



---

**SCHOOL OF ARCHITECTURE, COMPUTING  
& ENGINEERING**

**MSc Information Security & Digital Forensics**

**Εργασία του μαθήματος CN7019 – Digital Forensics**

**ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ  
ΛΙΑΜΠΑΣ ΧΡΗΣΤΟΣ**

**ΕΠΙΜΕΛΕΙΑ ΕΡΓΑΣΙΑΣ  
U2020737  
U2121211**

**ΙΔΡΥΜΑ  
ΜΗΤΡΟΠΟΛΙΤΙΚΟ ΚΟΛΛΕΓΙΟ CAMPUS  
ΑΜΑΡΟΥΣΙΟΥ**

*22 Μαΐου 2023*

## **Πίνακας περιεχομένων**

<b>1. ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ ΥΠΟΘΕΣΗΣ .....</b>	<b>- 2 -</b>
<b>1.1. ΠΛΗΡΟΦΟΡΙΕΣ ΥΠΟΘΕΣΗΣ.....</b>	<b>- 2 -</b>
<b>1.2. ΕΠΙΣΚΟΠΗΣΗ ΥΠΟΘΕΣΗΣ .....</b>	<b>- 2 -</b>
<b>1.3. ΑΝΑΛΗΨΗ ΥΠΟΘΕΣΗΣ .....</b>	<b>- 3 -</b>
<b>2. ΣΗΜΑΝΤΙΚΑ ΑΡΧΕΙΑ .....</b>	<b>- 4 -</b>
<b>2.1. ΣΥΝΤΟΜΕΥΣΕΙΣ ΕΦΑΡΜΟΓΩΝ ΣΤΟΝ ΦΑΚΕΛΟ «TOOLS» ΤΟΥ «DESKTOP».....</b>	<b>- 4 -</b>
<b>2.2. ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΣΤΟΝ ΦΑΚΕΛΟ «MY DOCUMENTS» ΓΙΑ ΧΡΗΣΗ ΣΕ ΔΙΑΦΟΡΑ ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ (NT, UNIX).....</b>	<b>- 6 -</b>
<b>3. ΑΠΟΤΕΛΕΣΜΑΤΑ ΑΝΑΛΥΣΗΣ ΨΗΦΙΑΚΩΝ ΠΙΕΙΣΤΗΡΙΩΝ.....</b>	<b>- 7 -</b>
<b>3.1. ΕΝΤΟΠΙΣΜΟΣ ΟΠΟΙΟΥΔΗΠΟΤΕ ΛΟΓΙΣΜΙΚΟΥ ΠΟΥ ΣΥΝΔΕΕΤΑΙ ΑΜΕΣΑ ΜΕ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΑΗΜΑΤΑ .....</b>	<b>- 7 -</b>
<b>3.2. ΕΝΤΟΠΙΣΜΟΣ ΣΤΟΙΧΕΙΩΝ ΠΟΥ ΑΠΟΔΕΙΚΝΥΟΥΝ ΤΗ ΧΡΗΣΗ ΤΟΥ ΠΑΡΑΠΑΝΩ ΛΟΓΙΣΜΙΚΟΥ . - 9 -</b>	
<b>3.3. ΕΝΤΟΠΙΣΜΟΣ ΟΠΟΙΩΝΔΗΠΟΤΕ ΔΕΔΟΜΕΝΩΝ ΜΠΟΡΕΙ ΝΑ ΕΧΟΥΝ ΠΑΡΑΧΘΕΙ ΑΠΟ ΤΗ ΧΡΗΣΗ ΤΟΥ ΠΑΡΑΠΑΝΩ ΛΟΓΙΣΜΙΚΟΥ .....</b>	<b>- 12 -</b>
<b>3.4. ΕΝΤΟΠΙΣΜΟΣ ΟΠΟΙΩΝΔΗΠΟΤΕ ΔΕΔΟΜΕΝΩΝ ΜΠΟΡΕΙ ΝΑ ΕΧΟΥΝ ΥΠΟΚΛΑΠΕΙ .....</b>	<b>- 12 -</b>
<b>3.5. ΕΝΤΟΠΙΣΜΟΣ ΤΗΣ ΗΜΕΡΟΜΗΝΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ... - 14 -</b>	
<b>3.6. ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΕ .....</b>	<b>- 16 -</b>
<b>3.7. ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΟΝΟΜΑΤΟΣ ΛΟΓΑΡΙΑΣΜΟΥ (ACCOUNT NAME) ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ..... - 18 -</b>	
<b>3.8. ΕΠΙΒΕΒΑΙΩΣΗ Η ΔΙΑΦΕΥΣΗ ΤΗΣ ΥΠΟΨΙΑΣ ΓΙΑ ΠΡΟΤΕΡΗ ΜΕΤΑΚΙΝΗΣΗ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΣΕ ΆΛΛΗ ΓΕΩΓΡΑΦΙΚΗ ΠΕΡΙΟΧΗ.....</b>	<b>- 19 -</b>
<b>3.9. ΕΝΤΟΠΙΣΜΟΣ ΕΠΙΠΛΕΟΝ ΧΡΗΣΤΩΝ ΠΟΥ ΕΙΧΑΝ ΠΡΟΣΒΑΣΗ ΣΤΟΝ ΥΠΟΛΟΓΙΣΤΗ .....</b>	<b>- 22 -</b>
<b>3.10. ΕΝΤΟΠΙΣΜΟΣ ΤΟΥ ΚΑΤΑΣΚΕΥΑΣΤΗ ΤΗΣ ΚΑΡΤΑΣ ΔΙΚΤΥΟΥ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΕ ΓΙΑ ΤΙΣ ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ .....</b>	<b>- 25 -</b>
<b>3.11. ΕΠΑΛΗΘΕΥΣΗ Η ΔΙΑΦΕΥΣΗ ΤΩΝ ΚΑΤΑΘΕΣΕΩΝ ΤΩΝ ΣΥΝΕΡΓΩΝ ΤΟΥ ΠΡΟΚΕΙΜΕΝΟΥ ΝΑ ΑΣΚΗΘΕΙ ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ ΠΟΙΝΙΚΗ ΔΙΩΣΗ .....</b>	<b>- 27 -</b>
<b>3.12. ΔΙΕΡΕΥΝΗΣΗ ΙΧΝΩΝ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ .....</b>	<b>- 32 -</b>
<b>3.13. ΔΙΕΡΕΥΝΗΣΗ ΙΧΝΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΕΓΚΑΗΜΑΤΩΝ .....</b>	<b>- 36 -</b>
<b>3.14. ΔΙΕΡΕΥΝΗΣΗ ΥΠΑΡΞΗΣ ΕΠΙΠΛΕΟΝ ΣΥΝΕΡΓΩΝ .....</b>	<b>- 37 -</b>
<b>3.15. ΔΙΕΡΕΥΝΗΣΗ ΥΠΑΡΞΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ (VIRUS, WORMS, BACKDOOR ΚΑΠ) ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΕΠΙΚΑΛΕΣΤΕΙ Ο ΔΡΑΣΤΗΣ ΩΣ ΕΛΑΦΡΥΝΤΙΚΟ..... - 40 -</b>	
<b>3.16. ΕΠΙΠΛΕΟΝ ΕΥΡΗΜΑΤΑ .....</b>	<b>- 44 -</b>
<b>4. CHAIN OF CUSTODY .....</b>	<b>- 49 -</b>
<b>5. ΠΑΡΑΡΤΗΜΑ.....</b>	<b>- 51 -</b>
<b>5.1. ΕΠΙΤΕΥΞΗ ΣΤΟΧΟΥ.....</b>	<b>- 51 -</b>
<b>5.2. ΑΤΟΜΙΚΗ ΣΥΝΕΙΣΦΟΡΑ.....</b>	<b>- 51 -</b>
<b>5.3. ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ .....</b>	<b>- 52 -</b>
<b>5.4. ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ .....</b>	<b>- 52 -</b>

# 1. Συνοπτικά στοιχεία υπόθεσης

## 1.1. Πληροφορίες υπόθεσης

Όνομασία υπόθεσης	Greg Schardt 's (Mr. Evil) Case
Αρμόδιος φορέας	University of East London (UEL) – Metropolitan College
Ονόματα ερευνητών	Μάνιος Αθανάσιος Μπάντης Χρήστος
Emails ερευνητών	amanios19b@amcstudent.edu.gr cbantis20b@amcstudent.edu.gr
Ημ/νια ανάκτησης πειστηρίων	20/09/2021
Πειστήρια	1 Laptop μάρκας Dell 1 PCMCIA ασύρματη κάρτα δικτύου 1 εξωτερική κεραία συχνότητας 802.11b
Μοντέλο / Σειριακός αριθμός (laptop)	Latitude CPi / #VLQLW
Ημερομηνία συγγραφής έκθεσης	22/05/2023

Πίνακας 1 - Πληροφορίες υπόθεσης

## 1.2. Επισκόπηση υπόθεσης

Στις 20/9/2021, ένα laptop μάρκας Dell με σειριακό αριθμό #VLQLW βρέθηκε παρατημένο, μαζί με μία PCMCIA ασύρματη κάρτα δικτύου και μία εξωτερική κεραία συχνότητας 802.11b. Υπάρχει η υποψία ότι το συγκεκριμένο laptop έχει χρησιμοποιηθεί σε παράνομες ηλεκτρονικές δραστηριότητες, παρόλο που δεν μπορεί να συσχετιστεί με έναν ύποπτο, που το μικρό του όνομα είναι Gregory.

Υπάρχει η αδιευκρίνιστη πληροφορία ότι ο Gregory -ενδεχομένως- να χρησιμοποιεί το ψευδώνυμο “Mr. Evil” ή “Mr. Bad”. Κάποιοι από τους συνεργούς του, κατά την ανακριτική διαδικασία ομολόγησαν ότι εκείνος είχε σκοπό να σταθμεύσει το αυτοκίνητό του έξω από σημεία τα οποία θα ήταν εντός της εμβέλειας ασύρματων σημείων πρόσβασης (wireless access points), όπως στα Starbucks και σε άλλα hotspots της T-Mobile. Στόχος του ήταν να κάνει intercept πακέτα διαδικτυακής κίνησης για να υποκλέψει ονόματα και κωδικούς χρηστών, καθώς και αριθμούς πιστωτικών καρτών.

### 1.3. Ανάληψη υπόθεσης

Έγινε λήψη δύο αρχείων τύπου «disk image» με ονόματα «4Dell Latitude CPi.E01» και «4Dell Latitude CPi.E02» αντίστοιχα, τα οποία αποτελούν το εικονικό αντίγραφο του πειστηρίου, επί του οποίου πραγματοποιήθηκε η εξέταση. Επίσης, δόθηκαν τα μοναδικά ψηφιακά αποτυπώματα (hash values) των παραπάνω αρχείων (Πίνακας 2).

Όνομα εικονικού δίσκου	Hash Value
4Dell Latitude CPi.E01	943243e71eda7481fee7b83f06698993
4Dell Latitude CPi.E02	4931253cc91dffdef5867c3dfbd99516

Πίνακας 2 - Τα hash values των εικονικών δίσκων

Έπειτα, πραγματοποιήθηκε η ταυτοποίηση των hash values των εικονικών δίσκων με τα δοθέντα hash values. Πιο συγκεκριμένα, πληκτρολογώντας την εντολή «certutil -hashfile (όνομα αρχείου) md5» στο «cmd» υπολογίζεται το hash value του αρχείου που ορίζεται από τον χρήστη. Συνεπώς, βάσει των τιμών της παρακάτω εικόνας και του παραπάνω πίνακα επαληθεύεται πως τα αρχεία εικονικών δίσκων είναι αληθή και ακριβή αντίγραφα της σκηνής του εγκλήματος.

```
Command Prompt
certutil -hashfile "4Dell Latitude CPi.E01" md5
MD5 hash of 4Dell Latitude CPi.E01:
943243e71eda7481fee7b83f06698993
CertUtil: -hashfile command completed successfully.

certutil -hashfile "4Dell Latitude CPi.E02" md5
MD5 hash of 4Dell Latitude CPi.E02:
4931253cc91dffdef5867c3dfbd99516
CertUtil: -hashfile command completed successfully.
```

Εικόνα 1 - Επαλήθευση των hashes των εικονικών δίσκων

Κατά τη διάρκεια της διαδικασίας που θα ακολουθηθεί, από τη λήψη των πειστηρίων έως την φύλαξή τους σε ασφαλές μέρος, θα γίνει χρήση του συνόλου των πρακτικών του ΑCPO, καθώς δεν θα τροποποιηθούν από κανένα αρμόδιο (ή μη) άτομο τα δεδομένα του εικονικού δίσκου και θα πραγματοποιηθεί καταγραφή και διατήρηση των διεργασιών που θα λάβουν χώρα.

Για την ευκολότερη ανάγνωση και κατανόηση του περιεχομένου, στο υπόλοιπο της έκθεσης η διαδρομή «/img\_4Dell Latitude CPi.E01/vol\_vol2/» θα αντικατασταθεί με «C:/».

## 2. Σημαντικά αρχεία

### 2.1. Συντομεύσεις εφαρμογών στον φάκελο «Tools» του «Desktop»

Όνομα	123 WASP.lnk
Φυσικό μέγεθος	1024 Bytes
Λογικό μέγεθος	628 Bytes
Ημ/νία δημιουργίας	2004-08-20 18:13:08 EEST
Ημ/νία τροποποίησης	2004-08-20 18:13:08 EEST
Ημ/νία προσπέλασης	2004-08-20 18:24:40 EEST
Διαδρομή	C:/Documents and Settings/Mr. Evil/Desktop/Tools/123 WASP.lnk
Όνομα	Agent.lnk
Φυσικό μέγεθος	650 Bytes
Λογικό μέγεθος	650 Bytes
Ημ/νία δημιουργίας	2004-08-20 18:08:19 EEST
Ημ/νία τροποποίησης	2004-08-20 18:08:19 EEST
Ημ/νία προσπέλασης	2004-08-20 18:55:34 EEST
Διαδρομή	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Agent.lnk
Όνομα	Cain v2.5.lnk
Φυσικό μέγεθος	1536 Bytes
Λογικό μέγεθος	1496 Bytes
Ημ/νία δημιουργίας	2004-08-20 18:06:01 EEST
Ημ/νία τροποποίησης	2004-08-20 18:06:01 EEST
Ημ/νία προσπέλασης	2004-08-20 18:34:52 EEST
Διαδρομή	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Agent.lnk/Documents and Settings/Mr. Evil/Desktop/Tools/Cain v2.5.lnk
Όνομα	CuteFTP.lnk
Φυσικό μέγεθος	1024 Bytes
Λογικό μέγεθος	827 Bytes
Ημ/νία δημιουργίας	2004-08-20 18:09:02 EEST
Ημ/νία τροποποίησης	2004-08-20 18:09:02 EEST
Ημ/νία προσπέλασης	2004-08-20 18:11:12 EEST
Διαδρομή	C:/Documents and Settings/Mr. Evil/Desktop/Tools/CuteFTP.lnk
Όνομα	CuteHTML.lnk
Φυσικό μέγεθος	1024 Bytes
Λογικό μέγεθος	932 Bytes
Ημ/νία δημιουργίας	2004-08-20 18:09:04 EEST
Ημ/νία τροποποίησης	2004-08-20 18:09:04 EEST
Ημ/νία προσπέλασης	2004-08-20 18:24:40 EEST
Διαδρομή	C:/Documents and Settings/Mr. Evil/Desktop/Tools/CuteHTML.lnk
Όνομα	Ethereal.lnk
Φυσικό μέγεθος	700 Bytes
Λογικό μέγεθος	700 Bytes
Ημ/νία δημιουργίας	2004-08-27 18:29:44 EEST

<b>Ημ/νία τροποποίησης</b>	2004-08-27 18:29:44 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-27 18:34:54 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/Ethereal.lnk
<b>Όνομα</b>	Faber Toys.lnk
<b>Φυσικό μέγεθος</b>	1024 Bytes
<b>Λογικό μέγεθος</b>	706 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:07:24 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:07:24 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-25 18:27:30 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/Faber Toys.lnk
<b>Όνομα</b>	Look@Host.lnk
<b>Φυσικό μέγεθος</b>	2048 Bytes
<b>Λογικό μέγεθος</b>	1562 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-25 18:56:11 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-25 18:56:11 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-27 18:18:04 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/Look@Host.lnk
<b>Όνομα</b>	Look@LAN.lnk
<b>Φυσικό μέγεθος</b>	2048 Bytes
<b>Λογικό μέγεθος</b>	1555 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-25 18:56:11 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-25 18:56:11 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-27 18:18:04 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/Look@LAN.lnk
<b>Όνομα</b>	mIRC.lnk
<b>Φυσικό μέγεθος</b>	638 Bytes
<b>Λογικό μέγεθος</b>	638 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:10:04 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:09:56 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-25 19:20:24 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/mIRC.lnk
<b>Όνομα</b>	Network Stumbler.lnk
<b>Φυσικό μέγεθος</b>	1024 Bytes
<b>Λογικό μέγεθος</b>	753 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-27 18:12:17 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-27 18:12:17 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-27 18:12:43 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr.Evil/Desktop/Tools/Network Stumbler.lnk
<b>Όνομα</b>	Shortcut to whois.lnk
<b>Φυσικό μέγεθος</b>	1024 Bytes
<b>Λογικό μέγεθος</b>	638 Bytes
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:11:19 EEST

<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:11:19 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-26 18:13:56 EEST
<b>Διαδρομή</b>	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Shortcut to whois.lnk

Πίνακας 3 - Συντομεύσεις εφαρμογών στον φάκελο «Tools» του «Desktop»

## 2.2. Κακόβουλο λογισμικό στον φάκελο «My Documents» για χρήση σε διάφορα Λειτουργικά Συστήματα (NT, Unix)

Όνομα	ARCHIVE
<b>Μέγεθος</b>	1,97 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:18:07 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:18:09 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:18:09 EEST
<b>Διαδρομή</b>	C:/My Documents/ARCHIVE
Όνομα	COMMANDS
<b>Μέγεθος</b>	3,08 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:18:12 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:18:16 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:18:16 EEST
<b>Διαδρομή</b>	C:/My Documents/COMMANDS
Όνομα	DICTIONARIES
<b>Μέγεθος</b>	37,6 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:18:16 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:18:41 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:18:41 EEST
<b>Διαδρομή</b>	C:/My Documents/DICTIONARIES
Όνομα	ENUMERATION
<b>Μέγεθος</b>	20,7 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:18:41 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:18:41 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:18:41 EEST
<b>Διαδρομή</b>	C:/My Documents/ENUMERATION
Όνομα	EXPLOITATION
<b>Μέγεθος</b>	46,7 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:19:09 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:19:12 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:19:12 EEST
<b>Διαδρομή</b>	C:/My Documents/EXPLOITATION
Όνομα	FOOTPRINTING
<b>Μέγεθος</b>	90,2 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:19:49 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:19:49 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:19:49 EEST
<b>Διαδρομή</b>	C:/My Documents/FOOTPRINTING
Όνομα	MISCELLANEOUS
<b>Μέγεθος</b>	1,3 MB

<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:21:04 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:21:04 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:21:04 EEST
<b>Διαδρομή</b>	C:/My Documents/MISCELLANEOUS
<b>Όνομα</b>	NOVELL
<b>Μέγεθος</b>	2,91 MB
<b>Ημ/νία δημιουργίας</b>	2004-08-20 18:21:05 EEST
<b>Ημ/νία τροποποίησης</b>	2004-08-20 18:21:08 EEST
<b>Ημ/νία προσπέλασης</b>	2004-08-20 18:21:08 EEST
<b>Διαδρομή</b>	C:/My Documents/NOVELL

Πίνακας 4 - Κακόβουλο λογισμικό στον φάκελο «My Documents»

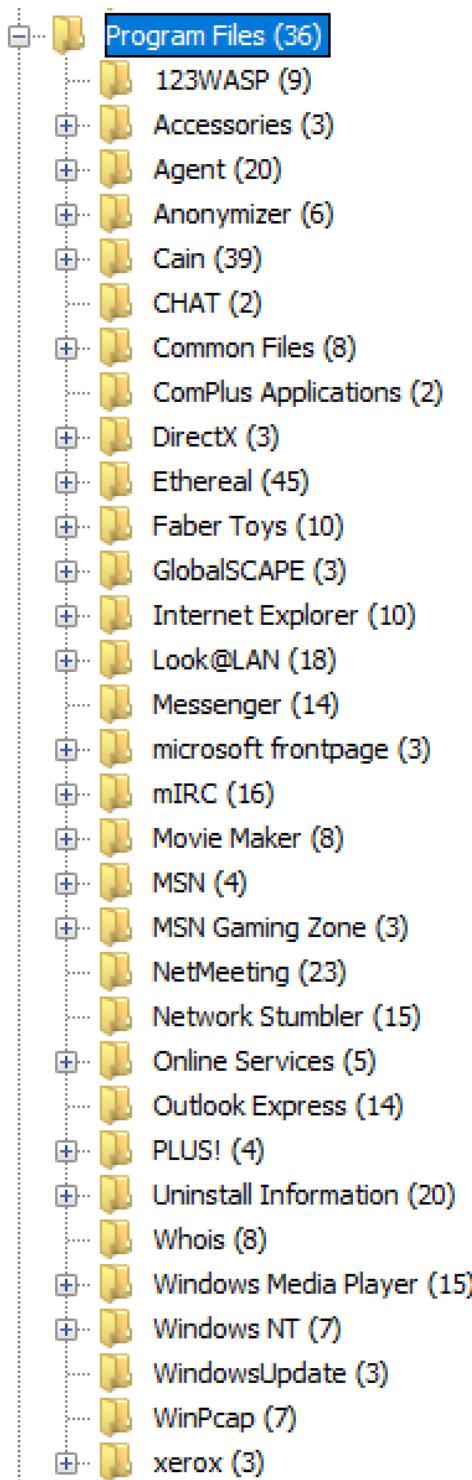
### 3. Αποτελέσματα ανάλυσης ψηφιακών πειστηρίων

#### 3.1. Εντοπισμός οποιουδήποτε λογισμικού που συνδέεται άμεσα με ηλεκτρονικά εγκλήματα

3.1.1. Εντός του φακέλου «C:/Program Files» εντοπίστηκαν τα παρακάτω λογισμικά (Εικόνα 2):

- **123Wasp (Version 2.01)** – Εργαλείο ανάκτησης των κωδικών των λογαριασμών που είναι συνδεδεμένοι σε έναν υπολογιστή, οι οποίοι είναι αποθηκευμένοι στο αρχείο με κατάληξη «.pwl» στην διαδρομή «C:/Windows» (Απευθύνεται στις εκδόσεις των Windows 95, Windows 98 και Windows ME, καθώς μόνο σε αυτά συναντώνται αυτά τα αρχεία – στις νεότερες εκδόσεις έχουν καταργηθεί).
- **Anonymizer Bar 2.0** – Εργαλείο απόκρυψης της διεύθυνσης IP με σκοπό την ανώνυμη περιήγηση στο διαδίκτυο, προσφέροντας ανώνυμους εξυπηρετητές «proxy».
- **Cain & Abel (Version 2.5)** – Εργαλείο ανάκτησης κωδικών πρόσβασης που επιτρέπει την ανάκτηση διάφορων ειδών κωδικών πρόσβασης μέσω παρακολούθησης του δικτύου (sniffing) και αποκρυπτογράφησης κρυπτογραφημένων κωδικών πρόσβασης, χρησιμοποιώντας μεθόδους όπως «Dictionary», «Brute-Force» και «Cryptanalysis».
- **Ethereal (Version 0.10.6)** – Εργαλείο παρακολούθησης του δικτύου (sniffing) και ανάλυσης της κίνησης του δικτύου (network traffic analyzer).
- **Look@LAN (Version 2.50)** – Εργαλείο παρακολούθησης δικτύου.
- **Network Stumbler (Version 0.4.0)** – Εργαλείο που επιτρέπει την ανίχνευση ασύρματων τοπικών δικτύων (WLAN) χρησιμοποιώντας 802.11a/b/g. Συχνά

χρησιμοποιείται για «WarDriving» και στόχευση κατευθυνόμενων κεραιών για συνδέσεις WLAN μεγάλων αποστάσεων.

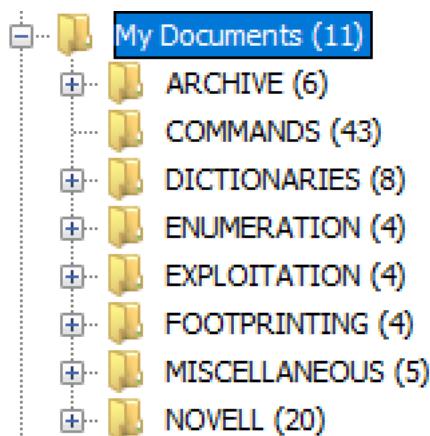


Εικόνα 2 - Τα περιεχόμενα του φακέλου «C:/Program Files»

3.1.2. Εντός του φακέλου «C:/My Documents» εντοπίστηκαν οι παρακάτω βοηθητικές κακόβουλες συλλογές εργαλείων (Εικόνα 3). Σε αυτές περιλαμβάνονται sniffers, brute-

force crackers, port scanners και exploits, τα οποία κατηγοριοποιούνται ανάλογα των σκοπό και το λειτουργικό σύστημα που απευθύνονται:

- **ARCHIVE**
- **COMMANDS**
- **DICTIONARIES**
- **ENUMERATION**
- **EXPLOITATION**
- **FOOTPRINTING**
- **MISCELLANEOUS**
- **NOVELL**



*Eικόνα 3 - Τα περιεχόμενα του φακέλου «C:/My Documents»*

### 3.2. Εντοπισμός στοιχείων που αποδεικνύουν τη χρήση του παραπάνω λογισμικού

3.2.1. Μεταβαίνοντας στον φάκελο «C:/Program Files» και ελέγχοντας τις ημερομηνίες δημιουργίας και τελευταίας προσπέλασης εξάγονται τα παρακάτω συμπεράσματα:

Όνομα	Ημ/νία Δημιουργίας	Ημ/νία τελευταίας προσπέλασης	Συμπέρασμα
123Wasp	2004-08-20 18:13:08 EEST	2004-08-20 18:13:08 EEST	Δεν εκτελέστηκε ποτέ
Anonymizer (Folder)	2004-08-20 18:05:06 EEST	2004-08-27 18:32:07 EEST	Εκτελέστηκε εφτά (7) ημέρες μετά την εγκατάσταση
Anonymizer (AnonymizerBar.dll)	2002-07-12 03:31:30 EEST	2004-08-20 18:05:09 EEST	Το παρόν αρχείο βιβλιοθήκης φαίνεται

			πως δημιουργήθηκε δύο (2) χρόνια πριν την εγκατάσταση του λογισμικού, κάτι που δηλώνει ενδεχόμενη ενημέρωση του λογισμικού
<b>Cain &amp; Abel</b>	2004-08-20 18:05:58 EEST	2004-08-27 18:14:45 EEST	Εκτελέστηκε εφτά (7) ημέρες μετά την εγκατάσταση
<b>Ethereal</b>	2004-08-13 05:15:35 EEST	2004-08-27 18:34:54 EEST	Εκτελέστηκε δεκατέσσερις (14) ημέρες μετά την εγκατάσταση
<b>Look@LAN</b>	2004-02-18 01:35:21 EEST	2004-08-26 17:58:49 EEST	Εκτελέστηκε εκατόν ενενήντα (190) ημέρες μετά την εγκατάσταση
<b>Network Stumbler</b>	2004-04-21 10:16:58 EEST	2004-08-27 18:12:37 EEST	Εκτελέστηκε εκατόν είκοσι οκτώ (128) ημέρες μετά την εγκατάσταση

Πίνακας 5 - Στοιχεία που αποδεικνύουν τη χρήση κακόβουλου λογισμικού

3.2.2. Ελέγχοντας τα αρχεία «prefetch» των Windows στην τοποθεσία «C:/Windows/Prefetch». Ένα αρχείο prefetch δημιουργείται κάθε φορά που εκτελείται για πρώτη φορά ένα λογισμικό και περιέχει δεδομένα που εκμεταλλεύεται το λειτουργικό σύστημα με σκοπό την αύξηση της απόδοσής του. Στα παραγόμενα, από τη σάρωση του εικονικού δίσκου από το εργαλείο «Autopsy» (<https://www.autopsy.com/>) , «Data Artifacts» βρίσκεται η καρτέλα «Run Programs», η οποία περιέχει το σύνολο των prefetch αρχείων, παρέχοντας διάφορες πληροφορίες, όπως τον αριθμό των εκτελέσεων για κάθε ένα από αυτά (Εικόνα 4).

Run Programs	
Source Name	Count
CAIN.EXE-23D61279.pf	2
LOOKATLAN.EXE-1F991DD9.pf	2
NETSTUMBLER.EXE-0BFEE568.pf	1
ETHEREAL.EXE-1C148EEF.pf	1

Εικόνα 4 - Η καρτέλα «Run Programs» του εργαλείου «Autopsy»

3.2.3. Εξάγοντας το αρχείο «NTUSER.DAT» μέσω του εργαλείου «Autopsy» (<https://www.autopsy.com/>) από τον φάκελο «C:/Documents and Setting/Mr. Evil» και εισάγοντας το στην εφαρμογή «UserAssist v2.6.0.0» (<https://blog.didierstevens.com/programs/userassist/>). Εντός του αρχείου, στην διαδρομή

«NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist» περιέχονται τα κρυπτογραφημένα, με ROT-13<sup>1</sup>, κλειδιά τα οποία εμφανίζουν πληροφορίες σχετικά με την εκτέλεση των λογισμικών στο λειτουργικό σύστημα. Παρακάτω παρουσιάζεται ο αριθμός των εκτελέσεων των κακόβουλων λογισμικών του εικονικού δίσκου (Εικόνα 5).

UserAssist 2.6.0.0						
Commands Help		Index	Name	Session	Counter	Last
115	UEME_RUNPATH:C:\Program Files\Ethereal\ethereal.exe			4	1	8/27/2004 6:34:54 PM
111	UEME_RUNPATH:C:\Program Files\Network Stumbler\NetStumbler.exe			4	1	8/27/2004 6:12:35 PM
107	UEME_RUNPATH:C:\Program Files\Look@LAN\LookAtLan.exe			3	2	8/26/2004 6:06:14 PM
102	UEME_RUNPATH:C:\Program Files\Cain\Cain.exe			4	2	8/27/2004 6:33:02 PM
59	UEME_RUNPIDL:%csidl2%\Anonymizer Toolbar			1	2	

Εικόνα 5 - Ο αριθμός των εκτελέσεων των κακόβουλων λογισμικών του εικονικού δίσκου

Αξίζει να αναφερθεί πως για το εργαλείο «Anonymizer Toolbar» δεν έχει δημιουργηθεί αρχείο «prefetch», καθώς εκτελείται εντός του web browser.

<sup>1</sup> Αλγόριθμος αντικατάστασης χαρακτήρων κατά 13 θέσεις.

### 3.3. Εντοπισμός οποιωνδήποτε δεδομένων μπορεί να έχουν παραχθεί από τη χρήση του παραπάνω λογισμικού

Όνομα	Διαδρομή	Εφαρμογή	Περιγραφή
interception	C:\Documents and Settings\Mr. Evil\interception	Ethereal	Περιέχει τα αποτελέσματα της διαδικασίας υποκλοπής
recent	C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent	Ethereal	Παράγεται κάθε φορά που τερματίζεται η εφαρμογή και περιέχει τις πιο πρόσφατες ρυθμίσεις

Πίνακας 6 - Δεδομένα που έχουν παραχθεί από τη χρήση κακόβουλου λογισμικού

### 3.4. Εντοπισμός οποιωνδήποτε δεδομένων μπορεί να έχουν υποκλαπεί

Δεδομένου ότι το εργαλείο «Ethereal» χρησιμοποιείται για τη διενέργεια υποκλοπών, πραγματοποιήθηκε έρευνα στα παραγόμενα αρχεία του. Στο αρχείο «recent» που βρίσκεται στη διαδρομή «C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent» και αποθηκεύει τις πιο πρόσφατες ρυθμίσεις, βρέθηκε η διαδρομή του αρχείου που περιέχει πληροφορίες για την πιο πρόσφατη υποκλοπή (Εικόνα 6).

Name	S	C	O	Created Time	Access Time	Modified Time
[current folder]				2004-08-27 18:35:53 EEST	2004-08-27 18:40:31 EEST	2004-08-27 18:35:53
[parent folder]				2004-08-20 02:04:05 EEST	2004-08-27 18:42:40 EEST	2004-08-27 18:35:53
preferences			1	2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST	2004-08-27 18:35:53
recent			1	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25

The right pane also displays the contents of the 'recent' file, which includes configuration settings for Ethereal 0.10.6, capture files, display filters, and toolbar configurations.

```

# Recent settings file for Ethereal 0.10.6.
#
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.

##### Recent capture files (latest last) #####
recent.capture_file: C:\Documents and Settings\Mr. Evil\interception
#####
##### Recent display filters (latest last) #####
recent.display_filter: (ip.addr eq 192.168.254.2 and ip.addr eq 207.68.174.248) and (tcp.port eq 1337 and tcp.port eq 80)
#
# Main Toolbar show (hide).

```

Εικόνα 6 - Οι πληροφορίες για την πιο πρόσφατη υποκλοπή από το αρχείο «recent»

Εντός των αρχείου «interception» εμφανίζονται τα δεδομένα που υποκλάπηκαν.

Φαίνεται πως το θύμα περιηγούνταν στο διαδίκτυο μέσω ενός «Pocket PC», με λειτουργικό σύστημα «Windows CE – Version 4.20», επεξεργαστή «Intel(R) PXA255» και ανάλυση οθόνης 240x320px με βάθος χρώματος 16bit (Εικόνα 7). Οι ιστότοποι που επισκέφθηκε κατά τη διάρκεια της διαδικασίας υποκλοπής ήταν οι «mobile.msn.com» (Εικόνα 8) και «MSN Hotmail» (Εικόνα 9).

The screenshot shows a digital forensic interface. At the top, it displays a file listing for 'Listing /img\_4Dell Latitude CPi.E01/vol\_vol2/Documents and Settings/Mr. Evil' with 19 results. Below this is a table view with columns: Name, S, C, O, Created Time, Access Time, Modified Time, Change Time, and Size. The table lists several files including 'Templates', '.gtk-bookmarks', 'interception' (marked with a yellow warning icon), 'NTUSER.DAT', 'ntuser.dat.LOG', and 'ntuser.ini'. Below the table is a detailed view of the 'interception' file. It shows the following network traffic:

```
Content-Type: text/html; charset=utf-8
Content-Length: 214
Expires: -1
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0">here</a>.</h2>
</body></html>
U/A*
GET /hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0 HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color 16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: Ic=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFvRAbKrt=q6edOGfSSmKzj3T1CIh6FdbNqQyPyqubrB97DYRuotwoA5kp1Td3eTz3TUz45LQ$$; MSPPProf=5ynNj8z2mEl3KQzUnhBOK5dmrXWUjam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLzfLhhQB8q*Sto5O8d!UJp8ulxJB5g4RJME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVIAO1b2zXMIxnmPnOpEtasIPX0coWMO$$
```

Εικόνα 7 - Πληροφορίες για την συσκευή του θύματος

```
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
```

Εικόνα 8 - Ο ιστότοπος «mobile.msn.com» που επισκέφθηκε το θύμα

```

Content-Type: text/html; charset=utf-8
Content-Length: 7983
Expires: -1
<html>
<head>
<title>MSN Hotmail</title>
</head>

```

Εικόνα 9 - Ο ιστότοπος «MSN Hotmail» που επισκέφθηκε το θύμα

Οι παραπάνω ισχυρισμοί επαληθεύονται από το περιεχόμενο του αρχείου «packets.pcap» που παράγεται από την εφαρμογή «Bulk\_Extractor» (προεγκατεστημένη στο λειτουργικό σύστημα «Kali Linux») (Εικόνα 10). Το αρχείο αυτό περιέχει την κίνηση του δικτύου μια δεδομένη χρονική στιγμή, η οποία στη συγκεκριμένη περίπτωση είναι η στιγμή της προαναφερθείσας υποκλοπής.

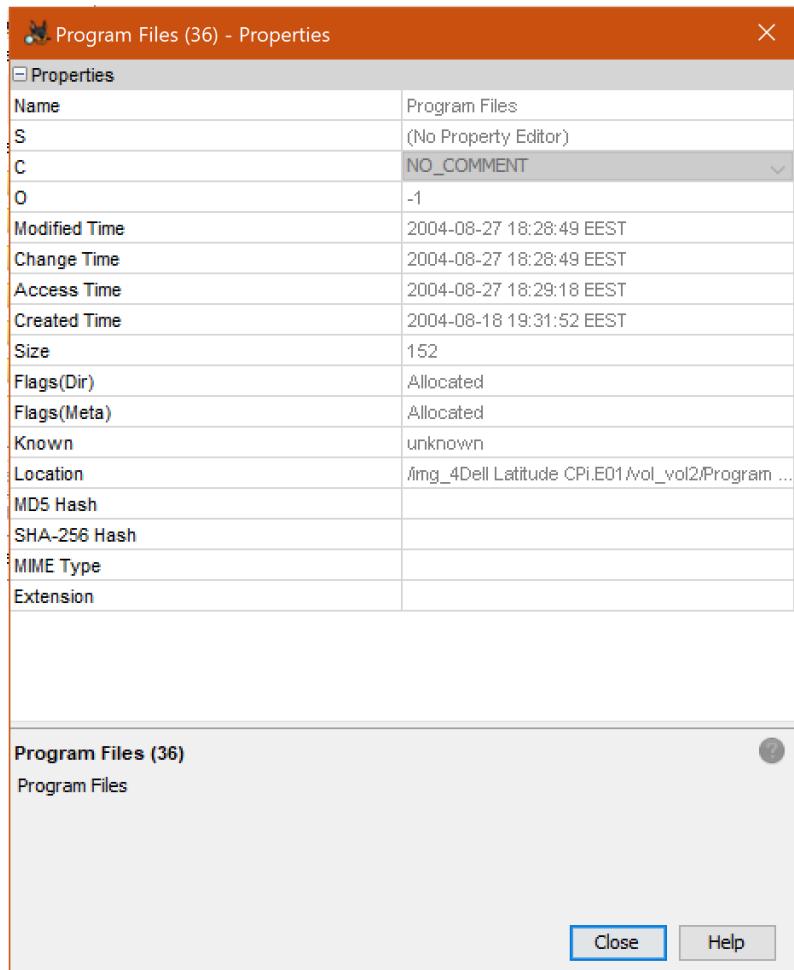
Apply a display filter ... <Ctrl-/>					
Packet list		Narrow & Wide	Case sensitive	String	ppc
No.	Time	Source	Destination	Protocol	Length Info
14	1.364758	192.168.254.2	207.68.174.248	TCP	66 [TCP Dup ACK 7#3] 1337 → 80 [ACK] Seq=1582 Ack=574 Win=3
15	-1093620994...	207.68.174.248	192.168.254.2	TCP	1506 [TCP Out-Of-Order] 80 → 1337 [ACK] Seq=574 Ack=1582 Win=
16	1.399233	192.168.254.2	207.68.174.248	TCP	60 1337 → 80 [ACK] Seq=1582 Ack=6382 Win=26387 Len=0
17	1.400459	192.168.254.2	207.68.174.248	TCP	60 [TCP Window Update] 1337 → 80 [ACK] Seq=1582 Ack=6382 Wi
18	1.412929	192.168.254.2	207.68.174.248	TCP	60 [TCP Window Update] 1337 → 80 [ACK] Seq=1582 Ack=6382 Wi
19	-1093620994...	207.68.174.248	192.168.254.2	HTTP	1506 Continuation
20	1.500755	192.168.254.2	207.68.174.248	TCP	60 1337 → 80 [ACK] Seq=1582 Ack=7834 Win=32768 Len=0
21	-1093620994...	207.68.174.248	192.168.254.2	HTTP	1348 Continuation
22	1.666420	192.168.254.2	207.68.174.248	TCP	60 1337 → 80 [RST] Seq=1582 Win=0 Len=0
23	1.696013	192.168.254.2	207.68.174.248	TCP	62 1338 → 80 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM
24	-1093620994...	207.68.174.248	192.168.254.2	TCP	62 80 → 1338 [SYN, ACK] Seq=0 Ack=1 Win=17424 Len=0 MSS=145
25	1.794097	192.168.254.2	207.68.174.248	TCP	60 1338 → 80 [ACK] Seq=1 Ack=1 Win=32768 Len=0
26	1.808842	192.168.254.2	207.68.174.248	HTTP	937 GET /content/images/img_ppc_sharkfin_MSNLogo.gif HTTP/1.
27	-1093620994...	207.68.174.248	192.168.254.2	TCP	54 80 → 1338 [ACK] Seq=1 Ack=84 Win=16544 Len=0
↓ Frame 26: 937 bytes on wire (7496 bits), 937 bytes captured           ↓ Ethernet II, Src: HewlettP_80:47:17 (00:0f:20:80:47:17)           ↓ Internet Protocol Version 4, Src: 192.168.254.2, Dst: 207.68.174.248           ↓ Transmission Control Protocol, Src Port: 1338, Dst Port: 80           ↓ Hypertext Transfer Protocol           ↓ GET /content/images/img_ppc_sharkfin_MSNLogo.gif HTTP/1.1           Accept: */*           UA-OS: Windows CE (Pocket PC) - Version 4.20\r\n           UA-color: color16\r\n           UA-pixels: 240x320\r\n           UA-CPU: Intel(R) PXA255\r\n           UA-Voice: FALSE\r\n           Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093           UA-Language: JavaScript\r\n           Accept-Encoding: gzip, deflate\r\n					
0070	0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 41				.Accept: */*\r\nUA-
0080	2d 4f 53 3a 20 57 69 6e 64 6f 77 73 20 43 45 20				-OS: Win doW's CE
0090	28 50 6f 63 6b 65 74 20 50 43 29 20 2d 20 56 65				(Pocket PC) - Ve
00a0	72 73 69 6f 6e 20 34 2e 32 30 0d 0a 55 41 2d 63				rsion 4. 20..UA-c
00b0	6f 6c 6f 72 3a 20 63 6f 6c 6f 72 31 36 0d 0a 55				olor: co lor16..U
00c0	41 2d 70 69 78 65 6c 73 3a 20 32 34 38 78 33 32				A-pixels : 240x32
00d0	30 0d 0a 55 41 2d 43 50 55 3a 20 49 6e 74 65 6c				0..UA-CP U: Intel
00e0	28 52 29 20 50 58 41 32 35 35 0d 0a 55 41 2d 56				(R) PXA2 55..UA-V
00f0	6f 69 63 65 3a 20 46 41 4c 53 45 0d 0a 52 65 66				oice: FA LSE..Ref
0100	65 72 65 72 3a 20 68 74 74 70 3a 2f 2d 6f 62				erer: ht tp://mob
0110	69 6c 65 2e 6d 73 6e 2e 63 6f 6d 2f 68 6d 2f 66				ile.msn. com/hm/f
0120	6f 6c 64 65 72 2e 61 73 70 78 3f 74 73 3d 31 30				older.as px?ts=109
0130	39 33 36 30 31 32 39 34 26 66 74 73 3d 31 30 39				93601294 &fts=109
0140	33 35 36 36 34 35 39 26 66 6f 6c 64 65 72 3d 41				3566459& folder=A
0150	43 54 49 56 45 26 6d 73 67 3d 30 0d 0a 55 41 2d				CTIVE&ms g=0..UA-

Εικόνα 10 - Το περιεχόμενο του αρχείου «packets.pcap» που παράγεται από την εφαρμογή «Bulk\_Extractor»

### 3.5. Εντοπισμός της ημερομηνίας εγκατάστασης του λειτουργικού συστήματος

Κατόπιν έρευνας που διεξήχθη στα αρχεία του συστήματος αποδείχθηκε πως τον αρχικό λειτουργικό σύστημα του υπολογιστή ήταν το «Windows 98», το οποίο στη συνέχεια ενημερώθηκε σε «Windows XP Professional». Πιο συγκεκριμένα, σύμφωνα με την ημερομηνία δημιουργίας του φακέλου «Program Files», που δημιουργείται κατά

την εγκατάσταση του λειτουργικού συστήματος, συμπεραίνεται πως τα «Windows 98» εγκαταστάθηκαν στις 2004-08-18 19:31:52 EEST (Εικόνα 11).



Εικόνα 11 - Πληροφορίες του φακέλου «Program Files»

Έπειτα, η ενημέρωση σε «Windows XP Professional» ξεκίνησε, σύμφωνα με την ημερομηνία δημιουργίας του αρχείου «boot.ini»<sup>2</sup> που βρίσκεται στο «root» του «C:/», στις 2004-08-19 19:47:33 EEST (Εικόνα 12) και ολοκληρώθηκε, σύμφωνα με την τιμή του υποκλειδιού «InstallDate» του «Registry», που βρίσκεται στη διαδρομή «C:/Windows/system32/config/software\Microsoft\Windows NT\CurrentVersion», στις 2004-08-20 01:48:27 EEST (Εικόνα 13).

<sup>2</sup> Αρχείο που περιέχει τις ρυθμίσεις εκκίνησης για υπολογιστές με λειτουργικά συστήματα έως Windows XP

Listing  
/img\_4Dell Latitude CPi.E01/vol\_vol2

Table	Thumbnail	Summary
Name	Created Time	
AUTOEXEC.BAT	2004-08-18 19:53:34 EEST	
<b>boot.ini</b>	<b>2004-08-19 19:47:33 EEST</b>	
BOOTLOG.PRV	2004-08-18 19:56:12 EEST	
BOOTLOG.TXT	2004-08-19 18:39:26 EEST	

Εικόνα 12 - Η ημερομηνία δημιουργίας των αρχείου «boot.ini»

Metadata		
<b>Name:</b> CurrentVersion <b>Number of subkeys:</b> 57 <b>Number of values:</b> 17 <b>Modification Time:</b> 2004-08-27 15:08:22 GMT +00:00		
Values		
Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
<b>InstallDate</b>	REG_DWORD	<b>0x41252e3b (1092955707)</b>
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS

Εικόνα 13 - Η τιμή του «κλειδιού» «InstallDate» του Registry

Αξίζει να επισημανθεί πως η τιμή του κλειδιού «InstallDate» εμφανίζεται σε μορφή «Unix hex timestamp», συνεπώς χρήζει μετατροπής στην τοπική ζώνη ώρας, η οποία έγινε με τη βοήθεια του εργαλείου: <https://www.epochconverter.com/>.

### 3.6. Εντοπισμός του λειτουργικού συστήματος που χρησιμοποιήθηκε

Σύμφωνα με την τιμή του υποκλειδιού «ProductName» του «Registry», που βρίσκεται στη διαδρομή «C:/Windows/system32/config/software\Microsoft\Windows NT\CurrentVersion», το λειτουργικό σύστημα που βρέθηκε ότι χρησιμοποιήθηκε στον υπολογιστή-πειστήριο είναι το «Windows XP» (Εικόνα 14). Επίσης, λόγω της μη ύπαρξης του υποκλειδιού «CSDVersion», προκύπτει πως δεν έχει γίνει εγκατάσταση κάποιου «Service Pack».

Values		
Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	55274-640-0147306-23684
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34...
LicenseInfo	REG_BIN	34 54 AE DC C7 2E 3D E5 8B 15 06 1A 8C 74 A6 55...

Εικόνα 14 - Το λειτουργικό σύστημα του υπολογιστή-πειστηρίου

Ακόμη, βάσει του περιεχομένου του αρχείου «boot.ini» που βρίσκεται στο «root» του «C:/», το οποίο περιλαμβάνει τις επιλογές εκκίνησης των υπολογιστών με λειτουργικό σύστημα έως «Windows XP» (από την έκδοση «Vista» και έπειτα έχει αντικατασταθεί από το «Boot Configuration Data - BCD»), η πλήρης ονομασία της έκδοσης του λειτουργικού συστήματος είναι «Windows XP Professional» (Εικόνα 15).

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context					
Strings	Indexed Text	Translation										
Page: 1 of 1 Page	<input type="button" value="←"/> <input type="button" value="→"/>	Matches on page: - of - Match	<input type="button" value="←"/> <input type="button" value="→"/>									
100% <input type="button" value="🔍"/> <input type="button" value="➕"/>												
<pre>[boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect</pre>												

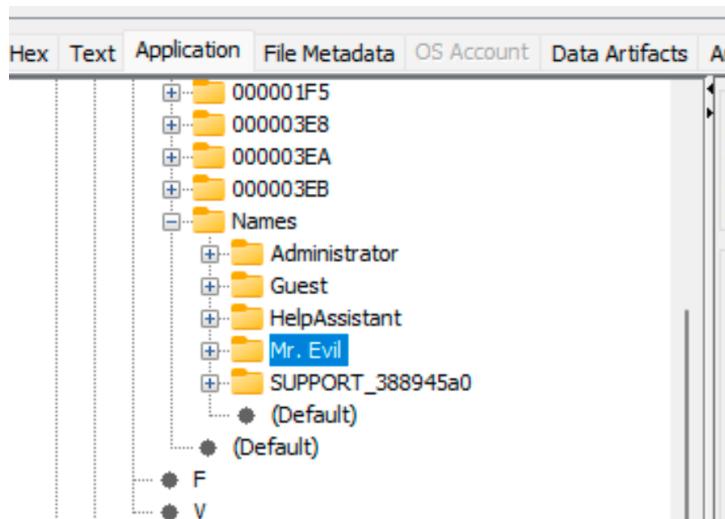
Εικόνα 15 - Η πλήρης ονομασία της έκδοσης του λειτουργικού συστήματος του υπολογιστή-πειστηρίου

### **3.7. Εντοπισμός του ονόματος λογαριασμού (account name) του υπολογιστή**

Η ανάλυση του αρχείου Registry «SAM», που περιλαμβάνει πληροφορίες για όλους τους υπάρχοντες λογαριασμούς χρηστών και βρίσκεται στη διαδρομή «C:/Windows/system32/config/SAM», έχει ως αποτέλεσμα την εύρεση του υποκλειδιού «Users», στον οποίο περιέχονται πέντε (5) υποκλειδιά που αντιστοιχούν στους λογαριασμούς χρηστών του υπολογιστή. Εντός του κάθε υποκλειδιού υπάρχουν δύο τιμές «F» και «V» και πιο συγκεκριμένα, στην δεύτερη εξ αυτών, εμφανίζεται το όνομα του χρήστη. Στην παρούσα περίπτωση, ο λογαριασμός του χρήστη συσχετίζεται με το υποκλειδί «000003EB» και το όνομά του είναι «Mr. Evil» (Εικόνα 16), κάτι που επιβεβαιώνεται από το περιεχόμενο του υποκλειδιού «Names», που βρίσκεται εντός του ίδιου υποκλειδιού και σχετίζεται με τα ονόματα των λογαριασμών των χρηστών του συστήματος (Εικόνα 17).

SAM		Metadata
SAM		Name: V
Domains		Type: REG_BIN
Account		0x70 00 00 00 00 00 00 00 00 CC 00 00 00 00 00 00 00 00 00 00 00 00 00
Aliases		0x80 00 00 00 CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Groups		0x90 CC 00 00 00 08 00 00 00 01 00 00 00 D4 00 00 00
Users		0xa0 04 00 00 00 00 00 00 00 D8 00 00 00 14 00 00 00
000001F4		0xb0 00 00 00 EC 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00
000001F5		0xc0 F0 00 00 00 04 00 00 00 00 00 00 00 01 00 14 80
000003E8		0xd0 9C 00 00 00 AC 00 00 00 14 00 00 00 44 00 00 00
000003EA		0xe0 02 00 30 00 02 00 00 00 02 C0 14 00 44 00 05 01
000003EB	F	0xf0 01 01 00 00 00 00 01 00 00 00 00 02 C0 14 00
	V	0x100 FF 07 0F 00 01 01 00 00 00 00 05 07 00 00 00
		0x110 02 00 58 00 03 00 00 00 00 24 00 44 00 02 00
		0x120 01 05 00 00 00 00 00 05 15 00 00 00 92 E0 3C 77
		0x130 54 19 0E 29 A8 37 D6 65 EB 03 00 00 00 00 18 00
		0x140 FF 07 0F 00 01 02 00 00 00 00 05 20 00 00 00
		0x150 20 02 00 00 00 00 14 00 5B 03 02 00 01 01 00 00
		0x160 00 00 00 01 00 00 00 00 01 02 00 00 00 00 00 05
		0x170 20 00 00 00 20 02 00 00 01 02 00 00 00 00 00 05
		0x180 20 00 00 20 02 00 00 4D 00 72 00 2E 00 20 00
		0x190 45 00 76 00 69 00 6C 00 01 02 00 00 07 00 00 00
		0x1a0 01 00 01 00 01 00 01 DB 99 01 CE 00 2E AA F0
		0x1b0 5F E8 1E AD 0A CA 0E C8 01 00 01 00 01 00 01 00

*Eikόνα 16 - Το υποκλειδί «000003EB» του αργείου Registry «SAM»*



Εικόνα 17 - Το υποκλειδί «Names» του αρχείου Registry «SAM»

### 3.8. Επιβεβαίωση ή διάψευση της υποψίας για πρότερη μετακίνηση του υπολογιστή σε άλλη γεωγραφική περιοχή

3.8.1. Πρώτη σκέψη ως προς την ανάλυση της τοποθεσίας του υπόπτου αποτέλεσε η εξέταση των διευθύνσεων «IP», με τις οποίες αλληλεπίδρασε. Βάσει του εργαλείου <https://www.geolocation.com/>, αυτές οι διευθύνσεις αντιστοιχούσαν στις εξής περιοχές:

- **Νέα Υόρκη** (207.68.174.248 - C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent)
- **Σανιβέλ - Καλιφόρνια** (64.68.82.189 - C:/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/JIRVJY9X/search[2])
- **Πλάνο - Τέξας** (216.62.23.121 - C:/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/whatismyip[1])
- **Χονγκ Κονγκ - Κίνα** (207.46.130.100 - C:/WINDOWS/system32/config/SysEvent.Evt)
- **Ρέτμοντ - Ουάσινγκτον** (65.54.179.230 – C:/pagefile.sys)

3.8.2. Στη συνέχεια, εξετάστηκαν τα αρχεία Registry με τη βοήθεια του εργαλείου «Registry Explorer» (<https://ericzimmerman.github.io/#!index.md>). Στο αρχείο «system» (C:/WINDOWS/system32/config/system) βρέθηκαν ορισμένες

διεγραμμένες και μη αντιστοιχισμένες τιμές (Εικόνα 18), οι οποίες περιείχαν τις παρακάτω διευθύνσεις IP, που βάσει του εργαλείου <https://www.geolocation.com/> αντιστοιχούσαν στις εξής περιοχές:

- **Χιούστον – Τέξας** (151.164.11.201)
- **Ρίτσαρντσον – Τέξας** (151.164.1.8)

Εικόνα 18 - Οι διεγραμμένες και μη αντιστοιχισμένες τιμές του αρχείου Registry «system»

3.8.3. Κατά την περιήγηση στο σύστημα αρχείων του πειστηρίου βρέθηκε το αρχείο «hiberfil.sys» (C:/hiberfil.sys) (Εικόνα 19), που υποδεικνύει πως ο ύποπτος είχε ενεργοποιημένη την λειτουργία «Hibernation».

Εικόνα 19 - Το αρχείο «hiberfil.sys»

Για την ανάγνωση του παραπάνω αρχείου ακολουθήθηκε η παρακάτω διαδικασία:

1. Πραγματοποιήθηκε λήψη και εγκατάσταση του εργαλείου Volatility 2 (<https://github.com/volatilityfoundation/volatility/wiki/Installation>) σε λειτουργικό σύστημα Kali Linux.
2. Έγινε μετατροπή του αρχείου «hiberfil.sys» σε μορφή «raw memory dump» μέσω της εντολής «vol.py imagedump -f hiberfil.sys -O winxp.img».
3. Αναζητήθηκαν οι συνδέσεις δικτύου που ήταν ενεργές τη στιγμή που τέθηκε σε εφαρμογή η λειτουργία «Hibernation» (Εικόνα 20) με τη χρήση της εντολής «vol.py -f winxp.img --profile=WinXPSP2x86 connscan».

Offset(P)	Local Address	Remote Address	Pid
0x002aa298	192.168.1.111:1183	130.94.133.187:80	1156
0x0108edd8	0.0.0.0:0	0.0.0.0:0	2157104624
0x010b1350	192.168.1.111:1184	209.185.12.42:80	1156
0x01833e68	192.168.1.111:1182	130.94.133.187:80	1156
0x05241420	192.168.1.111:1148	67.114.52.28:80	1524
0x05d26678	192.168.1.111:1175	204.193.136.54:6667	1564
0x06baa540	112.0.0.0:46079	0.0.0.0:45264	4289366312
0x07122820	0.0.0.0:0	0.0.0.0:0	4289091640
0x07847628	192.168.1.111:1179	67.15.24.20:80	1156

Εικόνα 20 - Οι συνδέσεις δικτύου που ήταν ενεργές τη στιγμή που τέθηκε σε εφαρμογή η λειτουργία «Hibernation»

Με τη χρήση του εργαλείου <https://www.geolocation.com/>, οι διευθύνσεις αυτές αντιστοιχούν στις παρακάτω περιοχές:

- **Ρέτμοντ – Ουάσινγκτον** (130.94.133.187, 67.114.52.28)
- **Φοίνιξ - Αριζόνα** (209.185.12.42)
- **Σουάνι – Τζόρτζια** (204.193.136.54)
- **Σαν Χοσέ – Καλιφόρνια** (64.15.24.20)

3.8.4. Παρά τις διάφορες IP που αλληλεπιδρούσε ο ύποπτος, δε φαίνεται να υφίστανται αδιάσειστα στοιχεία ως προς την επιβεβαίωση της υποψίας για πρότερη μετακίνηση του υπολογιστή σε άλλη γεωγραφική περιοχή. Αυτό επαληθεύεται αρχικά, από την ημερομηνία τελευταίας εγγραφής του κλειδιού «TimeZoneInformation» (C:/Windows/System32/config/system\ControlSet001\Control\TimeZoneInformation) η οποία είναι στις 2004-08-19, δηλαδή την ημερομηνία που ξεκίνησε η εγκατάσταση του λειτουργικού συστήματος (Εικόνα 21) και έπειτα, από το περιεχόμενο «NTP» (Network Time Protocol) της τιμής «Type» στη διαδρομή «C:/Windows/System32/config/system\ControlSet001\Services/W32Time/Parameters» (Εικόνα 22), που σημαίνει πως η ώρα του συστήματος συγχρονίζοταν αυτόματα μέσω διαδικτύου. Αξίζει να σημειωθεί πως, σύμφωνα με το κλειδί «TimeZoneInformation», που αναφέρεται παραπάνω, η ζώνη ώρας του συστήματος είχε ρυθμιστεί σε «Central Standard Time» (UTC -6), δηλαδή εντασσόταν στο «timezone» «US & Canada». (Εικόνα 23). Ως εκ τούτου, εφόσον δεν έγινε αλλαγή στην ζώνη ώρας του υπολογιστή από τη στιγμή της εγκατάστασης του λειτουργικού συστήματος, δεν πραγματοποιήθηκε μετακίνηση του σε άλλη γεωγραφική περιοχή.

<input type="checkbox"/>	Key:	ControlSet001\Control\TimeZoneInformation
Selected hive: system	Last write:	2004-08-19 17:20:02

Εικόνα 21 - Η ημερομηνία τελευταίας εγγραφής του κλειδιού «TimeZoneInformation»

	Value Name	Value Type	Data
?	RBC	RBC	RBC
	ServiceMain	RegSz	SvchostEntry_W32Time
	ServiceDll	RegExpandSz	C:\WINDOWS\System32\w32time.dll
▶	NtpServer	RegSz	time.windows.com,0x1
▶	Type	RegSz	NTP

Εικόνα 22 – Το περιεχόμενο «NTP» της τιμής «Type»

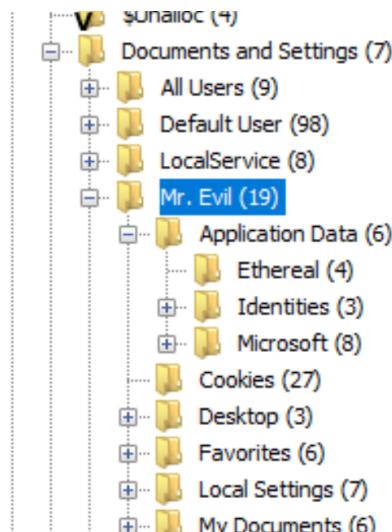
Value Name	Value Data
RBC	RBC
Bias	360
StandardName	Central Standard Time
StandardBias	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	Central Daylight Time
DaylightBias	-60
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
ActiveTimeBias	300

Εικόνα 23 - Το Time Zone του συστήματος

### 3.9. Εντοπισμός επιπλέον χρηστών που είχαν πρόσβαση στον υπολογιστή

Έπειτα από ανάλυση του φακέλου «C:/Document and Settings» διαπιστώθηκε πως ο μοναδικός λογαριασμός χρήστη που δημιουργήθηκε ονομάζεται «Mr. Evil» (Εικόνα 24), ωστόσο, υφίσταται πιθανότητα ύπαρξης περισσότερων λογαριασμών χρηστών, των οποίων οι φάκελοι-προφίλ δεν έχουν δημιουργηθεί. Αυτό μπορεί να οφείλεται σε περιπτώσεις απομακρυσμένης πρόσβασης μέσω «Remote Desktop Protocol - RDP», κάνοντας χρήση της προεπιλεγμένης «πόρτας» (port) 3389. Λόγω αυτού, απαιτήθηκε πιο ενδελεχής έρευνα στο «Registry» και πιο συγκεκριμένα, στο αρχείο «C:/Windows/system32/config/SAM», που περιέχει πληροφορίες για τους υπάρχοντες λογαριασμούς χρηστών. Το αποτέλεσμα της έρευνας είναι πως βρίσκονται καταχωρημένοι πέντε (5) λογαριασμοί χρηστών με τα ακόλουθα ονόματα: Administrator, Guest, HelpAssistant, Mr. Evil, SUPPORT\_388945a0. Εισάγοντας το αρχείο «SAM» σε ένα «registry viewer» και συγκεκριμένα στο «AccessData Registry Viewer» (<https://www.exterro.com/ftk-product-downloads/registry-viewer-2-0-0>) για

περεταίρω ανάλυση, εξήγηθη το συμπέρασμα πως ο μοναδικός χρήστης που χρησιμοποιούσε τον υπολογιστή ήταν ο «Mr. Evil», καθώς κανένας από τους υπόλοιπους λογαριασμούς δεν είχε πραγματοποίησε σύνδεση. Ένα ακόμη στοιχείο που προέκυψε από την ανάλυση είναι πως ο χρήστης «Mr. Evil» είχε συνδεθεί δεκαπέντε (15) φορές, με την τελευταία να πραγματοποιήθηκε στις 2004-08-27 18:08:23 EEST (15:08:23 UTC) (Εικόνα 25).



Εικόνα 24 - Το περιεχόμενο του φακέλου «C:/Document and Settings»

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 A0 73 46 B2 47 8C C4 01 00 00 ...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 10 00 ...

**Key Properties**

Last Written Time	27/Aug/2004 15:08:23 UTC
RID unique identifier	1003
User Name	Mr. Evil
Logon Count	15
Last Logon Time	27/Aug/2004 15:08:23 UTC
Last Password Change Time	19/Aug/2004 23:03:54 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	«need "SysKey" file»
Country Code	0 (System Default)

**LM Hash**  
LanMan password hash.

Εικόνα 25 - Πληροφορίες για τον λογαριασμό χρήστη «Mr. Evil»

Κατά τη διάρκεια της έρευνας εντοπίστηκε στην διαδρομή «C:/Windows/System32/config/software\Microsoft\Windows NT\Current Version\Winlogon» το υποκλειδί «RegisteredOwner», που υποδηλώνει πως ο ιδιοκτήτης του υπολογιστή ονομάζεται «Greg Schardt» (Εικόνα 26), πράγμα που επαληθεύει την υποψία ότι το μικρό όνομα του υπόπτου που συσχετίζεται με τον υπολογιστή είναι «Gregory» και κατά συνέπεια χρησιμοποιεί το ψευδώνυμο «Mr. Evil».

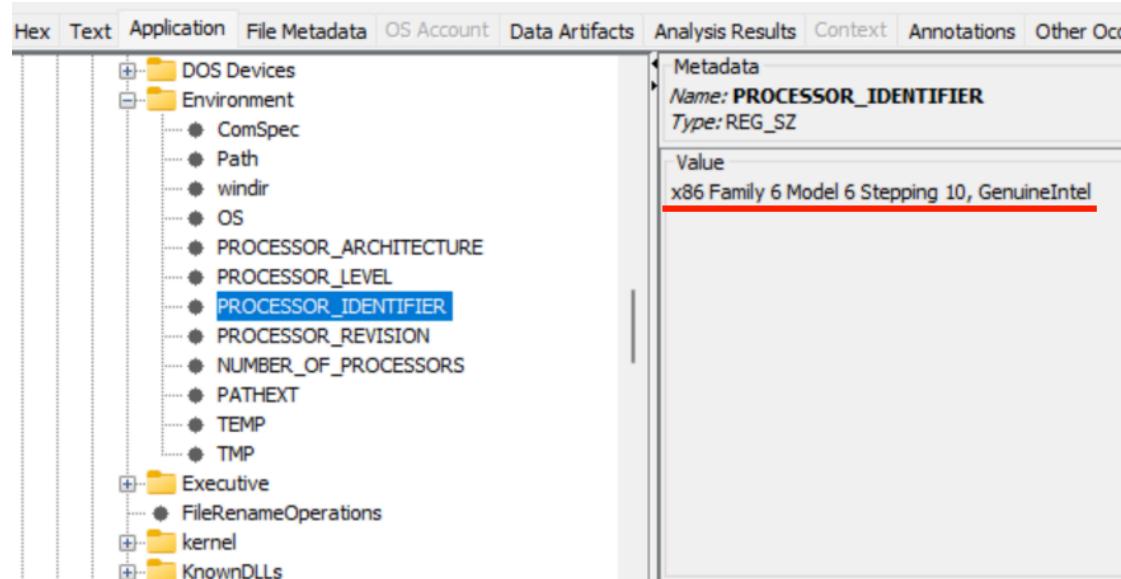
Metadata
Name: RegisteredOwner
Type: REG_SZ

Value
Greg Schardt

Εικόνα 26 - Το όνομα του ιδιοκτήτη του υπολογιστή

Εφόσον αποδείχθηκε πως ο Greg Schardt είναι ο ιδιοκτήτης του συστήματος και χρησιμοποιεί τον μοναδικό ενεργό λογαριασμό του συστήματος (Mr. Evil), είναι πολύ πιθανό ο λογαριασμός αυτός να είναι και ο διαχειριστής του συστήματος, δηλαδή να ανήκει στο «Local Administrators Group». Το πρώτο βήμα για την απόδειξη αυτού του ισχυρισμού είναι η εύρεση τις δεκαεξαδικής (hex) τιμής που αντιπροσωπεύει το γκρουπ των διαχειριστών, η οποία, σύμφωνα με την «Microsoft» (<https://learn.microsoft.com/en-us/dotnet/api/system.security.principal.windowsprincipal.isinrole?view=net-7.0>), είναι «0x220». Επόμενο βήμα είναι η αναζήτηση με βάση το μοναδικό αναγνωριστικό αριθμό (unique ID number) του «Mr. Evil», δηλαδή το «000003EB», στην διαδρομή «SAM\SAM\Domains\BuiltIn\Aliases\Members», ούτως ώστε να βρεθεί η τιμή που περιέχει (20 02 00 00) (πλήρης διαδρομή «SAM\SAM\Domains\BuiltIn\Aliases\Members\S-1-5-21-2000478354-688789844-1708537768\000003EB»). Στη συνέχεια είναι απαραίτητη η εύρεση της έκδοσης του επεξεργαστή, καθώς μέσω αυτής καθίσταται δυνατή η ανάγνωση του παραπάνω

κλειδιού. Σύμφωνα με την τιμή του κλειδιού «PROCESSOR\_IDENTIFIER» που βρίσκεται στη διαδρομή «C:/Windows/System32/config/system\ControlSet001\Control\Session Manager\Environment» (Εικόνα 27), ο επεξεργαστής είναι «Intel» με αρχιτεκτονική «x86». Γνωρίζοντας πως οι επεξεργαστές «Intel» με αρχιτεκτονική «x86» χρησιμοποιούν τον κανόνα (convention) «Little-endian» για την ταξινόμηση των δεδομένων που μεταφέρονται από τον καταχωρητή (Register) στην μνήμη (Memory) (<https://levelup.gitconnected.com/little-endian-vs-big-endian-eb2a2c3a9135>), η παραπάνω τιμή «20 02 00 00» διαβάζεται από τα δεξιά προς τα αριστερά, συνεπώς μετατρέπεται σε «0x00000220», το οποίο είναι ίδιο με το «0x220» που ορίζει η «Microsoft» ως διαχειριστή (Administrator). Άρα ο λογαριασμός «Mr. Evil» είναι και διαχειριστής του συστήματος.



Εικόνα 27 - Πληροφορίες για τον επεξεργαστή του συστήματος

### 3.10. Εντοπισμός του κατασκευαστή της κάρτας δικτύου που χρησιμοποιήθηκε για τις παράνομες δραστηριότητες

Για την εύρεση των καρτών δικτύου που ήταν συνδεδεμένες στον υπολογιστή ακολουθήθηκε η διαδρομή «C:/Windows//System32/config/software\Microsoft\Windows NT\CurrentVersion\NetworkCards», στην οποία υπήρχαν δύο υποκλειδιά που αντιστοιχούσαν σε δύο διαφορετικές κάρτες δικτύου (Εικόνες 28 και 29).

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences									
			<ul style="list-style-type: none"> <li>ModuleCompatibility</li> <li>Network</li> <li>NetworkCards           <ul style="list-style-type: none"> <li>11               <ul style="list-style-type: none"> <li>● ServiceName</li> <li>● Description</li> </ul> </li> <li>2               <ul style="list-style-type: none"> <li>● ServiceName</li> <li>● Description</li> </ul> </li> </ul> </li> <li>● OpenGLDrivers</li> <li>Perflib</li> <li>PerHwIdStorage</li> <li>Ports</li> <li>Prefetcher</li> <li>Print</li> </ul>		<p>Metadata</p> <p>Name: 2</p> <p>Number of subkeys: 0</p> <p>Number of values: 2</p> <p>Modification Time: 2004-08-19 17:07:19 GMT+00:00</p> <p>Values</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>ServiceName</td> <td>REG_SZ</td> <td>{6E4090C2-FAEF-489A-8575-505D21FC1049}</td> </tr> <tr> <td>Description</td> <td>REG_SZ</td> <td>Xircom CardBus Ethernet 100 + Modem 56 (Ether...</td> </tr> </tbody> </table>	Name	Type	Value	ServiceName	REG_SZ	{6E4090C2-FAEF-489A-8575-505D21FC1049}	Description	REG_SZ	Xircom CardBus Ethernet 100 + Modem 56 (Ether...				
Name	Type	Value																
ServiceName	REG_SZ	{6E4090C2-FAEF-489A-8575-505D21FC1049}																
Description	REG_SZ	Xircom CardBus Ethernet 100 + Modem 56 (Ether...																

Εικόνα 28 - Η κάρτα δικτύου μάρκας «Xircom»

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences									
			<ul style="list-style-type: none"> <li>ModuleCompatibility</li> <li>Network</li> <li>NetworkCards           <ul style="list-style-type: none"> <li>11               <ul style="list-style-type: none"> <li>● ServiceName</li> <li>● Description</li> </ul> </li> <li>2               <ul style="list-style-type: none"> <li>● ServiceName</li> <li>● Description</li> </ul> </li> </ul> </li> <li>● OpenGLDrivers</li> <li>Perflib</li> <li>PerHwIdStorage</li> <li>Ports</li> <li>Prefetcher</li> <li>Print</li> <li>ProfileList</li> </ul>		<p>Metadata</p> <p>Name: 11</p> <p>Number of subkeys: 0</p> <p>Number of values: 2</p> <p>Modification Time: 2004-08-27 15:31:44 GMT+00:00</p> <p>Values</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>ServiceName</td> <td>REG_SZ</td> <td>{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}</td> </tr> <tr> <td>Description</td> <td>REG_SZ</td> <td>Compaq WL110 Wireless LAN PC Card</td> </tr> </tbody> </table>	Name	Type	Value	ServiceName	REG_SZ	{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}	Description	REG_SZ	Compaq WL110 Wireless LAN PC Card				
Name	Type	Value																
ServiceName	REG_SZ	{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}																
Description	REG_SZ	Compaq WL110 Wireless LAN PC Card																

Εικόνα 29 - Η κάρτα δικτύου μάρκας «Compaq»

Για τον εντοπισμό της κάρτας δικτύου που χρησιμοποιήθηκε για τις παράνομες δραστηριότητες, πραγματοποιήθηκε έρευνα στα αρχεία του εργαλείου «Look@LAN», το οποίο χρησιμοποιείται για την ανάλυση της κίνησης του δικτύου. Πιο συγκεκριμένα, το αρχείο «irunin.ini» που βρίσκεται στη διαδρομή «C:/Program Files/Look@LAN/irunin.ini», περιέχει δεδομένα όπως το όνομα του χρήστη (%LANUSER%), τη διεύθυνση IP (%LANIP%) και την διεύθυνση «MAC» της κάρτας δικτύου που χρησιμοποιήθηκε (%LANNIC%) (Εικόνα 30). Αναζητώντας τη διεύθυνση «MAC» στη βάση δεδομένων του εργαλείου <https://www.adminsub.net/>, βρέθηκε ότι αντιστοιχεί στον κατασκευαστή «XIRCOM» (Εικόνα 31).

```

[Config]
ConfigFile=C:\Program Files\Look@LAN\irunin.dat
LanguageFile=C:\Program Files\Look@LAN\irunin.lng
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER %="Mr. Evil"
%LANIP%="192.168.1.111"
%LANNIC%="0010a4933e09"

```

*Eικόνα 30 - Τα περιεχόμενα του αρχείου «irunin.ini»*

## MAC Address Finder

MAC address or vendor:

Enter **first 6 characters** or **full MAC address**. Or search by Vendor name,  
e.g. **cisco** or **apple**

Database updated - April 25, 2020

### Search results for "0010a4933e09"

MAC	Vendor
0010A4	XIRCOM

*Eικόνα 31 - Αναζήτηση βάσει διεύθυνσης «MAC» στο εργαλείο «<https://www.adminsub.net/>»*

**3.11. Επαλήθευση ή διάψευση των καταθέσεων των συνεργών του προκειμένου να ασκηθεί συμπληρωματική ποινική δίωξη**

Σύμφωνα με τις ομολογίες των συνεργών του κατηγορούμενου, πως είχε σκοπό να σταθμεύσει το αυτοκίνητό του έξω από σημεία τα οποία θα ήταν εντός της εμβέλειας ασύρματων σημείων πρόσβασης, όπως τα Starbucks και άλλα hotspots της T-Mobile, με στόχο την υποκλοπή πακέτων διαδικτυακής κίνησης, πραγματοποιήθηκε αναζήτηση στο περιεχόμενο του εικονικού δίσκου χρησιμοποιώντας λέξεις κλειδιά όπως: «T-Mobile» και «Starbucks». Τα αποτελέσματα της αναζήτησης με την λέξη κλειδί «T-Mobile» έδειξαν πως ο ύποπτος παρουσίασε ενδιαφέρον για την εταιρία τηλεπικοινωνιών, καθώς είχε επισκεφθεί έναν ιστότοπο που ανέφερε τις επιχειρηματικές κινήσεις της, στις οποίες περιλαμβανόταν και η συνεργασία της με άλλες επιχειρήσεις παρέχοντάς τους τεχνολογικές λύσεις, όπως το «hotspot» (Εικόνα 32).

Name	Keyword Preview	Location	Modified Time	Change Time	Access T...
netstumbler[1].htm	reached an agreement with <T-Mobile> USA Inc. to install ...	/Img_4Dell Latitude CPI.E01/vol_vo2/Documents and Settin...	2004-08-27 18:09:47 EEST	2004-08-27 18:09:47 EEST	2004-08-

**Startup Promises Pre-Standard WiMAX Mobility**  
A startup came out of stealth mode last week saying that it will offer wireless broadband systems based on the unratified 802.16e standard for mobile wireless broadband.  
[READ MORE](#)

**Embedded Wi-Fi Market Undergoing Major Shift**  
One of the hottest technology markets, Wireless LAN (WLAN), or Wi-Fi, is undergoing a fundamental shift, according to In-Stat/MDR. The high-tech market research firm reports that in 2003 removable Wi-Fi PC card adapters were displaced as the most popular Wi-Fi adapter by embedded Mini PCI card adapters.  
[READ MORE](#)

**Red Roof Inns To Get Wi-Fi Hotspots**  
Accor North America has reached an agreement with T-Mobile USA Inc. to install wireless Internet access throughout all of its Red Roof Inns over the next year, officials said.  
[READ MORE](#)

Εικόνα 32 - Ιχνος ιστοτόπου που ανέφερε τις επιχειρηματικές κινήσεις της «T-Mobile»

Όσον αφορά στη λέξη κλειδί «Starbucks», βρέθηκε ίχνος από μια επίσκεψη του σε έναν ιστότοπο σχετικό με «Wardriving», το οποίο αποδεικνύει το ενδιαφέρον του υπόπτου για το συγκεκριμένο είδος επίθεσης (Εικόνα 33).

wardriving[1]	<wardriving[1]		/Img_4Dell Latitude CPI.E01/vol_vol2/Documents and Setting... 2004-08-27 18:09:22 EEST	2004-08-27 18:09:22 EEST	2004-08-27 18
netstumbler.chm	U V W	<Wardriving<	... /Img_4Dell Latitude CPI.E01/vol_vol2/Program Files/Netwo... 2004-04-21 09:42:58 EEST	2004-08-27 18:12:16 EEST	2004-08-27 18
wardriving[1]-slack	«wardriving[1]-slack		/Img_4Dell Latitude CPI.E01/vol_vol2/Documents and Setting... 2004-08-27 18:09:22 EEST	2004-08-27 18:09:22 EEST	2004-08-27 18
code[1].php	WarLinux - "The bootable «wardriving» linux distribution"		/Img_4Dell Latitude CPI.E01/vol_vol2/Documents and Setting... 2004-08-27 18:09:30 EEST	2004-08-27 18:09:30 EEST	2004-08-27 18
index.dat	http://www.wardriving.com/«wardriving[1]HTTP/1.1 200 OK		/Img_4Dell Latitude CPI.E01/vol_vol2/Documents and Setting... 2004-08-27 18:44:34 EEST	2004-08-27 18:44:34 EEST	2004-08-20 02

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

Download Images

Εικόνα 33 - Ιχνος ιστοτόπου σχετικού με «Wardriving»

Επίσης, εξετάστηκαν τα αρχεία που παράγονται από τη χρήση του μοναδικού εργαλείου υποκλοπής που ήταν εγκατεστημένο στον υπολογιστή (C:/Documents and Setting/Mr. Evil/Application Data/Ethereal), το Ethereal (C:/Program Files/Ethereal). Αποτέλεσμα της εξέτασης ήταν η εύρεση του στοιχείου πως η προεπιλεγμένη ρύθμιση της κάρτας δικτύου ήταν να χρησιμοποιείται σε «Promiscuous Mode» (λειτουργία της κάρτας δικτύου, σύμφωνα με την οποία όλα τα πακέτα του δικτύου προωθούνται στην κεντρική μονάδα επεξεργασίας – CPU και χρησιμοποιείται κυρίως για υποκλοπή πακέτων δικτύου), κατά την εκτέλεση του «Ethereal». (Εικόνα 34).

preferences		4	2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST
recent		4	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST

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

Strings Indexed Text Translation

Page: 1 of 2 Page Matches on page: - of - Match 100% Reset

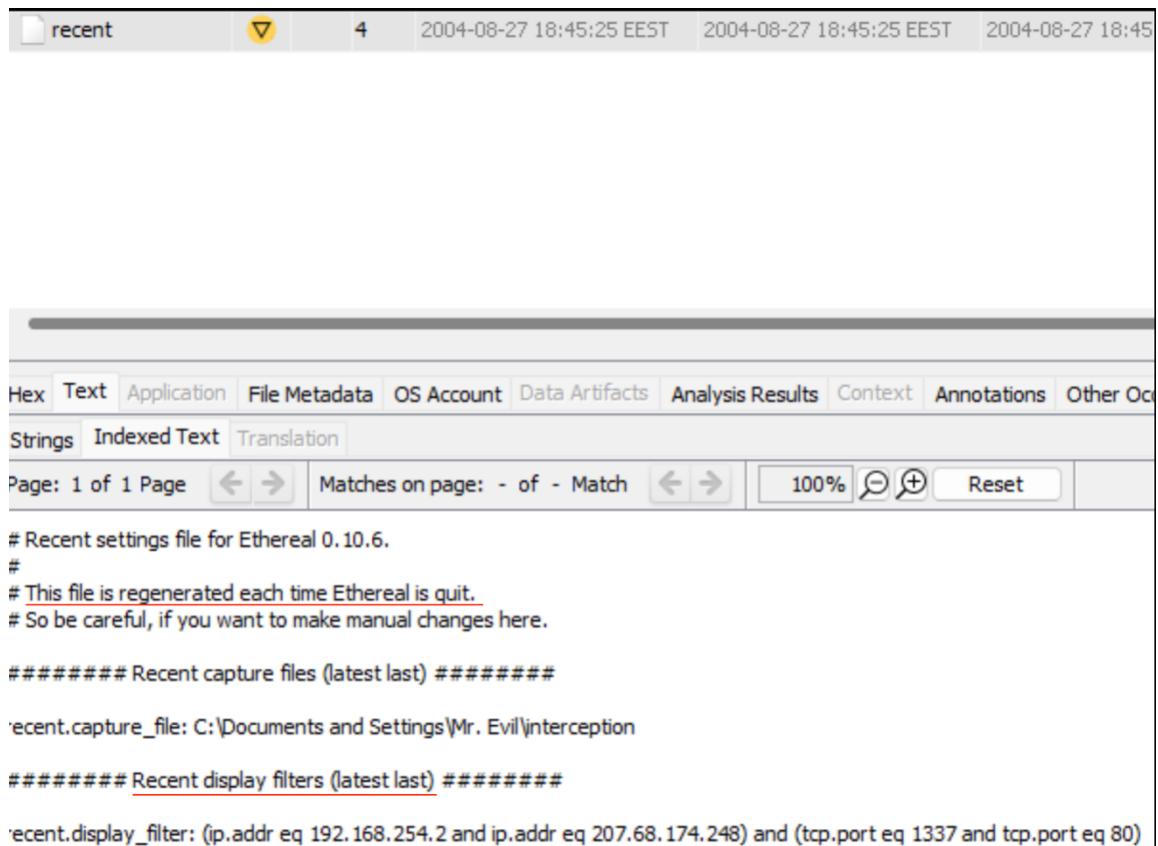
```
stream.server.tg: 00007f
stream.server.bg: ededfb

##### Capture #####
# Default capture device
capture.device: ORINOCO PC Card (Microsoft's Packet Scheduler) : \Device\NPF_{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}

# Capture in promiscuous mode?
# TRUE or FALSE (case-insensitive).
capture.prom_mode: TRUE
```

Εικόνα 34 - Απόδειξη πως η κάρτα δικτύου λειτουργούσε σε «Promiscuous Mode»

Έπειτα, διεξήχθη ανάλυση των διευθύνσεων IP στις οποίες συνδέθηκε ο χρήστης και εκτέλεσε το εργαλείο υποκλοπής. Παραμένοντας στον ίδιο υποφάκελο, εντοπίστηκε το αρχείο «recent», το οποίο δημιουργείται κάθε φορά που τερματίζεται η λειτουργία της εφαρμογής και περιέχει το τελευταίο «φίλτρο» που εφαρμόστηκε κατά τη διαδικασία υποκλοπής δεδομένων. Σε αυτό το αρχείο βρέθηκε μια διεύθυνση IP – στόχος (207.68.174.248) στις «πόρτες» «1337» και «80» (Εικόνα 35).



```
# Recent settings file for Ethereal 0.10.6.
#
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.

##### Recent capture files (latest last) #####
'recent.capture_file: C:\Documents and Settings\Mr. Evil\Interception

##### Recent display filters (latest last) #####
'recent.display_filter: (ip.addr eq 192.168.254.2 and ip.addr eq 207.68.174.248) and (tcp.port eq 1337 and tcp.port eq 80)
```

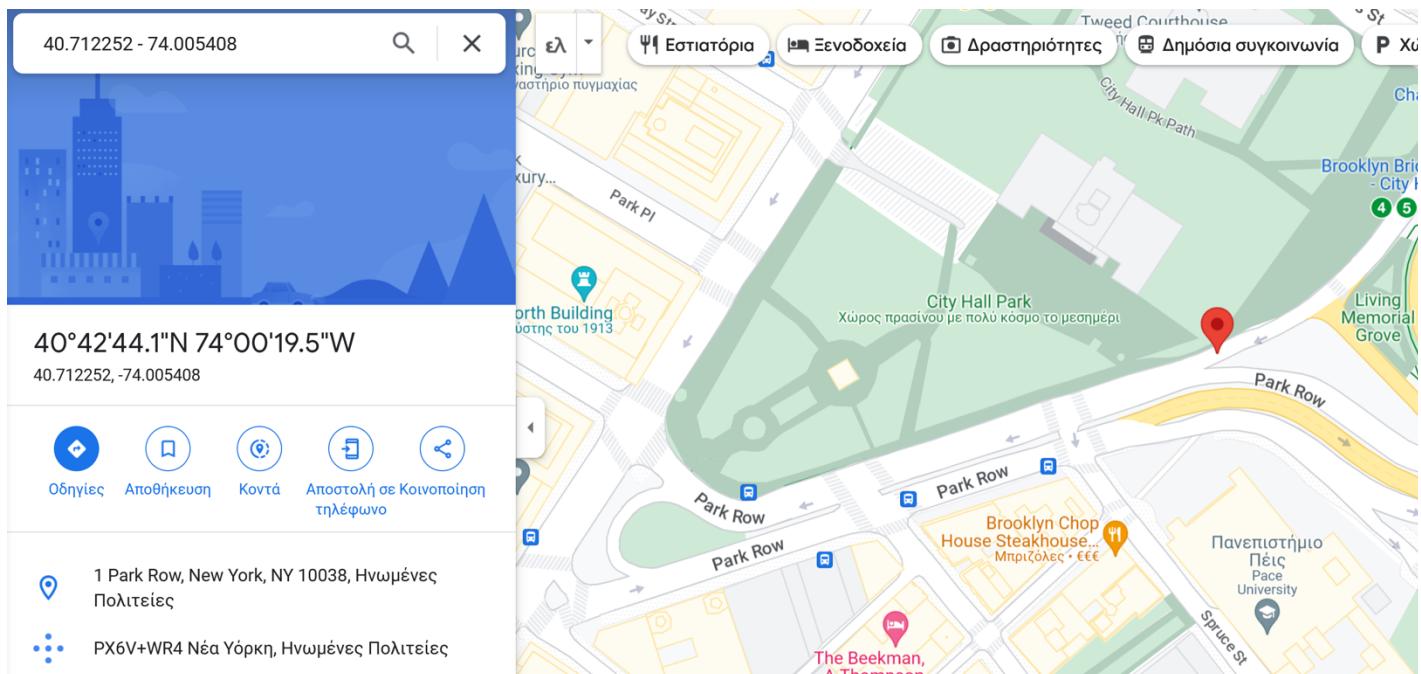
Εικόνα 35 - Το τελευταίο «φίλτρο» που εφαρμόστηκε κατά τη διαδικασία υποκλοπής δεδομένων

Στη συνέχεια, διερευνήθηκε περαιτέρω η διεύθυνση-στόχος με τη χρήση του εργαλείου <https://www.geolocation.com/>, όπου εισάγοντας την διεύθυνση εμφανίζονται σχετικές πληροφορίες, όπως η κατά προσέγγιση τοποθεσία και οι συντεταγμένες (Εικόνα 36).

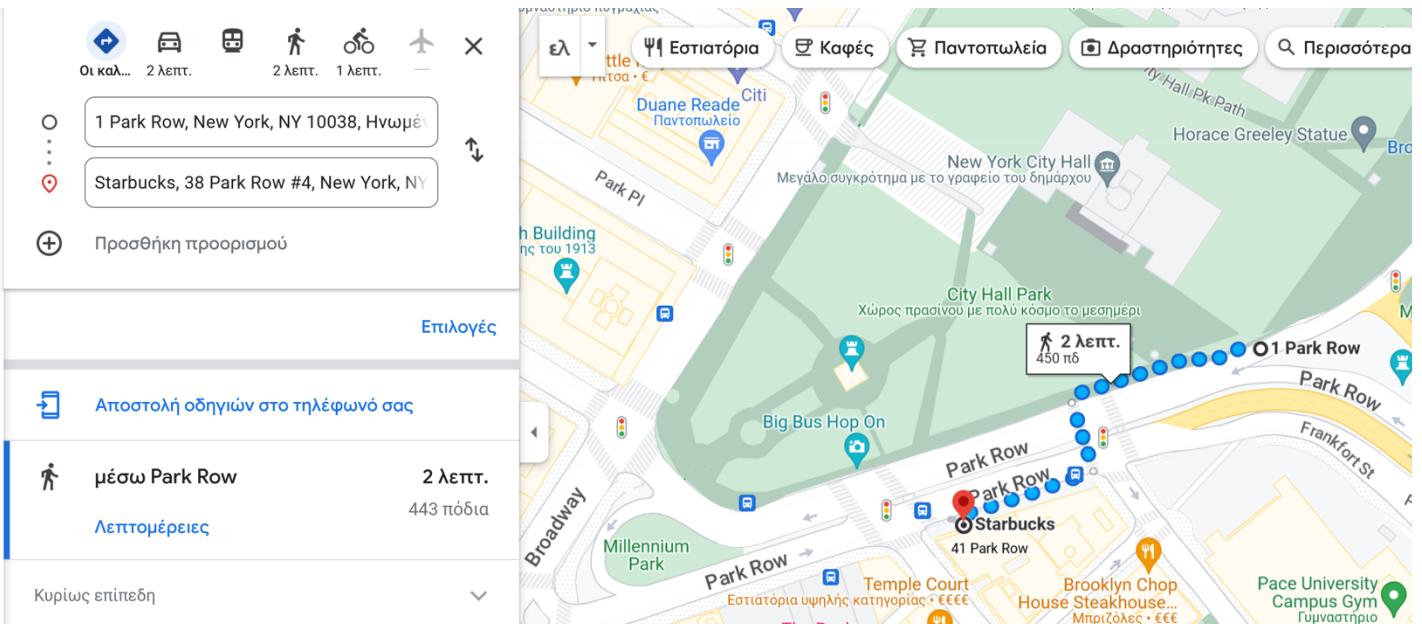
Country	Region	City
United States of America 	New York	New York City
ZIP or Postal Code	Latitude	Longitude
10116	40.712252	-74.005408
ISP	Domain Name	Usage Type
Microsoft Corporation	microsoft.com [WHOIS] [Check Mail Server]	DCH
Weather	Time Zone	Local Time
<a href="#">View Weather</a>	America/New_York	2023-05-15T10:47:39-04:00
Address Type	Category	District
Unicast	Business Software	-
AS Number	AS Name	
8075	Microsoft Corporation	
Proxy	Proxy Provider	
No	-	

Εικόνα 36 - Πληροφορίες σχετικά με την διεύθυνση-στόχο

Κατόπιν, εισάγοντας τα δεδομένα των συντεταγμένων στην εφαρμογή «Google Maps» (<https://www.google.com/maps>), γίνεται αντιληπτό πως η τοποθεσία αντιστοιχεί στην διεύθυνση «1 Park Row, New York» (Εικόνα 37), η οποία, όπως διακρίνεται και στην Εικόνα 38, βρίσκεται πολύ κοντά (450 πόδια – 137 μέτρα) σε ένα κατάστημα «Starbucks».



Εικόνα 37 - Η τοποθεσία που αντιστοιχεί στην διεύθυνση-στόχο



Εικόνα 38 - Η απόσταση της τοποθεσίας της διεύθυνσης-στόχου από το κοντινότερο «Starbucks»

Συνεπώς, οι καταθέσεις των συνεργών του είναι αληθείς και ευσταθούν ως στοιχεία για την άσκηση συμπληρωματικής ποινικής δίωξης.

### 3.12. Διερεύνηση ιχνών παιδικής πορνογραφίας

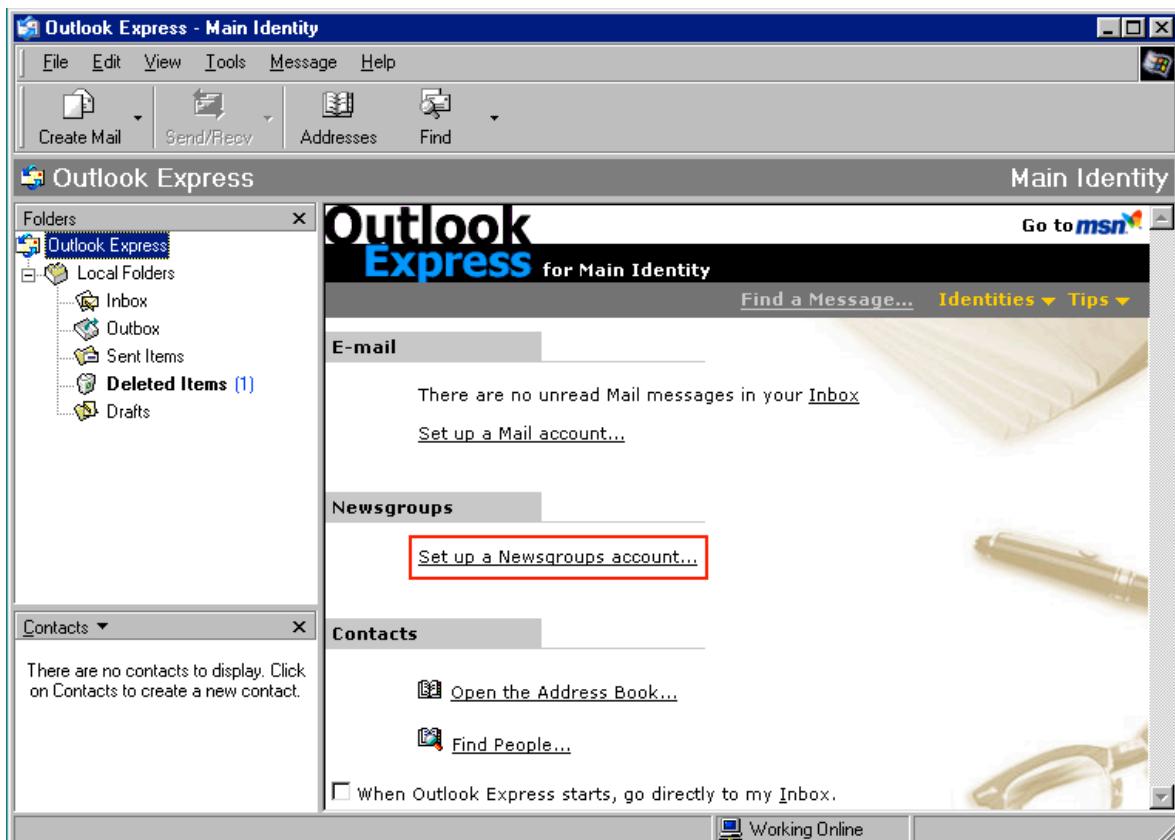
Πρώτο βήμα στην διερεύνηση ιχνών παιδικής πορνογραφίας αποτέλεσε η αναζήτηση για εικόνες με σχετικό περιεχόμενο. Καθώς δε βρέθηκε κάποιο στοιχείο, σειρά είχε η αναζήτηση στους φακέλους της εφαρμογής «Outlook Express» («C:/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express»), που χρησιμοποιούσε ο ύποπτος για την διαχείριση της ηλεκτρονικής αλληλογραφίας του. Εντός του φακέλου εντοπίστηκε πληθώρα αρχείων από ομάδες ενημερώσεων (news groups), με θεματολογίες όπως το hacking και το λογισμικό ηλεκτρονικών υπολογιστών. Ανάμεσα τους, υπάρχει το αρχείο με όνομα «Folder.dbx», το οποίο περιλαμβάνει όλα τα news groups στα οποία διατηρούνται συνδρομή ο ύποπτος. Αναφορικά με τα ζητούμενα της ανάλυσης των πειστηρίων, μεταξύ άλλων, βρέθηκαν τα παρακάτω news groups:

- alt.binaries.erotic.children
- free.binaries.pictures.children
- free.binaries.pictures.child.erotica.female=:,
- free.binaries.erotica.teen.female.nonude

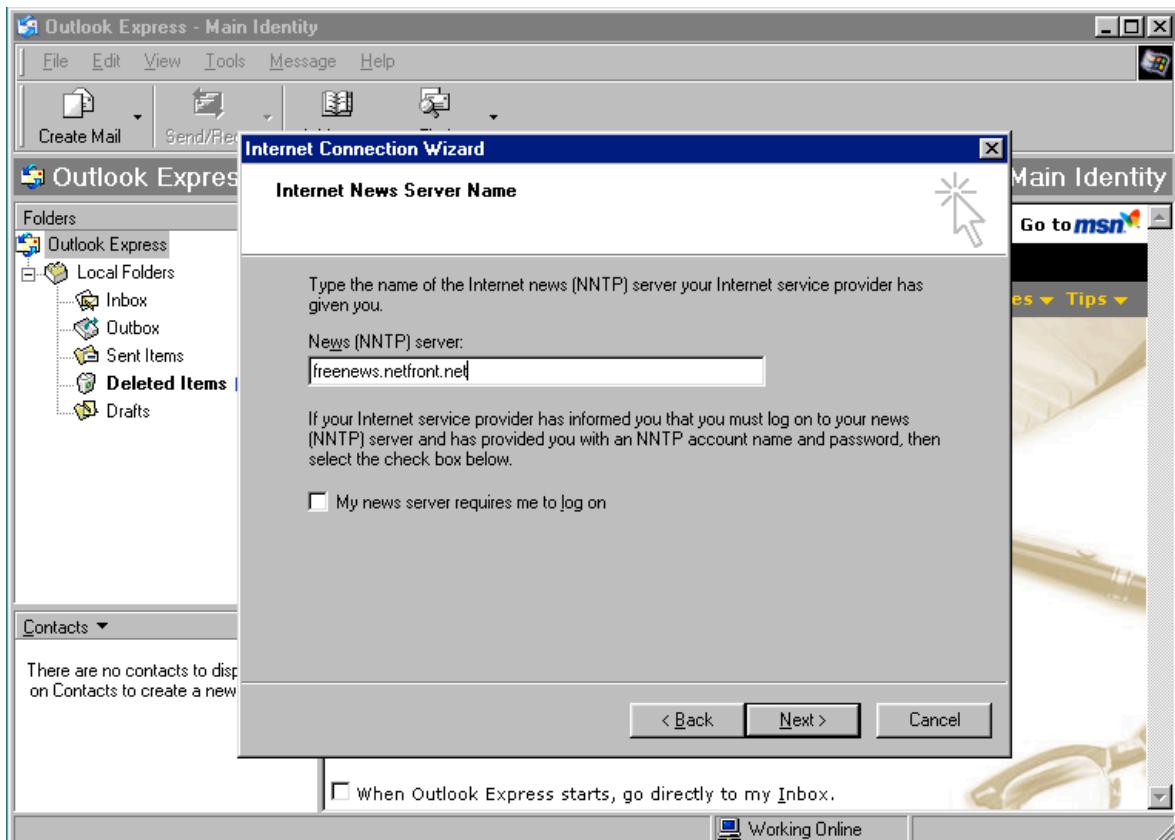
- free.binaries.pictures.child.erotica.for.peter-j-ross
- free.binaries.nospam.teenfeem.repost
- free.binaries.pictures.barefoot.children
- free.binaries.pictures.child.erotica.for
- free.binaries.pictures.child.erotica.male
- alt.japanese.neojapan.pedophilia
- alt.pedophile.bob-curtis
- alt.pedophile.bruce-ediger
- alt.pedophile.david-ratcliffe
- alt.pedophile.grady-booch
- alt.pedophile.jason-durbin
- alt.pedophile.nick-sandru
- alt.pedophile.richard-tietjens
- alt.pedophile.robbie-honerkamp
- alt.svens.house.of.12.year-old.lust

Όλα τα παραπάνω αποτελούν ομάδες ενημερώσεων που εγγράφηκε ο ύποπτος με τη θέληση του, στα οποία οι χρήστες έχουν τη δυνατότητα αποστολής και αναπαραγωγής μηνυμάτων και πολυμέσων. Συνεπώς, γίνεται αντιληπτό το ενδιαφέρον του υπόπτου για το συγκεκριμένο θέμα.

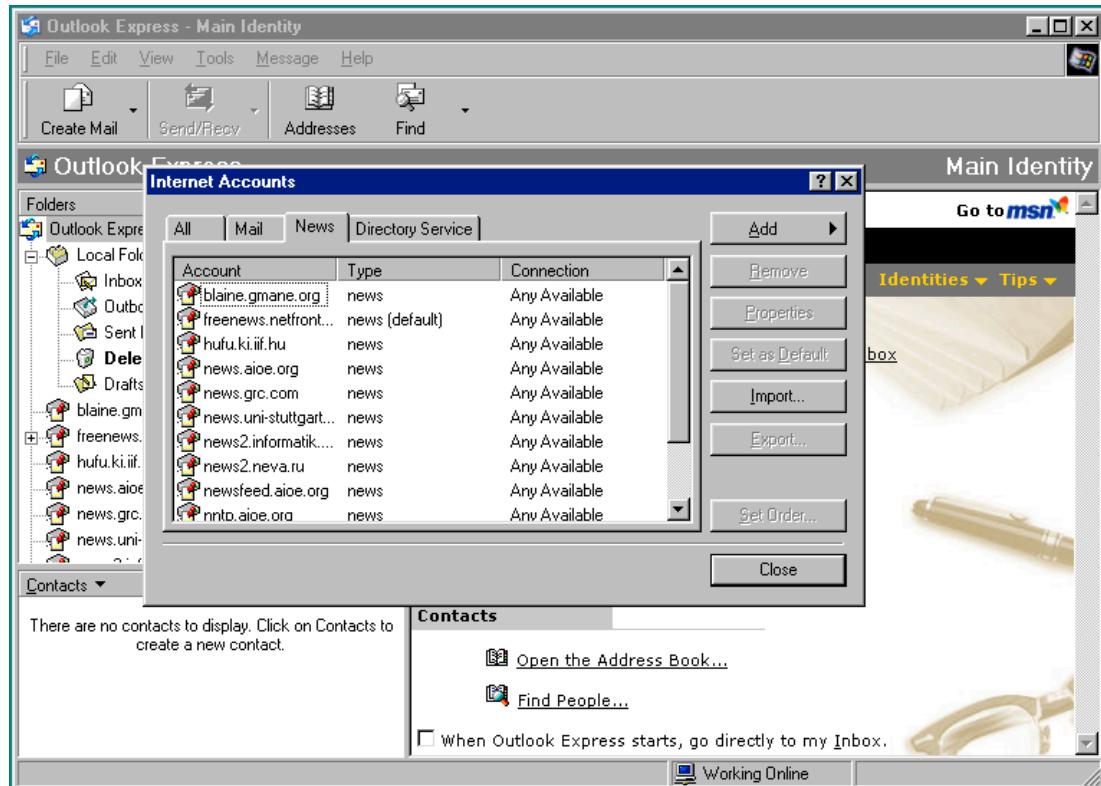
Για την ορθότερη κατανόηση και ανάλυση των πράξεων του υπόπτου, κρίθηκε απαραίτητη η αναπαράσταση των κινήσεων του από την εκκίνηση της εφαρμογής «Outlook Express», έως την πραγματοποίηση συνδρομής σε ένα news group. Πιο συγκεκριμένα, δημιουργήθηκε μια εικονική μηχανή (virtual machine) με λειτουργικό σύστημα «Windows 98», στο οποίο βρίσκεται προεγκατεστημένη η εφαρμογή ηλεκτρονικού ταχυδρομείου, δημιουργήθηκε ένας λογαριασμός ομάδων ενημερώσεων (Εικόνα 39) και στη συνέχεια, πραγματοποιήθηκε συνδρομή σε ορισμένες από αυτές (Εικόνες 40 και 41).



Εικόνα 39 - Δημιουργία λογαριασμού ομάδων ενημερώσεων στο εργαλείο «Outlook Express»

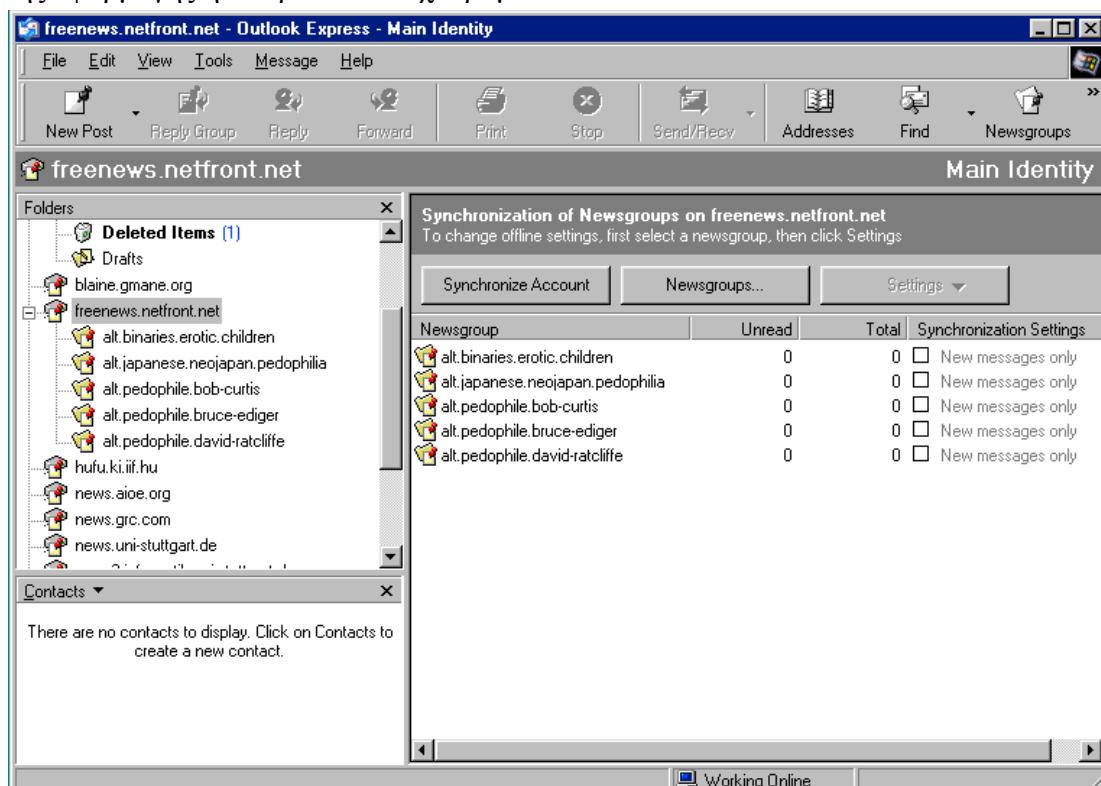


Εικόνα 40 - Πληκτρολόγηση της διεύθυνσης ενός NNTP server



Εικόνα 41 - Ορισμένες από τις ομάδες ενημερώσεων

Παρακάτω (Εικόνα 42) παρουσιάζεται μια πιθανή μορφή του περιβάλλοντος της εφαρμογής ηλεκτρονικού ταχυδρομείου του υπόπτου.



Εικόνα 42 - Πιθανή μορφή του περιβάλλοντος της εφαρμογής ηλεκτρονικού ταχυδρομείου του υπόπτου

### 3.13. Διερεύνηση ιχνών οικονομικών εγκλημάτων

Αρχικά εξετάστηκαν τα αποτελέσματα της ανάλυσης του εργαλείου «Autopsy» (<https://www.autopsy.com/>) για ευρήματα σχετικά με την ύπαρξη στοιχείων πιστωτικών καρτών στον εικονικό δίσκο-πειστήριο. Η εξέταση αυτή οδήγησε στο αρχείο «alt.2600.cardz.dbx» (Εικόνα 43), που αντιστοιχεί σε ένα «news group» στο οποίο είχε πραγματοποιήσει συνδρομή ο ύποπτος μέσω της εφαρμογής «Outlook Express». Ένα «news group» αποτελεί μια ομάδα κοινοποίησης μηνυμάτων ηλεκτρονικού ταχυδρομείου στην οποία ένας χρήστης αλληλεπιδρά είτε διαμοιράζοντας περιεχόμενο, είτε απλά κάνοντας περιήγηση σε αυτό. Η ανάγνωση του αρχείου πραγματοποιήθηκε με τη βοήθεια του εργαλείου «SysInfo Tools DBX File Viewer» (<https://www.sysinfotools.com/recovery/dbx-file-viewer.php>), κατά την οποία βρέθηκαν μηνύματα ηλεκτρονικού ταχυδρομείου με θέματα όπως «CC's (Credit Card) CVV2 4 (for Sale)», «US and Int. PayPal's for sale», «Free Credit Card Validator and Extractor» και «Ebay Accts Available» (Εικόνα 44), που αποδεικνύουν την άμεση ή έμμεση εμπλοκή του υπόπτου με υποθέσεις οικονομικών εγκλημάτων.

Source Name	S	C	O	Account Type	ID	Card Number	Keyword	Keyword Preview
alt.2600.cardz.dbx	3			CREDIT_CARD	20040723072643	20040723072643	20040723072643	net00000002ccpowah<<20040723072643>>

Result: 1 of 5      Result: < >

Type	Value
Account Type	CREDIT_CARD
ID	20040723072643
Card Number	20040723072643
Keyword	20040723072643
Set Name	Credit Card Numbers
Keyword Preview	net00000002ccpowah<<20040723072643<.15298.00000209@mb-m
Keyword Search Type	2
Source File Path	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13
Artifact ID	-9223372036854757722

Εικόνα 43 - Το αρχείο «alt.2600.cardz.dbx»

		From	Subject	To	Email Status	Date/Time	
		"id scanz <idscanz@aol.co...	ebay accs available		Existing	Sun Jul 11 10:01:58 2004	
		"PsYcHo <rawling@trance...	CC's with CW2 4 Sale		Existing	Sun Jul 11 13:49:08 2004	
		"id scanz <idscanz@aol.co...	CC's with CW2 4 Sale		Existing	Mon Jul 12 02:16:52 2004	
		"just_me <who_cares162@...	Free non ratio ftp's		Existing	Mon Jul 12 16:02:07 2004	
		"CardMaster19 <yabapmatt...	Magnetic Stripe Encoding Problem		Existing	Wed Jul 14 23:34:56 2004	
		"sarah@gmail.com <sarah...	My Silicon Titties 9668		Existing	Fri Jul 16 23:11:20 2004	
		"den <"user <dadano\"@h...	QUESTIONS ANSWERED		Existing	Sat Jul 17 22:53:53 2004	
		"castro <ceazeza@sapo.pt..."	New way to get Credit Cards!		Existing	Sun Jul 18 02:03:11 2004	
		"officerdibble <officerdibble...	New way to get Credit Cards!		Existing	Sun Jul 18 15:32:12 2004	
		"officerdibble <officerdibble...	fuckin idiots		Existing	Sun Jul 18 15:38:04 2004	
		"rad-montreal <redbel@hot...	Magnetic Stripe Encoding Problem		Existing	Sun Jul 18 21:26:22 2004	
		"rad-montreal <redbel@hot...	Magnetic Stripe Encoding Problem		Existing	Sun Jul 18 21:27:23 2004	
		"rad-montreal <redbel@hot...	carerz partner from canada needed		Existing	Mon Jul 19 21:49:06 2004	
		"rad-montreal <redbel@hot...	cading partner from canada needed		Existing	Tue Jul 20 20:43:21 2004	
		"Amisima <dh7777@counte...	ICVerify		Existing	Wed Jul 21 00:43:18 2004	
		"John Cronin <gatekeeper...	where are all the		Existing	Wed Jul 21 21:19:38 2004	
		"Hans van Eynsbergen <Ha...	Osama Found Hanged		Existing	Thu Jul 22 19:49:19 2004	
		"Yomamma bin Crawdad... <	Osama Found Hanged		Existing	Fri Jul 23 03:49:05 2004	
		"id scanz <idscanz@aol.co...	ccpowah		Existing	Fri Jul 23 14:26:43 2004	
		"Ammon-Ra <ammon-ra@of...	US and Int. PayPal's for sale		Existing	Fri Jul 23 23:04:04 2004	
		"robot junkie <robotjunkie39...	Free one for all you! Good cc inside		Existing	Fri Jul 23 23:09:33 2004	
		"id scanz <idscanz@aol.co...	german aol axx - lol		Existing	Sat Jul 24 21:35:19 2004	
		"robot junkie <robotjunkie39...	US and Int. PayPal's for sale		Existing	Sun Jul 25 05:11:46 2004	
		"robot junkie <robotjunkie39...	free one for al of you guts who need one HURRY HURRY MY FRIENDS		Existing	Sun Jul 25 09:40:47 2004	
		"take me <yesiam@imabadi...	free card, FULL info, working now! snatch it quick!		Existing	Sun Jul 25 18:34:29 2004	
		"AllNet2007 <hoobooo4777...	Tutorial site		Existing	Sun Jul 25 19:28:40 2004	
		"id scanz <idscanz@aol.co...	free card, FULL info, working now! snatch it quick!		Existing	Sun Jul 25 22:17:33 2004	
		"ppro <ppro@proweb.com">	EGOLD - MAKE THOUSANDS - UNLIMITED DEPOSITS IN YOUR EGOLD ACCT-EARLY STAGES, G...		Existing	Mon Jul 26 13:51:21 2004	
		"Rona <wyldtgu@vivwsdgs...	New & used car prices		Existing	Mon Jul 26 15:48:10 2004	
		"johny <anonymous_pal4ev...	free credit card validator and extractor		Existing	Mon Jul 26 23:34:22 2004	
		"johny <anonymous_pal4ev...	free credit card validator and extractor - link		Existing	Tue Jul 27 00:00:49 2004	
		"id scanz <idscanz@aol.co...	free credit card validator and extractor - link		Existing	Tue Jul 27 01:35:11 2004	
		"Lincoln'smole <bitalker3@...	ebay accs available		Existing	Tue Jul 27 01:54:23 2004	

Εικόνα 44 - Μηνύματα ηλεκτρονικού ταχυδρομείου που σχετίζονται με οικονομικά εγκλήματα

### 3.14. Διερεύνηση ύπαρξης επιπλέον συνεργών

Μετά την εξέταση του εικονικού δίσκου-πειστηρίου, φαίνεται πως ο ύποπτος ενεργούσε μεμονωμένα, καθώς δε βρέθηκαν στοιχεία που να εμπλέκουν επιπλέον συνεργούς. Αναλυτικότερα, δε βρέθηκαν μηνύματα ηλεκτρονικού ταχυδρομείου ή διαδικτυακές συνομιλίες (mIRC) που να αποδεικνύουν την ύπαρξη συνεργών. Επίσης, έγινε αντιληπτό, μέσω του καταλόγου «Nethood» (C:/Documents and Settings/Mr. Evil/Nethood), εντός του οποίου διατηρείται το ιστορικό των υπολογιστών στους οποίους ένας χρήστης είχε πρόσβαση μια δεδομένη χρονική στιγμή, πως ο ύποπτος συνδεόταν εξ αποστάσεως σε έναν δικτυακό τόπο (4.12.220.254), το όνομα του οποίου ήταν «ANDREWS-1», για την πρόσβαση σε δικτυακούς τόμους [«andrews (c)», «a», «d», «e»], σε έναν οδηγό οπτικών μέσων [«CD Drive (F)»] (Εικόνα 45), για την χρήση ενός εκτυπωτή μάρκας «HP» (HP LaserJet 2100), μέσω της δικτυακής πόρτας (port) «Ne00» (Εικόνα 46) (τοποθεσία αποδεικτικού στοιχείου: C:/Documents and Setting/Mr. Evil/NTUSER.DAT), αλλά και για την ανάγνωση και τον διαμοιρασμό αρχείων (Εικόνα 48) (τοποθεσία

αποδεικτικού στοιχείου: C:/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/index.dat). Αναφορικά με το τελευταίο, στη διαδρομή «C:/Windows/system32/config/software\Microsoft\Windows NT\CurrentVersion/Explorer/RecentDocs» περιέχονται, σε φθίνουσα σειρά, τα τελευταία εφτά (7) αρχεία που προσπέλασε ο ύποπτος (Εικόνα 49). Τέλος, στη διαδρομή «C:/Documents and Setting/Mr. Evil/NTUSER.DAT\Microsoft\Windows NT\CurrentVersion/Explorer/ComputerDescriptions», βρίσκεται το ιστορικό των τοποθεσιών στις οποίες πραγματοποιούσε συχνότερη σύνδεση ο ύποπτος (Εικόνα 50). Παρ' όλ' αυτά, δεν ήταν εφικτή η άμεση συσχέτιση του με έναν ή περισσότερους συνεργούς.



Εικόνα 45 - Τα περιεχόμενα του φακέλου «Nethood»

Εικόνα 46 - Πληροφορίες για τον εκτυπωτή «HP LaserJet 2100»

Εικόνα 47 - Πληροφορίες για τον εκτυπωτή «HP LaserJet 2100» στο Registry

Εικόνα 48 - Απόδειξη διαμοιρασμού αρχείων από/προς έναν δικτυακό τόπο

```

recentdocs v.20100405
(INTUSER.DAT) Gets contents of user's RecentDocs key
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Thu Aug 26 15:08:15 2004 (UTC)
    7 = Temp on m1200 (4.12.220.254)
    6 = yng13.bmp
    5 = channels
    4 = channels.txt
    3 = GhostWare
    2 = Receipt.rtf
    1 = Anonymizer
    0 = keys.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.bmp
LastWrite Time Thu Aug 26 15:08:12 2004 (UTC)
MRUListEx = 0
    0 = yng13.bmp
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.rtf
LastWrite Time Fri Aug 20 15:09:16 2004 (UTC)
MRUListEx = 0
    0 = Receipt.rtf
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time Fri Aug 20 15:50:40 2004 (UTC)
MRUListEx = 1,0
    1 = channels.txt
    0 = keys.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Thu Aug 26 15:08:14 2004 (UTC)
MRUListEx = 3,2,1,0
    3 = Temp on m1200 (4.12.220.254)
    2 = channels
    1 = GhostWare
    0 = Anonymizer
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\NetHood
LastWrite Time Thu Aug 26 15:08:15 2004 (UTC)
MRUListEx = 0
    0 = \\4.12.220.254\Temp

```

Εικόνα 49 - Λίστα των τελευταίων εφτά (7) αρχείων που προσπέλασε ο ύποπτος

Value Name	Value Type	Data
RBC	RegSz	RBC
4.12.220.254	RegSz	m1200
TOWER	RegSz	Tower
TOWER2	RegSz	
ECSAP_LAB_SRVR	RegSz	
ECSAP_LMS	RegSz	ECSAP_LMS
N-1A9ODN6ZKK4LQ	RegSz	
BB	RegSz	
D77KSG41	RegSz	
PREFERRE-GG31M4	RegSz	
SM181068849	RegSz	
ANDREWS-1	RegSz	

Εικόνα 50 - Το ιστορικό των τοποθεσιών που συνδεόταν συχνότερα ο ύποπτος

### 3.15. Διερεύνηση ύπαρξης κακόβουλου λογισμικού (virus, worms, backdoor κλπ) που μπορεί να επικαλεστεί ο δράστης ως ελαφρυντικό

Ως προς την διαδικασία διερεύνησης ύπαρξης κακόβουλου λογισμικού στον εικονικό δίσκο-πειστήριο, πραγματοποιήθηκε «mount» του εικονικού δίσκου σε έναν τοπικό υπολογιστή με λειτουργικό σύστημα «Kali Linux»., ώστε στη συνέχεια, να διεξαχθεί σάρωση με τη βοήθεια του εργαλείου «Clamav» (<https://www.clamav.net/>).

Αρχικά, έγινε εγκατάσταση του εργαλείου «EWF-tools», κάνοντας χρήση της εντολής «apt install ewf-tools». Έπειτα, μέσω της εντολής «ewfmount 4Dell\ Latitude\ CPi.E01 output/», τα αρχεία που περιέχουν οι εικονικοί δίσκοι «4Dell Latitude CPi.E01» και «4Dell Latitude CPi.E02» μετατρέπονται σε «RAW» μορφή και τοποθετούνται στον φάκελο «output». Στη συνέχεια, εκτελώντας την εντολή «mount output/ewf1 /mnt -o ro,offset=\$((512\*512))», τα περιεχόμενα του φακέλου «output» προσαρτώνται στον φάκελο «/mnt», που πλέον αποτελεί σκληρό δίσκο στο τοπικό σύστημα.

Κατόπιν, καθίσταται δυνατή η σάρωση του σκληρού δίσκου με την εντολή «clamscan -ir /mnt», τα αποτελέσματα της οποίας φαίνονται παρακάτω (Εικόνα 51):

```

1 /mnt/My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
2 /mnt/My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
3 /mnt/My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND
4 /mnt/My Documents/ENUMERATION/NT/enum/enum.tar.gz: Win.Tool.EnumPlus-1 FOUND
5 /mnt/My Documents/ENUMERATION/NT/enum/files/enum.exe: Win.Tool.EnumPlus-1 FOUND
6 /mnt/My Documents/ENUMERATION/NT/Legion/Chrono.dll: Win.Trojan.Bruteforce-3 FOUND
7 /mnt/My Documents/ENUMERATION/NT/NetTools.ex_: Win.Trojan.Spión-4 FOUND
8 /mnt/My Documents/ENUMERATION/NT/ntreskit.zip: Win.Trojan.Nemo-1 FOUND
9 /mnt/My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe: Win.Tool.Brutus-3 FOUND
10 /mnt/My Documents/EXPLOITATION/NT/brutus.zip: Win.Tool.Brutus-3 FOUND
11 /mnt/My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe: Win.Exploit.WinNT-3 FOUND
12 /mnt/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe: Win.Trojan.Lsadump-1 FOUND
13 /mnt/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip: Win.Trojan.Lsadump-1 FOUND
14 /mnt/My Documents/EXPLOITATION/NT/netbus/NetBus170.zip: Win.Trojan.Netbus-2 FOUND
15 /mnt/My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE: Win.Trojan.Sehole-1 FOUND
16 /mnt/My Documents/EXPLOITATION/NT/sechole/sechole3.zip: Win.Trojan.Sehole-1 FOUND
17 /mnt/My Documents/FOOTPRINTING/NT/superscan/superscan.exe: Win.Trojan.Agent-6240252-0 FOUND
18 /mnt/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz: Unix.Malware.Agent-6781976-0 FOUND
19 /mnt/Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND
20
21
22 ----- SCAN SUMMARY -----
23 Known viruses: 8666818
24 Engine version: 1.0.1
25 Scanned directories: 766
26 Scanned files: 11305
27 Infected files: 19
28 Data scanned: 2166.89 MB
29 Data read: 1768.03 MB (ratio 1.23:1)
30 Time: 2281.042 sec (38 m 1 s)
31 Start Date: 2023:05:19 11:02:22
32 End Date: 2023:05:19 11:40:23

```

*Εικόνα 51 - Σάρωση του σκληρού δίσκου του υπόπτου για κακόβουλο λογισμικό*

Αναλυτικότερα:

- **My Documents/COMMANDS/enum.exe:** Εργαλείο που υποκλέπτει πληροφορίες σχετικά με χρήστες, ομάδες, κοινόχρηστα στοιχεία και βασικές πληροφορίες σε συστήματα με εκδόσεις λειτουργικού Windows NT, 2000 και XP.
- **My Documents/COMMANDS/SAMDUMP.EXE:** Εργαλείο που αποτυπώνει τα «hash» των κωδικών πρόσβασης των χρηστών που βρίσκονται στο αρχείο «SAM» (C:/Windows/system32/config/SAM) σε λειτουργικά συστήματα Windows NT, 2000, XP και Vista.
- **My Documents/COMMANDS/snitch.exe:** Εργαλείο που επαναφέρει τους αστερίσκους, που βρίσκονται στα πεδία των κωδικών πρόσβασης, στους χαρακτήρες που αποκρύπτουν.
- **My Documents/ENUMERATION/NT/enum/enum.tar.gz:** Ομοίως με το «My Documents/COMMANDS/enum.exe», με τη διαφοροποίηση πως βρίσκεται σε μορφή συμπιεσμένου αρχείου (tar.gz).
- **My Documents/ENUMERATION/NT/enum/files/enum.exe:** Ομοίως με το «My Documents/COMMANDS/enum.exe».

- **My Documents/ENUMERATION/NT/Legion/Chrono.dll**: Αρχείο βιβλιοθήκης του κακόβουλου λογισμικού «Legion», που χρησιμοποιείται ως «NetBIOS scanner».
- **My Documents/ENUMERATION/NT/Legion/NetTools.exe**: Εκτελέσιμο αρχείο του κακόβουλου λογισμικού «Legion», που χρησιμοποιείται ως «NetBIOS scanner».
- **My Documents/ENUMERATION/NT/ntreskit.zip**: Συμπιεσμένο αρχείο που περιέχει εκτελέσιμα αρχεία, τα οποία χρησιμοποιούνται για enumeration.
- **My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe**: Εργαλείο που πραγματοποιεί επιθέσεις «ωμής βίας» με σκοπό την ανάκτηση κωδικών.
- **My Documents/EXPLOITATION/NT/brutus.zip**: Ομοίως με το «My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe»
- **My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe**: Εργαλείο που επιτρέπει σε έναν απλό χρήστη να αποκτήσει δικαιώματα διαχειριστή.
- **My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe**: Εργαλείο που αποτυπώνει τα «hash» των χρηστών από την μνήμη RAM.
- **My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip**: Ομοίως με το «My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe».
- **My Documents/EXPLOITATION/NT/netbus/NetBus170.zip**: Εργαλείο για απομακρυσμένη διαχείριση υπολογιστή.
- **My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE**: Εργαλείο που επιτρέπει σε έναν απλό χρήστη να αποκτήσει πρόσβαση σε επίπεδο εντοπισμού σφαλμάτων (debug-level access), και κατόπιν να εκτελέσει κακόβουλο κώδικα, ώστε να αποκτήσει δικαιώματα διαχειριστή.
- **My Documents/EXPLOITATION/NT/sechole/sechole3.zip**: Ομοίως με το «My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE».
- **My Documents/FOOTPRINTING/NT/superscan/superscan.exe**: Εφαρμογή σάρωσης πορτών (ports).
- **My Documents/FOOTPRINTING/UNIX/unix\_hack.tgz**: Σύμφωνα με το εργαλείο «Autopsy», αποτελεί «zipbomb», δηλαδή ένα συμπιεσμένο αρχείο

που σκοπός του είναι η «κατάρρευση» ενός συστήματος κατά την αποσυμπίεσή του.

- **Program Files/Cain/Abel.dll:** Αρχείο βιβλιοθήκης του κακόβουλου λογισμικού «Cain and Abel», το οποίο αποτελεί εργαλείο ανάκτησης κωδικών πρόσβασης, επιτρέποντας την ανάκτηση διάφορων ειδών κωδικών πρόσβασης μέσω παρακολούθησης του δικτύου (sniffing).

Τα παραπάνω εργαλεία, στην πλειοψηφία τους, αποτελούν εργαλεία «hacking» και δε μπορεί κάποιος να τα εκμεταλλευτεί για να αποκτήσει απομακρυσμένη πρόσβαση στον υπολογιστή του υπόπτου. Η μόνη εξαίρεση σε αυτό, είναι το εργαλείο «NetBus170.zip», που χρησιμοποιείται γι' αυτό το σκοπό. Όμως, εξετάζοντας τις ημερομηνίες δημιουργίας και προσπέλασής του (Εικόνα 52), εξάγεται το συμπέρασμα πως δεν εκτελέστηκε ποτέ. Συνεπώς, τυχόν ισχυρισμοί του υπόπτου, πως δεν δρούσε ο ίδιος κατά την διάρκεια των επιθέσεων, δεν ευσταθούν.

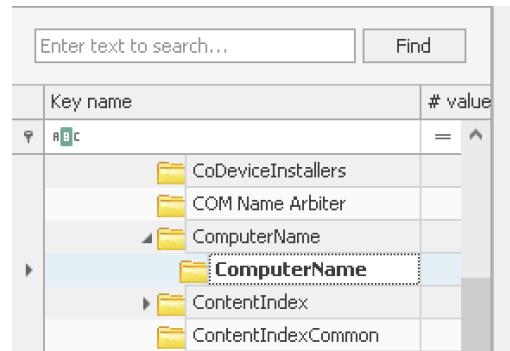
/img_4Dell Latitude CPi.E01/vol_vo1/My Documents/EXPLOITATION/NT/netbus					
<a href="#">Table</a> <a href="#">Thumbnail</a> <a href="#">Summary</a>					
Name	S	C	O	Created Time	Access Time
📁 [current folder]				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
📁 [parent folder]				2004-08-20 18:19:12 EEST	2004-08-20 18:19:48 EEST
Hosts.txt				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
Memo.txt				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
NetBus.rtf	▼		3	2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
NetBus170.zip			2	2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST

Εικόνα 52 - Οι ημερομηνίες δημιουργίας και προσπέλασης του αρχείου «NetBus170.zip»

### 3.16. Επιπλέον ευρήματα

#### 3.16.1. Όνομα υπολογιστή

Το όνομα του υπολογιστή είναι «N-1A9ODN6ZXK4LQ»  
(C:/Windows/System32/config/system\ControlSet001\Control\ComputerName\ComputerName») (Εικόνα 53).



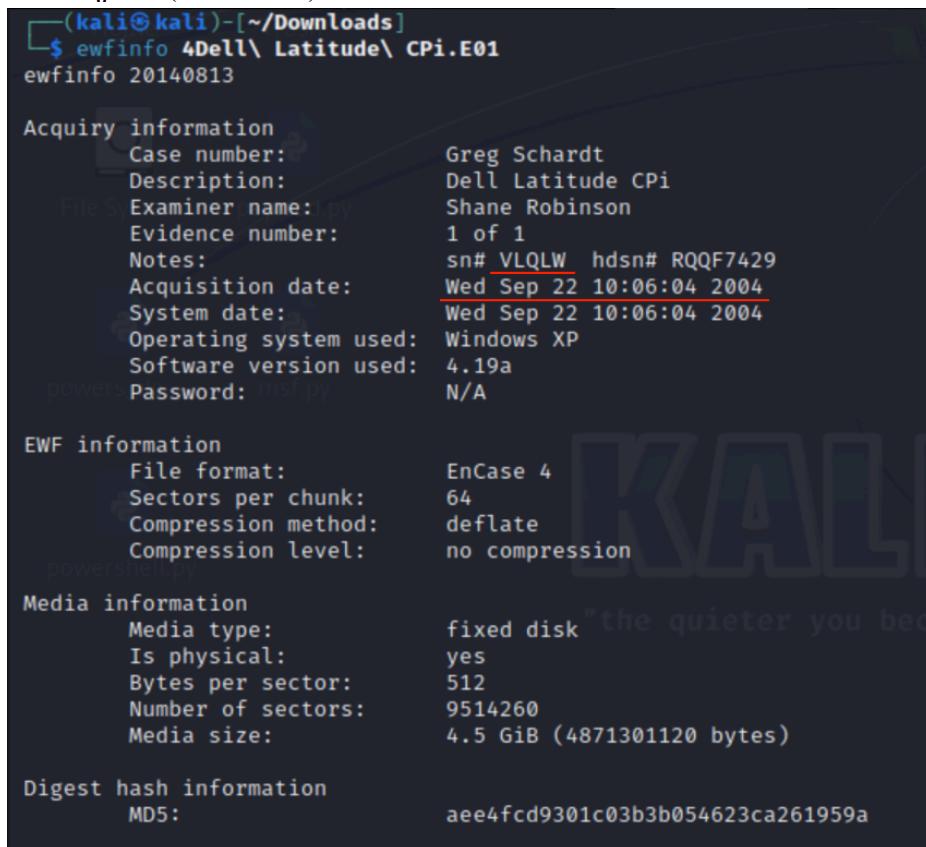
Key name	# value
RBC	=
CoDeviceInstallers	
COM Name Arbiter	
ComputerName	
ComputerName	
ContentIndex	
ContentIndexCommon	

Value Name	Value Type	Data
RBC	RBC	RBC
ComputerName	RegSz	N-1A9ODN6ZXK4LQ

Εικόνα 53 - Το όνομα του υπολογιστή

#### 3.16.2. Σειριακός αριθμός laptop και ημερομηνία δημιουργίας του image

Μετά την εγκατάσταση του εργαλείου «EWF-tools», μέσω της εντολής «ewfinfo 4Dell\ Latitude\ CPi.E01» ανακτήθηκαν οι λεπτομέρειες του εικονικού δίσκου-πειστηρίου (Εικόνα 54).



```
(kali㉿kali)-[~/Downloads]
$ ewfinfo 4Dell\ Latitude\ CPi.E01
ewfinfo 20140813

Acquiry information
Case number: Greg Schardt
Description: Dell Latitude CPi
Examiner name: Shane Robinson
Evidence number: 1 of 1
Notes: sn# VLQLW hdsn# RQQF7429
Acquisition date: Wed Sep 22 10:06:04 2004
System date: Wed Sep 22 10:06:04 2004
Operating system used: Windows XP
Software version used: 4.19a
powershell.py Password: N/A

EWF information
File format: EnCase 4
Sectors per chunk: 64
Compression method: deflate
Compression level: no compression
powershell.py

Media information
Media type: fixed disk "the quieter you bec
Is physical: yes
Bytes per sector: 512
Number of sectors: 9514260
Media size: 4.5 GiB (4871301120 bytes)

Digest hash information
MD5: aee4fcfd9301c03b3b054623ca261959a
```

Εικόνα 54 - Οι λεπτομέρειες του εικονικού δίσκου-πειστηρίου

### 3.16.3. Ουρά εκτύπωσης και εκτυπωτές

Δεν βρέθηκαν ίχνη αρχείων στην ουρά εκτύπωσης (C:/Windows/System32/spool/PRINTERS). Ο μοναδικός εκτυπωτής που ήταν συνδεμένος στο σύστημα, βάσει του υποκλειδιού «Printers» (C:/Windows/System32/config/software/Microsoft\Windows NT\CurrentVersion\Print\Printers), είναι ο εκτυπωτής «HP LaserJet 2100» (Εικόνα 55) στην δικτυακή διαδρομή «\\ANDREWS-1\HPLaserJ».

Key name	# values	# subk	Type	Name	Value
Print	0				
Printers	1				
Auto HP LaserJet 2100...	26				
ProfileList	3				

Key name	Type	Value
Security	RegBinary	01-00-04-80-F0-00-00-00-0C-01-00
SpoolDirectory	RegSz	
Port	RegSz	\ANDREWS-1\HPLaserJ

Εικόνα 55 - Ο μοναδικός εκτυπωτής που ήταν συνδεμένος στο σύστημα

### 3.16.4. Συνδεμένες συσκευές

Στον υπολογιστή του υπόπτου υπήρχε ένας σκληρός δίσκος μάρκας «IBM» με σύνδεση «IDE», μία μονάδα «CD-ROM» μάρκας «Toshiba» (C:/Windows/System32/config/system\ControlSet001\Control\DeviceClasses) (Εικόνα 56), όπως επίσης και μια συσκευή «USB Hub» (C:/Windows/System32/config/system\ControlSet001\Enum\USB\ROOT\_HUB\4&15736a3f&0) (Εικόνα 57).

Key name	# values	# subk	Timestamp	Guid Folder	Type	Name	Serial Number
CrashControl	7		2004-08-27 15:08:03	{53f56307-b6bf-11d0-94f2-00a0c91efbf8b}	IDE	DiskIBM-DBCA-204860_58230d196c8080.0.0_BC30A8DF	
CriticalDeviceDatabase	0		2004-08-27 15:08:10	{53f56307-b6bf-11d0-94f2-00a0c91efbf8b}	IDE	CdRomTOSHIBA_CD-ROM_XM-1902B_1A15	5835c6ca118080.0.0

Εικόνα 56 - Ο σκληρός δίσκος και η μονάδα δίσκου CD-ROM του υπολογιστή

Key name	# values	# subk	Value Name	Type	Data
ISAPNP	0		Capabilities	RegDword	128
LPTENUM	0		UINumber	RegDword	0
PCI	0		HardwareID	RegMultiSz	USB\ROOT_HUB&VID8086&PID7112&REV0001 USB\RO...
PCIIDE	0		Service	RegSz	usbhub
PCMCIA	0		ConfigFlags	RegDword	0
Root	0		ClassGUID	RegSz	{36FC9E60-C465-11CF-8056-444553540000}
STORAGE	0		Class	RegSz	USB
SW	0		Driver	RegSz	{36FC9E60-C465-11CF-8056-444553540000}\0001
USB	0		Mfg	RegSz	(Standard USB Host Controller)
ROOT_HUB	0		DeviceDesc	RegSz	USB Root Hub
4&15736a3f&0	10				

Εικόνα 57 - Η συσκευή «USB Hub» που ήταν συνδεμένη στον υπολογιστή

### **3.16.5. Ημερομηνία και ώρα τελευταίας απενεργοποίησης του υπολογιστή**

Σύμφωνα με την ημερομηνία που πραγματοποιήθηκε η πιο πρόσφατη εγγραφή στο κλειδί «Windows» της διαδρομής (C:/Windows/System32/config/system\ControlSet001\Control\Windows), που περιέχει την τιμή «ShutdownTime», η ημερομηνία της τελευταίας απενεργοποίησης του υπολογιστή ήταν στις 2004-08-27 και ώρα 15:46:33 UTC (Εικόνα 58).

<input type="checkbox"/>	Key:	ControlSet001\Control\Windows
Selected hive: system	Last write:	2004-08-27 15:46:33

Εικόνα 58 - Η ημερομηνία της τελευταίας απενεργοποίησης του υπολογιστή

### **3.16.6. Στοιχεία σύνδεσης του υπόπτου στην εφαρμογή mIRC**

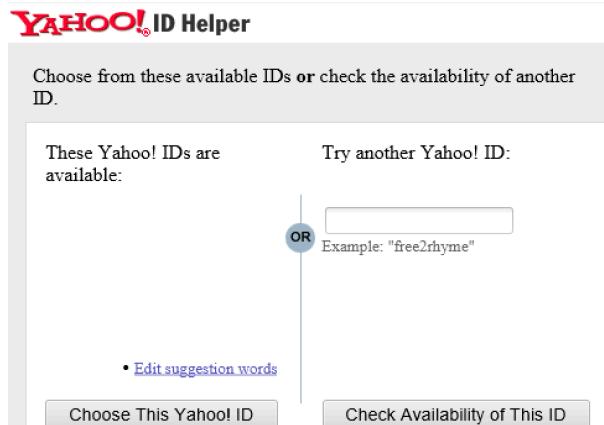
Τα στοιχεία σύνδεσης του υπόπτου είναι:

user=Mini Me  
email=none@of.ya  
nick=Mr  
anick=mrevilrulez

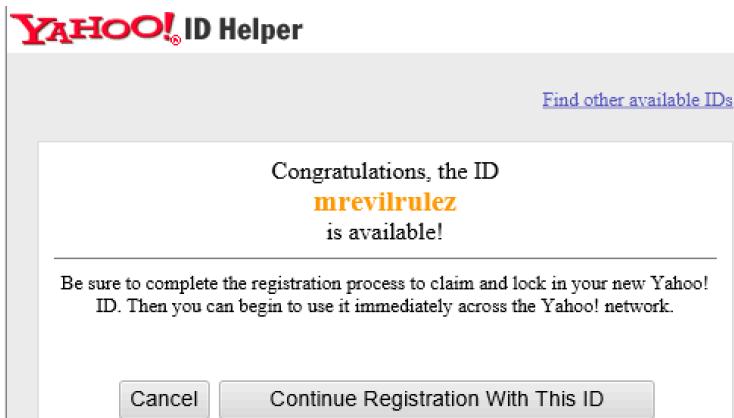
και συναντώνται στο αρχείο «mirc.ini», που βρίσκεται στη διαδρομή (C:\Program Files\mIRC\mirc.ini)

### **3.16.7. Η κύρια διεύθυνση email του υπόπτου**

Εξετάζοντας το διαδικτυακό ιστορικό του υπόπτου (C:\Documents and Settings\Mr. Evil\Local Settings\Temporary Internet Files\Content.IE5) βρέθηκαν ίχνη δραστηριότητας από την δημιουργία του λογαριασμού του στο «Yahoo» (Εικόνες 59 και 60).



Εικόνα 59 - Προσπάθεια εύρεσης μη δεσμευμένου «Yahoo ID» από τον ύποπτο



*Eikόνα 60 - Εύρεση μη δεσμευμένου «Yahoo ID» από τον ύποπτο*

Στις εικόνες 61 και 62 φαίνεται πως ο ύποπτος κατάφερε να δημιουργήσει τον λογαριασμό του, η διεύθυνση του οποίου είναι: [mrevirulez@yahoo.com](mailto:mrevirulez@yahoo.com).

*Eikόνα 61 - Το περιβάλλον εισερχομένων email(inbox) του υπόπτου*

*Eikόνα 62 - Το email καλωσορίσματος του υπόπτου από το «Yahoo! Mail»*

### 3.16.8. Ανακτηθείσα λίστα διεργασιών πριν το τελευταίο hibernation

Για την ανάκτηση της λίστας διεργασιών πριν το τελευταίο hibernation ακολουθήθηκε η εξής διαδικασία:

1. Πραγματοποιήθηκε λήψη και εγκατάσταση του εργαλείου Volatility 2 (<https://github.com/volatilityfoundation/volatility/wiki/Installation>) σε λειτουργικό σύστημα Kali Linux.
2. Έγινε μετατροπή του αρχείου «hiberfil.sys» σε μορφή «raw memory dump» μέσω της εντολής «vol.py imagedump -f hiberfil.sys -O winxp.img».
3. Με την χρήση της εντολής «vol.py -f winxp.img --profile=WinXPSP2x86 pslist» εξήχθησαν οι παρακάτω διεργασίες (Εικόνα 63):

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x80a91800	System	4	0	46	217	—	0	0 2004-08-20 15:01:04 UTC+0000
0x8097ada8	smss.exe	416	4	3	21	—	0	0 2004-08-20 15:01:09 UTC+0000
0x8094f020	csrss.exe	472	416	11	306	0	0	0 2004-08-20 15:01:11 UTC+0000
0x80936970	winlogon.exe	500	416	22	500	0	0	0 2004-08-20 15:01:15 UTC+0000
0x80925318	services.exe	544	500	18	259	0	0	0 2004-08-20 15:01:15 UTC+0000
0x80923968	lsass.exe	556	500	21	311	0	0	0 2004-08-20 15:01:15 UTC+0000
0x80a2b0d0	svchost.exe	736	544	10	230	0	0	0 2004-08-20 15:01:22 UTC+0000
0x808e95e8	svchost.exe	788	544	82	1209	0	0	0 2004-08-20 15:01:22 UTC+0000
0x808d5890	svchost.exe	888	544	4	83	0	0	0 2004-08-20 15:01:25 UTC+0000
0x808cdb20	svchost.exe	900	544	15	163	0	0	0 2004-08-20 15:01:25 UTC+0000
0xffbda020	spoolsv.exe	1004	544	10	132	0	0	0 2004-08-20 15:01:27 UTC+0000
0xffba8020	explorer.exe	1312	1232	14	338	0	0	0 2004-08-20 15:01:33 UTC+0000
0ffb6f020	mssmsgs.exe	1556	1312	3	119	0	0	0 2004-08-20 15:01:38 UTC+0000
0ffa7020	mirc.exe	1564	1312	4	117	0	0	0 2004-08-20 15:39:10 UTC+0000
0ffb4b020	logonui.exe	608	500	3	129	0	0	0 2004-08-20 19:00:19 UTC+0000

Εικόνα 63 - Η λίστα διεργασιών πριν το τελευταίο hibernation

### 3.16.9. Ιχνη χρήσης προϊόντος για smart cards στο Registry

Στη διαδρομή «C:/Windows/System32/config/software\Schlumberger» βρέθηκαν ίχνη προϊόντος της εταιρίας «Schlumberger», που εξειδικεύεται στην κατασκευή έξυπνων καρτών (Εικόνα 64).

The screenshot shows the Windows Registry Editor window. On the left, there is a tree view of registry keys. The path 'Software\Schlumberger' is expanded, showing its subkeys: 'Smart Cards and Terminals' and 'Smart Cards'. 'Smart Cards' is further expanded to show subkeys for various smart card models: 'Cryptoflex 16K', 'Cryptoflex 4K', 'Cryptoflex 8K (no RSA key genera...', 'Cryptoflex 8K (V2)', 'Cryptoflex 8K (with RSA key gene...', 'Cyberflex Access 16K', 'Schlumberger Cryptoflex ActivCard', 'Schlumberger Cryptoflex e-gate', and 'Schlumberger Cyberflex Access C...'. The right pane of the window displays a list of these keys with their names and values.

Schlumberger	0
Smart Cards and Terminals	0
Smart Cards	0
Cryptoflex 16K	4
Cryptoflex 4K	4
Cryptoflex 8K (no RSA key genera...	4
Cryptoflex 8K (V2)	4
Cryptoflex 8K (with RSA key gene...	4
Cyberflex Access 16K	4
Schlumberger Cryptoflex ActivCard	4
Schlumberger Cryptoflex e-gate	4
Schlumberger Cyberflex Access C...	4

Εικόνα 64 - Ιχνη προϊόντος της εταιρίας «Schlumberger» στο Registry

# CHAIN OF CUSTODY

CONFIDENTIAL  
DO NOT COPY

-EVIDENCE-

TO BE OPENED ONLY BY AUTHORIZED AGENTS

Case No #: 01

Submitting Agent: Μάνιος Αθανάσιος, Μπάντης Χρήστος

Device Type: Laptop

Manufacturer: Dell

Serial Number: #VLQLW

RAM: -

OS: Windows XP Professional

Architecture: x86

State: OFF

Connectivity: Ethernet, WiFi, Modem 56K

Victim's Full Name: -

Victim's SSN: -

Suspect's Full Name / Description: Greg Schardt (Mr. Evil)

Evidence Recovered By: -

Evidence Bag Sealed By: -

Date Sealed: 20/9/2021

Time Sealed: 8:30 PM

Phone #: 2133330300

Cell #: 6970334536, 6973979235

## CHAIN OF CUSTODY

Label	Released By (ID#)	Received By (ID#)	Date / Time	Location / Comments
Τσάντα αποδεικτικών στοιχείων (σφραγισμένη)	#45 Αστυνόμος Παπαδόπουλος Κωνσταντίνος	#34 Μπάντης Χρήστος	08/05/2023	Παρελήφθη σφραγισμένη τσάντα αποδεικτικών στοιχείων υπόψιν κ. Μάνιου Αθανάσιου

<b>Τσάντα αποδεικτικών στοιχείων (σφραγισμένη)</b>	#34 Μπάντης Χρήστος	#23 Μάνιος Αθανάσιος	08/05/2023	<b>Μεταβίβαση σφραγισμένης τσάντας αποδεικτικών στοιχείων υπόψιν κ. Μάνιου Αθανάσιου</b>
<b>Τσάντα αποδεικτικών στοιχείων (σφραγισμένη)</b>	#23 Μάνιος Αθανάσιος	#23 Μάνιος Αθανάσιος	09/05/2023	<b>Αποσφράγιση τσάντας αποδεικτικών στοιχείων με περιεχόμενα: 1 Laptop μάρκας Dell με σειριακό αριθμό #VLQLW, 1 PCMCIA ασύρματη κάρτα δικτύου, 1 εξωτερική κεραία συχνότητας 802.11b</b>
<b>1 Laptop μάρκας Dell με σειριακό αριθμό #VLQLW, 1 PCMCIA ασύρματη κάρτα δικτύου, 1 εξωτερική κεραία συχνότητας 802.11b</b>	#23 Μάνιος Αθανάσιος	#12 Γιώργος Γεωργίου (Υπεύθυνος αποθήκευσης και φύλαξης στοιχείων)	11/05/2023	<b>Αποθήκευση και φύλαξη των κάτωθι στοιχείων: 1 Laptop μάρκας Dell με σειριακό αριθμό #VLQLW, 1 PCMCIA ασύρματη κάρτα δικτύου, 1 εξωτερική κεραία συχνότητας 802.11b</b>

**FOR AGENCY LAB ONLY**

CONDITION OF EVIDENCE BAG UPON RECEIPT: SEALED

LAB CASE #: 01

RECEIVED BY: Μπάντης Χρήστος

OPENED BY: Μάνιος Αθανάσιος

DATE: 09/05/2023 TIME: 10:00 AM DURATION: 48 ώρες

NOTES: Η τσάντα αποδεικτικών στοιχείων μεταφέρθηκε από τον κ. Μπάντη και παρελήφθη σφραγισμένη από τον κ. Μάνιο, υποδεικνύοντας πως τα στοιχεία παρέμειναν αναλλοίωτα κατά τη μεταφορά τους.

**-SIGNATURES-**

Μπάντης Χρήστος

Μάνιος Αθανάσιος

## **5. Παράρτημα**

### **5.1. Επίτευξη στόχου**

Η παρούσα τεχνική έκθεση πραγματεύεται τη διερεύνηση ενός ηλεκτρονικού εγκλήματος και την ανάλυση των κατασχεμένων πειστηρίων με σκοπό την επιβεβαίωση ή την διάψευση ενοχής του υπόπτου. Όσον αφορά στα ζητούμενα της, καλύφθηκαν πλήρως και λεπτομερώς, μηδενός εξαιρουμένου, με επαρκείς πληροφορίες και απεικονίσεις, ώστε τα αποδεικτικά στοιχεία να παρουσιάζονται κατανοητά. Η αιτιολόγηση των επιλογών που έγιναν κατά την συλλογή αποδεικτικών στοιχείων είναι εκτενής, η περιγραφή της διαδικασίας επαλήθευσης του ακριβούς αντιγράφου των αρχικών ψηφιακών πειστηρίων είναι αναλυτική, όπως είναι και η επεξήγηση των αποτελεσμάτων της έρευνας. Συμπερασματικά, έχει καταστεί σαφές πως βάσει των στοιχείων της τεχνικής ανάλυσης του παρόντος ηλεκτρονικού εγκλήματος, ο ύποπτος έχει διαπράξει εγκληματικές ενέργειες που αφορούν στην υποκλοπή στοιχείων αγνώστων. Συμπληρωματικά, στον υπολογιστή του υπόπτου βρέθηκαν ίχνη παιδικής πορνογραφίας και οικονομικών εγκλημάτων. Τέλος, οποιοσδήποτε ισχυρισμός του υπόπτου πως δεν τέλεσε ο ίδιος τις προαναφερθείσες ενέργειες, καταρρίπτεται πλήρως.

### **5.2. Ατομική συνεισφορά**

- Μάνιος Αθανάσιος

Η ατομική συνεισφορά στην εργασία αποδείχθηκε ισότιμη και κατανεμημένη. Οι γνώσεις που αποκτήθηκαν στην ηλεκτρονική εγκληματολογία και τις τεχνικές διερεύνησης ενός εγκλήματος αποδείχθηκαν πολύ σημαντικές και απαραίτητες. Η απόφαση που ελήφθη συμπληρώθηκε από τα ηλεκτρονικά αποδεικτικά στοιχεία που εντοπίστηκαν, τα οποία αποτελούν κρίσιμο κομμάτι της διαδικασίας. Ο συνδυασμός της ατομικής συνεισφοράς και της συλλογικής γνώσης επέτρεψε μια ολοκληρωμένη και ακριβή ανάλυση του εγκλήματος. Η ερευνητική διαδικασία σε αυτόν τον τομέα αποδείχθηκε κρίσιμης σημασίας για την αξιολόγηση και την ερμηνεία των ψηφιακών αποδεικτικών στοιχείων, καθώς και για την επιτυχή απόδοση της δικαιοσύνης. Επιπλέον, οι ατομικές παρατηρήσεις και σχόλια σχετικά με την ανάλυση των στοιχείων συνέβαλαν στην πλήρη κατανόηση των περιστάσεων του εγκλήματος και στην ακριβή αξιολόγηση των ανακαλυφθέντων στοιχείων. Επιπρόσθετα η ανταλλαγή απόψεων μεταξύ των μελών της ομάδας ενίσχυσε την κοινή κατανόηση και συνεισέφερε στην

πληρέστερη αξιολόγηση της υπόθεσης. Τέλος, η συνολική αποτελεσματικότητα της έρευνας βασίστηκε στην ισορροπημένη συνεργασία και την ομαδική προσπάθεια για την επίτευξη των κοινών στόχων.

#### - Μπάντης Χρήστος

Στο πλαίσιο της ατομικής συνδρομής ως προς την επίτευξη του αποτελέσματος της εργασίας, αφιερώθηκε χρόνος σε όλους τους τομείς που αφορούν στην αποπεράτωση της. Με αφετηρία τη θέση αυτή, εξετάστηκαν επιμελώς τα ψηφιακά αποδεικτικά στοιχεία, εντοπίζοντας βασικά αντικείμενα και μοτίβα που είναι καίριας σημασίας για την έρευνα. Η ενεργή συμμετοχή των μελών της ομάδας, συνεισφέροντας με γνώσεις και απόψεις στις διεξοδικές έρευνες και αναλύσεις που πραγματοποιήθηκαν, αποτέλεσε βοήθημα ως προς τον διαμοιρασμό πληροφοριών και τη λύση συλλογικών σύνθετων προβλημάτων. Όλα τα παραπάνω οδήγησαν στην ολοκληρωμένη κατανόηση της υπόθεσης, ενισχύοντας την ικανότητα της ομάδας να αποκαλύψει σημαντικές πληροφορίες και να εξάγει ακριβή συμπεράσματα, επιβεβαιώνοντας εν τέλει, την ενοχή του υπόπτου. Μέσω της ατομικής συμμετοχής προήχθη η προσωπική εξέλιξη, ενθαρρύνοντας την κριτική σκέψη, την έρευνα και την ανάπτυξη δεξιοτήτων. Επίσης, απόρροια της παρούσας εργασίας είναι η επέκταση των τεχνικών γνώσεων, εμβαθύνοντας τόσο στη δομή των υπολογιστικών συστημάτων, όσο και στον τρόπο που δρουν οι ύποπτοι που εμπλέκονται σε ηλεκτρονικά εγκλήματα.

### 5.3. Κατάλογος πινάκων

Πίνακας 1 - Πληροφορίες υπόθεσης .....	- 2 -
Πίνακας 2 - Τα hash values των εικονικών δίσκων .....	- 3 -
Πίνακας 3 - Συντομεύσεις εφαρμογών στον φάκελο «Tools» του «Desktop» .....	- 6 -
Πίνακας 4 - Κακόβουλο λογισμικό στον φάκελο «My Documents» .....	- 7 -
Πίνακας 5 - Στοιχεία που αποδεικνύουν τη χρήση κακόβουλου λογισμικού .....	- 10 -
Πίνακας 6 - Δεδομένα που έχουν παραχθεί από τη χρήση κακόβουλου λογισμικού .....	- 12 -

### 5.4. Κατάλογος εικόνων

Εικόνα 1 - Επαλήθευση των hashes των εικονικών δίσκων .....	- 3 -
Εικόνα 2 - Τα περιεχόμενα του φακέλου «C:/Program Files» .....	- 8 -
Εικόνα 3 - Τα περιεχόμενα του φακέλου «C:/My Documents» .....	- 9 -
Εικόνα 4 - Η καρτέλα «Run Programs» του εργαλείου «Autopsy» .....	- 11 -

Εικόνα 5 - Ο αριθμός των εκτελέσεων των κακόβουλων λογισμικών του εικονικού δίσκου.....	-
11 -	
Εικόνα 6 - Οι πληροφορίες για την πιο πρόσφατη υποκλοπή από το αρχείο «recent» .....	- 12 -
Εικόνα 7 - Πληροφορίες για την συσκευή του θύματος .....	- 13 -
Εικόνα 8 - Ο ιστότοπος «mobile.msn.com» που επισκέφθηκε το θύμα .....	- 13 -
Εικόνα 9 - Ο ιστότοπος «MSN Hotmail» που επισκέφθηκε το θύμα .....	- 14 -
Εικόνα 10 - Το περιεχόμενο του αρχείου «packets.pcap» που παράγεται από την εφαρμογή «Bulk_Extractor» .....	- 14 -
Εικόνα 11 - Πληροφορίες του φακέλου «Program Files» .....	- 15 -
Εικόνα 12 - Η ημερομηνία δημιουργίας του αρχείου «boot.ini».....	- 16 -
Εικόνα 13 - Η τιμή του «κλειδιού» «InstallDate» του Registry .....	- 16 -
Εικόνα 14 - Το λειτουργικό σύστημα του υπολογιστή-πειστηρίου .....	- 17 -
Εικόνα 15 - Η πλήρης ονομασία της έκδοσης του λειτουργικού συστήματος του υπολογιστή-πειστηρίου .....	- 17 -
Εικόνα 16 - Το κλειδί «000003EB» του αρχείου Registry «SAM» .....	- 18 -
Εικόνα 17 - Το κλειδί «Names» του αρχείου Registry «SAM» .....	- 19 -
Εικόνα 18 - Οι διεγραμμένες και μη αντιστοιχισμένες τιμές του αρχείου Registry «system»....	-
20 -	
Εικόνα 19 - Το αρχείου «hiberfil.sys» .....	- 20 -
Εικόνα 20 - Οι συνδέσεις δικτύου που ήταν ενεργές τη στιγμή που τέθηκε σε εφαρμογή η λειτουργία «Hibernation» .....	- 21 -
Εικόνα 21 - Η ημερομηνία τελευταίας εγγραφής του κλειδιού «TimeZoneInformation» .	- 21 -
Εικόνα 22 – Το περιεχόμενο «NTP» της τιμής «Type» .....	- 22 -
Εικόνα 23 - Το Time Zone του συστήματος.....	- 22 -
Εικόνα 24 - Το περιεχόμενο του φακέλου «C:/Document and Settings».....	- 23 -
Εικόνα 25 - Πληροφορίες για τον λογαριασμό χρήστη «Mr. Evil».....	- 23 -
Εικόνα 26 - Το όνομα του ιδιοκτήτη του υπολογιστή .....	- 24 -
Εικόνα 27 - Πληροφορίες για τον επεξεργαστή του συστήματος.....	- 25 -
Εικόνα 28 - Η κάρτα δικτύου μάρκας «Xircom».....	- 26 -
Εικόνα 29 - Η κάρτα δικτύου μάρκας «Compaq» .....	- 26 -
Εικόνα 30 - Τα περιεχόμενα του αρχείου «irunin.ini».....	- 27 -
Εικόνα 31 - Αναζήτηση βάσει διεύθυνσης «MAC» στο εργαλείο « <a href="https://www.adminsub.net/">https://www.adminsub.net/</a> » .....	- 27 -
Εικόνα 32 - Ιχνος ιστοτόπου που ανέφερε τις επιχειρηματικές κινήσεις της «T-Mobile».	- 28 -
Εικόνα 33 - Ιχνος ιστοτόπου σχετικού με «Wardriving» .....	- 29 -
Εικόνα 34 - Απόδειξη πως η κάρτα δικτύου λειτουργούσε σε «Promiscuous Mode» .....	- 29 -

Εικόνα 35 - Το τελευταίο «φίλτρο» που εφαρμόστηκε κατά τη διαδικασία υποκλοπής δεδομένων .....	- 30 -
Εικόνα 36 - Πληροφορίες σχετικά με την διεύθυνση-στόχο .....	- 31 -
Εικόνα 37 - Η τοποθεσία που αντιστοιχεί στην διεύθυνση-στόχο .....	- 31 -
Εικόνα 38 - Η απόσταση της τοποθεσίας της διεύθυνσης-στόχου από το κοντινότερο «Starbucks» .....	- 32 -
Εικόνα 39 - Δημιουργία λογαριασμού ομάδων ενημερώσεων στο εργαλείο «Outlook Express» .....	- 34 -
Εικόνα 40 - Πληκτρολόγηση της διεύθυνσης ενός NNTP server.....	- 34 -
Εικόνα 41 - Ορισμένες από τις ομάδες ενημερώσεων.....	- 35 -
Εικόνα 42 - Πιθανή μορφή του περιβάλλοντος της εφαρμογής ηλεκτρονικού ταχυδρομείου του υπόπτου .....	- 35 -
Εικόνα 43 - Το αρχείο «alt.2600.cardz.dbx» .....	- 36 -
Εικόνα 44 - Μηνύματα ηλεκτρονικού ταχυδρομείου που σχετίζονται με οικονομικά εγκλήματα .....	- 37 -
Εικόνα 45 - Τα περιεχόμενα του φακέλου «Nethood» .....	- 38 -
Εικόνα 46 - Πληροφορίες για τον εκτυπωτή «HP LaserJet 2100» .....	- 38 -
Εικόνα 47 - Πληροφορίες για τον εκτυπωτή «HP LaserJet 2100» στο Registry.....	- 39 -
Εικόνα 48 - Απόδειξη διαμοιρασμού αρχείων από/προς έναν δικτυακό τόπο .....	- 39 -
Εικόνα 49 - Λίστα των τελευταίων εφτά (7) αρχείων που προσπέλασε ο ύποπτος.....	- 39 -
Εικόνα 50 - Το ιστορικό των τοποθεσιών που συνδεόταν συχνότερα ο ύποπτος .....	- 40 -
Εικόνα 51 - Σάρωση του σκληρού δίσκου του υπόπτου για κακόβουλο λογισμικό .....	- 41 -
Εικόνα 52 - Οι ημερομηνίες δημιουργίας και προσπέλασης του αρχείου «NetBus170.zip»- 43	
-	
Εικόνα 53 - Το όνομα του υπολογιστή .....	- 44 -
Εικόνα 54 - Οι λεπτομέρειες του εικονικού δίσκου-πειστηρίου.....	- 44 -
Εικόνα 55 - Ο μοναδικός εκτυπωτής που ήταν συνδεμένος στο σύστημα.....	- 45 -
Εικόνα 56 - Ο σκληρός δίσκος και η μονάδα δίσκου CD-ROM του υπολογιστή .....	- 45 -
Εικόνα 57 - Η συσκευή «USB Hub» που ήταν συνδεμένη στον υπολογιστή .....	- 45 -
Εικόνα 58 - Η ημερομηνία της τελευταίας απενεργοποίησης του υπολογιστή .....	- 46 -
Εικόνα 59 - Προσπάθεια εύρεσης μη δεσμευμένου «Yahoo ID» από τον ύποπτο .....	- 46 -
Εικόνα 60 - Εύρεση μη δεσμευμένου «Yahoo ID» από τον ύποπτο .....	- 47 -
Εικόνα 61 - Το περιβάλλον εισερχομένων email(inbox) του υπόπτου.....	- 47 -
Εικόνα 62 - Το email καλωσορίσματος του υπόπτου από το «Yahoo! Mail».....	- 47 -
Εικόνα 63 - Η λίστα διεργασιών πριν το τελευταίο hibernation.....	- 48 -
Εικόνα 64 - Ήχη προϊόντος της εταιρίας «Schlumberger» στο Registry .....	- 48 -