Terry@m57.biz , Jo@m57.biz
	Subject		Lunch
	Body		<p>Anyone for lunch today?</p> <p>I'll be heading out at about noon. Going to try this new Basque place I found - cool !</p> <p>Pat</p> <p>-----</p> <p>From: Charlie Sent: Thursday, November 19, 2009, 08:38 To: Pat, cc Jo Subject: RE: Searches</p> <p>I've been searching through a lot of patents. How about tomorrow at 10am for the meeting?</p> <p>Charlie</p>
2009-11-20	Source		[inbox]
10:55	From → To		Pat@m57.biz , --> Jo@m57.biz , Charlie@m57.biz ,
	Subject		Invention
	Body		<p>Well,</p> <p>this one's certainly interesting... aquarium watch...</p> <p>Pat (Attached PETEFFS.pdf file)</p>
2009-11-20	Source		[Inbox]
11:08	From → To		Pat@m57.biz --> Jo@m57.biz , Terry@m57.biz Charlie@m57.biz
	Subject		Friday
	Body		Lunch.... Anyone ?

			Pat
2009-11-20	Source		[inbox]
14:29	From → To		Jo@m57.biz --> Pat@m57.biz
	Subject		Equipment Disposal
	Body		<p>Pat,</p> <p>My computer had to be swapped out today. I just want to make sure it is properly disposed of. There could be company information on there that we don't want to share with the rest of the world. Right?</p> <p>- Jo</p> <p>-----</p> <p>From: Pat Sent: Friday, November 20, 2009, 14:41 To: Terry, Jo Subject: RE: Equipment Disposal</p> <p>Jo,</p> <p>yes, I would be concerned about that too, thanks for thinking about that.</p> <p>Terry - what did you /are you going to/ do with Jo's computer?</p> <p>We need to make sure it is properly erased! Thank you.</p> <p>Pat</p> <p>-----</p> <p>From: Terry Sent: Friday, November 20, 2009, 14:43 To: Pat, Jo Subject: RE: Equipment Disposal</p> <p>Pat,</p> <p>I understand. Don't worry - I'll take care of everything.</p>

			Terry
2009-11-20	Source		[Sent Items/deleted]
14:48	From → To		Jo@m57.biz --> js9999sj@yahoo.com
	Subject		Oh man...
	Body		<p>----DY bgColor=#ffffff> Jordan,</p> <p>I almost had a big problem today. I had some of my pics on my work computer and the IT guy swapped it out because it was corrupted. The computer was running slow, so I thought he would just run an update or something. So I lost the pics. I contacted the boss to make sure the thing would get----posed of properly and he agreed. But man, that was a close call. My heart skipped a couple of beats...</p> <p>- Jo -----</p> <p>Source: [Inbox/deleted] From: Jordan Sent: Friday, November 20, 2009, 14:51 To: Jo Subject: RE: Oh man...</p> <p>Dude, that was a close call. You have to be more careful. I'll send you some stuff next week to help you out. Be more careful!</p> <p>Jordan</p>
2009-11-20	Source		[Inbox]
13:06	From → To		Charlie@m57.biz --> Jo@m57.biz
	Subject		RE: Docs
	Body		<p>Jo Smith wrote: > Charlie, > > > 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> <p>Jo,</p> <p>This is good stuff. Thanks for sending....Just keep passing on stuff like this.</p> <p>Charlie</p>
	2009-11-21 15:27	Source	[inbox]
		From → To	Pat@m57.biz , --> Jo@m57.biz , Charlie@m57.biz , Terry@m57.biz ,
		Subject	First week
		Body	<p>Dear Team,</p> <p>congratulations on our first week complete ! I have been really impressed with all of your work. We are off to a great start, and I think this M57.biz is on the fast track to being a great success. Thanks, and have a great weekend.</p> <p>Pat</p>
	2009-11-23	Source	[] The initial email was deleted but from the remaining emails in [deleted] we could find it
	10:16:35	From → To	js9999sj@yahoo.com --> Jo@m57.biz
		Subject	useful tools
		Body	<p>Jo,</p> <p>Here is a useful tool for your pics. It's an executable---- file, so you don't need to install anything (in case your IT admin won't allow it). Just run the program and make sure the mask is large enough. I also attached an example file. The decode password is "password:" and just set the destination name as test.bmp. try it out and let me know if you have any questions. Also, make sure to remane your pics to something innocuous!!! no need to draw attention to yourself.</p> <p>- Jordan</p> <p>-----</p> <p>Source: [Inbox/deleted] From: Jordan Sent: Monday, November 23, 2009, 10:07 To: Jo</p>

		<p>Subject: useful tools</p> <p>Attached files: diit-1.5.jar, test.png -----</p> <p>Source: [Sent Items/deleted] From: Jo Sent: Monday, November 23, 2009, 10:24 To: Jordan Subject: RE: useful tools</p> <p>thanks. I will try it out. - Jo -----</p> <p>Source: [Sent Items/deleted] From: Jo Sent: Monday, November 23, 2009, 10:26 To: Jordan Subject: RE: useful tools</p> <p>cool! It's a car----sp; this is nice - I will definitely use this from now on. - Jo -----</p> <p>Source: [Sent Items/deleted] From: Jo Sent: Tuesday, December 01, 2009, 08:52:32 To: Jordan Subject: RE: useful tools</p> <p>hey Jordan. this thing is kind of slow. do you have any faster ones or am I doing something wrong? - Jo -----</p> <p>Source: [Inbox/deleted] From: Jordan Sent: Thursday, December 03, 2009, 09:28:09 To: Jo Subject: RE: useful tools</p> <p>Jo -</p> <p>Sorry - didn't check my email for a few days. Is the cover image really big? how about the----ge you want to hide? There are some other ones I can check out. In the mean time, you may want to try truecrypt.</p> <p>http://www.truecrypt.org/ It's pretty self-explanatory.</p>
--	--	--

			<p>- Jordan</p> <p>-----</p> <p>Source: [Sent Items/deleted] From: Jo Sent: Thursday, December 03, 2009, 13:01 To: Jordan Subject: RE: useful tools</p> <p>Wow! this thing is great. I can't believe it's this easy. Thanks!</p> <p>- Jo</p>
2009-11-24	Source		[Inbox]
10:40	From → To		Pat@m57.biz --> Jo@m57.biz , Terry@m57.biz Charlie@m57.biz
	Subject		Holiday
	Body		<p>Dear Team,</p> <p>things are progressing well this week. I do want to meet with Jo and Charlie at some point (just pop in when convenient) today, but otherwise let's take the rest of the week off for the Holiday.</p> <p>Thanks for all your hard work; enjoy.</p> <p>Pat</p> <p>-----</p> <p>Source: [Sent Items] From: Jo Sent: Tuesday, November, 24, 2009, 14:03 To: Pat Subject: RE: Holiday</p> <p>Thanks Pat. You are an awesome boss.</p> <p>- Jo</p>
2009-11-25 16:08	Source		[Inbox]
	From → To		Pat@m57.biz --> Jo@m57.biz , Charlie@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</p>

			<p>short vacation start having a look at it. This is with a new company, so let's impress them !</p> <p>Thanks Pat</p> <p>-----</p> <p>From: Charlie Sent: Monday, November 30, 2009, 08:46 To: Pat, cc Jo Subject: RE: New business</p> <p>I'll start looking into this. Did everyone have a good weekend?</p>
2009-11-30	Source		[Sent Items]
08:54	From → To		Jo@m57.biz --> Charlie@m57.biz
	Subject		teleporter
	Body		<p>Hey Charlie,</p> <p>Found this patent for teleportation. What do you think?</p> <p>- Jo</p> <p>Attached file: US5041044.pdf</p>
2009-11-30	Source		[Inbox]
09:07	From → To		Pat@m57.biz --> Jo@m57.biz , Terry@m57.biz , Charlie@m57.biz
	Subject		This week
	Body		<p>Dear Team,</p> <p>welcome back ! I trust everyone had a great albeit brief vacation.</p> <p>OK, so time to get back to work ! We have a lot on our plates; let's knock these projects out of the football park.</p> <p>I want to meet with each of you today, just come by at your leisure. I want to see where we're at, especially with the first two projects. We need to start preparing the deliverables on those soon.</p> <p>Thanks, Pat</p>

2009-11-30	Source		[Inbox]
09:49	From → To		Terry@m57.biz --> Pat@m57.biz , Jo@m57.biz , Charlie@m57.biz
	Subject		Printed Installed
	Body		<p>Everyone,</p> <p>I setup and installed the new printer today on the network. It should be running smoothly. If you are having any problems with the printer, then shoot me an email.</p> <p>Thanks,</p> <p>Terry IT Administrator, M57.biz terry@m57.biz</p>
2009-12-01	Source		[inbox]
10:47	From → To		Pat@m57.biz , --> Jo@m57.biz , Charlie@m57.biz ,
	Subject		Lunch/coffee
	Body		<p>Anyone for lunch today?</p> <p>Jo, we're almost out of coffee! Need to do another trip soon...</p> <p>Pat -----</p> <p>Source: [Sent Items] From: Jo Sent: Tuesday, December 01, 2009, 11:53 To: Pat, cc Charlie, Terry Subject: RE: Lunch/coffee</p> <p>Sure. Any requests?</p>
2009-12-02 13:53	Source		[Inbox]
	From → To		Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz (With High Importance)
	Subject		New project
	Body		Jo, Charlie,

			<p>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.</p> <p>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.</p> <p>Thanks Pat</p> <p>-----</p> <p>Source: [Sent Items] From: Jo Sent: Tuesday December 3, 2009, 08:51 To: Charlie Subject: RE: New project</p> <p>Do you want this one? I was looking for that teleporter thing.</p> <p>- Jo</p> <p>-----</p> <p>From: Charlie Sent: Tuesday December 3, 2009, 08:52 To: Pat, cc Jo Subject: RE: New project</p> <p>I can start looking at it.</p> <p>Charlie</p>
2009-12-03	Source		[inbox]
13:58	From → To		Terry@m57.biz --> Charlie@m57.biz Jo@m57.biz
	Subject		Fw: GGworld For You
	Body		<p>Did you guys see this? It is so funny!</p> <p>----- Original Message -----</p> <p>From: Pat McGoo To: terry@m57.biz Sent: Thursday, December 03, 2009 9:46 AM Subject: Fw: GGworld For You</p> <p>Terry,</p>

			<p>I got this email today - it looks like a really good deal - what do you think? Perhaps we could all go in together on this, and make some money to fund more inventions !</p> <p>This is exciting.</p> <p>Pat</p> <p>----- Original Message ----- From: Jasper McRachelvick To: pat@m57.biz Sent: Thursday, December 03, 2009 9:42 AM Subject: GGworld For You</p> <p>Dear Sir,</p> <p>may I intorduce miself. I am Mr. Jasper McRachelvick, esquire, of the commonwealth of the nederlanden. I am experiencing a newly once and lifetime chance of renewing contracts for tar-paving in the country. The leader of the business, a Mr. M. Zimberstern, has agreed to contract for very good prices if my company is able to produce a downpayment on new equipment. This project is expected to return some twelve hundred percent on all investments ! I would like to offer you the opportunity to invest in this endeavor. Your contribution of 25,000 U.S. dollars will ensure a return, with 6 months, of your original investment plus 25,000 each quarter after dat for 12. It is superb great deal !! Please send me your return informatoin, and my secretary will be contacting you very soonest.</p> <p>Best regards, Jasper McRachelvick Business leader</p> <p>----- From: Charlie Sent: Friday, December 4, 2009, 08:49 To: Terry, cc Jo Subject: Re: Fw: GGworld For You</p> <p>Ha ha! I always thought Pat was a little lacking upstairs.</p>
--	--	--	--

	2009-12-04 09:16		
		Source	[Inbox]
		From →	Jo@m57.biz -->
		To	Pat@m57.biz
		Subject	Teleporter Patent Info
	2009-12-04 09:22	Body	<p>Pat,</p> <p>Here is some information on the teleporter you asked for.</p> <p>- Jo</p> <p>Attached File: US5041044.PDF (retrieved by [Outbox/deleted] and in [Sent Items])</p> <p>-----</p> <p>From: Pat Sent: Friday, December 7, 2009, 08:59 To: Jo Subject: Re: Teleporter Patent Info</p> <p>Thanks Jo, good work. Give me a day or so to go over it, we can finalize some issues later in the week.</p> <p>Regards, Pat</p>
		Source	[Inbox]
		From →	Terry@m57.biz -->
		To	Pat@m57.biz , cc Charlie@m57.biz , Jo@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 -----</p> <p>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 09:42	Source		[Inbox]
	From →		Pat@m57.biz -->
	To		Jo@m57.biz
	Subject		Meeting
	Body		<p>Jo,</p> <p>please stop by today before lunch, I want to go over some of your research with you.</p> <p>Thanks, Pat</p>
2009-12-07	Source		[Inbox]
12:56	From →		Charlie@m57.biz -->
	To		Pat@m57.biz , Terry@m57.biz , Jo@m57.biz
	Subject		Great Lunch
	Body		<p>I just had a great lunch at this little place down the street. The spicy catfish was just perfect. Highly recommended.</p>
2009-12-10	Source		[inbox]
14:11	From →		Pat@m57.biz , -->
	To		Terry@m57.biz cc Jo@m57.biz
	Subject		Computer Serial Number
	Body		<p>Terry,</p> <p>is this serial number from that computer Jo used to have? C1111</p> <p>Pat</p>
2009-12-10	Source		[Sent Items/Deleted]
14:15	From →		Jo@m57.biz -->
	To		js9999sj@yahoo.com
	Subject		advice?
	Body		<p>Hey Jordan. I need some advice. My boss is asking questions about my old computer - the one that had to be replaced. He's asking about the serial</p>

			<p>number. I'm sure it's not a big deal, but should I take any additional precautions?</p> <p>- Jo</p> <p>-----</p> <p>Source: [Inbox/deleted] From: Jordan Sent: Thursday, December 10, 2009, 14:20 To: Jo Subject: Re: advice?</p> <p>Jo -</p> <p>&nb----/DIV></p> <p>Well, that IT guy said he scrubbed it before getting rid of it, right? So you are probably ok. And you have True Crypt installed now, right? Just make sure your password is something a hard - don't make it your name or something stupid. I think with True Crypt you can even use a file as the password.</p> <p>- Jordan</p>
	2009-12-11	Source	[inbox]
	08:56	From → To	Pat@m57.biz , --> Charlie@m57.biz Jo@m57.biz
		Subject	Important meeting
		Body	<p>Team,</p> <p>we are going to have a meeting first thing this morning. As soon as you get in please come in to the conference room. I received a call yesterday from the Police - they are going to be here to talk to us.</p> <p>Pat</p>
Considerations	<ul style="list-style-type: none"> - Fortunately, a suspected DBX file was not protected and encrypted with a password. - DBX file parsing → Inbox, Deleted Items, Contacts... - Deleted e-mail recovery from unused area of DBX file. 		

List external storage devices attached to PC.

	Device Name	Volume Name	Serial No.	First Connected Time	Connected Time After Reboot
Possible Answer (Timezone is applied)	USB 2.0 Flash Disk USB Device		51491E64	2009-11-20 10:33:25	2009-11-23 13:54:45
	Generic Flash Disk USB Device		2B9ECCFF	2009-11-24 14:01:50	2009-11-24 14:01:50
	Imation USB Flash Drive USB Device		AADA04411400000B	2009-12-10 14:41:17	2009-12-10 14:41:17
Considerations	- C:\Windows\inf\setupapi.dev.log - HKLM\SYSTEM\ControlSet001\Enum\USBSTOR\~ - HKLM\SYSTEM\MountedDevices\ - HKCU\Jo\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\ - Volume name information is not available on Windows XP.				

Identify all traces related to ‘renaming’ of files in Windows Desktop.

(It should be considered only during a date range between 2009-12-09 and 2009-12-12.)

[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.]

	Timestamp	USN	Path	Event
Possible Answer (Timezone is applied)	2009-12-10 14:41:45	52049632	C:\Documents and Settings\Jo\Desktop\New Folder	Renamed Old
		52049784	C:\Documents and Settings\Jo\Desktop\Papers	Renamed New
	2009-12-10 14:43:53	53592496	C:\Documents and Settings\Jo\Recent\Hidden.lnk	Renamed Old
		53592664	C:\System Volume Information_restore{B467CED3-3B47-4617-B471-E2E64806610B}\RP37\A0001380.lnk	Renamed New
	2009-12-11 08:41:12	54384968	C:\Documents and Settings\Jo\Desktop\Pics	Renamed Old
		54385112	C:\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc2	Renamed New
	2009-12-11 08:41:12	54385184	C:\Documents and Settings\Jo\Desktop\newFiles	Renamed Old
		54385336	C:\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc2	Renamed New
Considerations	- \Extend\UsnJrnl:\$J - \MFT - \LogFile			

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

Possible Answer	192.168.1.1
Considerations	<p>HKCU\Jo\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\ > timestamp: 2009-11-20 16:07:03 > value: a > data: \\192.168.1.1\m57</p> <p>HKCU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\ > timestamp: 2009-11-20 16:06:46 > value: a > data: \\192.168.1.1\m57</p>

List all directories that were traversed in 'E:'.

	Timestamp	Directory Path	Source
Possible Answer (Timezone is applied)	2009-12-03 12:49:08	E:\Pics\	ShellBag (created)
	2009-12-03 12:49:08	E:\Pics\Hidden\	ShellBag (created)
	2009-12-03 12:49:08	E:\Pics\Patents\	ShellBag (created)
	2009-12-03 12:49:08	E:\Pics\New Patents\	ShellBag (created)
		E:\Pics\	ShellBag (last accessed)
	2009-12-10 14:43:51	E:\Pics\Hidden\	ShellBag (last accessed)
		E:\Pics\Patents\	ShellBag (last accessed)
		E:\Pics\New Patents\	ShellBag (last accessed)
Considerations	- 'Timestamp' may not be accurate. - 'Patents' & 'New Patents' also exist in Desktop\Pics		

List all files that were opened in 'E:'.

	Timestamp	Directory Path	Source
Possible Answer (Timezone is applied)	2009-12-03 12:50:09	E:\Pics\Hidden\patent01.JPG	Recent Documents
	2009-12-10 14:43:53	E:\Pics\Hidden\patent03.JPG	Recent Documents
Considerations	- C:\Documents and Settings\Jo\Recent		

List all directories that were traversed in the company's network drive Z:\.

	Timestamp	Directory Path	Source
--	-----------	----------------	--------

Possible Answer (Timezone is applied)	2009-12-04 18:31:46	\\192.168.1.1\m57\ram\windd\32bits_i386	ShellBag (created)
Considerations	- 'Timestamp' may not be accurate. - Z:\ is mapped on \\192.168.1.1\m57 - That directory was traversed by us.		

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

Possible Answer (Timezone is applied)	Timestamp	Directory Path	Source
Considerations	- We could not find anything.		

Find traces related to cloud services on PC.

(Service name, log files...)

Possible Answer	Cloud Service	Type	Traces
Considerations	- We could not find anything.		

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		Modified Time
Considerations	- We could not find anything.		

What kinds of data were stored in Windows Search database?

Possible Answer	
Considerations	- We could not find anything.

Παράρτημα Ε - Ανάλυση δίσκου & USB

Αρχείο	MD5 Hash
C:\Documents and Settings\Jo\Desktop\newFiles2	b88878b692f2d7e0294f92ec41d6027f
C:\Documents and Settings\Jo\Desktop\Papers\Papers10\12097.RPCs.Fernando+Loring.pdf	8a4964b39ef4dcacc6eef5d12619e1b2
C:\Documents and Settings\Jo\Application Data\TrueCrypt\Configuration.xml	56d947a6f848d0fe10efc1afdf50c750
E:\Pics\diit-1.5.jar	dc6a4cd2af804f2dd69dcd4f9b524a70
E:\Pics\test.png	366076e5436a184e5757cf4490fa821e
E:\Pics\testHide.bmp	357f27379673b5ed1669ae250d23ced7
E:\Pics\Patents\patent001.PNG	92f0390b061fb5f1bfa3f341c8d32088
E:\Pics\Hidden\patent01.JPG	41707a9e62ed87c0723213578cd7cb5c
E:\Pics\Hidden\patent02.JPG	8df15d6a0c673d94bcf1f40e5c4669a8
E:\Pics\Hidden\patent03.JPG	b9e0d7f8502c46652d6bb67fe3979850
E:\Pics\Hidden\patent04.JPG	4d4f507879f85cc4c5bb6d9567cce7c1
E:\Pics\Hidden\patent05.JPG	ac0aceb421b7aa71b878ecc6bf946dad
E:\Pics\Hidden\patent06.JPG	26e683226ccdd689f6edd8d79c419030
E:\Pics\Hidden\patent07.JPG	da0be16faab79674096bbb142c6015cd
E:\Pics\Hidden\patent08.JPG	e429a1a19559107884431abfc2f5c159
E:\Pics\Hidden\patent09.JPG	26dc9d006f0aea72db0f5d602dd06833
E:\Pics\Hidden\patent10.JPG	1d2c66844fd363eb4c677fcb80fa6783
E:\Pics\Hidden\patent11.JPG	3676c8916bec14eac4fe377c1ef25033
E:\Pics\Hidden\patent12.JPG	7734fa2a037501a0d286141b84cd8b0b
E:\Pics\Hidden\patent13.JPG	5012306bfe33494c3f3e50c51e4c753e
E:\Pics\Hidden\patent14.JPG	3367461d85a41cf267d2b33d2ed2c9d9
E:\Pics\Hidden\patent15.JPG	d28dcc8cb60483bed6eadf464d4ffb8b
E:\Pics\Hidden\patent16.JPG	c832ce3275473723e188909c02503d34
E:\Pics\Hidden\patent17.JPG	7f21345d5a867e4898cf1785c7fb89a8
E:\Pics\Hidden\patent18.JPG	ddbba5be529b7f05c2cf95904ccc69fa
E:\Pics\Hidden\patent19.JPG	9db3bd1347796079fb958fb42db5f9a6
E:\Pics\Hidden\patent20.JPG	56855f3dc79ee8cb0f9b4c52ce7c002a
E:\Pics\Hidden\patent21.JPG	fb8e23314716e0df49d8a63ceaabca59
E:\Pics\Hidden\patent22.JPG	c6b895ce0ed359a4acd8da35dd0bb58e
E:\Pics\Hidden\patent23.JPG	fa3054835b64bbe95f2e0d68da4ea37e
E:\Pics\Hidden\patent24.JPG	fcda34e4b47464fb628d9dbe24bfb7d7
E:\Pics\Hidden\patent25.JPG	27f1fabab6626df5acf1415ad077159e
E:\Pics\Hidden\patent26.JPG	a15dbf3f674bd2374e18656d5ce597eb
E:\Pics\Hidden\patent27.JPG	e4b01acd9b3636dfe0d2f4296fbb0fc4
E:\Pics\Hidden\patent28.JPG	343368e62aef7ea0dcb1acd380f9fba

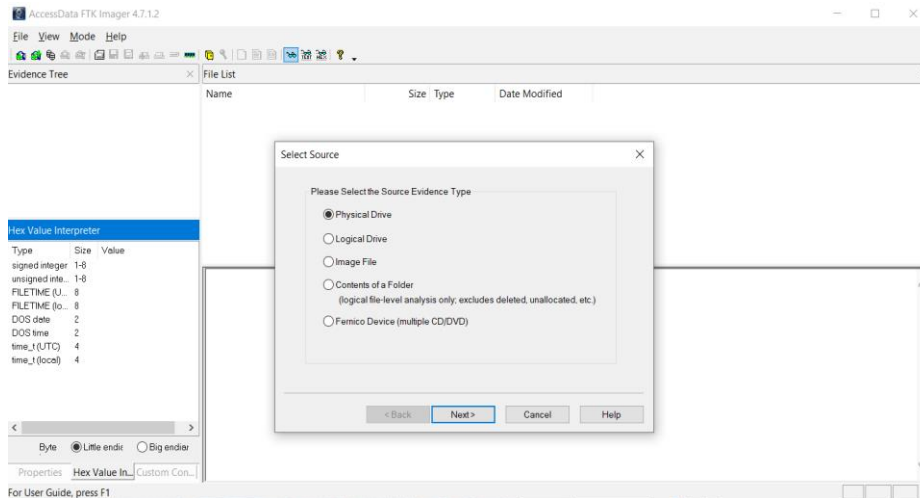
E:\Pics\Hidden\patent29.JPG	457a63bb2e78aad474ef8769c0c7df52
E:\Pics\Hidden\patent30.JPG	7c18169b43df55372b77fdc1e2f6bf1a
E:\Pics\Hidden\patent31.JPG	ac853d62e09f01e0eead8e72f0949265
E:\Pics\Hidden\patent32.JPG	c0eeb5e2b19798744de9ef9637d9df91
E:\Pics\Hidden\patent33.JPG	cc24b8438b7bd56840aadf8d461e6393
E:\Pics\Hidden\patent34.JPG	c462f74d41985e1b34b47b621a329d0e
E:\Pics\Hidden\patent35.JPG	c6ca89b8e82c38fb3596efe12939b011
E:\Pics\Hidden\patent36.JPG	e9fb41a9cc22e178b5f32bc4653fe23a
E:\Pics\Hidden\patent37.JPG	fbf97ea41be456b66a67b73422435f12
E:\Pics\Hidden\patent38.JPG	48807a261075c570d95ddd414bd7efed
E:\Pics\Hidden\patent39.JPG	e04bf2a9ff810d64fc1b3af9434db4e0
E:\Pics\Hidden\patent40.JPG	d34f7a82b7a6b4085ba0e47ad186612a
E:\Pics\Hidden\patent41.JPG	66b70d793c8d12b83c71bd77281922f4
E:\Pics\Hidden\patent42.JPG	b374ae60106eaf6f03c671de33d92c8f
E:\Pics\Hidden\patent43.JPG	e0fb109599cfc477215e531196c97367
E:\Pics\Hidden\HighQuality\hr_patent01.JPG	1dd00f2e51aeebe7541cea4ade2e20b5
E:\Pics\Hidden\HighQuality\hr_patent02.JPG	6af8563ce22a5583d05e0bfd08dd0c45
E:\Pics\Hidden\HighQuality\hr_patent03.JPG	f8cf8a0bcba85dabd154d6b68cd42faa
E:\Pics\Hidden\HighQuality\hr_patent04.JPG	b1230dac0bf7d83f49689c2fd0780e5c
E:\Pics\Hidden\HighQuality\hr_patent05.JPG	f90ec99b6526d2cb9af28b3b9dc11ccd
E:\Pics\Hidden\HighQuality\hr_patent06.JPG	24e75f2c16005106b48727f585907505
E:\Pics\Hidden\HighQuality\hr_patent07.JPG	5461e5442ef570b8cf5df6aecfc810d5
E:\Pics\Hidden\HighQuality\hr_patent08.JPG	f99b749cbffd302e0bb6ad978cd9fa37
E:\Pics\Hidden\HighQuality\hr_patent09.JPG	acf7540e7b25b6615acb9fe157c2f840
E:\Pics\Hidden\HighQuality\hr_patent10.JPG	42d13827189a207e3d2daa0373d4f6ec
E:\Pics\Hidden\HighQuality\hr_patent11.JPG	faf3f87f9788af223b031ffb7e25a832
E:\Pics\Hidden\HighQuality\hr_patent12.JPG	88750ffb5ebdf1d61d34e571c1bf03b1
E:\Pics\Hidden\HighQuality\hr_patent13.JPG	c08c85eda6073c22e783971d0c8164da
E:\Pics\Hidden\HighQuality\hr_patent14.JPG	fbe1e0d871926f1559be0c0b1c42e642
E:\Pics\Hidden\HighQuality\hr_patent15.JPG	77e8f7f4b47c9b994673cea3e9d5493e
E:\Pics\Hidden\HighQuality\hr_patent16.JPG	d13316f10bb7ba29c3a7ca0ab2d1f64b
E:\Pics\Hidden\HighQuality\hr_patent17.JPG	6ec30ca3eab6aacd4c80a7d0a2e5e556
E:\Pics\Hidden\HighQuality\hr_patent18.JPG	6c7220b4f726c2d35ebb7869119c13c0
E:\Pics\Hidden\HighQuality\hr_patent19.JPG	4f7e7ac5dba27537a2aed65e2cb6f9b9
E:\Pics\Hidden\HighQuality\hr_patent20.JPG	2bda1806540188fe66ea1184941f1f0b
E:\Pics\Hidden\HighQuality\hr_patent21.JPG	4314a4a4a4056d9806ea4b2744b9d7f0
E:\Pics\Hidden\HighQuality\hr_patent22.JPG	b60c2e59c1dc2f72904c9db6fc5be579
E:\Pics\Hidden\HighQuality\hr_patent23.JPG	96a17649ebba181a80d01d2f0acbc68d
E:\Pics\Hidden\HighQuality\hr_patent24.JPG	a22331bb482a6e8ff86e20b419cfce85
E:\Pics\Hidden\HighQuality\hr_patent25.JPG	ac30bbacbf138bf0ab2570b5f2236418

E:\Pics\Hidden\HighQuality\hr_patent26.JPG	0cb35a5132a44d88f86d658dc1119247
E:\Pics\Hidden\HighQuality\hr_patent27.JPG	8c7c12c12568848a7dda22e010e7ed1f
E:\Pics\Hidden\HighQuality\hr_patent28.JPG	6c93cbbe0944f63488c9da2c49ab65f8
E:\Pics\Hidden\HighQuality\hr_patent29.JPG	d34638b0f8f8241433ae550ecd6fdcaa
E:\Pics\Hidden\HighQuality\hr_patent30.JPG	e8af6ed9337b17d2273dee0c9e67a2ff
E:\Pics\Hidden\HighQuality\hr_patent31.JPG	682e08d29708e944318b3f41eb2be995
E:\Pics\Hidden\HighQuality\hr_patent32.JPG	1b6ca277955778b941111273cfb1688b
E:\Pics\Hidden\HighQuality\hr_patent33.JPG	5d357df02bf4642700d1c00ddd33e237
E:\Pics\Hidden\HighQuality\hr_patent34.JPG	31fbad29da748a5565e3fff2ac2fbedc
E:\Pics\Hidden\HighQuality\hr_patent35.JPG	aeeba1f87911ed0612cfe928fef6a45
E:\Pics\Hidden\HighQuality\hr_patent36.JPG	bb5ca88e16e5feb6d6429832a0fdb078
E:\Pics\Hidden\HighQuality\hr_patent37.JPG	82ac80415cc8b726a039f318d1e60640
E:\Pics\Hidden\HighQuality\hr_patent38.JPG	12e7d2d02e861a2e750d4cabb1bb8258
E:\Pics\Hidden\HighQuality\hr_patent39.JPG	5bbdd58f906d9a2b2fdb4b8afc8c91be
E:\Pics\Hidden\HighQuality\hr_patent40.JPG	25566a2aec959d3ad15a540e5987b63f
E:\Pics\Hidden\HighQuality\hr_patent41.JPG	71d91612ed2b1559c444f3fc768f9000
E:\Pics\Hidden\HighQuality\hr_patent42.JPG	22a6dab3380087356b7271a1ecb730fc
E:\Pics\Hidden\HighQuality\hr_patent43.JPG	5bd90d1d6941f8c8763562578c61c11a
E:\Pics\Hidden\HighQuality\hr_patent44.JPG	977a311ada6a94becc9696e4dc9fa3ed
E:\Pics\Hidden\HighQuality\hr_patent45.JPG	639ef9a273043e3d3545ae479590f974
E:\Pics\Hidden\HighQuality\hr_patent46.JPG	a560befd331d1f42a371ba526c2a5fff
E:\Pics\Hidden\HighQuality\hr_patent47.JPG	78efa86dd183fb11f54870765913f6d2
E:\Pics\Hidden\HighQuality\hr_patent48.JPG	0b1ae52267e29eb3e262d32553226843
E:\Pics\Hidden\HighQuality\hr_patent49.JPG	b1ee6681fa420932319b75bd1e36eb21
E:\Pics\Hidden\HighQuality\hr_patent50.JPG	5503b07a7c5359cc0065af949521a82e
E:\Pics\Hidden\HighQuality\hr_patent51.JPG	6290743a27a7e3f7fbb8a30d3ea6b978
E:\Pics\Hidden\HighQuality\hr_patent52.JPG	47fc7ba4ff774f34c962936eb1523b67
E:\Pics\Hidden\HighQuality\hr_patent53.JPG	821fec5584d6879176ed8e2a0f603bc2
E:\Pics\Hidden\HighQuality\hr_patent54.JPG	46b650c5057da784fab52bf444a412ce
E:\Pics\Hidden\HighQuality\hr_patent55.JPG	8c3145b9d0e42dcfe87d17213555b18b
E:\Pics\Hidden\HighQuality\hr_patent56.JPG	0962d93fcf9ac8cba46725817fa44124
E:\Pics\Hidden\HighQuality\hr_patent57.JPG	dd35ef460699754825dbb9b70b2e72c8
E:\Pics\Hidden\HighQuality\hr_patent58.JPG	9bb1e562859f26e06aac10cc33ee9ea4
E:\Pics\Hidden\HighQuality\hr_patent59.JPG	96d19f2a725664591fe7796b6d72b799
E:\Pics\Hidden\HighQuality\hr_patent60.JPG	1fd631ac140fbbe1a40003ec3dd385ae
E:\Pics\Hidden\HighQuality\hr_patent61.JPG	3832c7903a995df4254baa3eca9e4bd7
E:\Pics\Hidden\HighQuality\hr_patent62.JPG	9a5364a26ac26d44d678d473774a5b97
E:\Pics\Hidden\HighQuality\hr_patent63.JPG	d994947181a7d60704f70f74d61b7421
E:\Pics\Hidden\HighQuality\hr_patent64.JPG	4f33d26ea0d47ea17cedd5067549d3fa
E:\Pics\Hidden\HighQuality\hr_patent65.JPG	9da06941e3eec2a2f19d20b0a0cf21ed

E:\Pics\Hidden\HighQuality\hr_patent66.JPG	1018f333d3eec3a90cc8c3eb1824455c
E:\Pics\Hidden\HighQuality\hr_patent67.JPG	259acd4e434c8836ae1eb8069b5f36f1
E:\Pics\Hidden\HighQuality\hr_patent68.JPG	bf44428dafc755aa57f38036aaa79ada
E:\Pics\Hidden\HighQuality\hr_patent69.JPG	34a248ffbc03c1b96e2225b788f71fd6
E:\Pics\Hidden\HighQuality\hr_patent70.JPG	67d55dd34df85cf719815085abd3d791
E:\Pics\Hidden\HighQuality\hr_patent71.JPG	43cfc2daf0ece60e9d944bc6ca980711
E:\Pics\Hidden\HighQuality\hr_patent72.JPG	a003a6d4fe290c9dfec624bc85714357
E:\Pics\Hidden\HighQuality\hr_patent73.JPG	bb6e0d23b12a26d23dfbcffa45b84a89
E:\Pics\Hidden\HighQuality\hr_patent74.JPG	e02ea82a5b0026315c2fc09ac4e2b07f
E:\Pics\Hidden\HighQuality\hr_patent75.JPG	0e8198723a5b907b6e63775f7860a09b
E:\Pics\Hidden\HighQuality\hr_patent76.JPG	51820571527fec74620fb4267263095a
E:\Pics\Hidden\HighQuality\hr_patent77.JPG	74f5d3efceb55c97aad22b80ad5940c0
E:\Pics\Hidden\HighQuality\hr_patent78.JPG	356b8b48ae6347d97812c753e3ce6898
E:\Pics\Hidden\HighQuality\hr_patent79.JPG	6dd8b686b9ae92ab42dd13de438a3018
E:\Pics\Hidden\HighQuality\hr_patent80.JPG	75cf887f54352a236b9ac0c3390c1b0c
E:\Pics\Hidden\HighQuality\hr_patent81.JPG	c4356c212ab7c3b6823563b0a86bf4f9
E:\Pics\Hidden\HighQuality\hr_patent82.JPG	1c8e78ed45253d6608c324165ffc2479
E:\Pics\Hidden\Videos\Cat.m4v	569136edd90a1abf74a858b9d822c134
E:\Pics\Hidden\Videos\Cat.mov	3bf06fd991c312bd852c5f7b84d78174
E:\Pics\Hidden\Videos\KittyMontage.mov	7d4058485071e25d482fd18fb2ac58bd
E:\Pics\Hidden\Videos\MontereyKitty.m4v	fb422a6213606d4a2a5d7e471e75fb46
E:\Pics\Hidden\Videos\MontereyKittyHQ.m4v	6d8481b35bbf65bd2580a267f2a04af5
E:\Pics\Hidden\Videos\TiggerTheCat.m4v	1ff00fa337ad8b964729eb4573ea5a6c

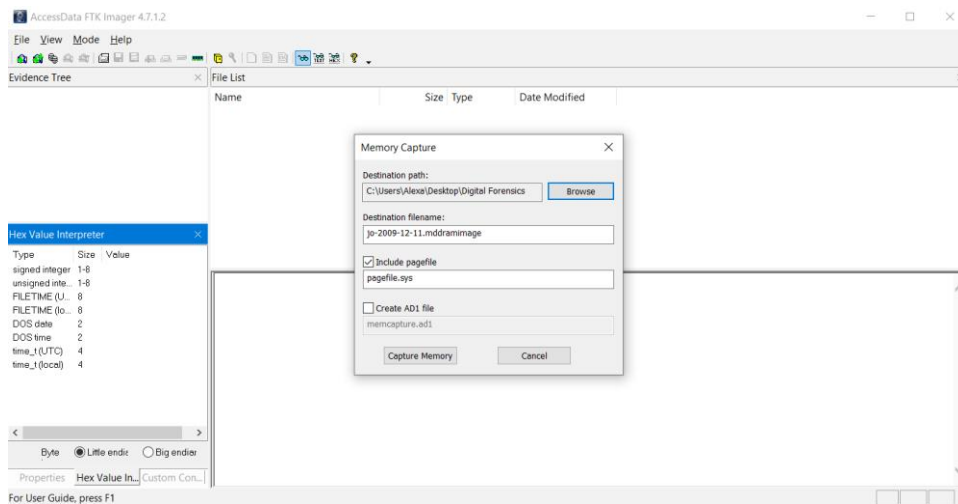
Ο δίσκος E: ήταν κρυπτογραφημένος με το εργαλείο TrueCrypt και κωδικό κρυπτογράφησης το αρχείο 12097.RPCs.Fernando+Loring.pdf.

Παράρτημα ΣΤ - Αντίγραφο μνήμης



4 τρόπος λήψης αντιγράφου δίσκου H/Y και USB flash drive

(ΣΤ-1)

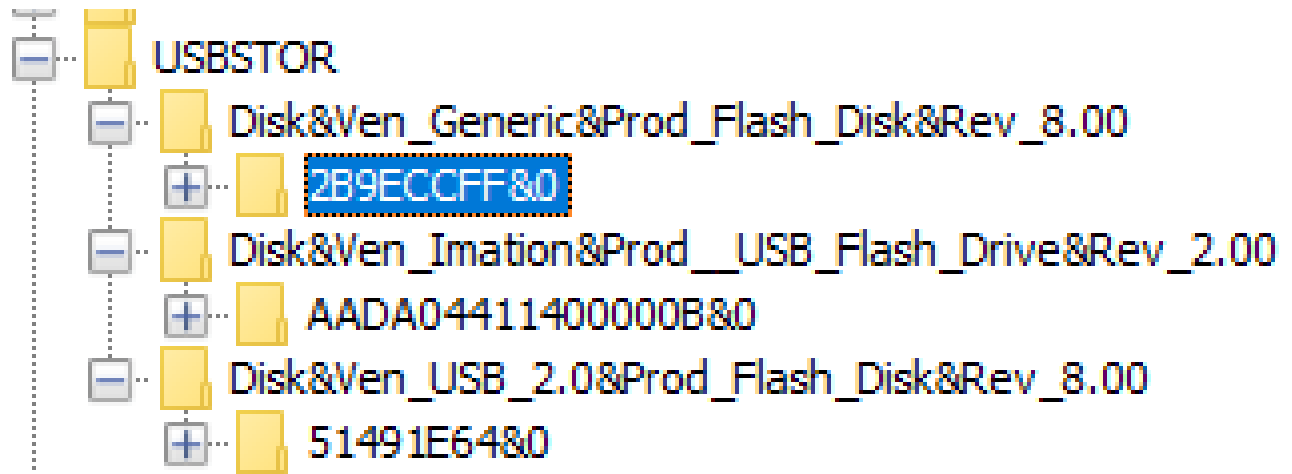


5 τρόπος λήψης αντιγράφου μνήμης H/Y

(ΣΤ-2)











Παράρτημα Z - Screenshots forensics εργασιών ΑΕΓ

Παρακάτω παρατίθεται ένα σύνολο εικόνων (στιγμιότυπα οθόνης) που αντιπροσωπευτικά υποστηρίζουν σε διάφορα σημεία την ανάλυσή μας και αποτελούν αναπόσπαστο υλικό των συμπερασμάτων μας.



Z-1 (Ιστορικό συσκευών που έχουν συνδεθεί στον Υπολογιστή)

Save Table as CSV

Source Name	S	C	O	△ Date/Time	Device Make	Device Model	Device ID	Data Source
 system			0	2009-11-20 19:55:41 EET	Dell Computer Corp.	Model L100 Keyboard	5&2f6f8af0&0&1	jo-2009-12-11-002.E01
 system			0	2009-11-20 19:55:42 EET	Dell Computer Corp.	Mouse	5&2f6f8af0&0&2	jo-2009-12-11-002.E01
 system			0	2009-11-23 23:54:44 EET	Alcor Micro Corp.	Flash Drive	51491E64	jo-2009-12-11-002.E01
 system			0	2009-11-25 00:01:49 EET		Vid_0000&Pid_7777	2B9ECCFF	jo-2009-12-11-002.E01
 system			0	2009-12-11 00:41:16 EET	Imation Corp.	Flash Drive	AADA04411400000B	jo-2009-12-11-002.E01
 system			0	2009-12-11 21:04:47 EET		ROOT_HUB	4&389651e0&0	jo-2009-12-11-002.E01
 system			0	2009-12-11 21:04:48 EET		ROOT_HUB	4&28fef180&0	jo-2009-12-11-002.E01
 system			0	2009-12-11 21:04:48 EET		ROOT_HUB	4&5e88044&0	jo-2009-12-11-002.E01
 system			0	2009-12-11 21:04:48 EET		ROOT_HUB20	4&36326108&0	jo-2009-12-11-002.E01
 system			0	2009-12-11 21:04:51 EET	Logitech, Inc.	Optical Wheel Mouse	5&2f6f8af0&0&1	jo-2009-12-11-002.E01

Z-2 (φαίνονται πληροφορίες σχετικές με το USB που βρέθηκε στο γραφείο του πιθανού δράστη)

Listing									
Web History									
3984 Res									
Table Thumbnail Summary									
Save Table as CSV									
Source Name	S	C	O	URL	Date Accessed	Title	Program Name		
places.sqlite			0	http://en-us.start3.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official	2009-12-03 02:09:54 EET	firefox	FireFox Analyzer	n	
places.sqlite			0	http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official	2009-12-03 18:51:24 EET	Mozill...	FireFox Analyzer	g	
places.sqlite			0	http://en-us.start3.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official	2009-12-03 18:51:29 EET	firefox	FireFox Analyzer	n	
places.sqlite			0	http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official	2009-12-03 19:00:09 EET	Mozill...	FireFox Analyzer	g	
places.sqlite			0	http://www.google.com/*****	2009-12-03 19:00:25 EET	404 N...	FireFox Analyzer	g	
places.sqlite			0	http://www.google.com/docCrawler%20will%20discover%20documents%20for%201...	2009-12-03 19:02:21 EET	404 N...	FireFox Analyzer	g	
places.sqlite			0	http://www.google.com/docCrawler%20will%20discover%20documents%20for%201...	2009-12-03 19:05:07 EET	404 N...	FireFox Analyzer	g	
places.sqlite			0	http://www.google.com/*****	2009-12-03 19:05:13 EET	404 N...	FireFox Analyzer	g	
places.sqlite			0	http://usms.nist.gov/resources/MNs/MNspreadsheetTagged.csv	2009-12-03 19:07:05 EET	MNsp...	FireFox Analyzer	n	
places.sqlite			0	http://www.easc.noaa.gov/Security/webfile/erso.doc.gov/briefings/STU.doc	2009-12-03 19:07:47 EET	STU.doc	FireFox Analyzer	n	
index.dat				file/Pics/Hidden/patent01.JPG	2009-12-03 20:50:09 EET		Internet Explorer Analyzer		
places.sqlite			0	http://www.truecrypt.org/	2009-12-03 22:42:30 EET	TrueC...	FireFox Analyzer	t	
places.sqlite			0	http://www.truecrypt.org/downloads	2009-12-03 22:43:24 EET	TrueC...	FireFox Analyzer	t	

Z-3(από το ιστορικό του περιηγητή, επίσκεψη στο site www.truecrypt.org/downloads, και πρόσβαση μέσω περιηγητή στην εικόνα [patent01.jpg](#) στο Pics/Hidden)

Listing									
Web Downloads									
10 Results									
Table Thumbnail Summary									
Save Table as CSV									
Source Name	S	C	O	URL	Date Accessed	Path			
downloads.sqlite			1	http://www.python.org/ftp/python/2.6.4/py...	2009-11-23 20:20:12 EET	C:/Documents and Settings/Jo/My Documents/Downloads/python-2.6.4.msi	Fi		
downloads.sqlite			0	http://www.easc.noaa.gov/Security/webfile/...	2009-11-24 23:18:18 EET	C:/Documents and Settings/Jo/My Documents/Downloads/STU.doc	Fi		
downloads.sqlite			0	http://appldnld.apple.com.edgesuite.net/con...	2009-11-25 00:08:36 EET	C:/Documents and Settings/Jo/My Documents/Downloads/QuickTimeInsta...	Fi		
downloads.sqlite			1	http://www.freepatentsonline.com/pdf_colle...	2009-11-30 18:46:59 EET	C:/Documents and Settings/Jo/My Documents/Downloads/US5041044.pdf	Fi		
downloads.sqlite			0	http://ardownload.adobe.com/pub/adobe/re...	2009-11-30 18:48:51 EET	C:/Documents and Settings/Jo/My Documents/Downloads/AdbRdr920_e...	Fi		
downloads.sqlite			0	http://fpdownload.adobe.com/get/flashplaye...	2009-12-01 00:44:07 EET	C:/Documents and Settings/Jo/My Documents/Downloads/install_flash_pl...	Fi		
downloads.sqlite			1	http://www.truecrypt.org/download/transien...	2009-12-03 22:43:41 EET	C:/Documents and Settings/Jo/My Documents/Downloads/TrueCrypt Set...	Fi		
Firefox%20Setup%20...						/Documents and Settings/Administrator/Local Settings/Temporary Interne...			
R.79733[1].EXE:Zone...						/Documents and Settings/Administrator/Local Settings/Temporary Interne...			
OOo_3.1.1_Win32Int...						/Documents and Settings/Administrator/My Documents/OOo_3.1.1_Win3...			

Z-4 (επιτυχής download του εργαλείου truecrypt από τον Jo)

Listing									
Web History									
3984 Results									
Table Thumbnail Summary									
Save Table as CSV									
Source Name	S	C	O	URL	Date Accessed	Title	Program Name		
places.sqlite			0	http://www.carmax.com/enUS/search-results/default.html?AWc=1&ANI=0&search=wi...	2009-12-10 19:02:06 EET	Used ...	Firefox Analyzer	c	^
places.sqlite			0	http://www.carmax.com/enUS/search-results/******...	2009-12-10 19:04:56 EET		Firefox Analyzer	c	
places.sqlite			0	http://www.carmax.com/enUS/search-results/docCrawler%20will%20discover%20doc...	2009-12-10 19:08:09 EET	Page ...	Firefox Analyzer	c	
places.sqlite			0	http://www.carmax.com/enUS/search-results/docCrawler%20will%20discover%20doc...	2009-12-10 19:08:37 EET	Page ...	Firefox Analyzer	c	
places.sqlite			0	http://www.carmax.com/enUS/search-results/******...	2009-12-10 19:12:43 EET		Firefox Analyzer	c	
places.sqlite			0	http://usms.nist.gov/resources/MNs/MNspreadsheetTagged.csv	2009-12-10 19:15:31 EET	MNsp...	Firefox Analyzer	n	
places.sqlite			0	http://www.easc.noaa.gov/Security/webfile/erso.doc.gov/briefings/STU.doc	2009-12-10 19:16:40 EET	STU.doc	Firefox Analyzer	n	
places.sqlite			0	http://www.cnn.com/	2009-12-10 19:26:00 EET	CNN...	Firefox Analyzer	c	
places.sqlite			0	http://acs.lbl.gov/Projects/OPKeyX/Publications/SWS04/sws04.ps.gz	2009-12-10 19:35:12 EET	sws0...	Firefox Analyzer	lt	
places.sqlite			0	http://acs.lbl.gov/Projects/OPKeyX/Publications/PKC05/pkc05.ps.gz	2009-12-10 19:35:21 EET	pkc05...	Firefox Analyzer	lt	
index.dat				file/Pics/Hidden/patent03.JPG	2009-12-10 22:43:53 EET		Internet Explorer Analyzer		
index.dat				res://C:\Program Files\Outlook Express\msoeres.dll\frntpage.htm	2009-12-11 19:46:20 EET		Internet Explorer Analyzer		
index.dat				res://C:\Program Files\Outlook Express\msoeres.dll\next.gif	2009-12-11 19:46:21 EET		Internet Explorer Analyzer		v

Z-5 (πρόσβαση μέσω περιηγητή στην εικόνα patent03.jpg στο Pics/Hidden)

Sat 21/11/2009 00:51

Jordan Stanford <j99999s@yahoo.com>
Re: oh man...

To: Jo Smith

Dude, that was a close call. You have to be more careful. I'll send you some stuff next week to help you out. Be more careful!

Jordan

<----- N style="font-weight: bold">From: Jo Smith <j99999s@yahoo.com>
To: Jordan Stanford <j99999s@yahoo.com>
Sent: Fri, November 20, 2009 2:47:46 PM
Subject: oh man...

Jordan,

I almost had a big problem today. I had some of my pics on my work computer and the IT guy swapped it out because it was corrupted. The computer was running slow, so I thought he would just run an update or something. So I lost the pics. I contacted the boss to make sure the thing would get disposed of properly and he agreed. But man, that was a close call. My heart skipped a coup---f beats...

- Jo

Z-6 (ανησυχία του κ. Jo Smith που έχασε τις εικόνες και καθυστέρηση από τον κ. Jordan Stanford)

Thu 03/12/2009 23:01

Re: useful tools

To

Jordan Stanford

Wow! this thing is great. I can't believe it's this easy. Thank!

- Jo

----- Original Message -----

From: [Jordan Stanford](#)

To: [Jo Smith](#)

Sent: Thursday, December 03, 2009 9:28 AM

Subject: Re: useful tools

Jo -

Sorry - didn't check my email for a few days. Is the cover image really big? how about the-----ge you want to hide? There are some other ones I can check out. In the mean time, you may want to try truecrypt.

<http://www.truecrypt.org/>

It's pretty self-explanatory.

- Jordan

From: Jo Smith <js9999sj@yahoo.com>

To: Jordan Stanford <js9999sj@yahoo.com>

Sent: Tue, December 1, 2009 8:52:32 AM

Subject: Re: useful tools

-----TYLE type=Text (css>DIV { MARGIN:0px;})

hey Jordan, this thing is kind of slow. do you have any faster ones or am I doing something wrong?

- Jo

----- Original Message -----

From: [Jordan Stanford](#)

To: [Jo Smith](#)

Sent: Monday, November 23, 2009 10:16 AM

Subject: useful tools

Jo,

Here is a useful tool for your pics. It's an executable JAR file, so you don't need to install anything (in case your IT admin won't allow it)&-----; Just run the program and make sure the mask is large enough. I also attached an example file. The decode password is "password" and just set the destination name as test.bmp. try it out and let me know if you have any questions. Also, make sure to rename your pics to something innocuous!!!! no need to draw attention to yourself.

- Jordan

Z-7 (αποστολή του εργαλείου diit και του TrueCrypt από τον κ.Stanford προς τον κ. Smith)

Fri 11/12/2009 00:20

Jordan Stanford <js9999sj@yahoo.com>

Re: advice?

To

Jo Smith

Jo -

&nb-----/DIV>

Well, that IT guy said he scrubbed it before getting rid of it, right? So you are probably ok. And you have True Crypt installed now, right? Just make sure your password is something a hard - don't make it your name or something stupid. I think with True Crypt you can even use a file as the password.

- Jordan

From: Jo Smith <js9999sj@yahoo.com>

To: Jordan Stanford <js9999sj@yahoo.com>

Sent: Thu, December 10, 2009 2:14:54 PM

Subject: advice?

Hey Jordan. I need some advice. My boss is asking questions about my old computer - the one that had to be replaced. He's asking about the serial number. I'm sure it's not a big deal, but should I take any additional precautions?

- Jo

Z-8 (ανησυχία του κ. Smith και ενθάρρυνση του κ. Stanford να βάλει πιο δύσκολο κωδικό στο TrueCrypt ή ακόμα και χρήση αρχείου ως password)

2009-12-11 08:37:01	54303680	TRUECRYPT.EXE-3A2A0F93.pf	\\WINDOWS\\Prefetch\\TRUECRYPT.EXE-3A2A0F93.pf	Data_Truncated	Normal	Archive , Not_Content_Indexed
2009-12-11 08:37:01	54303792	TRUECRYPT.EXE-3A2A0F93.pf	\\WINDOWS\\Prefetch\\TRUECRYPT.EXE-3A2A0F93.pf	Data_Added , Data_Truncated	Normal	Archive , Not_Content_Indexed
2009-12-11 08:37:01	54303904	TRUECRYPT.EXE-3A2A0F93.pf	\\WINDOWS\\Prefetch\\TRUECRYPT.EXE-3A2A0F93.pf	Data_Added , Data_Truncated , File_Closed	Normal	Archive , Not_Content_Indexed
2009-12-11 08:37:02	54304016	TRUECRYPT.EXE-3A2A0F93.pf	\\WINDOWS\\Prefetch\\TRUECRYPT.EXE-3A2A0F93.pf	Data_Overwritten	Normal	Archive , Not_Content_Indexed
2009-12-11 08:37:14	54304128	bda56377-4103-4cd3-ace8-a9f64fb3aff5.tmp	\\Documents and Settings\\All Users\\Application Data\\avg9\\Temp\\bda56377-4103-4cd3-ace8-a9f64fb3aff5...	File_Created	Normal	Archive , Temporary
2009-12-11 08:37:14	54304272	bda56377-4103-4cd3-ace8-a9f64fb3aff5.tmp	\\Documents and Settings\\All Users\\Application Data\\avg9\\Temp\\bda56377-4103-4cd3-ace8-a9f64fb3aff5...	File_Created , File_Closed , File_Deleted	Normal	Archive , Temporary
2009-12-11 08:37:15	54304416	64854646-719b-4c1d-afdb-9db92cac12ff...	\\Documents and Settings\\All Users\\Application Data\\avg9\\Temp\\64854646-719b-4c1d-afdb-9db92cac12...	File_Created	Normal	Archive , Temporary
2009-12-11 08:37:15	54304560	64854646-719b-4c1d-afdb-9db92cac12ff...	\\Documents and Settings\\All Users\\Application Data\\avg9\\Temp\\64854646-719b-4c1d-afdb-9db92cac12...	File_Created , File_Closed , File_Deleted	Normal	Archive , Temporary
2009-12-11 08:37:17	54304768	Pics	\\Documents and Settings\\Jo\\Desktop\\Pics	File_Created	Normal	Directory
2009-12-11 08:37:17	54304840	Pics	\\Documents and Settings\\Jo\\Desktop\\Pics	File_Created , File_Closed	Normal	Directory

Z-9 (έναρξη encryption με TrueCrypt του φακέλου Pics στην επιφάνεια εργασίας του Jo την 11-12-2009 08:37:01)


TimeStamp(UTC-8)	USN	File/Directory Name	Full Path(from \$MFT)	Event	Source Info	File Attribute
2009-12-11 08:38:20	54378352	TRUECRYPT FORMAT.EXE-0066F001.pf	(\WINDOWS\Prefetch)\TRUECRYPT FORMAT.EXE-0066F001.pf	Data_Overwritten, File_Closed	Normal	Archive, Not_Content_Indexed
2009-12-11 08:38:43	54378496	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Created	Normal	Archive
2009-12-11 08:38:43	54378576	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Created, File_Closed	Normal	Archive
2009-12-11 08:38:43	54378656	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Closed, File_Deleted	Normal	Archive
2009-12-11 08:38:46	54378736	Configuration.xml	\Documents and Settings\Jo\Application Data\TrueCrypt\Configuration.xml	Data_Truncated	Normal	Archive
2009-12-11 08:38:46	54378832	Configuration.xml	\Documents and Settings\Jo\Application Data\TrueCrypt\Configuration.xml	Data_Added, Data_Truncated	Normal	Archive
2009-12-11 08:38:46	54378928	Configuration.xml	\Documents and Settings\Jo\Application Data\TrueCrypt\Configuration.xml	Data_Added, Data_Overwritten, Data_Truncated	Normal	Archive
2009-12-11 08:38:46	54379024	Configuration.xml	\Documents and Settings\Jo\Application Data\TrueCrypt\Configuration.xml	Data_Added, Data_Overwritten, Data_Truncated, File_Cl...	Normal	Archive
2009-12-11 08:38:46	54379120	2f2c34d1-cf83-4f60-bd2c-3e1b3504b7e...tmp	\Documents and Settings\All Users\Application Data\avg9\Temp\2f2c34d1-cf83-4f60-bd2c-3e1b3504b7e...	File_Created	Normal	Archive, Temporary
2009-12-11 08:38:46	54379264	2f2c34d1-cf83-4f60-bd2c-3e1b3504b7e...tmp	\Documents and Settings\All Users\Application Data\avg9\Temp\2f2c34d1-cf83-4f60-bd2c-3e1b3504b7e...	File_Created, File_Closed, File_Deleted	Normal	Archive, Temporary
2009-12-11 08:39:32	54379408	4b5d15d5-d252-4adb-bd58-74484416bf16....	\Documents and Settings\All Users\Application Data\avg9\Temp\4b5d15d5-d252-4adb-bd58-74484416bf16....	File_Created	Normal	Archive, Temporary
2009-12-11 08:39:32	54379552	4b5d15d5-d252-4adb-bd58-74484416bf16....	\Documents and Settings\All Users\Application Data\avg9\Temp\4b5d15d5-d252-4adb-bd58-74484416bf16....	File_Created, File_Closed, File_Deleted	Normal	Archive, Temporary
2009-12-11 08:39:32	54379696	12097.RPCs.Fernando+Loring.pdf	\Documents and Settings\Jo\Desktop\Papers\Papers10\12097.RPCs.Fernando+Loring.pdf	Basic_Info_Changed	Normal	Archive
2009-12-11 08:39:32	54379816	12097.RPCs.Fernando+Loring.pdf	\Documents and Settings\Jo\Desktop\Papers\Papers10\12097.RPCs.Fernando+Loring.pdf	Basic_Info_Changed, File_Closed	Normal	Archive
2009-12-11 08:39:40	54379936	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Created	Normal	Archive
2009-12-11 08:39:40	54380016	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Created, Data_Added	Normal	Archive
2009-12-11 08:39:40	54380096	newFiles2	\Documents and Settings\Jo\Desktop\newFiles2	File_Created, Data_Added, Data_Overwritten	Normal	Archive

Z-10 (λήξη encryption με TrueCrypt του φακέλου Pics στην επιφάνεια εργασίας του Jo την 11-12-2009 08:39:40, και δημιουργία αρχείου newFiles2 με χρησιμοποίηση ως password του αρχείου 12097.RPCs.Fernando+Loring.pdf)

TimeStamp(UTC-8)	USN	File/Directory Name	Full Path(from \$MFT)	Event	Source Info	File Attribute
2009-12-11 08:41:12	54384968	Pics	\Documents and Settings\Jo\Desktop\Pics	File_Renamed_Old	Normal	Directory
2009-12-11 08:41:12	54385040	Dc1	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc1	File_Renamed_New	Normal	Directory
2009-12-11 08:41:12	54385112	Dc1	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc1	File_Renamed_New, File_Closed	Normal	Directory
2009-12-11 08:41:12	54385184	newFiles	\Documents and Settings\Jo\Desktop\newFiles	File_Renamed_Old	Normal	Archive
2009-12-11 08:41:12	54385264	Dc2	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc2	File_Renamed_New	Normal	Archive
2009-12-11 08:41:12	54385336	Dc2	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc2	File_Renamed_New, File_Closed	Normal	Archive
2009-12-11 08:41:12	54385408	JNF02	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\JNF02	Data_Added	Normal	Archive, Hidden
2009-12-11 08:41:12	54385480	JNF02	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\JNF02	Data_Added, File_Closed	Normal	Archive, Hidden
2009-12-11 08:41:17	54385552	Dc2	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\Dc2	File_Closed, File_Deleted	Normal	Archive
2009-12-11 08:41:17	54385624	desktop.ini	\RECYCLER\S-1-5-21-606747145-1547161642-1644491937-1003\desktop.ini	File_Closed, File_Deleted	Normal	Hidden, System

Z-11 (διαγραφή του αρχικού φακέλου Pics με όλο το υλικό την 08:41:12 11-12-2009)

Listing
Keyword search 1 - test.png
183 Results

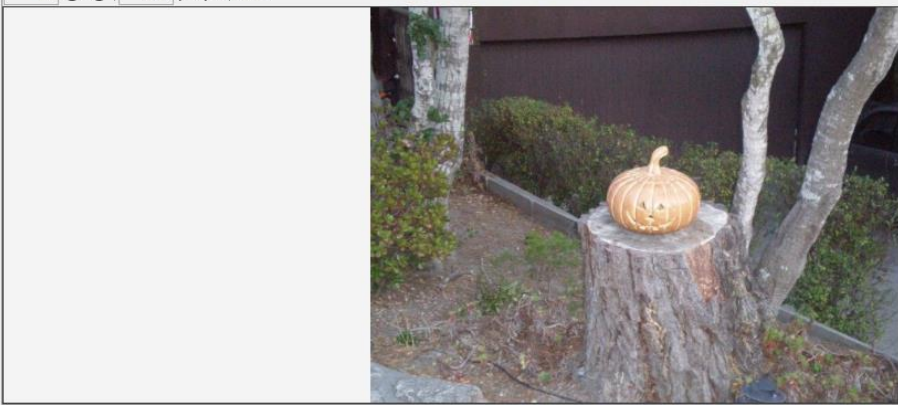

Table
Thumbnail
Summary

Save Table as CSV

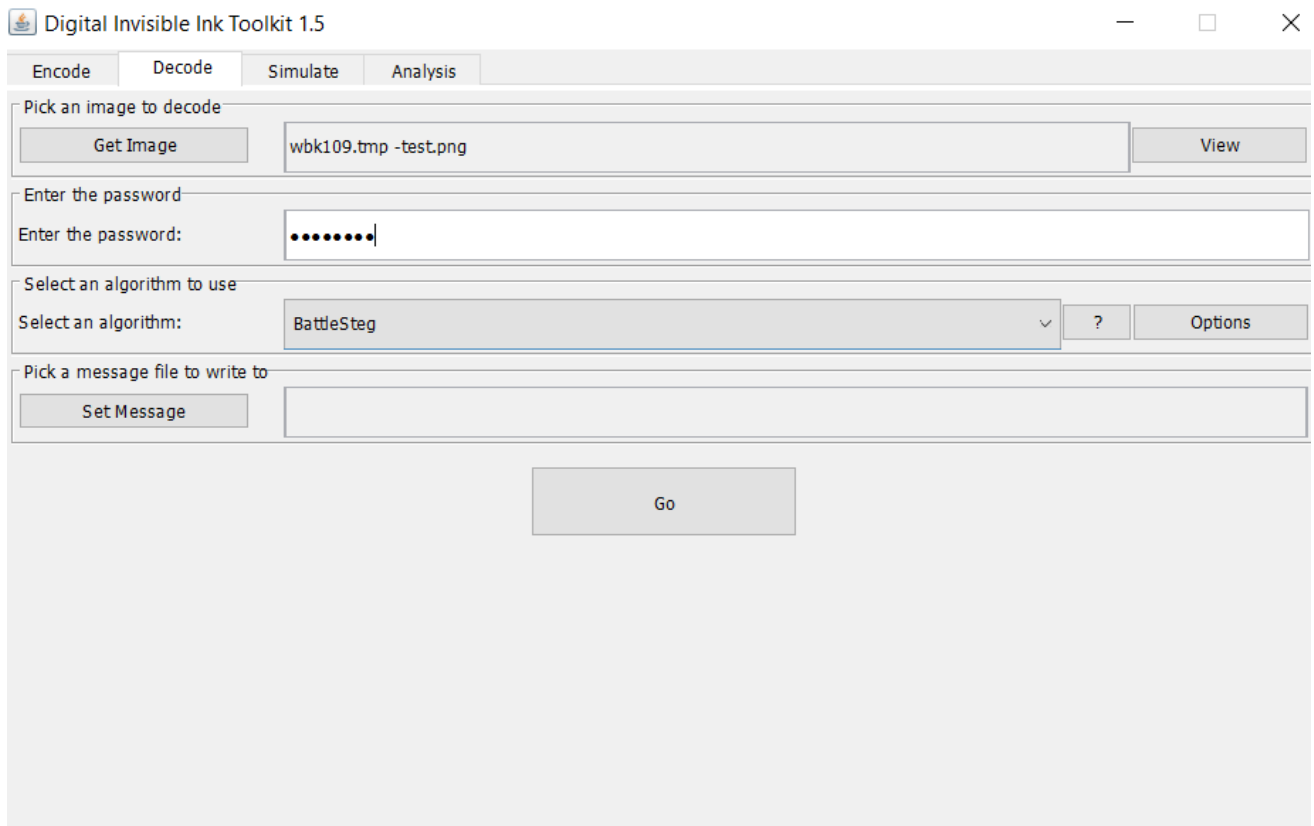
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
CABVHI99				2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	0	Allocated	Allo
wbk107.tmp			0	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	979	Allocated	Allo
wbk109.tmp			0	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	2009-11-23 20:24:29 EET	489044	Allocated	Allo
CAZI3G2W				2009-11-23 20:24:42 EET	2009-11-23 20:24:42 EET	2009-11-23 20:24:42 EET	2009-11-23 20:24:42 EET	0	Allocated	Allo
CA68Y533				2009-11-23 20:24:45 EET	2009-11-23 20:24:45 EET	2009-11-23 20:24:45 EET	2009-11-23 20:24:45 EET	0	Allocated	Allo
CAAQTANB				2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	0	Allocated	Allo
wbk110.tmp			0	2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	2009-11-23 20:26:02 EET	883	Allocated	Allo
bg_blue_2[1].gif			0	2009-11-25 05:40:22 EET	2009-11-25 05:40:22 EET	2009-11-25 05:40:22 EET	2009-11-25 05:40:22 EET	1567	Allocated	Allo
12EBE0C8A051CE46E97C56A8AD25D5[1].jpg			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	1910	Allocated	Allo
48F8CDC1A94A7D6317CB7CDC12CEF[1].jpg			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2521	Allocated	Allo
5F07AE29DA42B1FEE67372895850[1].jpg			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	17992	Allocated	Allo
81303897F4B96EE7967393CBC968[1].jpg			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2762	Allocated	Allo
buttons[1].gif			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	958	Allocated	Allo
dap[1].js			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:22 EET	13786	Allocated	Allo
kv_logof[1].png			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2382	Allocated	Allo
kvurf11.png			0	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	2009-11-25 05:40:23 EET	123	Allocated	Allo

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

0°
79%
Reset
Tags Menu



Z-12 (η στεγανογραφημένη εικόνα test.png που έστειλε ο Jordan στον Jo, και περιείχε την εικόνα testHide.bmp)



Z-13 (Decode test.png με το εργαλείο diit-1.5 και κωδικό password)



Z-14 (η εικόνα testHide.bmp από την επικοινωνία με email των Jo & Jordan)

Listing

Keyword search 1 - rsa

/img_jo-2009-12-11-002.E01/vol_vol2/Documents and Settings/Jo/Application Data/TrueCrypt

Table

Thumbnail

Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[parent folder]				2009-12-03 22:44:37 EET	2009-12-03 22:44:37 EET	2009-12-11 21:04:46 EET	2009-11-20 21:58:53 EET	56	Allocated	Allocated	unknown	/img_jo-2009-12-11-002.E01/vol_vol2/Documents and Sett...
[current folder]				2009-12-03 22:45:55 EET	2009-12-09 23:10:25 EET	2009-12-11 18:36:51 EET	2009-12-03 22:44:37 EET	280	Allocated	Allocated	unknown	/img_jo-2009-12-11-002.E01/vol_vol2/Documents and Sett...
Configuration.xml			0	2009-12-11 19:09:08 EET	2009-12-11 19:09:08 EET	2009-12-11 19:09:08 EET	2009-12-03 22:45:55 EET	2463	Allocated	Allocated	unknown	/img_jo-2009-12-11-002.E01/vol_vol2/Documents and Sett... 5

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Indexed Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

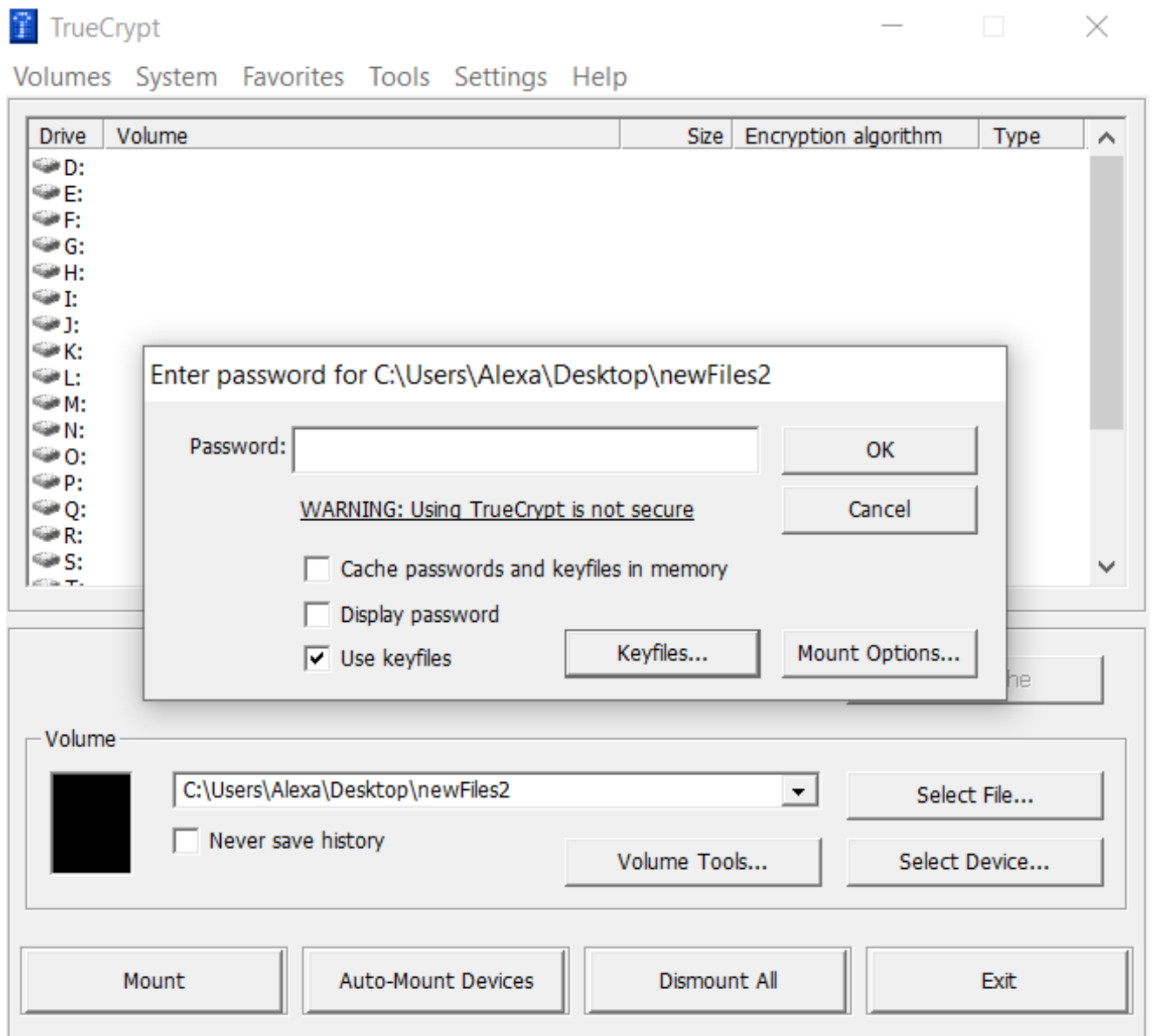
Reset

Text Source: File Text

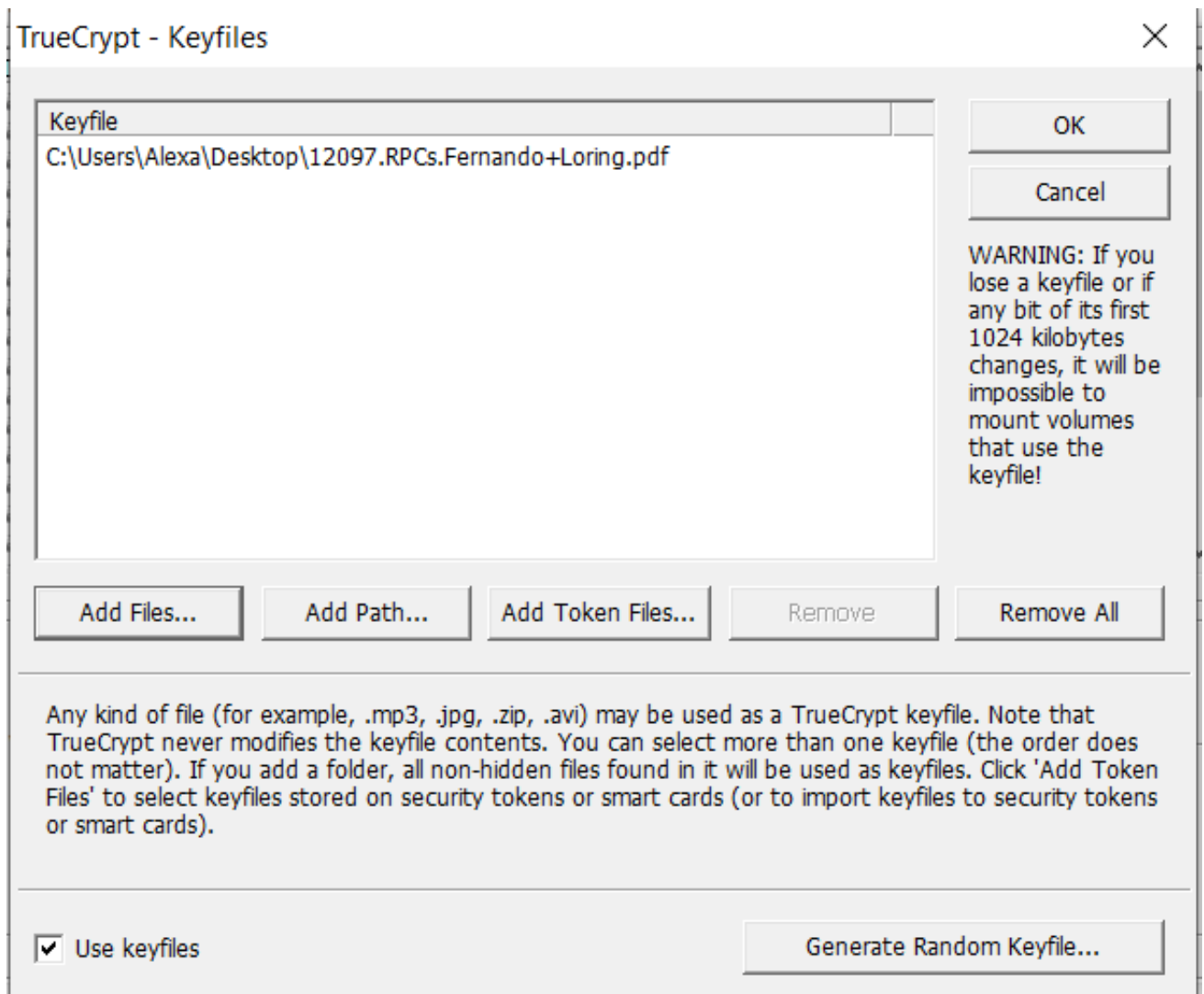
```

<?xml version="1.0" encoding="utf-8"?>
<TrueCrypt>
  <configuration>
    <config key="OpenExplorerWindowAfterMount">0</config>
    <config key="CloseExplorerWindowsOnDismount">1</config>
    <config key="SaveVolumeHistory">0</config>
    <config key="CachePasswords">0</config>
    <config key="WipePasswordCacheOnExit">0</config>
    <config key="WipeCacheOnAutoDismount">1</config>
    <config key="StartOnLogon">0</config>
    <config key="MountDevicesOnLogon">0</config>
    <config key="MountFavoritesOnLogon">0</config>
    <config key="MountVolumesReadOnly">0</config>
    <config key="MountVolumesRemovable">0</config>
    <config key="PreserveTimestamps">1</config>
    <config key="EnableBackgroundTask">1</config>
    <config key="CloseBackgroundTaskOnNoVolumes">0</config>
    <config key="DismountOnLogOff">1</config>
    <config key="DismountOnPowerSaving">0</config>
    <config key="DismountOnScreenSaver">0</config>
    <config key="ForceAutoDismount">1</config>
    <config key="MaxVolumeIdleTime">-60</config>
    <config key="HiddenSectorDetectionStatus">0</config>
    <config key="UseKeyfiles">0</config>
    <config key="LastSelectedDrive">E:</config>
    <config key="CloseSecurityTokenSessionsAfterMount">0</config>
    <config key="HotkeyModAutoMountDevices">0</config>
    <config key="HotkeyCodeAutoMountDevices">0</config>
    <config key="HotkeyModDismountAll">0</config>
    <config key="HotkeyCodeDismountAll">0</config>
    <config key="HotkeyModWipeCache">0</config>
  
```

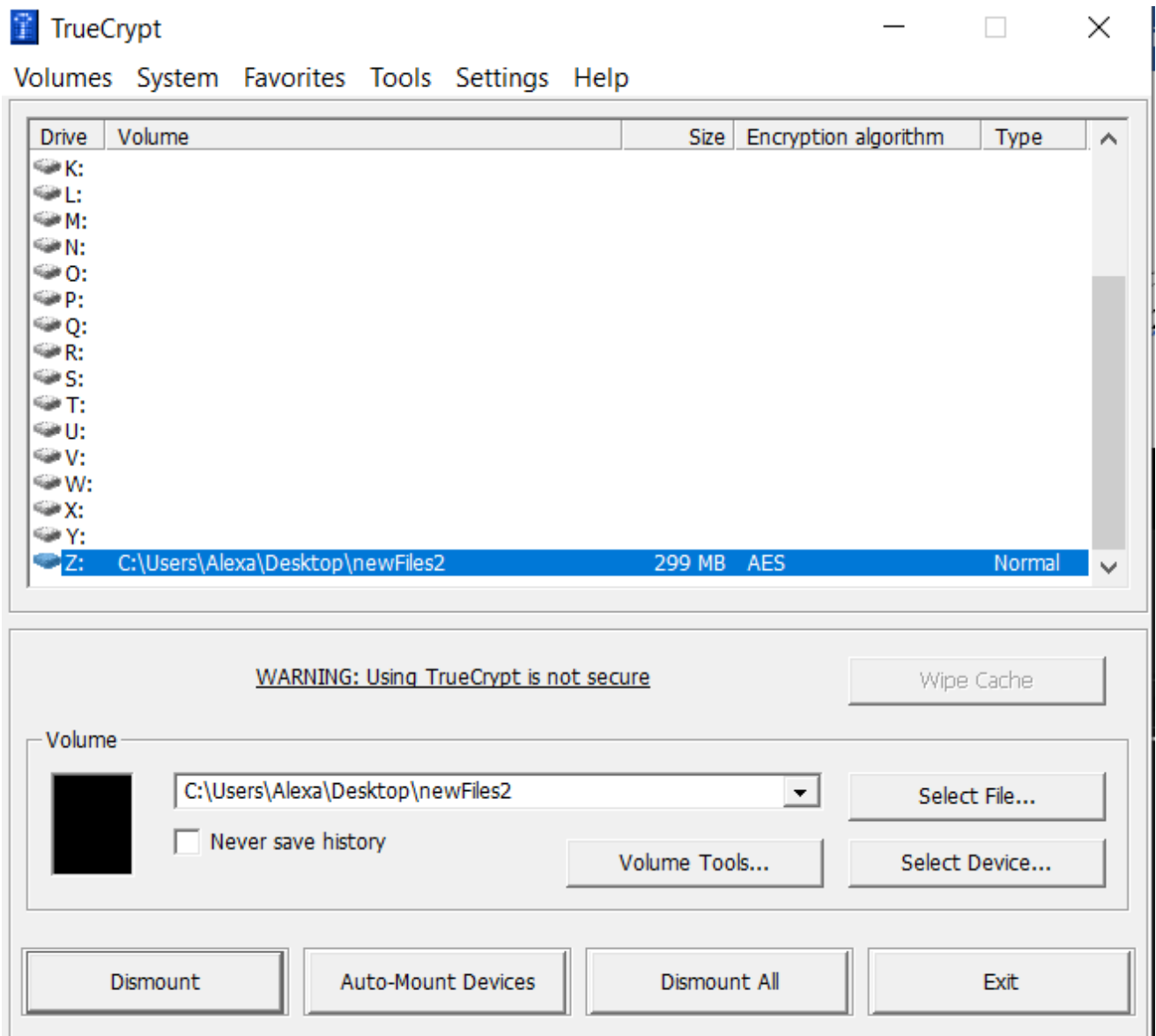
Z-15 (το configuration στο TrueCrypt από τον Jo, Wipe Cache On Auto Dismount / true, Last Selected Drive / E:)



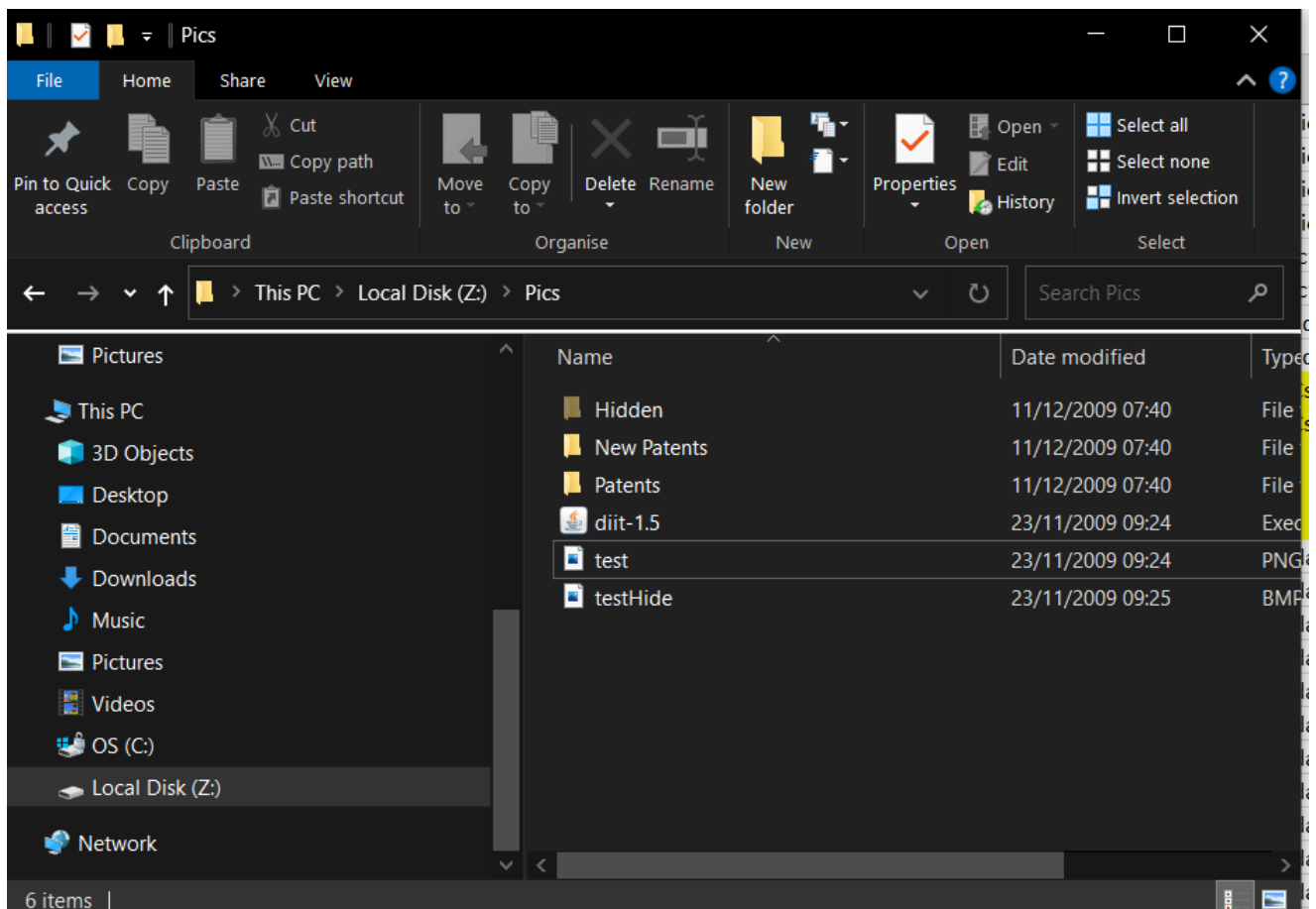
Z-16 (part 1, TrueCrypt tool: use of password moment)



Z-17 (part 2, TrueCrypt tool, password is 12097.RPCs.Fernando+Loring.pdf)



Z-18 (part 3, TrueCrypt use tool, η επιτυχής εμφάνιση του κρυπτογραφημένου δίσκου από το αρχείο newFiles2, που στο δικό μας μηχάνημα πήρε το όνομα Z:/)



Z-19 (τα αρχικά έγγραφα μετά το άνοιγμα του δίσκου E:/)

Table Thumbnail Summary						
Source Name	S	C	O	MD5 Hash	Comment	File Path
hr_patent63.JPG				d994947181a7d60704f70f74d61b7421		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent63.JPG
hr_patent62.JPG				9a5364a26ac26d44d678d473774a5b97		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent62.JPG
hr_patent66.JPG				1018f333d3eec3a90cc8c3eb1824455c		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent66.JPG
hr_patent64.JPG				4f33d26ea0d47ea17cedd5067549d3fa		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent64.JPG
hr_patent68.JPG				bf44428dafc755aa57f38036aaa79ada		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent68.JPG
hr_patent67.JPG				259acd4e434c8836ae1eb8069b5f36f1		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent67.JPG
hr_patent70.JPG				67d55dd34df85cf719815085abd3d791		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent70.JPG
hr_patent69.JPG				34a248ffbc03c1b96e2225b788f71fd6		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent69.JPG
hr_patent72.JPG				a003a6d4fe290c9dfec624bc85714357		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent72.JPG
hr_patent71.JPG				43cfc2daf0ece60e9d944bc6ca980711		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent71.JPG
hr_patent74.JPG				e02ea82a5b0026315c2fc09ac4e2b07f		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent74.JPG
hr_patent73.JPG				bb6e0d23b12a26d23dfbcffa45b84a89		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent73.JPG
hr_patent76.JPG				51820571527fec74620fb4267263095a		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent76.JPG
hr_patent75.JPG				0e8198723a5b907b6e63775f7860a09b		/img_jo-2009-12-11-002.E01/vol_vol2\$/OrphanFiles/hr_patent75.JPG

Z-20 (Hashes MD5 των διαγεγραμμένων αρχείων)

