ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ:

ΑΣΦΑΛΗΣ ΑΠΟΣΥΡΣΗ ΔΙΣΚΩΝ

ΚΑΛΛΙΟΠΗ ΜΠΟΥΚΟΥΒΑΛΑ

ΜΕ/0546

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ

ΑΣΦΑΛΗΣ ΑΠΟΣΥΡΣΗ ΔΙΣΚΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ:

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ:..... 2

ΠΕΡΙΛΗΨΗ..... 4

1. ΓΕΝΙΚΑ ΘΕΜΑΤΑ 5

1.1 ΕΙΣΑΓΩΓΗ - ΠΕΡΙΓΡΑΦΗ ΠΡΟΒΛΗΜΑΤΟΣ 7
1.2 ΝΟΜΟΘΕΤΙΚΑ ΠΛΑΙΣΙΑ..... 11
1.3 ΝΟΜΟΘΕΣΙΑ ΣΤΗΝ ΕΛΛΑΔΑ..... 13
1.4 ΠΩΣ ΦΑΙΝΟΝΤΑΙ ΤΑ ΔΙΑΓΡΑΜΜΕΝΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΣΥΣΤΗΜΑ..... 16
1.5 ΤΥΠΟΙ ΑΝΑΚΤΗΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ 19
1.6 ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΤΟΝ ΧΡΟΝΟ ΚΑΘΑΡΙΣΜΟΥ ΕΝΟΣ ΔΙΣΚΟΥ 21
1.7 ΛΑΘΗ ΧΡΗΣΤΩΝ..... 22
1.8 ΕΥΡΗΜΑΤΑ ΕΡΕΥΝΩΝ..... 25
1.9 ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ 27
1.10 FORENSICS..... 29
1.11 ΤΕΧΝΙΚΕΣ ΔΙΑΓΡΑΦΗΣ ΔΕΔΟΜΕΝΩΝ..... 31
1.12 ΕΡΓΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ.. 35
1.12.1 Εργαλεία Απόσυρσης..... 35
1.12.2 Εργαλεία Ανάκτησης 38
1.13 ΓΝΩΣΤΕΣ ΜΕΘΟΔΟΛΟΓΙΕΣ ΕΡΕΥΝΑΣ..... 39
1.14 ΓΕΝΙΚΕΣ ΣΥΜΒΟΥΛΕΣ ΠΡΟΛΗΨΗΣ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ 45

2. ΕΡΕΥΝΑ..... 47

2.1 ΣΚΟΠΟΣ..... 48
2.2 ΓΙΑΤΙ ΜΙΑ ΤΕΤΟΙΑ ΕΡΕΥΝΑ ΕΙΝΑΙ ΧΡΗΣΙΜΗ ΣΤΗΝ ΕΛΛΑΔΑ..... 48
2.3 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ 50
2.3.1 Γενικά..... 50
2.3.2 Αποτελέσματα..... 52
2.3.2.1 Αποτελέσματα από φοιτητές πληροφορικής:.....52

2.3.2.2 Αποτελέσματα από τους υπόλοιπους φοιτητές: 60
2.3.3 Συμπεράσματα 68
2.3.3.1 Για φοιτητές πληροφορικής: 68
2.3.3.2 Για τους υπόλοιπους φοιτητές: 69
2.4 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ..... 71
2.5 ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ 72
3. ΠΑΡΑΡΤΗΜΑΤΑ 73
ΠΑΡΑΡΤΗΜΑ Α 74
ΠΑΡΑΡΤΗΜΑ Β 78
ΠΑΡΑΡΤΗΜΑ Γ..... 80
ΒΙΒΛΙΟΓΡΑΦΙΑ..... 82

ΘΕΜΑ ΔΙΠΛΩΜΑΤΙΚΗΣ:

ΑΣΦΑΛΗΣ ΑΠΟΣΥΡΣΗ ΔΙΣΚΩΝ

ΠΕΡΙΛΗΨΗ

Η διπλωματική εργασία αφορά στο θέμα της ασφαλούς απόσυρσης δίσκων και στην ευαισθητοποίηση των χρηστών στην Ελλάδα σχετικά με το ζήτημα αυτό. Το θέμα της ασφαλούς απόσυρσης δίσκων αναφέρεται στην απόσυρση των παλιών δίσκων από τις εταιρείες και τους οικιακούς χρήστες, με τέτοιο τρόπο ώστε να διασφαλίζεται πως τα δεδομένα που υπήρχαν στον δίσκο δεν είναι ανακτήσιμα από άτομα που θα μπορούσαν να τα χρησιμοποιήσουν με κακόβουλο σκοπό. Το θέμα αυτό εξετάζεται στο θεωρητικό επίπεδο, αλλά και με ένα μικρό ερωτηματολόγιο.

Στο πρώτο κεφάλαιο περιγράφονται τα κυριότερα θέματα που αφορούν στο ζήτημα της ασφαλούς απόσυρσης σκληρών δίσκων σε θεωρητικό επίπεδο.

Στο δεύτερο κεφάλαιο εξετάζεται το πρόβλημα από τη πλευρά της Ελλάδας και περιέχονται τα αποτελέσματα του ερωτηματολογίου και τα συμπεράσματα που προέκυψαν από αυτά.

1. ΓΕΝΙΚΑ ΘΕΜΑΤΑ

Στο κεφάλαιο που ακολουθεί περιγράφονται τα κυριότερα θέματα που αφορούν στο ζήτημα της ασφαλούς απόσυρσης σκληρών δίσκων σε θεωρητικό επίπεδο.

Τα υποκεφάλαια που αναπτύσσονται είναι:

1.1 Εισαγωγή - Περιγραφή προβλήματος:
Μια γενική περιγραφή του προβλήματος της απόσυρσης των παλιών σκληρών δίσκων με ασφαλή τρόπο.

1.2 Νομοθετικά Πλαίσια:
Μια γενική αναφορά στα νομοθετικά πλαίσια που ισχύουν σε διάφορες χώρες.

1.3 Νομοθεσία στην Ελλάδα:
Μια παρουσίαση της νομοθεσίας που ισχύει στην Ελλάδα και αφορά στο κομμάτι της ασφαλούς καταστροφής των δεδομένων από ιδιωτικούς ή δημοσίους φορείς στην Ελλάδα.

1.4 Πως φαίνονται τα δεδομένα στο σύστημα:
Μια ανάλυση σχετικά με το τι γίνεται με τα διαγραμμένα αρχεία στα πιο κοινά συστήματα αρχείων.

1.5 Τύποι Ανακτημένων Δεδομένων:
Μια πιθανή κατηγοριοποίηση των τύπων των δεδομένων που μπορεί να βρεθούν σε ένα σκληρό δίσκο ως προς τον τρόπο ανάκτησης τους.

1.6 Παράγοντες που επηρεάζουν τον χρόνο καθαρισμού ενός δίσκου:
Οι παράγοντες που επηρεάζουν τον χρόνο που χρειάζεται ένας σκληρός δίσκος για να διαγραφεί από τα δεδομένα του με ασφαλή τρόπο.

1.7 Λάθη χρηστών:

Τα λάθη των χρηστών όσον αφορά στις πεποιθήσεις τους και στη συμπεριφορά τους σχετικά με την απόσυρση των παλιών δίσκων τους.

1.8 Ευρήματα Ερευνών:

Οι τύποι των δεδομένων που παραμένουν στους δίσκους όπως έχει προκύψει από τα ευρήματα ερευνών.

1.9 Κατηγορίες Απειλών:

Οι κατηγορίες των κινδύνων που μπορούν να προκύψουν από τη μη ασφαλή απόσυρση των δίσκων.

1.10 Forensics:

Μια αναφορά στην επιστήμη των forensics.

1.11 Τεχνικές Διαγραφής Δεδομένων:

Μια παρουσίαση των τεχνικών διαγραφής των δεδομένων από τους δίσκους.

1.12 Εργαλεία Λογισμικού που χρησιμοποιούνται:

Μια επισκόπηση σχετικά με τα εργαλεία λογισμικού που κυκλοφορούν.

1.13 Γνωστές μεθοδολογίες έρευνας:

Μια βασική μεθοδολογία για την διεκπεραίωση μιας έρευνας για την ανάκτηση δεδομένων από δίσκους.

1.14 Γενικές Συμβουλές για την αντιμετώπιση του προβλήματος:

Κάποια γενικά βήματα που μπορούν να ληφθούν για να μειωθεί η πιθανότητα να ανακτηθούν ευαίσθητα προσωπικά δεδομένα από κακόβουλους χρήστες.

1.1 ΕΙΣΑΓΩΓΗ - ΠΕΡΙΓΡΑΦΗ ΠΡΟΒΛΗΜΑΤΟΣ

Στο υποκεφάλαιο αυτό ακολουθεί μια περιγραφή του προβλήματος της απόσυρσης των παλιών σκληρών δίσκων με ασφαλή τρόπο. Πρόκειται για ένα ζήτημα το οποίο επηρεάζει τους οικιακούς χρήστες, τους οργανισμούς, την βιομηχανία και την πανεπιστημιακή κοινότητα.

Χαρακτηριστικά σκληρών δίσκων:

Έχει σημειωθεί δραματική αύξηση στην χωρητικότητα των μέσων αποθήκευσης σε συνδυασμό με μια μείωση στις τιμές τους. Σύμφωνα με την Gartner Dataquest οι αγορές σκληρών δίσκων για υπολογιστές desktop (3.5 ίντσες) θα αυξηθούν από 190.8 εκατομμύρια που ήταν το 2003, σε 298.7 εκατομμύρια μέχρι το 2008. Οι αγορές σκληρών δίσκων για laptops (2.5 ίντσες) θα αυξηθούν από 3.6 εκατομμύρια που ήταν το 2003, σε περίπου 20 εκατομμύρια το 2008 **[23]**. Η χρήσιμη ζωή ενός δίσκου κυμαίνεται από δύο ως τρία χρόνια προτού θεωρηθεί παλιός, και έχει πολύ μικρή αξία στην αγορά μεταχειρισμένου υλικού υπολογιστών. Εφόσον οι παλιοί δίσκοι δε καταστραφούν με φυσικό τρόπο, τότε μπορούν να προκύψουν διάφοροι κίνδυνοι για την ιδιωτικότητα των πληροφοριών που αφορούν στους κατόχους τους. Το κόστος από την διαρροή αυτών των πληροφοριών είναι πάρα πολύ μεγάλο.

Σε σχέση με τα υπόλοιπα αποθηκευτικά μέσα, οι σκληροί δίσκοι παρουσιάζουν κάποια ιδιαίτερα προβλήματα όσον αφορά στην διασφάλιση της εμπιστευτικότητας των δεδομένων. Ένας λόγος είναι ότι τα φυσικά και τα ηλεκτρονικά πρότυπα για τα υπόλοιπα μέσα αποθήκευσης έχουν εξελιχθεί γρήγορα και χωρίς να υπάρχει συμβατότητα μεταξύ τους, τα τελευταία χρόνια. Από την άλλη πλευρά οι διεπαφές των σκληρών δίσκων έχουν μείνει ίδιες και έχουν συμβατότητα με πολύ παλαιότερα μοντέλα. Αυτό έχει ως αποτέλεσμα, να υπάρχει η δυνατότητα κάποιοι να χρησιμοποιούν δίσκους που να είναι 10 ετών σε καινούργιους υπολογιστές απλά συνδέοντας τους. Τα

φυσικά, τα ηλεκτρονικά και τα λογικά πρότυπα έχουν παραμείνει πολύ σταθερά. Ένας δεύτερος παράγοντας που επιβαρύνει το ζήτημα της εμπιστευτικότητας των δεδομένων είναι η μακροπρόθεσμη συνέπεια των πληροφοριών που διατηρούν τα συστήματα αρχείων **[9]**.

Γιατί υπάρχει πρόβλημα;

Οι οργανισμοί τόσο του δημόσιου όσο και του ιδιωτικού τομέα χρησιμοποιούν μέσα αποθήκευσης ηλεκτρονικών υπολογιστών, για την αποθήκευση πληροφοριών που σχετίζονται με την επιχείρηση και τις υπηρεσίες που προσφέρουν, καθώς επίσης για πληροφορίες που αφορούν στους υπαλλήλους τους και στους πελάτες τους. Οι οικιακοί χρήστες χρησιμοποιούν τους προσωπικούς τους υπολογιστές και αποθηκεύουν σε αυτούς πληροφορίες που αφορούν στους ίδιους και στις οικογένειες τους. Το είδος των πληροφοριών που αποθηκεύονται στους υπολογιστές κάνει πολύ σημαντικό το ζήτημα της ασφαλούς απόσβεσης των δίσκων. Οι περισσότεροι οργανισμοί και οικιακοί χρήστες δεν γνωρίζουν αρκετά για το τι μπορεί να συμβεί στους σκληρούς δίσκους τους, αφού αποσβεστούν **[1] [8]**.

Είναι αρκετά συχνό φαινόμενο ένας οργανισμός να δωρίζει παρωχημένο υλικό υπολογιστών για φιλανθρωπικούς σκοπούς ή σε σχολεία **[3]**. Από τη στιγμή που ένας υπολογιστής φύγει από τον έλεγχο του οργανισμού όπου ανήκει, τότε η πληροφορία που είναι αποθηκευμένη σε αυτόν είναι διαθέσιμη σε οποιονδήποτε μπορεί να τον αποκτήσει, κάτι που έχει πιθανότατα σημαντικές συνέπειες στον οργανισμό. Αυτό ισχύει φυσικά εφόσον ο οργανισμός δεν έχει λάβει μέτρα για την ασφαλή απόσβεση των δίσκων του ή δε έχει αναθέσει αυτό το έργο σε μια αξιόπιστη εταιρεία. Το ίδιο ισχύει και για τους οικιακούς χρήστες και δε πρέπει να πιστεύεται ότι κανείς δε θα θελήσει να αποκτήσει αυτές τις πληροφορίες **[1]**. Οι οργανισμοί θα έχουν πάρα πολλές προσωπικές και ευαίσθητες πληροφορίες αποθηκευμένες στα συστήματα τους, όπως πληροφορίες για τους υπαλλήλους τους, πληροφορίες για τους πελάτες τους και επιχειρησιακά πλάνα **[1]**, τραπεζικούς λογαριασμούς και λογαριασμούς

μισθοδοσίας, επιχειρησιακά μυστικά που αφορούν σε ορισμένα προϊόντα, καθώς και ιατρικά δεδομένα **[3]**. Οι υπολογιστές των οικιακών υπολογιστών μπορεί να συλλεχθούν ώστε να συγκεντρωθεί πληροφόρηση για τις δραστηριότητες των χρηστών, για παράδειγμα τις ιστοσελίδες που επισκέφτηκαν, τα αρχεία που κατέβηκαν, chat logs, καθώς και τις εφαρμογές που έχουν εγκατασταθεί και εκτελεστεί στο σύστημα **[3]**.

Οι περισσότερες τεχνικές που χρησιμοποιούνται κατά τη διάρκεια της ζωής του hardware για να διασφαλίσουν την ασφάλεια των δεδομένων (firewalls, antivirus μέτρα και κρυπτογραφικοί έλεγχοι), αποτυγχάνουν όταν οι δίσκοι αποσύρονται χωρίς να έχει διασφαλιστεί η διαγραφή των δεδομένων τους. Για παράδειγμα, όποια προστασία προσέφερε το λειτουργικό σύστημα του υπολογιστή, όταν κάποιος θα αφαιρέσει τον δίσκο και τον εγκαταστήσει σε ένα δεύτερο σύστημα, δε θα είναι πλέον χρήσιμη και τότε θα μπορεί ο επιτιθέμενος να αποκτήσει πρόσβαση στα δεδομένα **[9]**. Είναι προφανές ότι οι εταιρείες δε λαμβάνουν υπόψη τον κίνδυνο διαρροής πληροφοριών από δίσκους που δεν έχουν αποσυρθεί σωστά κατά την διαχείριση του κινδύνου τους **[25]**.

Έρευνες έχουν δείξει ότι αρκετοί άνθρωποι παίρνουν ηλεκτρονικά τμήματα από αγορά μεταχειρισμένων και τα χρησιμοποιούν χωρίς να το γνωρίζει ο αρχικός χρήστης τους. Έτσι, για να διασφαλιστεί η προστασία της ιδιωτικότητας κάθε ατόμου, θα πρέπει να διασφαλίζεται ότι τα δεδομένα θα διαγράφονται με ασφαλή τρόπο από τους σκληρούς δίσκους προτού αποσυρθούν **[9]**. Επίσης αποτελεί σημαντικό πρόβλημα το ότι οι πωλητές μεταχειρισμένων διαφημίζουν το γεγονός ότι οι δίσκοι τους προέρχονται από μεγάλες εταιρίες, διευκολύνοντας περισσότερο τους εγκληματίες στην επιλογή των δίσκων **[25]**.

Η μεγάλη πλειοψηφία των χρηστών, θεωρεί πως ο προφανής τρόπος διαγραφής δεδομένων είναι μέσω εντολών «delete» και «erase», καθώς και ότι με αυτόν τον τρόπο τα δεδομένα διαγράφονται μόνιμα **[9]**. Στη

πραγματικότητα τα δεδομένα παραμένουν στον δίσκο αναλλοίωτα, εκτός κι αν επικαλυφθούν με άλλα. Αρκετοί χρήστες πιστεύουν επίσης, ότι με την εντολή «format» διαγράφονται όλα τα δεδομένα ενός δίσκου, ενώ στην πραγματικότητα τα περισσότερα παραμένουν αναλλοίωτα. Μόνο οι πιο έμπειροι χρήστες αναγνωρίζουν το πρόβλημα και χρησιμοποιούν εξειδικευμένα εργαλεία για τη διαγραφή των δεδομένων τους **[3]**. Έτσι φαίνεται πως οι χρήστες δεν έχουν την απαραίτητη γνώση, ή τα εργαλεία για να διαγράψουν με ασφαλή τρόπο τα δεδομένα τους **[4]**.

Ακόμα και αν υπάρχει η γνώση και τα κατάλληλα εργαλεία για την ασφαλή διαγραφή των δίσκων, ο χρόνος που χρειάζεται για να σβηστούν αποτελεί ένα πολύ σημαντικό ζήτημα. Αφότου ένας σκληρός δίσκος δεν χρειάζεται πλέον και έχει αφαιρεθεί από τον υπολογιστή, μένει πολύς λίγος χρόνος στην εταιρεία για να σβήσει με ασφαλή τρόπο τα δεδομένα. Έτσι προκύπτει ότι δεν είναι πρακτικό, σε όρους χρόνου και ανθρώπινου δυναμικού, να αφαιρεθεί κάθε δίσκος και να καθαριστεί από τα δεδομένα του με ασφαλή τρόπο ακόμα και για έναν μεγάλο οργανισμό. Αυτό το πρόβλημα εντείνεται καθώς οι χωρητικότητα των σκληρών δίσκων συνεχώς αυξάνεται **[20]**.

Στην περίπτωση των δίσκων που προέρχονται από το οικιακό περιβάλλον είναι πιο εύκολο να κατανοηθεί ότι οι χρήστες δεν έχουν την απαραίτητη γνώση ή τα διαθέσιμα εργαλεία ώστε να καθαρίσουν τα δεδομένα από τον δίσκο τους σε ικανοποιητικό βαθμό. Από την άλλη πλευρά, λόγο της αυξανόμενης δημοσιότητας που λαμβάνει το θέμα αναμένεται η σταδιακή τους ευαισθητοποίηση, και ότι με τον καιρό θα αρχίσουν να λαμβάνουν τα απαραίτητα βήματα για τη λύση του προβλήματος **[8]**.

<u>Ο κίνδυνος είναι υπαρκτός:</u>

Από τη στιγμή λοιπόν που ο σκληρός δίσκος δεν είναι κρυπτογραφημένος και αποσυρθεί, οι εμπιστευτικές πληροφορίες που περιέχει είναι διαθέσιμες σε οποιονδήποτε πάρει στα χέρια του τον δίσκο. Αποκαλύψεις τέτοιου τύπου

γίνονται όλο και πιο συχνές και η διαρροή πληροφοριών με αυτόν τον τρόπο γίνεται όλο και πιο συνηθισμένη **[8]**. Επίσης, υπάρχουν άτομα που ψάχνουν αυτήν την πληροφορία και έχουν τα κατάλληλα εργαλεία, καθώς και την τεχνογνωσία για να τα καταφέρουν να ανακτήσουν τις πληροφορίες που αναζητούν **[3]**.

1.2 ΝΟΜΟΘΕΤΙΚΑ ΠΛΑΙΣΙΑ

Στο υποκεφάλαιο αυτό γίνεται μια γενική αναφορά στα νομοθετικά πλαίσια που ισχύουν σε διάφορες χώρες, στα περιεχόμενα τους και στα προβλήματα που μπορεί να προκύπτουν από αυτά.

Είναι σημαντική η ύπαρξη νομοθετικών πλαισίων για να καθοριστεί η ευθύνη των οργανισμών τόσο ως προς τον ίδιο τον οργανισμό, όσο και ως προς τα άτομα, των οποίων διαχειρίζεται τα προσωπικά δεδομένα. Το καθήκον αυτό ενσωματώνεται σε μια ποικιλία νόμων. Οι πιο σημαντικοί τομείς είναι οι Νόμοι Προστασίας Δεδομένων και οι προδιαγραφές για τις εταιρείες, οι οποίες εκφράζονται σε κανονισμούς για τη πολιτική των οργανισμών, όπως το Σύμφωνο της Βασιλείας ΙΙ για την Ευρωπαϊκή Ένωση ή το νομοθετικό πλαίσιο του Sarbanes Oxley στις ΗΠΑ. Οι Νόμοι Προστασίας Δεδομένων απαιτούν πως κάθε οργανισμός που θα κρατάει προσωπικά δεδομένα, μέσω των οποίων μπορεί να αναγνωριστεί το άτομο στο οποίο ανήκουν, θα πρέπει αρχικά να το δηλώνει στην αρμόδια αρχή, αλλά και να διασφαλίζει πως χρησιμοποιούνται τα δεδομένα αποκλειστικά για τους σκοπούς για τους οποίους αποκτήθηκαν και να παρέχει στα δεδομένα αυτά το αντίστοιχο επίπεδο προστασίας **[1]**.

Οι νόμοι αναφέρουν πως:

- Οι αρμοδιότητες και οι υποχρεώσεις του υπεύθυνου επεξεργασίας προσωπικών δεδομένων βασίζονται σε οχτώ αρχές **[1] [7]**:
    - Η επεξεργασία των δεδομένων πρέπει να είναι σύμφωνα με τον νόμο.

- Η επεξεργασία των δεδομένων πρέπει να γίνεται για συγκεκριμένους νόμιμους σκοπούς.
- Τα δεδομένα που θα ζητηθούν για επεξεργασία θα πρέπει να είναι επαρκή, να σχετίζονται με το σκοπό της και να είναι τα απολύτως απαραίτητα.
- Τα δεδομένα θα πρέπει να είναι ακριβή και ενημερωμένα.
- Τα δεδομένα δε θα πρέπει να κρατούνται για μεγαλύτερο χρονικό διάστημα από ότι είναι απαραίτητο για την επεξεργασία τους.
- Τα προσωπικά δεδομένα θα πρέπει να δέχονται επεξεργασία σύμφωνη με τα δικαιώματα των υποκειμένων τους.
- Τα προσωπικά δεδομένα πρέπει να είναι ασφαλή.
- Τα δεδομένα δε θα πρέπει να μεταφέρονται σε άλλες χώρες χωρίς επαρκή προστασία.

- Επιπρόσθετα πρέπει να λαμβάνονται τα αντίστοιχα μέτρα ασφάλειας για να διασφαλίζεται πως τα δεδομένα θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, από μεταβολές και απώλεια ή διαρροή τους **[1]**.
- Εφόσον οι οργανισμοί αποτύχουν να εκτελέσουν το καθήκον που έχουν μπορούν να θεωρηθούν υπεύθυνοι και η FSA μπορεί να λάβει δράση εναντίον του οργανισμού εξαιτίας αυτής της αποτυχίας **[1]**.

Ωστόσο πρέπει να τονιστεί ότι υπάρχει μεγάλη διακύμανση στους νόμους από χώρα σε χώρα. Για παράδειγμα, επίσημες οδηγίες από το Υπουργείο Άμυνας των US προτείνουν πως για να είναι αποτελεσματικός ο καθαρισμός των δεδομένων από τους δίσκους, να γίνεται επικάλυψη των δεδομένων τρεις φορές, αρχικά με έναν χαρακτήρα, μετά με τον συμπληρωματικό του και έπειτα με έναν τυχαίο χαρακτήρα. Για τους δίσκους που περιέχουν ευαίσθητα δεδομένα προτείνονται αυστηρές προδιαγραφές με 35 επικαλύψεων των δεδομένων που περιέχουν **[22]**. Από την άλλη πλευρά, στην Αυστραλία δεν υπάρχουν επίσημα νομοθετικά πλαίσια για τη διαγραφή των δεδομένων από αποσυρμένους δίσκους **[25]**.

Τέλος, υπάρχουν κάποια γενικά ζητήματα όσον αφορά στις επίσημες οδηγίες για την ασφαλή απόσυρση αποθηκευτικών μέσων. Αρχικά, υπάρχει η πιθανότητα να είναι παλιές και να μη καλύπτουν τις τεχνολογικές εξελίξεις, τόσο στον τομέα της ασφαλούς κατάργησης, όσο και στον τομέα της ανάκτησης των δεδομένων από τα μέσα αποθήκευσης. Το δεύτερο ζήτημα με τις επίσημες οδηγίες είναι ότι μπορεί να είναι ηθελημένα ανακριβείς, ώστε να παραπλανήσουν αντίπαλες υπηρεσίες πληροφοριών **[14]**.

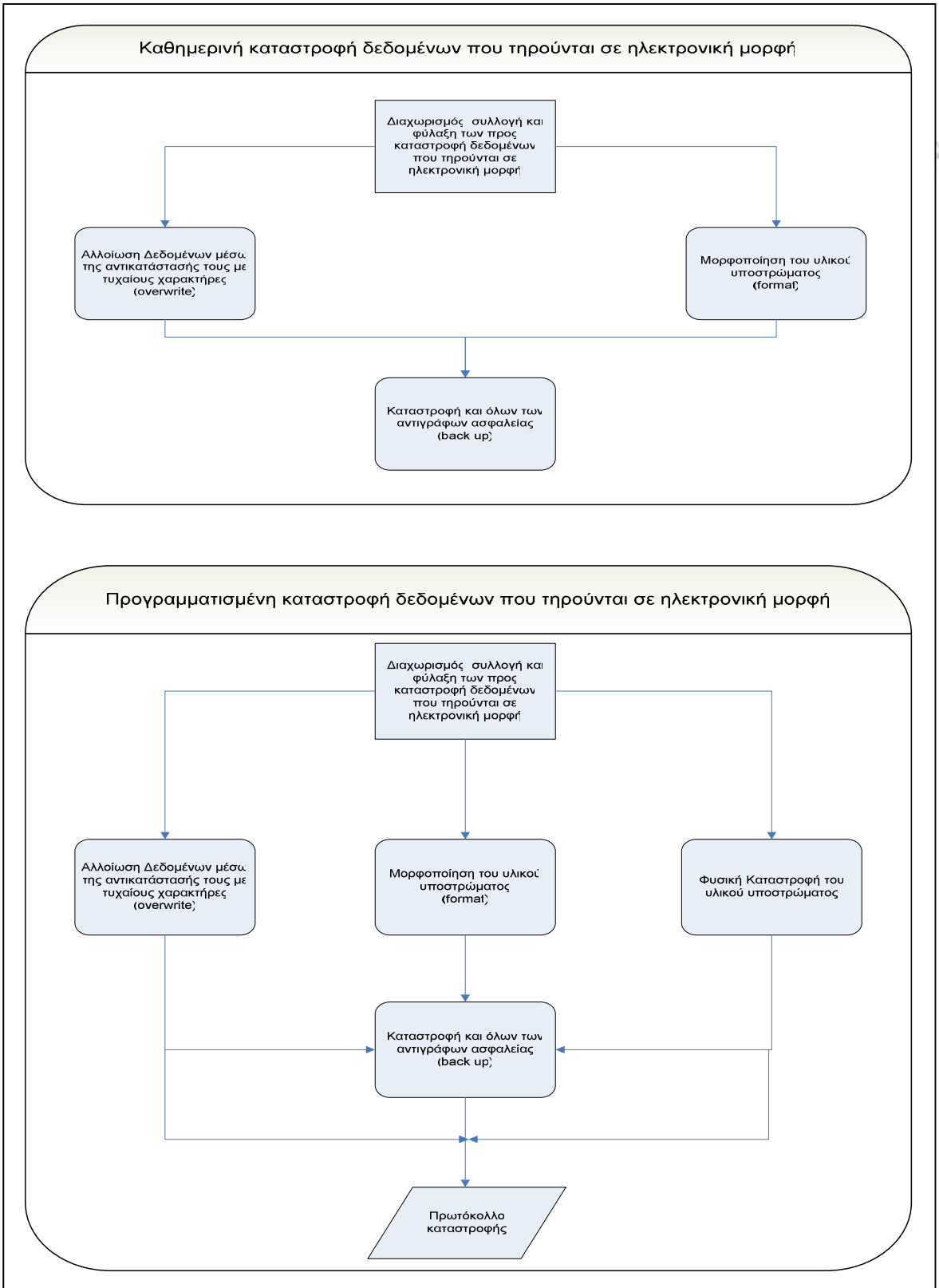
1.3 ΝΟΜΟΘΕΣΙΑ ΣΤΗΝ ΕΛΛΑΔΑ

Στο υποκεφάλαιο που ακολουθεί παρουσιάζονται επιγραμματικά τα σημεία σε νόμους και σε οδηγίες που αφορούν στο κομμάτι της ασφαλούς καταστροφής των δεδομένων από ιδιωτικούς ή δημοσίους φορείς στην Ελλάδα.

Ο κύριος νόμος που ισχύει στην Ελλάδα και αφορά στην επεξεργασία των προσωπικών δεδομένων είναι ο «ΝΟΜΟΣ 2472/1997 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ» **[16]**. Στον νόμο αυτό τονίζεται ότι τα δεδομένα πρέπει να συλλέγονται για καθορισμένους σκοπούς και να υφίστανται επεξεργασία σύμφωνη με τους σκοπούς αυτούς. Επίσης τα δεδομένα που συλλέγονται δε πρέπει να είναι περισσότερα από τα απαραίτητα για την εκάστοτε επεξεργασία και τέλος να μη διατηρούνται μετά το πέρας της περιόδου που απαιτείται για την επεξεργασία τους. Είναι καθήκον του υπεύθυνου της επεξεργασίας, και συνεπώς των φορέων που επεξεργάζονται τα δεδομένα, να τηρηθεί ο νόμος και τονίζεται από αυτόν ότι η παραβίαση του επισύρει συνέπειες.

Πιο συγκεκριμένα για την καταστροφή των δεδομένων μετά το πέρας της επεξεργασίας τους, έχει εκδοθεί από την Αρχή Προστασίας Προσωπικών δεδομένων η οδηγία «ΑΡ.1/2005 για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας» **[17]**. Όπως φάνηκε

παραπάνω, σύμφωνα με τον νόμο 2472/1997 είναι υποχρεωτική η καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας ή γενικότερα της περιόδου τήρησης των προσωπικών δεδομένων (άρθρο 4 παρ. 1 δ). Ο υπεύθυνος επεξεργασίας πρέπει είτε να καταστρέψει τα δεδομένα ή να τα καταστήσει ανώνυμα, δηλαδή να μη μπορεί να αναγνωριστεί ο κάτοχος τους. Τα δεδομένα χωρίζονται ανάλογα με το χρονικό διάστημα που χρειάζεται για την επεξεργασία τους, σε δεδομένα που καταστρέφονται καθημερινά ή προγραμματισμένα, είτε τμηματικά ή συνολικά. Τονίζεται πως τα προσωπικά δεδομένα πρέπει να καταστρέφονται ***με ασφαλή τρόπο***, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους, όπως είναι η κάθε μορφή διάθεσης σε τρίτους. Ως ασφαλής τρόπος καταστροφής των δεδομένων θεωρείται κάθε σύνολο διαδικασιών και μέτρων, τα οποία θα διασφαλίζουν πως μετά από την ολοκλήρωση της εφαρμογής τους δεν θα είναι δυνατό να αναγνωρισθούν τα υποκείμενα των δεδομένων. Η καταστροφή των δεδομένων θα πρέπει να είναι μη αναστρέψιμη, δηλαδή να μην είναι δυνατή η ανάκτηση των δεδομένων μετά την καταστροφή τους με τεχνικά ή άλλα μέσα. Αν τα δεδομένα είναι έντυπης μορφής (έγγραφα) τότε προτείνεται ως τρόπος καταστροφής τους ο τεμαχισμός τους, η πολτοποίηση τους ή η αποτέφρωσή τους. Αν τα δεδομένα είναι ηλεκτρονικής μορφής και φυλάσσονται σε ηλεκτρονικά αποθηκευτικά μέσα (σκληρούς δίσκους υπολογιστών, CD, DVD, δισκέττες, κ.λπ.), τονίζεται ότι δεν επαρκεί η απλή διαγραφή τους και προτείνεται για την ασφαλή καταστροφή τους να αλλοιωθούν μέσω αντικατάστασης τους με άλλα δεδομένα (overwrite). Η αλλοίωση μπορεί να γίνει με τη χρήση ειδικών προγραμμάτων (file erasers, file shredders, file pulveritizers). Στην περίπτωση της καθημερινής καταστροφής δεδομένων, ένας εναλλακτικός τρόπος καταστροφής είναι να μορφοποιηθεί το υλικό υπόστρωμα (format). Στην περίπτωση της προγραμματισμένης καταστροφής του συνόλου των δεδομένων προτείνεται η φυσική καταστροφή των μέσων αποθήκευσής τους (π.χ. με θρυμματισμό, κονιορτοποίηση, αποτέφρωση).



Ασφαλής καταστροφή δεδομένων που τηρούνται σε ηλεκτρονική μορφή συμφωνά με την οδηγία ΑΡ.1/2005, άρθρο 6

1.4 ΠΩΣ ΦΑΙΝΟΝΤΑΙ ΤΑ ΔΙΑΓΡΑΜΜΕΝΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΣΥΣΤΗΜΑ

Στο υποκεφάλαιο που ακολουθεί θα προσπαθήσουμε να αναλύσουμε τι γίνεται με τα διαγραμμένα αρχεία στα πιο κοινά συστήματα αρχείων. Σκοπός αυτής της ανάλυσης είναι να φανεί ότι τα αρχεία που θεωρούμε διαγραμμένα στη πραγματικότητα κρατούνται στο σύστημα και μπορούν να ανακτηθούν είτε τα ίδια τα αρχεία, είτε τμήματά τους, είτε πληροφορίες σχετικά με αυτά.

Είναι βασικό να τονιστεί ότι ο όρος διαγραφή εξαρτάται από το σύστημα που χρησιμοποιείται. Στις περισσότερες περιπτώσεις όταν σβήνουμε ένα αρχείο, επικαλύπτεται με δεδομένα ο δείκτης που έδειχνε τη θέση του αρχείου. Ωστόσο το αρχείο παραμένει άθικτο **[9]**.

Κάδος ανακύκλωσης στο σύστημα αρχείων FAT:

Όταν σβήνουμε ένα αρχείο στο σύστημα αρχείων FAT (File Allocation Table) συμβαίνουν δύο πράγματα. Αρχικά, το σύστημα τροποποιεί το πρώτο χαρακτήρα του ονόματος του αρχείου, για να δείξει ότι το αρχείο έχει διαγραφεί και ότι η εγγραφή καταλόγου μπορεί να χρησιμοποιηθεί ξανά. Έπειτα, το σύστημα μετακινεί όλα τα clusters που καταλαμβάνει το FAT στα ελεύθερα clusters του σκληρού δίσκου. Το αρχείο παραμένει άθικτο **[9]**. Το πραγματικό σύστημα που αποτελεί τον κάδο ανακύκλωσης λέγεται «Recycled» και περιέχει φακέλους που έχουν διαγραφεί από τον χρήστη και έχουν τοποθετηθεί στον κάδο ανακύκλωσης. Είναι αρχεία του συστήματος, τα οποία είναι απλά σε κατάσταση ετοιμότητας για διαγραφή. Με αυτόν τον τρόπο είναι εύκολο να υπάρχει διάκριση μεταξύ των αρχείων που έχει σβήσει ο χρήστης και των αρχείων που έχουν σβηστεί από το σύστημα **[2]**.

Η ύπαρξη των δεδομένων στο αρχείο INFO2 (ή INFO ανάλογα με το λειτουργικό σύστημα) δίνουν σε κάποιον, που γνωρίζει αρκετά ώστε να ψάχνει για αυτά, πληροφορίες σχετικά με την ημερομηνία και την ώρα

διαγραφής του αρχείου, καθώς και την αρχική θέση του αρχείου στον υπολογιστή, πριν αυτό διαγραφεί **[2]**.

Αφού διαγραφεί το αρχείο από τον κάδο ανακύκλωσης μετατρέπεται σε διαγραμμένο FAT αρχείο και οι εγγραφές του INFO2 αρχείου καθαρίζονται. Ωστόσο, ακόμα και έτσι είναι δυνατή η ανάκτηση των διαγραμμένων αρχείων INFO2 και συνεπώς χρήσιμων πληροφοριών για τον χρήστη ή τον οργανισμό **[2]**.

Κάδος ανακύκλωσης στο σύστημα αρχείων NTFS **[2]**:

Η ανάκτηση των δεδομένων που προέρχονται από το NTFS (New Technology File System) σύστημα είναι πολύ πιο απλή σε σχέση με αυτά που προέρχονται από το FAT σύστημα. Αυτό οφείλεται στα χαρακτηριστικά του συστήματος, τα οποία αναλύονται παρακάτω.

Στο σύστημα αρχείων NTFS, ο κρυφός φάκελος που διατηρεί το σύστημα ονομάζεται «Recycler» αντί για «Recycled», την ονομασία δηλαδή που είχε στο FAT σύστημα. Ένα πολύ σημαντικό χαρακτηριστικό του κάδου ανακύκλωσης του συστήματος αρχείων NTFS είναι ότι διαχωρίζει τα αρχεία ανάλογα με το ID ασφάλειας του χρήστη (SID΄s) και τα διαγραμμένα αρχεία κάθε χρήστη τοποθετούνται στον φάκελο που σχετίζεται με το SID του. Κάθε ξεχωριστός φάκελος έχει το δικό του INFO2 αρχείο, έτσι οι λεπτομέρειες σχετικά με τις διαγραφές των αρχείων παρέχουν πλέον πληροφορία και σχετικά με τον χρήστη που την πραγματοποίησε.

Ο τρόπος ο οποίος χρησιμοποιείται για να δείξει την θέση των αρχείων στο δίσκο από το σύστημα NTFS είναι κάπως διαφορετικό από τον τρόπο που χρησιμοποιούσε το FAT σύστημα. Αυτό έχει ως αποτέλεσμα, οι ανακτημένες πληροφορίες από το NTFS να είναι πιο αξιόπιστες από αυτές του FAT συστήματος. Στο NTFS ο κεντρικός κατάλογος των δεδομένων που φυλάσσονται στον δίσκο κρατείται σε ένα αρχείο του συστήματος το MFT

(Master File Table). Το κρυφό αυτό αρχείο στην πραγματικότητα είναι μια σχεσιακή βάση δεδομένων που δείχνει τα περιεχόμενα του δίσκου και περιέχει μια καταχώρηση για κάθε αρχείο και φάκελο στον δίσκο. Εκτός από το λογικό και φυσικό μέγεθος του κάθε αρχείου, το MFT αρχείο περιέχει πληροφορίες σχετικά με το όνομα του αρχείου, τις ημερομηνίες και τις ώρες, καθώς και τις ιδιότητες του συστήματος DOS. Σε ορισμένες περιπτώσεις μπορεί να περιέχει πληροφορίες σχετικά με τον ιδιοκτήτη και τα δικαιώματα του κάθε χρήστη του υπολογιστή σε αυτό.

Οι καταχωρήσεις του αρχείου διαχωρίζονται σε διαφορετικές περιοχές δεδομένων που ονομάζονται «Attributes» (δε πρέπει να τις μπερδέψουμε με τις ιδιότητες των αρχείων στο DOS για παράδειγμα Read Only, Hidden κ.τ.λ.). Το συγκεκριμένο «Attribute» δείχνει στα δεδομένα στο δίσκο. Όταν διαγράφεται ένα αρχείο στο σύστημα NTFS συμβαίνουν δύο πράγματα. Αρχικά, το MFT αρχείο χαρακτηρίζεται έτσι ώστε να φαίνεται ότι δείχνει σε διαγραμμένο αρχείο. Έπειτα, ένα αρχείο του συστήματος που λέγεται $Bitmap ενημερώνεται έτσι ώστε να δείχνει πως οι μονάδες καταχώρησης που χρησιμοποιούσε το αρχείο μπορούν να χρησιμοποιηθούν ξανά από το σύστημα.

Το αρχείο MTF δεν τροποποιείται εκτός και αν χρειαστεί να επικαλυφθεί από το ίδιο το αρχείο. Με αυτόν τον τρόπο όταν γίνει ανάκτηση αυτού του αρχείου, κάποιος γνωρίζει αμέσως την θέση που κατείχε κάθε αρχείου στον δίσκο πριν διαγραφεί. Με αυτόν τον τρόπο είναι πιο εύκολη η ανάκτηση του αρχείου από τον δίσκο. Δε είναι απαραίτητο δηλαδή να μαντέψει κάποιος τη θέση του αρχείου όπως ισχύει στο FAT σύστημα. Επίσης ακόμα και αν έχουν επικαλυφθεί τμηματικά το αρχείο. καθιστά εφικτή την ανάκτηση κάποιων τμημάτων του αρχείου αφού έτσι κι αλλιώς θα φαίνεται η θέση τους στο MTF αρχείο. Τέλος ακόμα και αν επικαλυφθούν ολοκληρωτικά τα αρχεία στο NTFS, είναι δυνατό να αποδειχθεί η ύπαρξή τους από το αρχείο MFT.

1.5 ΤΥΠΟΙ ΑΝΑΚΤΗΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ

Στο υποκεφάλαιο αυτό δίνεται μια πιθανή κατηγοριοποίηση των τύπων των δεδομένων που μπορεί να βρεθούν σε ένα σκληρό δίσκο ως προς τον τρόπο ανάκτησης τους. Μια τέτοια κατηγοριοποίηση διευκολύνει την κατανόηση για το πώς μπορεί να ανακτήσει κάποιος τα αντίστοιχα αρχεία από τον δίσκο, ανάλογα με τον τύπο τους.

Παρακάτω φαίνεται μια κατηγοριοποίηση των τύπων των ανακτημένων δεδομένων **[9]**:

- Κανονικά Αρχεία:

  Για αυτού του είδους τα αρχεία κρατείται πληροφορία στο σύστημα αρχείων. Περιλαμβάνονται τα ονόματα αρχείων, οι ιδιότητες τους καθώς και τα περιεχόμενα τους. Δε χρειάζεται να γίνει κάποια ιδιαίτερη ενέργεια για να ανακτηθούν.

- Προσωρινά Αρχεία:

  Σε αυτό το είδος των αρχείων περιλαμβάνονται τα αρχεία εκτυπώσεων του spooler, αρχεία εύρεσης που φυλάσσονται στην cache μνήμη, αρχεία από εφαρμογές βοήθειας και αρχεία από τους κάδους ανακύκλωσης. Δε χρειάζονται ειδικά εργαλεία για την ανάκτηση αυτού του τύπου αρχείων, αλλά χρειάζεται ειδική εκπαίδευση για να γνωρίζει κάποιος που να τα ψάξει.

- Διαγραμμένα Αρχεία:

  Όταν ένα αρχείο διαγράφεται από το σύστημα αρχείων, τα περισσότερα λειτουργικά συστήματα δε διαγράφουν το τμήμα στο σκληρό δίσκο όπου είναι γραμμένο το αρχείο. Απλά διαγράφουν την αναφορά στο αρχείο από τον φάκελο που περιέχεται. Επίσης ενημερώνεται το σύστημα πως οι μονάδες καταχώρησης που χρησιμοποιούσε το αρχείο μπορούν να χρησιμοποιηθούν ξανά. Αυτού του τύπου τα αρχεία

μπορούν να ανακτηθούν με παραδοσιακά «undelete» εργαλεία όπως αυτά που παρέχει το Norton Utilities.

- Διατηρημένα blocks δεδομένων:
  Πρόκειται για δεδομένα που μπορούν να ανακτηθούν από έναν σκληρό δίσκο, αλλά δεν φαίνονται να ανήκουν σε ένα συγκεκριμένο αρχείο. Μπορεί να πρόκειται είτε για δεδομένα που φυλάσσονται για την εικονική μνήμη ή δεδομένα που έχουν τμηματικά επικαλυφθεί από άλλα κ.τ.λ. Τέτοιου είδους δεδομένα μπορούν να προκύψουν από δίσκους στους οποίους έχει δοθεί η εντολή FORMAT των Windows ή newfs του Unix. Αν και αυτές οι εντολές υποδηλώνουν πως καθαρίζουν ολόκληρο τον δίσκο από τα δεδομένα του, στη πραγματικότητα αυτό δεν ισχύει και το μεγαλύτερο ποσοστό του δίσκου παραμένει άθικτο. Έτσι αυτά τα δεδομένα μπορούν να ανακτηθούν από τον σκληρό δίσκο με τη χρήση των κατάλληλων εργαλείων. Αυτά τα εργαλεία είναι προηγμένα εργαλεία ανάκτησης δεδομένων που κάνουν «Unformat» στον δίσκο ή forensics εργαλεία ειδικού σκοπού.

- Κρυφά δεδομένα του πωλητή (vendor) του δίσκου:
  Αυτού του είδους τα δεδομένα αποτελούνται από τμήματα δεδομένων που είναι προσβάσιμα αποκλειστικά με ειδικές εντολές του πωλητή (vendor) του δίσκου. Στη κατηγορία αυτή περιλαμβάνονται τα προγράμματα ελέγχου του σκληρού δίσκου και blocks που έχουν χρησιμοποιηθεί για διαχείριση των bad-blocks.

- Δεδομένα που έχουν επικαλυφθεί από άλλα:
  Αρκετοί θεωρούν ότι τέτοια δεδομένα μπορούν να ανακτηθούν από έναν σκληρό δίσκο με ειδικά εργαλεία.

1.6 ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΤΟΝ ΧΡΟΝΟ ΚΑΘΑΡΙΣΜΟΥ ΕΝΟΣ ΔΙΣΚΟΥ

Στο υποκεφάλαιο αυτό θα παρουσιαστούν κάποιοι παράγοντες που επηρεάζουν τον χρόνο που χρειάζεται ένας σκληρός δίσκος για να διαγραφεί από τα δεδομένα του με ασφαλή τρόπο.

Το χρονικό διάστημα που απαιτείται για την ασφαλή απόσυρση ενός σκληρού δίσκου αποτελεί ένα πολύ σημαντικό ζήτημα, ειδικά αν πρέπει να γίνει αλλαγή του μηχανήματος σε μη εργάσιμες ώρες (συνηθισμένη τακτική των οργανισμών). Συνήθως μέχρι την απόσυρση του υπολογιστή υπάρχει πολύς λίγος χρόνος, μαζί με την αφαίρεση του δίσκου από τον υπολογιστή και τον χρόνο για τον καθαρισμό. Δεν είναι πρακτικό λοιπόν για τους οργανισμούς, σε όρους χρονικού διαστήματος και ανθρώπινου δυναμικού, να καθαρίζουν με ασφαλή τρόπο τους δίσκους τους **[21]**. Σύμφωνα με την έρευνα που διεξήγαγαν οι Valli C. και Patak P. κατέληξαν στο συμπέρασμα πως για να ακολουθήσει κάποιος τις αυστηρές προδιαγραφές των 35 επικαλύψεων των δεδομένων που προτείνει το DoD των Ηνωμένων Πολιτειών για τον καθαρισμό δίσκων με ευαίσθητα δεδομένα, για δίσκους πάνω από 80GB, θα πρέπει ο χρόνος που χρειάζεται να εκτιμάται σε μέρες και όχι απλά σε ώρες **[24]**.

Σύμφωνα με την ίδια έρευνα κάποιοι από τους παράγοντες που επηρεάζουν το χρονικό διάστημα που απαιτείται για τον καθαρισμό ενός δίσκου είναι **[24]**:

- Η μνήμη RAM: Παρατηρείται διαφορά στο χρονικό διάστημα όταν η μνήμη είναι ένα stick από όταν είναι παραπάνω. Δηλαδή, 2 stick των 256MB έχουν χειρότερη απόδοση από 1 stick των 512MB. Συμφέρει λοιπόν όταν το μηχάνημα έχει πάνω από ένα stick, τότε να αφαιρούνται τα υπόλοιπα ώστε να επιταχυνθεί η διαδικασία. Επιπρόσθετα, παρατηρείται ότι η αρχιτεκτονική της μνήμης δεν επηρεάζει ιδιαίτερα τα αποτελέσματα (SDRAM ή DDR).

- Η CPU: Παρατηρείται ότι η ταχύτητα της επεξεργασίας της CPU επηρεάζει την διαδικασία. Για να επιταχυνθεί η διαδικασία θα πρέπει η CPU να είναι επαρκώς γρήγορη (μέχρι τα όρια του σκληρού δίσκου).
- Το λογισμικό που χρησιμοποιείται για τον καθαρισμό: Παρατηρείται πως κάποια προγράμματα πραγματοποιούσαν τον καθαρισμό με λάθος τρόπο σε πολύ μικρότερα χρονικά διαστήματα από το αναμενόμενο.

1.7 ΛΑΘΗ ΧΡΗΣΤΩΝ

Σε αυτό το υποκεφάλαιο προσπαθούμε να αποσαφηνίσουμε ποια είναι τα λάθη των χρηστών όσον αφορά στις πεποιθήσεις τους και τη συμπεριφορά τους για την απόσυρση των δίσκων τους. Λέγοντας χρήστες δεν εννοούμε μόνο τους οικιακούς αλλά και τους δημόσιους και ιδιωτικούς φορείς.

Τόσο οι ιδιωτικοί, όσο και οι δημόσιοι οργανισμοί χρησιμοποιούν υπολογιστές για να αποθηκεύουν τα δεδομένα τους, δηλαδή πληροφορίες για τη δουλεία τους και τις υπηρεσίες τους, τους υπαλλήλους τους και φυσικά τους πελάτες τους. Επίσης και οι οικιακοί χρήστες χρησιμοποιούν τους προσωπικούς τους υπολογιστές για να αποθηκεύσουν προσωπικά δεδομένα για τους ίδιους αλλά και για τις οικογένειές τους. Το πρόβλημα προκύπτει όταν αυτά τα μέσα αποθήκευσης αποσύρονται χωρίς να έχουν ληφθεί προσεχτικά βήματα ή μια ασφαλής διαδικασία ώστε να διατηρηθεί η ιδιωτικότητα των πληροφοριών που περιέχουν. Δυστυχώς, αρκετοί οργανισμοί αλλά και η πλειοψηφία των οικιακών χρηστών φαίνεται να αγνοούν τον κίνδυνο για το τι μπορεί να συμβεί στα δεδομένα τους αφού αποσυρθεί ο παλιός τους εξοπλισμός.

Έτσι υπάρχει περίπτωση οι δίσκοι με προσωπικά δεδομένα να περιέρχονται στα χέρια άλλων ανθρώπων είτε μέσω αγοράς τους από μεταχειρισμένα είδη, είτε μέσω δωρεών. Αυτό μπορεί να συμβεί χωρίς να έχει γνώση ο προηγούμενος χρήστης τους. Αφού, λοιπόν οι δίσκοι δεν προστατεύονται με κάποιο κρυπτογραφημένο σύστημα αρχείων, τότε τα δεδομένα που βρίσκονται στον δίσκο είναι προσβάσιμα σε οποιονδήποτε έχει στα χέρια του τον δίσκο.

Από ότι φαίνεται παραπάνω είναι πολύ πιθανό οι δίσκοι να περιέχουν ευαίσθητα προσωπικά δεδομένα. Έτσι αυτές οι πληροφορίες είναι εύκολο να διαρρεύσουν ή να χρησιμοποιηθούν από οποιονδήποτε μπορεί να δείξει κάποιο ενδιαφέρον για αυτές. Είναι σχεδόν σίγουρο ότι αυτό το ενδιαφέρον δε θα είναι καλόβουλο. Φαίνεται πως προς το παρόν δεν είναι αρκετά μεγάλο το ενδιαφέρον από κακόβουλους χρήστες για να λαμβάνουν με αυτόν τον τρόπο τα ευαίσθητα προσωπικά δεδομένα **[9]**. Ωστόσο το ενδιαφέρον αυτό μπορεί να μεγαλώσει στο μέλλον, γιατί παρόλο που τα δεδομένα προστατεύονται επαρκώς κατά την επεξεργασία τους, φαίνεται ότι δεν ισχύει το ίδιο και κατά την απόσυρση τους.

Έτσι είναι προφανές, ότι προτού αποσυρθούν οι δίσκοι πρέπει να καθαρίζονται με ασφαλή τρόπο από τα δεδομένα τους. Εδώ όμως προκύπτει ένα άλλο πρόβλημα όσον αφορά στις πεποιθήσεις των χρηστών. Αρκετοί άνθρωποι πιστεύουν ότι καταστρέφουν δεδομένα με το να σβήνουν αρχεία στον υπολογιστή. Στις περισσότερες όμως περιπτώσεις οι εντολές erase και delete δεν σβήνουν στη πραγματικότητα το αρχείο από τον δίσκο. Τα αρχεία, λοιπόν μένουν στο δίσκο μέχρι να επικαλυφθούν από άλλα. Το επόμενο βήμα θα ήταν να κάνει ο χρήστης format στον δίσκο του. Ωστόσο, αντίθετα από τη κοινή πεποίθηση ότι κάνοντας format σε ένα δίσκο τότε διαγράφονται όλα του τα δεδομένα, αυτό δεν ισχύει, αφού ένα μεγάλο ποσοστό των δεδομένων παραμένει αυτούσιο.

Παρακάτω ακολουθούν κάποιοι λόγοι που συνοψίζουν την συμπεριφορά των χρηστών:

- <u>Έλλειψη γνώσης του προβλήματος:</u> Ο χρήστης δε γνωρίζει ότι δεν έχουν διαγραφεί τα δεδομένα του και ότι υπάρχει πιθανότητα κάποιος κακόβουλος να ενδιαφερθεί για αυτά **[9]**.

- Έλλειψη ενδιαφέροντος για το πρόβλημα: Ο χρήστης γνωρίζει το πρόβλημα αλλά δε θεωρεί ότι η συσκευή περιέχει ευαίσθητα προσωπικά δεδομένα **[9]**.

- Έλλειψη ενδιαφέροντος για τα δεδομένα: Ο χρήστης γνωρίζει το πρόβλημα και ότι ο δίσκος μπορεί να περιέχει ευαίσθητα προσωπικά δεδομένα, αλλά δε τον ενδιαφέρει ακόμα και αν αυτά αποκαλυφθούν **[9]**.

- Αποτυχία να εκτιμηθεί σωστά ο κίνδυνος: Ο χρήστης γνωρίζει το πρόβλημα, αλλά δε θεωρεί πως ο μελλοντικός χρήστης της συσκευής θα αποκαλύψει τα δεδομένα. Θεωρεί, δηλαδή πως ο επόμενος χρήστης θα χρησιμοποιήσει τον δίσκο του απλά για αποθήκευση δεδομένων και όχι με κακόβουλο τρόπο εναντίον του **[9]**.

- Απόγνωση: Ο χρήστης γνωρίζει το πρόβλημα και πιστεύει ότι δε μπορεί να αποφευχθεί ο κίνδυνος **[9]**.

- Θεώρηση ότι κοστίζει πολύ η διαδικασία: Ο χρήστης θεωρεί ότι η διαδικασία καθαρισμού των δεδομένων από τους δίσκους κοστίζει πολύ σε χρόνο και σε ανθρώπινο δυναμικό **[21]**.

- Έλλειψη εργαλείων: Ο χρήστης γνωρίζει το πρόβλημα αλλά δεν έχει τα κατάλληλα εργαλεία για να καθαρίσει τον δίσκο από τα δεδομένα του με ασφαλή τρόπο **[9]**.

- Έλλειψη πρακτικής εξάσκησης ή ανικανότητα στον χειρισμό του εργαλείου: Ο χρήστης προσπαθεί να διαγράψει τα δεδομένα από τον δίσκο αλλά δε τα καταφέρνει **[9]**.

- Λάθος του εργαλείου: Ο χρήστης χρησιμοποιεί εξειδικευμένο εργαλείο για τον καθαρισμό του δίσκου από τα δεδομένα, αλλά αυτό δε συμπεριφέρεται όπως θα έπρεπε σύμφωνα με τις προδιαγραφές του **[9]**.

- Αποτυχία του hardware: Μπορεί να έχει πρόβλημα ο υπολογιστής στον οποίο βρίσκεται ο δίσκος, και έτσι να είναι αδύνατο να καθαριστεί ο δίσκος από τα δεδομένα εκτός κι αν μεταφερθεί και εγκατασταθεί σε άλλον υπολογιστή. Επίσης, αν συμβαίνει κάτι τέτοιο μπορεί να πιστέψει ο χρήστης ότι έχει χαλάσει ο δίσκος και συνεπώς πως τα δεδομένα του είναι ασφαλή, χωρίς να ισχύει κάτι τέτοιο **[9]**.

1.8 ΕΥΡΗΜΑΤΑ ΕΡΕΥΝΩΝ

Στο υποκεφάλαιο αυτό θα ασχοληθούμε με τους τύπους των δεδομένων που παραμένουν στους δίσκους (δηλαδή τα δεδομένα που φυλάσσουμε στους υπολογιστές μας), όπως έχει προκύψει από τα ευρήματα διάφορων ερευνών.

Οι εταιρείες όπως και τα ακαδημαϊκά ιδρύματα επεξεργάζονται διάφορα δεδομένα που αφορούν στην εσωτερική δομή των οργανισμών τους, εμπιστευτικά δεδομένα που αφορούν τον οργανισμό, πληροφορίες για τα μέλη τους και τους πελάτες τους (όσον αφορά στις εταιρείες). Οι οικιακοί χρήστες φυλάσσουν προσωπικά τους αρχεία για τους ίδιους και τις οικογένειες τους που δίνουν πληροφορίες για την προσωπική τους ζωή.

Έτσι λοιπόν είναι αναμενόμενο, εφόσον δεν έχει καθαριστεί με ασφαλή τρόπος ένας δίσκος, μετά την απόσυρσή του, κάποιος να μπορεί να αποκτήσει πρόσβαση στα δεδομένα που υπάρχουν σε αυτόν, από τη στιγμή που τα ευαίσθητα δεδομένα δεν είναι κρυπτογραφημένα.

Πιο συγκεκριμένα από τις διάφορες έρευνες που έχουν γίνει, τα δεδομένα που μπορεί να μένουν σε ένα δίσκο είναι τα ακόλουθα:

- Πληροφορίες μέσω των οποίων μπορεί να αναγνωριστεί ο οργανισμός.
- Πληροφορίες μέσω των οποίων μπορεί να αναγνωριστεί ο οικιακός χρήστης.
- Πληροφορίες σχετικά με αναγνωρίσιμο οργανισμό που αφορούν το λειτουργικό σύστημα που χρησιμοποιεί, έγγραφα που περιέχουν προσωπικές πληροφορίες καθώς και σημαντικά επαγγελματικά σχέδια, ηλεκτρονική αλληλογραφία και ιστορικό στο διαδίκτυο (ιστοσελίδες που έχουν επισκεφτεί οι χρήστες, φακέλους που έχουν κατεβάσει από το διαδίκτυο, chat logs) **[1] [3]**.
- Ονόματα χρήστη και κωδικούς πρόσβασης στο σύστημα **[1]**.
- Πληροφορίες για ευαίσθητα προσωπικά δεδομένα, όπως βάσεις δεδομένων για πελάτες, πληροφορίες για υπαλλήλους (ονόματα, διευθύνσεις, αριθμοί κοινωνικής ασφάλισης, οικογενειακές πληροφορίες, αριθμοί VAT, αποδείξεις πληρωμής προσωπικού) **[1] [8]**.
- Πληροφορίες για οικονομικές δραστηριότητες, όπως αποδείξεις πωλήσεων και αναφορές κέρδους και απωλειών **[1] [8]**.
- Πληροφορίες που αφορούν στο δίκτυο του οργανισμού, για παράδειγμα την δομή του δικτύου ονόματα servers και proxy, IP addresses **[1] [8]** και λεπτομέρειες για Εικονικά Ιδιωτικά Δίκτυα Εταιρειών (VPN) **[25]**.
- Πληροφορίες σχετικά με τα λογισμικά ασφαλείας που χρησιμοποιούνται στον οργανισμό **[1]**.
- Παράνομο υλικό όπως πορνογραφικό υλικό, αναφορές σε ιστοσελίδες με πορνογραφικό υλικό ή αντίστοιχες φωτογραφίες **[1] [8]**.
- Προσωπικές πληροφορίες του οικιακού χρήστη όπως όνομα και διεύθυνση, διεύθυνση ηλεκτρονικής αλληλογραφίας, πιθανούς κωδικούς πρόσβασης, φωτογραφίες, πληροφορίες για τραπεζικούς λογαριασμούς (αριθμούς λογαριασμών και Τράπεζα) **[4] [5]**.
- Πιστοποιητικά αυθεντικοποίησης τόσο για οικιακούς χρήστες όσο και για οργανισμούς **[5]**.

1.9 ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ

Στο προηγούμενο υποκεφάλαιο είδαμε τι είδους δεδομένα μπορεί να βρει κάποιος σε έναν δίσκο που έχει αποσυρθεί αλλά δεν έχει καθαριστεί με ασφαλή τρόπο. Σε αυτό το υποκεφάλαιο θα δούμε πως μπορεί να χρησιμοποιήσει κάποιος κακόβουλος τις πληροφορίες αυτές, δηλαδή τις κατηγορίες των κινδύνων που μπορεί να προκύψουν.

Οι επιπλοκές από τη δημοσιοποίηση των πληροφοριών που θα ληφθούν από αποσυρμένους δίσκους είναι πολλές, τόσο εάν πρόκειται για ιδιώτη ή για οργανισμό.

Κάποιες από αυτές είναι:

- Εμπορική Κατασκοπία (Industrial Espionage)
  Πληροφορίες από δίσκους που προέρχονται από εταιρικό περιβάλλον και αφορούν επαγγελματικά μυστικά και σχέδια, μπορεί να διαρρεύσουν στον επαγγελματικό τους τομέα. Το πιθανό κόστος για την εταιρεία από μια τέτοιου είδους διαρροή είναι πολύ μεγάλο **[1]**.

- Κλοπή Ταυτότητας (Identity Theft)
  Κλοπή ταυτότητας είναι η πράξη της κλοπής των προσωπικών δεδομένων κάποιου άλλου προσώπου **[19]**. Ανάλογα με το πλήθος των δεδομένων που μπορεί να βρεθούν για ένα συγκεκριμένο άτομο σε ένα δίσκο μπορεί να λάβει χώρα ολική κλοπή ταυτότητας κατά την οποία το άτομο «κλωνοποιείται» **[1]**. Οι πληροφορίες αυτές μπορούν να βρεθούν είτε σε οικιακούς ή σε εταιρικούς δίσκους και μπορούν να βλάψουν το άτομο είτε σε οικονομικό ή σε κοινωνικό επίπεδο. Αυτή η προσωπική πληροφορία μπορεί να χρησιμοποιηθεί με πολλούς σκοπούς, για παράδειγμα είτε για το άνοιγμα λογαριασμών ή για την λήψη δανείου **[4]**.

Σύμφωνα με εκτιμήσεις για τα επίπεδα κλοπής ταυτότητας στις ΗΠΑ αποκαλύπτουν ότι το 2004 ο αριθμός των ατόμων που ήταν θύματα κλοπής ταυτότητος κυμαίνεται σε 10 εκατομμύρια άτομα μόνο στις ΗΠΑ και με κόστος (για επιχειρήσεις και για άτομα) που κυμαίνεται στα 53 δισεκατομμύρια δολάρια. Το κόστος για το άτομο για να «επιδιορθώσει» την ταυτότητά του είναι κάπου στα 808 δολάρια και πρέπει να ασχοληθεί με το θέμα κάπου 175 ώρες **[1]**. Μία αναφορά στο Ηνωμένο Βασίλειο (UK), τοποθετεί το κόστος σε 1.3 δισεκατομμύρια λίρες Αγγλίας και εκτιμά ότι κάθε 4 λεπτά γίνεται μια κλοπή ταυτότητας **[13]**.

- Απάτη (Fraud)

  Τόσο σε οικιακούς όσο και σε εταιρικούς υπολογιστές είναι δυνατόν να βρεθούν αρκετές πληροφορίες ώστε να γίνει απάτη **[1]**.

- Εκβιασμός (Blackmail)

  Υπάρχει περίπτωση να βρεθούν πληροφορίες τόσο σε οικιακούς υπολογιστές όσο και σε εταιρικούς ώστε να μπορεί να λάβει χώρα εκβιασμός **[1] [6]**. Για παράδειγμα αν βρεθεί ότι ένας υπάλληλος είχε παράνομο πορνογραφικό υλικό στον υπολογιστή του, ή αν βρεθούν σε έναν οικιακό υπολογιστή αποδείξεις για παιδεραστία.

- Εισβολή σε δίκτυο (Hacking – Network Intrusion)

  Όπως φάνηκε στο προηγούμενο κεφαλαίο υπάρχει περίπτωση να βρεθούν σε εταιρικό υπολογιστή πληροφορίες που αφορούν στην δομή των δικτύων του οργανισμού, καθώς επίσης και ονόματα server, αριθμοί proxy και IP διευθύνσεις. Αν αυτή η πληροφορία πέσει στα χέρια ενός hacker, αυξάνει τις πιθανότητες του να επιτύχει η επίθεση του στο δίκτυο **[1]**.

Αυτές οι απειλές δε θεωρούνται αμελητέες. Επίσης πρέπει να τονιστεί το γεγονός ότι τα εργαλεία που χρησιμοποιούνται για απόσυρση δεδομένων από

δίσκους είναι ευρέως διαδεδομένα και προσβάσιμα σε οποιονδήποτε ενδιαφέρεται.

1.10 FORENSICS

Στο υποκεφάλαιο αυτό γίνεται μια μικρή αναφορά στην επιστήμη των forensics. Σκοπός του να τονιστεί η σημασία και η χρησιμότητα μιας έρευνας δίσκων για την επιστήμη αυτή.

Η ιατροδικαστική επιστήμη, που συχνά αναφέρεται ως forensics, είναι η εφαρμογή ενός ευρέως φάσματος επιστημών που έχει ως σκοπό να βρει απαντήσεις σε ερωτήματα που αφορούν το νομικό σύστημα. Έτσι μπορεί να σχετίζεται με εγκλήματα ή με μια αστική αγωγή **[15]**.

Τα forensics στον ψηφιακό τομέα είναι η εφαρμογή από επιστημονικές μεθόδους και τεχνικές, που έχουν ως σκοπό την ανάκτηση δεδομένων από ηλεκτρονικά ή ψηφιακά μέσα **[15]**. Ωστόσο ο τομέας αυτό είναι σχετικά καινούργιος και προς το παρόν υπάρχει έλλειψη ενός επίσημου και δομημένου εργασιακού περιβάλλοντος **[19]**.

Στην ιατροδικαστική επιστήμη οι σκληροί δίσκοι και οποιοδήποτε άλλο ψηφιακό μέσο αποθήκευσης χωρίζονται σε είδη. Μια κατηγοριοποίηση ενός σκληρού δίσκου στην επιστήμη αυτή βασίζεται στην χωρητικότητα του, στο λειτουργικό του σύστημα και στον συνδυασμό των δεδομένων που περιέχει **[6]**.

Η ανάκτηση δεδομένων από δίσκους δεν είναι απαραίτητο να συμβαίνει για εγκληματικούς σκοπούς αλλά και από ερευνητές που χρησιμοποιούν εργαλεία ανάκτησης δεδομένων από δίσκους για να βρουν πληροφορίες για εγκλήματα, δηλαδή από το νομικό σύστημα ενός κράτους. Οι πληροφορίες αυτές δεν είναι απαραίτητο να αφορούν σε ηλεκτρονικά εγκλήματα, αλλά μπορεί να σχετίζονται σε οποιοδήποτε είδος εγκλήματος, για το οποίο μπορεί να

χρησιμοποιηθεί ηλεκτρονικός υπολογιστής, όπως τρομοκρατικές ενέργειες, διακίνηση ναρκωτικών, εκβιασμός κ.α.. Οι αποδείξεις που ανακτώνται από το σύστημα μπορούν να είναι χρήσιμες και για τη δημιουργία ενός profile του χρήστη, ώστε να φαίνονται οι δραστηριότητες του. Από το σημείο αυτό διευκολύνεται η δημιουργία και την αναγνώριση της μεθόδου που χρησιμοποιήθηκε για το έγκλημα **[3]**. Από την άποψη του ερευνητή μπορεί να βρεθεί και πιθανή εγκληματική ενέργεια από την κατοχή ευαίσθητων προσωπικών δεδομένων που θα μπορούσαν να χρησιμοποιηθούν για τέτοιους σκοπούς **[6]**. Η πληροφορία που μπορεί να περιέχεται στον υπολογιστή ενός υπόπτου μπορεί να είναι εκτενής. Υπάρχει περίπτωση να βρεθούν προσωπικές πληροφορίες για τα θύματα, ηλεκτρονικά μηνύματα, η δραστηριότητα του δράστη στο διαδίκτυο κ.α. Επίσης αρκετά βοηθητικά για την καταδίκη ενός ενόχου είναι τα timestamps, καθώς φαίνεται η ακριβής ώρα που έγινε η εγκληματική πράξη. Άλλα αποδεικτικά στοιχεία μπορεί να είναι οι αποκλίσεις στα έξοδα ή αν φαίνονται μεγάλες αναλήψεις ποσών **[19]**.

Ο ερευνητής στον τομέα αυτόν δίνει μια άποψη και αναφορά, βασιζόμενος στον έλεγχο του υλικού που έχει ανακτηθεί. Με βάση αυτό το υλικό, μπορεί να αποφασίσει για το τι συνέβη και με τις πληροφορίες αυτές να μπορέσει το δικαστήριο να αποφασίσει αν θα καταδικάσει ή θα αθωώσει έναν ύποπτο **[3]**. Οι ερευνητές κυρίως ασχολούνται με δεδομένα που ανακτούν από συσκευές αποθήκευσης δεδομένων, που περιλαμβάνουν όχι μόνο σκληρούς δίσκους αλλά και φορητές συσκευές αποθήκευσης (USB μνήμες, εξωτερικούς σκληρούς δίσκους κ.α.) **[15]**. Για έναν ερευνητή, η ανάκτηση των διαγραμμένων αρχείων από τον δίσκο είναι ένα από τα πιο σημαντικά τμήματα της φάσης συλλογής αποδεικτικών στοιχείων. Πρέπει να χρησιμοποιεί τα σωστά εργαλεία με τον σωστό τρόπο, διαφορετικά υπάρχει περίπτωση να μην είναι ακριβή τα στοιχεία που θα προκύψουν **[32]**.

Ένας ειδικός στα forensics υπολογιστών:

- Αναγνωρίζει τις πηγές των ψηφιακών αποδείξεων.
- Ανακτά τις αποδείξεις.

- Αναλύει τις αποδείξεις.
- Παρουσιάζει τα ευρήματα του.

Σύμφωνα με έρευνες που έχουν γίνει, το σύστημα κρατάει αρκετή πληροφορία για έναν ερευνητή, έτσι ώστε να καταγράψει μια αναφορά της δραστηριότητας του χρήστη. Αυτό ισχύει ακόμα και για την περίπτωση που ο χρήστης του υπολογιστή έχει καλή γνώση των προσωπικών υπολογιστών και είναι ικανός. Έτσι είναι σημαντικό να θεωρήσουμε ότι ακόμα και καθαρίζοντας πολύ καλά έναν σκληρό δίσκο, είναι πέραν των δυνατοτήτων των απλών χρηστών το να μη μείνει κάποια ένδειξη πληροφορίας που να αφορά στις δραστηριότητες τους **[3]**.

1.11 ΤΕΧΝΙΚΕΣ ΔΙΑΓΡΑΦΗΣ ΔΕΔΟΜΕΝΩΝ

Στο υποκεφάλαιο αυτό περιγράφονται οι τρόποι διαγραφής δεδομένων από τους δίσκους. Δεν είναι όλοι τους τόσο αποτελεσματικοί και επίσης δεν ενδείκνυνται όλοι τους για τον οικιακό χρήστη λόγω κόστους. Έτσι μαζί με την παρουσίαση των τεχνικών θα παρουσιαστούν και κάποια από τα πλεονεκτήματα και τα μειονεκτήματα τους.

Αναφέρεται ότι στη παρουσίαση αυτή δεν συμπεριλαμβάνονται τα ειδικά λογισμικά απόσυρσης δεδομένων από δίσκους καθώς αυτά αναφέρονται σε ξεχωριστό υποκεφάλαιο.

Ο καθαρισμός ενός δίσκου από τα δεδομένα του με ασφαλή τρόπο θεωρείται μια περίπλοκη διαδικασία. Ο πιο σίγουρος τρόπος για να είμαστε βέβαιοι ότι τα δεδομένα του δίσκου δε μπορούν να ανακτηθούν, είναι η φυσική του καταστροφή.

Οι πιο συνηθισμένες τεχνικές διαγραφής δεδομένων από δίσκους είναι **[9]**:

- Η φυσική καταστροφή του δίσκου, καθιστώντας τον δίσκο άχρηστο για μελλοντική χρήση.

- Απομαγνητισμός του δίσκου με σκοπό να γεμίσει με τυχαίο τρόπο τις μαγνητικές περιοχές, έχοντας μεγάλη πιθανότητα να καταστήσει τον δίσκο άχρηστο για μελλοντική χρήση.
- Γράφοντας νέα τυχαία δεδομένα πάνω από τα δεδομένα του δίσκου έτσι ώστε να επικαλυφθούν τα παλιά και να μη μπορούν να ανακτηθούν.

Παρακάτω ακολουθεί μια λεπτομερής καταγραφή των τρόπων που μπορούν να διαγραφούν τα δεδομένα από τον δίσκο με τα πλεονεκτήματα τους και τα ελαττώματα τους. Περιέχονται και τρόποι που θεωρούν οι χρήστες λανθασμένα ως ασφαλείς.

- Καθαρισμός δεδομένων μέσω εντολών διαγραφής

  Αν και πολλοί άνθρωποι πιστεύουν ότι καταστρέφουν δεδομένα χρησιμοποιώντας τις εντολές **delete** ή **erase** κάτι τέτοιο δεν ισχύει **[9]**.

- Καθαρισμός δεδομένων γράφοντας δεδομένα πάνω από (επικαλύπτοντας) τα υπάρχοντα

  Επειδή η φυσική καταστροφή των δίσκων είναι σχετικά περίπλοκη διαδικασία και επειδή οι εντολές διαγραφής που προσφέρονται από τα λειτουργικά συστήματα δε καθαρίζουν τα δεδομένα από το δίσκο, αρκετοί προτιμούν να αντικαθιστούν εσκεμμένα τα δεδομένα στο δίσκο, γράφοντας άλλα δεδομένα από πάνω (overwriting), έτσι ώστε τα παλιά δεδομένα να μην είναι ανακτήσιμα. Μπορεί τα δεδομένα που θα γραφούν από πάνω να είναι μηδενικά (ASCII NULL bytes) ή τυχαίοι χαρακτήρες. Αν και αυτός ο τρόπος είναι αρκετά απλός στη κατανόηση, μπορεί να αποδειχθεί περίπλοκος από πρακτική άποψη. Επίσης δεν είναι και τόσο αποτελεσματικός **[9]**. Κάποιοι ερευνητές θεωρούν ότι το απλό overwrite δεν επαρκεί για να προστατεύσει τα δεδομένα από έναν αποφασισμένο hacker. Είναι θεωρητικά εφικτό να ανακτήσεις τα δεδομένα γιατί το μαγνητικό πεδίο του δίσκου αποτελείται από έναν συνδυασμό τόσο των παλιών όσο και των νέων δεδομένων (shadow

data). Για παράδειγμα όταν ο υπολογιστής προσπαθεί να γράψει ένα ή μηδέν στον δίσκο, το μέσο το καταγράφει έτσι, αλλά το πραγματικό αποτέλεσμα είναι πιο κοντά στο 1.05 όταν αντικαθιστά το ένα με ένα και 0.95 όταν αντικαθιστά το ένα με μηδέν. Έτσι είναι δυνατή η ανάκτηση ενός ή και δύο στρωμάτων δεδομένων, χωρίς μεγάλη δυσκολία, εφόσον υπάρχει ο κατάλληλος εξοπλισμός. Ο Gutmann προτείνει μια μέθοδο που περιλαμβάνει την επικάλυψη των δεδομένων 35 φορές, για να είναι πιο ασφαλής η διαγραφή τους ακόμα και από αρκετά εξελιγμένες τεχνικές ανάκτησης **[14]**. Παρά τις παραπάνω απόψεις, γενικά θεωρείται επαρκές μέτρο να γίνεται αντικατάσταση των δεδομένων του χρήστη με ένα ή δύο περάσματα τυχαίων αριθμών **[9]**. Στους πιο μοντέρνους δίσκους, οι οποίοι είναι συμβατοί με τα πρότυπα ATA και SATA, δίνεται η δυνατότητα της χρήσης της διαδικασίας Secure Erase. Πρόκειται για μια ειδική, χαμηλού επιπέδου λειτουργία πληροφοριών διαμόρφωσης, που επικαλύπτει τρείς φορές τα δεδομένα. Σε συμβατικά λειτουργικά συστήματα μπορεί να μη σβηστούν τα δεδομένα και επίσης θα εμποδιστεί ο χρήστης από το να ενεργοποιήσει τυχαία τις εντολές **[12]**. Σύμφωνα με τις επίσημες οδηγίες από το Υπουργείο Άμυνας των ΗΠΑ για να είναι αποτελεσματικός ο καθαρισμός των δεδομένων από τους δίσκους πρέπει να γίνεται επικάλυψη των δεδομένων τρεις φορές, αρχικά με έναν χαρακτήρα μετά με τον συμπληρωματικό του και έπειτα με έναν τυχαίο χαρακτήρα. Αυτό ισχύει για τα μη εμπιστευτικά δεδομένα. Για τα εμπιστευτικά δεδομένα προτείνεται η μέθοδος του Gutmann **[22]**.

- <u>Διαγραφείς δίσκων (Bulk erasers ή degaussers)</u>

  Οι διαγραφείς δίσκων σπάνια είναι αποτελεσματικοί. Για να είναι αποτελεσματικός ο διαγραφέας (να καθιστά αντιοικονομική την ανάκτηση των δεδομένων από τον δίσκο) πρέπει να παράγει μαγνητικό πεδίο τουλάχιστον 5 φορές πιο ισχυρό από αυτό του δίσκου **[14]**. Έτσι οι διαγραφείς που είναι διαθέσιμοι στην αγορά δεν παράγουν αρκετά ισχυρό μαγνητικό πεδίο για να επηρεάσουν την επιφάνεια του δίσκου.

Όσοι παράγουν ισχυρό πεδίο σχεδόν πάντα καθιστούν τον δίσκο άχρηστο. Εκτός αυτού, οι διαγραφείς δίσκων δε σβήνουν μόνο τα δεδομένα του χρήστη αλλά και χαμηλού επιπέδου ίχνη του δίσκου και πληροφορίες που σχετίζονται με τη διαμόρφωση του. Αν και είναι δυνατόν να επαναφερθούν οι κώδικες αυτοί χρησιμοποιώντας συγκεκριμένες εντολές, οι εντολές αυτές δεν είναι διαθέσιμες στον μέσο χρήστη αλλά μόνο στον πωλητή (vendor) του δίσκου **[9] [12]**. Επίσης χρησιμοποιείται εξειδικευμένος εξοπλισμός, ο οποίος είναι ακριβός και είναι δύσκολο να αποκτηθεί **[14]**.

- Ephemerizer

  Ο ephemerizer είναι ένας server που διαχειρίζεται τα κλειδιά των κρυπτογραφημένων δεδομένων. Ο ephemerizer δημιουργεί τα κλειδιά, τα διαθέτει για την κρυπτογράφηση, βοηθάει στην αποκρυπτογράφηση και καταστρέφει τα κλειδιά με το πέρας μιας χρονικής περιόδου. Με αυτόν τον τρόπο τα δεδομένα δεν είναι ανακτήσιμα μετά το πέρας της χρονικής περιόδου που κρατάει ο ephemerizer τα κλειδιά και το κόστος της διαχείρισης από τον ephemerizer μοιράζεται στους χρήστες. Τέλος διευκολύνει τον χρήστη γιατί δε χρειάζεται να διαχειρίζεται τα κλειδιά μόνος του **[10]**.

- Mechanical Shredding

  Τεμαχίζει τον δίσκο σε κύβους του ενός εκατοστού. Εκτός του ότι τα κομμάτια αυτά είναι τοξικά για το περιβάλλον, δεν είναι δυνατόν να επαναχρησιμοποιηθεί ο δίσκος. Επίσης, ακόμα και μια τόσο δραστική μέθοδος αφήνει ανακτήσιμα δεδομένα για τα σημερινά μέσα ανάκτησης **[12]**.

- The Digital Shredder

  Ο ψηφιακός καταστροφέας EDT (digital shredder) ενεργοποιεί στον δίσκο ένα ειδικό λειτουργικό περιβάλλον ώστε να μπορέσει να εκτελεστεί η λειτουργία Secure Erase (αναφέρεται πιο πάνω). Ο

τεχνικός πρέπει να αφαιρέσει τον δίσκο και να τον κλειδώσει στη μηχανή του ψηφιακού καταστροφέα, που είναι μια συσκευή στο μέγεθος μιας τοστιέρας και χρησιμοποιεί μια touch-screen διεπαφή. Η διαδικασία διαρκεί λίγο (κάπου μισή ώρα) και μετά από αυτήν τα δεδομένα δεν είναι ανακτήσιμα. Επίσης ο δίσκος παραμένει λειτουργικός. Ωστόσο το κόστος της διαδικασίας την καθιστά πολύ ακριβή για έναν οικιακό χρήστη **[12]**.

- Λιώσιμο δίσκου (Drive melting)

  Πρόκειται για έναν ιδιαίτερο τρόπο καταστροφής δίσκων. Ο δίσκος έχει τον δικό του μηχανισμό καταστροφής που παρέχει 17 διαφορετικά ερεθίσματα για να ανιχνεύουν την κλοπή ή το πείραγμα του δίσκου. Αυτά ενεργοποιούν ένα μικρό τμήμα του δίσκου που απελευθερώνει μια ισχυρή, μη τοξική χημική ουσία. Η ουσία αυτή καταστρέφει τον δίσκο μέσα σε 15 λεπτά, καθιστώντας τα δεδομένα μη ανακτήσιμα. Φυσικά ένας τέτοιος τρόπος ενδείκνυται για πολύ λίγες περιπτώσεις **[12]**.

1.12 ΕΡΓΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ

Το υποκεφάλαιο αυτό δεν έχει σαν σκοπό το να κάνει σύγκριση των διάφορων εργαλείων που υπάρχουν στην αγορά, αλλά περισσότερο για να δείξει ότι υπάρχουν τέτοια εργαλεία, τι μπορούν περίπου να κάνουν και να τονίσει το γεγονός ότι είναι διαθέσιμα σε οποιονδήποτε μπορεί να θελήσει να τα αποκτήσει.

1.12.1 Εργαλεία Απόσυρσης

Μπορεί να βελτιώνονται συνεχώς οι τρόποι ανάκτησης δεδομένων από δίσκους, αλλά συγχρόνως οι πιο έμπειροι χρήστες αρχίζουν και συνειδητοποιούν το πρόβλημα και να λαμβάνουν μέτρα για να αποφύγουν την ανίχνευση των δεδομένων τους. Αυτό δεν ισχύει απαραίτητα για χρήστες που

θέλουν να καλύψουν μια εγκληματική ενέργεια, αλλά γενικά για χρήστες που θέλουν να προστατεύσουν τα προσωπικά τους δεδομένα, καθώς και οργανισμούς που θέλουν να καλύψουν τα ευαίσθητα δεδομένα που έχουν μετά το πέρας της επεξεργασίας τους **[3]**.

Οι καθαριστές δίσκων (disk cleaners) είναι εργαλεία λογισμικού τα οποία διαγράφουν ή επικαλύπτουν τα δεδομένα, από τομέα σε τομέα, έτσι ώστε να τα καθιστούν μη ανακτήσιμα μέσω συμβατικών τεχνικών ανάκτησης δεδομένων. Η πλειοψηφία των εργαλείων αυτών παρέχουν την δυνατότητα επιλογής στον χρήστη να επαναλάβουν την διαδικασία έναν προκαθορισμό αριθμό φορών, ώστε να είναι σίγουρος ότι δε θα μείνει ούτε ίχνος δεδομένων στον δίσκο **[3]**. Τα εργαλεία αυτά είναι σχετικά εύκολα στη χρήση και ποικίλουν πολύ στο πεδίο δράσης τους, με μερικά να σβήνουν τα δεδομένα κατά αρχεία με επικάλυψη και άλλα να σβήνουν ολόκληρο τον δίσκο, από τα απλά αρχεία ως και το λειτουργικό σύστημα **[18]**.

Για να κατανοηθεί καλύτερα η λειτουργία των εργαλείων απόσυρσης πρέπει να φανεί πως δουλεύουν. Η διαδικασία που χρησιμοποιούν μοιάζει περισσότερο με επικάλυψη δεδομένων (overwriting) πάρα με καθαρισμό ενός δίσκου από τα δεδομένα του. Έτσι όταν ο χρήστης επιλέγει να «σβήσει» τα δεδομένα του, αυτά στη πραγματικότητα επικαλύπτεται κάθε bit τους με ένα μηδέν. Μετά από αυτό, τα δεδομένα παραμένουν στον δίσκο αλλά έχουν επικαλυφθεί με άλλα και με αυτόν τον τρόπο δεν είναι προσβάσιμα **[18]**.

Υπάρχουν αρκετά εργαλεία λογισμικού στην αγορά, τα οποία υποστηρίζουν πως καθαρίζουν τα δεδομένα από τον δίσκο με ασφαλή τρόπο. Υπάρχουν προϊόντα που παρέχονται δωρεάν αλλά και εργαλεία που κοστίζουν έως και 1695 $, καθώς και περισσότερα από 50 προϊόντα για ένα σύστημα υπολογιστών **[9]**. Αποδείχτηκε πως η δωρεάν έκδοση των εργαλείων αν και τείνει να δίνει την εντύπωση στον χρήστη ότι τα δεδομένα έχουν διαγραφεί, χωρίς κάτι τέτοιο να ισχύει στην πραγματικότητα. Αντίθετα τα εργαλεία που ακολουθούν τα επίσημες οδηγίες από το Υπουργείο Άμυνας των US τείνουν να

είναι τα πιο αποτελεσματικά **[3]**. Σκοπός των οδηγιών αυτών είναι να καθιστούν την ανάκτηση των δεδομένων από τους δίσκους με παραδοσιακές τεχνικές αδύνατη ή πολύ ακριβή **[20]**. Οι οδηγίες αυτές προτείνουν να γίνεται επικάλυψη των δεδομένων τρεις φορές, αρχικά με έναν χαρακτήρα, μετά με τον συμπληρωματικό του και έπειτα με έναν τυχαίο χαρακτήρα **[22]**. Τα εργαλεία αυτά χωρίζονται σε δύο κατηγορίες, σε αυτά που σβήνουν τα δεδομένα (wipers) και σε αυτά που τα «τρίβουν» (scrubbers). Οι wipers σβήνουν ακόμα και τα δεδομένα που υπάρχουν μεταξύ των αρχείων, όπως τα προσωρινά αρχεία, τα πρόχειρα αρχεία από τα κείμενα και προσωρινά αρχεία από το διαδίκτυο. Οι scrubbers διαγράφουν ολόκληρο τον σκληρό δίσκο ακόμα και το λειτουργικό σύστημα. Αν και είναι σχεδιασμένα κυρίως για εταιρείες, είναι δυνατό να τα χρησιμοποιούν και οικιακοί χρήστες **[18]**. Πρέπει να τονιστεί ότι αυτού του είδους ο καθαρισμός προτείνεται για όλες τις συσκευές εκτός από αυτές που περιέχουν πολύ σημαντικά μυστικά, οι οποίες καταστρέφονται με φυσικό τρόπο **[20]**. Τέλος, οι εταιρείες που παράγουν λειτουργικά συστήματα, όπως η Apple, ανακοινώνουν ότι στο μέλλον θα παρέχουν διαδικασίες για την ασφαλή διαγραφή του μέσου **[4]**.

Ακολουθούν κάποια ονόματα εργαλείων απόσυρσης **[18]**:

1. BCWIPE, της Jetico: www.jetico.com
2. CYBERCIDE AND CYBERSCRUB, της CyberScrub: www.cyberscrub.com.
3. DATAERASER, της Ontrack: www.ontrack.com/dataeraser.
4. DECLASFY, της Mares & Company: www.dmares.com.
5. ERASER, του Sami Tolvanen: www.tolvanen.com/eraser.
6. EVIDENCE ELIMINATOR, του Robin Hood Software: www.evidence-eliminator.com.
7. SECURECLEAN AND CLEANDRIVE, της White Canyon Software: www.accessdata.com.
8. WASHANDGO, της Abelsoft: www.abelssoft.com.
9. WIPECLEAN, της Symantec: www.symantec.com.
10. ZDELETE, της Lsoft: www.lsoft.net.

1.12.2 Εργαλεία Ανάκτησης

Τα εργαλεία ανάκτησης χρησιμοποιούνται για να ανακτήσουμε δεδομένα που έχουν διαγραφεί από δίσκους. Τα εργαλεία αυτά είναι πολύ λιγότερα σε αριθμό από τα εργαλεία απόσυρσης, γιατί είναι πολύ πιο δύσκολη η δημιουργία τους **[9]**. Έχουν παρόμοια λειτουργία με τις εντολές Unformat και Undelete των Windows **[8]** ή με δεκαεξαδικούς συντάκτες (hex editors) **[20]**.

Σχεδόν όλα τα εργαλεία ανάκτησης επιτρέπουν στον χρήστη να αναλύει σκληρούς δίσκους ή «images» από σκληρούς δίσκους (τεχνικές που χρησιμοποιούνται για να αντιγράφουν τα δεδομένα ενός δίσκου ώστε να διασφαλιστεί ότι δε θα αλλαχθούν τα αρχικά του δεδομένα **[1]**) σε διάφορα λειτουργικά συστήματα και παρέχουν στον χρήστη τους μια διεπαφή που μοιάζει με του Explorer. Φυσικά η χρήση αυτών των εργαλείων περιορίζεται από το αρχικό λειτουργικό σύστημα του δίσκου. Αυτό συμβαίνει γιατί σε κάθε διαφορετικό λειτουργικό σύστημα επικαλύπτεται διαφορετικό ποσοστό δεδομένων όταν διαγράφεται ένας φάκελος ή όταν γίνεται format. Τα εργαλεία επιτρέπουν την ανάκτηση φακέλων που είχαν «διαγραφεί», καθώς και πιο εξεζητημένες τεχνικές ανίχνευσης, όπου ψάχνουν να βρουν συγκεκριμένες λέξεις κλειδιά **[9]**.

Τέτοια εργαλεία είναι τα:

- Foremost: ψάχνει για δεκαεξαδικές κεφαλίδες και ουρές αρχείων και μετά σύμφωνα με αυτές τα ανακτά **[22]**.
- Autopsy: είναι ένα εργαλείο που παρέχεται δωρεάν στο διαδίκτυο και είχε γραφεί αρχικά για την πλατφόρμα των Linux **[22]**.
- SMART της ASRData: είναι ένα εμπορικό εργαλείο, το οποίο βασίζεται σε πλατφόρμα των Linux **[32]**.

Είναι πολύ σημαντικό να τονιστεί ότι τα εργαλεία ανάκτησης είναι διαθέσιμα σε οποιονδήποτε μπορεί να αποκτήσει τους δίσκους **[8]**.

1.13 ΓΝΩΣΤΕΣ ΜΕΘΟΔΟΛΟΓΙΕΣ ΕΡΕΥΝΑΣ

Στο υποκεφάλαιο αυτό θα επικεντρωθούμε στις μεθοδολογίες που προτείνονται για την διεκπεραίωση μιας έρευνας για την ανάκτηση δεδομένων από δίσκους. Θα προταθεί μια βασική μεθοδολογία με κάποια εναλλακτικά βήματα. Πρέπει να τονιστεί ότι το βασικότερο χαρακτηριστικό που απασχολεί όλες τις εναλλακτικές μεθόδους είναι ο χρόνος που χρειάζεται για την έρευνα (από την στιγμή που οι εταιρείες έχουν συγκεκριμένους πόρους και ανθρώπινο δυναμικό να διαθέσουν για την εργασία) **[11]**. Σκοπός μιας έρευνας για την ανάκτηση δεδομένων από δίσκους είναι να καθοριστεί τι είδους δεδομένα παραμένουν στους δίσκους (εφόσον βρεθούν) και πόσο εύκολο είναι να ανακτηθούν αυτά χρησιμοποιώντας κοινές τεχνικές και εργαλεία **[1]**.

Η μεθοδολογία που θα προταθεί για μια έρευνα στον τομέα των ψηφιακών forensics είναι προτιμότερο να προκύπτει από την εμπειρία από το να ακολουθείται μια διαδικασία από κάποιο βιβλίο. Μία εμπειρική μέθοδος είναι πολύ πιο αποτελεσματική για τον χειρισμό του μεγάλου όγκου των πληροφοριών, έτσι οδηγεί σε πιο αποτελεσματική ανάλυση, καθώς επίσης βοηθάει να μειωθεί το χρονικό διάστημα που χρειάζεται για την έρευνα. Οι ερευνητές πιστεύουν ότι δε πρέπει να κατηγοριοποιούν τους δίσκους σύμφωνα με κριτήρια που θέτουν οι ίδιοι, αλλά ανάλογα με τους δίσκους **[4]**.

Το αρχικό βήμα είναι να προμηθευτούν οι ερευνητές τους δίσκους. Μία από τις πιο συνηθισμένες πρακτικές για την προμήθεια αποθηκευτικών μέσων που μπορεί να περιέχουν αναγνωρίσιμες προσωπικές πληροφορίες είναι η αγορά μεταχειρισμένου εξοπλισμού. Συμφέρει ιδιαίτερα αν η αγορά είναι μέσω διαδικτύου (για παράδειγμα μια ιστοσελίδα ηλεκτρονικών πλειστηριασμών), επειδή προσφέρει ανωνυμία. Ένας άλλος τρόπος είναι μέσω συμβατικής αναζήτησης σε ανακυκλωμένο hardware. Ο εξοπλισμός που θεωρείται παλιός ή ελαττωματικός και που δεν έχουν σκοπό οι κάτοχοί του να ξαναχρησιμοποιήσουν, συχνά καταλήγει σε κάδους ανακύκλωσης **[4]**.

Ένα καλό δείγμα δίσκων θεωρούνται κάπου 150 δίσκοι (ή και περισσότεροι), έτσι ώστε τα αποτελέσματα να είναι ενδεικτικά του πληθυσμού. Μια καλή πρακτική είναι οι δίσκοι να προέρχονται από συγκεκριμένες γεωγραφικές περιοχές (π.χ. ΗΠΑ, Ηνωμένο Βασίλειο κ.α.). Ένα πρόσθετο βήμα που μπορεί να γίνει σε αυτό το σημείο είναι η αγορά νέων δίσκων ή δίσκων που να έχουν εξ ολοκλήρου καθαριστεί από τον προμηθευτή, σε ποσοστό κάπου το 10% του συνολικού αριθμού των δίσκων. Κατά την ανάλυση των δίσκων, οι ερευνητές δε γνωρίζουν ποιοι είναι αυτοί οι δίσκοι. Συνεπώς στα αποτελέσματα της ανάλυσης πρέπει να προκύψει ότι τουλάχιστον το 10% των δίσκων είναι καθαρισμένοι.

Η έρευνα χωρίζεται σε δύο βασικά στάδια. Στο πρώτο στάδιο ο ερευνητής ψάχνει για το αν υπάρχουν δεδομένα στους δίσκους, αν αυτά είναι εύκολα προσβάσιμα ή αν χρειάζεται να ανακτηθούν με τα κατάλληλα εργαλεία. Στο δεύτερο στάδιο ψάχνει συγκεκριμένα για πληροφορίες που θα οδηγήσουν στην αναγνώριση οργανισμών ή οικιακών χρηστών, συνήθειες του χρήστη ή αρχεία του, παράνομο υλικό κ.α. **[8]**.

Ακολουθούν τα βήματα πιο αναλυτικά που πρέπει να μπορεί να κάνει ένας ερευνητής. αφού προμηθευτεί τους δίσκους:

1. Τοποθετείται ένας σειριακός αριθμός – αναγνωριστικό σε όλους τους δίσκους **[1]**.

2. Αντιγράφονται τα περιεχόμενα των δίσκων (forensic imaging) και μετά φυλάσσονται οι δίσκοι σε ασφαλές μέρος **[1] [4] [8]**. Δημιουργείται δηλαδή ένα ακριβές αντίτυπο ολόκληρου του σκληρού δίσκου. Υπάρχουν αρκετά κατάλληλα εργαλεία λογισμικού για αυτή την διαδικασία. Στην ανάλυση χρησιμοποιείται το αντίγραφο του σκληρού δίσκου. Με αυτόν τον τρόπο διασφαλίζεται ότι δε θα μεταβληθούν τα περιεχόμενα του

αυθεντικού δίσκου **[4]**. Εργαλεία που μπορούν να χρησιμοποιηθούν είναι το EnCase της Guidance Software και το Knoppix Software για Linux **[1]**.

2.1. Οι σκληροί δίσκοι που δε μπορούν να αντιγραφούν είναι ελαττωματικοί λόγω φυσικής ζημιάς και χρειάζονται ειδικό εξοπλισμό για να ανακτηθούν τα δεδομένα τους. Έτσι τους αποκλείουμε **[6] [11]**. Αυτή η διαδικασία γίνεται χειρονακτικά και εξαρτάται από τους πόρους και τις μηχανές αντιγραφής που είναι διαθέσιμες. Είναι δύσκολο να εκτιμηθεί ο χρόνος που θα χρειαστεί για αυτήν την διαδικασία **[11]**.

2.2. Σε αυτό το βήμα πρέπει να βρεθούν οι δίσκοι που δεν έχουν δεδομένα και να αποκλειστούν **[6] [11]**. Αυτό μπορεί να γίνει με μια αυτόματη διαδικασία που θα ελέγχει αν περιέχουν δεδομένα οι δίσκοι ή αν έχουν κάποια δεδομένα τα οποία δεν έχουν ερευνητικό ενδιαφέρον **[11]**.

3. Το βήμα αυτό είναι πιο περίπλοκο από τα προηγούμενα. Περιλαμβάνει τη δημιουργία και την εκτέλεση τεσσάρων διαφορετικών εφαρμογών, οι οποίες θα εφαρμοστούν στα αντίτυπα των σκληρών δίσκων **[6] [11]**.

3.1. Η πρώτη εφαρμογή προσπαθεί να εντοπίσει ανάμεσα στα δεδομένα που δεν έχουν διαγραφεί και να ανακτήσει τα διαγραμμένα δεδομένα που αντιστοιχούν σε εικόνες ή φωτογραφίες κ.τ.λ. Εξετάζοντας τα headers και τα footers των διαφορετικών τύπων εικόνων, η εφαρμογή μπορεί να εξάγει ολόκληρη ή ένα τμήμα της εικόνας. Μια τέτοιου είδους εφαρμογή έχει επινοηθεί και αναπτυχτεί από το «Information Research Group» του Πανεπιστημίου του Glamorgan.

3.2. Η δεύτερη εφαρμογή εξάγει όλα τα thumb.db αρχεία, είτε εντοπίζοντας τα, είτε ανακτώντας τα εάν έχουν διαγραφεί. Τότε μία άλλη εφαρμογή διαβάζει τα thumb.db αρχεία και εξάγει τις εικόνες που έχουν αποθηκευτεί σε αυτά. Τα thumb.db αρχεία αποθηκεύουν μία εφεδρική έκδοση προεπισκόπησης των εικόνων του χρήστη ακόμα και αν έχουν διαγραφεί. Επίσης, είναι δυνατόν να βρεθεί μια

μικρή προεπισκόπηση μιας εικόνας όταν αυτή έχει αποθηκευτεί σε έναν φάκελο με άλλες, και είναι πιο εύκολο να ανακτηθεί αυτή από το να γίνει ανάκτηση της κανονικής εικόνας, η οποία κιόλας είναι πιθανόν να έχει γίνει overwrite αρκετές φορές. Ερευνητές από το «Information Research Group» του Πανεπιστημίου του Glamorgan έχουν επινοήσει και αναπτύξει ένα τέτοιο πρόγραμμα και επίσης κυκλοφόρησε πρόσφατα ένα εργαλείο που κάνει αυτή τη δουλεία, το Vinetto.

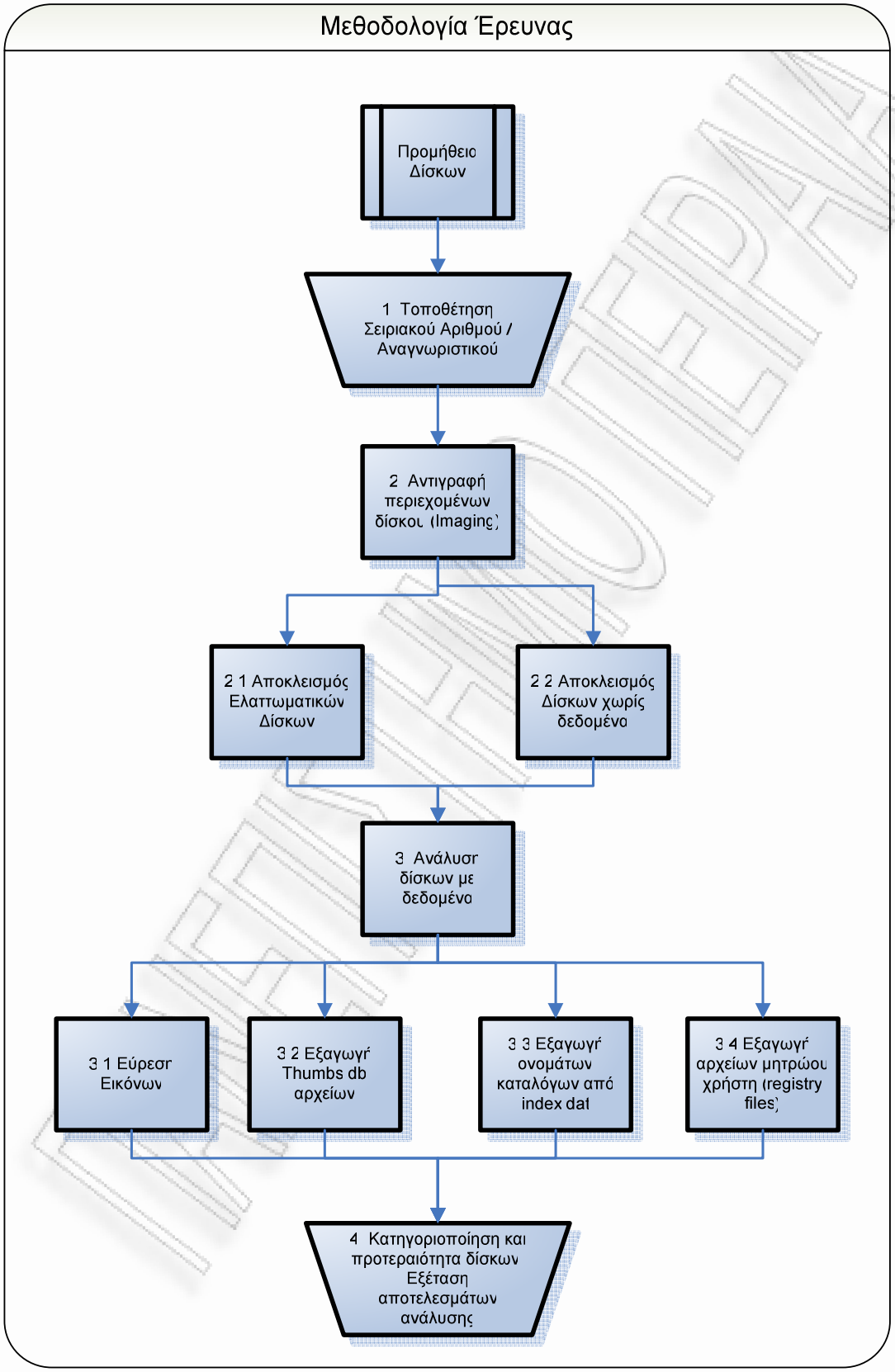
3.3. Η τρίτη εφαρμογή εξάγει τα ονόματα των καταλόγων από τα αρχεία index.dat και προσπαθεί να εντοπίσει ή να ανακτήσει τα περιεχόμενα τους. Στα αρχεία index.dat το λειτουργικό σύστημα απεικονίζει τις δραστηριότητες του χρήστη. Για την δημιουργία της εφαρμογής αυτής, τροποποιήθηκε η βασική ιδέα που χρησιμοποιήθηκε για τα thumb.db αρχεία, έτσι ώστε να εξάγει από τα index.dat αρχεία τα περιεχόμενα τους (ονόματα καταλόγων και διευθύνσεις ιστοσελίδων).

3.4. Η τέταρτη εφαρμογή προσπαθεί να εξάγει τα αρχεία μητρώου (registry files) του χρήστη. Επακολουθεί ανάλυση των αρχείων μητρώου για να βρεθεί πληροφορία ώστε να φτιαχτεί ένα προφίλ για τον χρήστη, όπως το λογισμικό που έχει εγκατασταθεί, το hardware που έχει εγκατασταθεί, η δραστηριότητα του χρήστη στο διαδίκτυο και διάφορες συνήθειες του.

4. Αφού προκύψουν τα αποτελέσματα των προηγούμενων εφαρμογών τότε, ο αναλυτής κατηγοριοποιεί τους δίσκους και τους δίνει προτεραιότητα, ανάλογα με τον χρόνο που εκτιμάει ότι θα χρειαστεί σε κάθε περίπτωση. Έτσι γνωρίζει αν οι δίσκοι περιέχουν παράνομο υλικό, και αν υπάρχουν παρόμοιοι φάκελοι και ονόματα χρήστη, δηλαδή αν υπάρχει περίπτωση να προέρχονται από τον ίδιο οργανισμό. Οι αναφορές από δίσκους που φαίνονται να προέρχονται από τον ίδιο οργανισμό πρέπει να συγκριθούν μεταξύ τους. Και επίσης διευκολύνει να γνωρίζει ο ερευνητής αν θα

χρειαστεί κάποια ειδική επεξεργασία για τους δίσκους, αν για παράδειγμα ένας από αυτούς είναι σε ξένη γλώσσα **[6] [11]**.

Μια πρόταση που θα μπορούσε να είναι ένα πρόσθετο βήμα είναι να γίνει διαχωρισμός των δίσκων πριν από την ανάλυση τους ανάλογα με τη χωρητικότητα τους. Είναι λογικό να υποτεθεί ότι ένας δίσκος με μεγάλη χωρητικότητα έχει περισσότερα δεδομένα από έναν με μικρή χωρητικότητα, και συνεπώς θα χρειαστεί περισσότερο χρόνο για να αναλυθεί. Με αυτόν τον τρόπο είναι πιο εύκολο να εκτιμηθεί ο χρόνος που θα χρειαστεί για την έρευνα. Επίσης καλό είναι να αναλυθούν αρχικά οι δίσκοι που φαίνονται (από τα δεδομένα τους) ότι ανήκουν σε οργανισμούς και έπειτα οι δίσκοι που φαίνεται να ανήκουν σε οικιακούς χρήστες **[6]**. Επίσης έχει προκύψει εμπειρικά ότι προκύπτουν πιο καλά αποτελέσματα από τους μεγάλους δίσκους, γιατί περιέχουν πιο πολλά δεδομένα και έτσι προσφέρουν πιο ρεαλιστικές μετρήσεις για την έρευνα **[11]**. Έπειτα οι δίσκοι που φαίνονται να περιέχουν πολύ λίγα δεδομένα μπορούν να αναλυθούν τελευταίοι. Τέλος, καλό είναι να ομαδοποιηθούν οι δίσκοι που φαίνονται να προέρχονται από την ίδια πηγή (δηλαδή οργανισμό), γιατί κάτι τέτοιο θα βοηθήσει στην σύγκριση των αποτελεσμάτων της ανάλυσης τους (ενώ αν υπάρχει μεγάλο χρονικό διάστημα μεταξύ των αναλύσεων τους, τότε δυσχεραίνεται η σύγκριση). Επίσης καλό είναι να γνωρίζει ο ερευνητής από την αρχή αν υπάρχουν δίσκοι σε ξένη γλώσσα, έτσι ώστε να στέλνονται στα κατάλληλα άτομα για να διεκπεραιώνουν αυτά την έρευνα στην γλώσσα αυτή (έτσι ώστε να μη χρειαστεί να βρεθεί μεταφραστής στη μέση της έρευνας). Με αυτούς τους τρόπους ελαχιστοποιείται ο χρόνος που χρειάζεται για την έρευνα **[6]** και βοηθάει στην εκτίμηση για τους πόρους που θα χρειαστούν **[11]**.


Μεθοδολογία Έρευνας
Προμήθειο Δίσκων
1 Τοποθέτηση Σειριακού Αριθμού / Αναγνωριστικού
2 Αντιγραφή περιεχομένων δίσκοι (Imaging)
2 1 Αποκλεισμός Ελαττωματικών Δίσκων
2 2 Αποκλεισμός Δίσκων χωρίς δεδομένα
3 Ανάλυσ δίσκων με δεδομένα
3 1 Εύρεσ Εικόνων
3 2 Εξαγωγή Thumbs db αρχείων
3 3 Εξαγωγή ονομάτων καταλόγων από index dat
3 4 Εξαγωγή αρχείων μητρώου χρήστη (registry files)
4 Κατηγοριοποίηση και προτεραιότητα δίσκων Εξέταση αποτελεσμάτων ανάλυσης

1.14 ΓΕΝΙΚΕΣ ΣΥΜΒΟΥΛΕΣ ΠΡΟΛΗΨΗΣ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ

Στο υποκεφάλαιο αυτό δίνονται κάποια γενικά βήματα που μπορούν να ληφθούν για να μειωθεί η πιθανότητα να ανακτηθούν ευαίσθητα προσωπικά δεδομένα από κακόβουλους χρήστες και έτσι να υπάρξει πρόληψη από τους κινδύνους που δημιουργούνται από μια τέτοια διαρροή.

Όπως φαίνεται σε παραπάνω υποκεφάλαια, οι κίνδυνοι στους οποίους υπόκεινται οι χρήστες καθώς και οι οργανισμοί, από την ανάκτηση των δεδομένων τους από κάποιον κακόβουλο χρήστη είναι πολλοί. Έτσι είναι απαραίτητο να διασφαλίζουν πως δεν υπάρχουν πληροφορίες στους δίσκους τους όταν αποσύρουν τον εξοπλισμό τους.

Ακολουθούν κάποια μέτρα που μπορούν να ληφθούν για να αντιμετωπιστεί το πρόβλημα:

- Μια γενική ενημέρωση του κοινού για το πρόβλημα και τον κίνδυνο από την διαρροή προσωπικών δεδομένων, καθώς και τα μέτρα που μπορούν να ληφθούν για να αποτραπεί η διαρροή. Η ενημέρωση του κοινού μπορεί να γίνει από την κυβέρνηση, τα μέσα μαζικής ενημέρωσης, τη βιομηχανία και την επιστημονική κοινότητα **[5] [6] [8]**.
- Οι οργανισμοί πρέπει να εφαρμόσουν διαχείριση κινδύνου και να καθορίσουν τον βαθμό της ασφάλειας την οποία πρέπει να έχουν, ώστε να αφαιρούνται με ασφαλή τρόπο τα δεδομένα από τους δίσκους **[8]**.
- Οι οργανισμοί πρέπει να καθορίσουν αυστηρές διαδικασίες για να διασφαλίζουν ότι οι δίσκοι που αποσύρονται έχουν καθαριστεί από τα δεδομένα τους σε ένα αποδεκτό επίπεδο. Στην περίπτωση που ένας τρίτος οργανισμός είναι υπεύθυνος για τον καθαρισμό των δεδομένων τότε θα πρέπει να υπάρχουν διαδικασίες για τον έλεγχο των αποσυρόμενων δίσκων **[4] [8] [9]**.
- Η φυσική καταστροφή των δίσκων μπορεί να συστηθεί στους οργανισμούς ως μια ικανοποιητική λύση για το πρόβλημα **[8]**.

- Οι οργανισμοί πρέπει να εκπαιδεύουν το προσωπικό τους για να επιτευχθεί ευαισθητοποίηση στο ζήτημα και στους κινδύνους που υπάρχουν και το πιθανό κόστος για την εταιρεία από τους κινδύνους αυτούς **[1] [4]**.
- Οι βιομηχανίες πληροφορικής και τηλεπικοινωνιών θα μπορούσαν να διαθέσουν τα εργαλεία και τις λειτουργίες στους χρήστες ώστε να μπορούν να αποσύρουν με ασφαλή τρόπο τον σκληρό τους δίσκο **[8] [9]**.
- Οι χρήστες και οι οργανισμοί μπορούν να εφαρμόσουν κρυπτογράφηση σε όλο τον δίσκο, έτσι ώστε ακόμα και να μην αποσυρθούν με ασφαλή τρόπο τα δεδομένα, να είναι πιο δύσκολο να ανακτηθούν **[4] [8]**. Οι προμηθευτές σκληρών δίσκων θα πρέπει να ενθαρρύνουν την κρυπτογράφηση των δίσκων ως μια ικανοποιητική λύση για προστασία **[9]**. Φυσικά μια τέτοια λύση δεν είναι εφικτή σε όλες τις χώρες, γιατί μπορεί να απαγορεύεται από την νομοθεσία. Έτσι ίσως χρειαστούν μετατροπές στα νομοθετικά πλαίσια ώστε να ισχύσουν **[4]**.
- Τα λειτουργικά συστήματα που θα υλοποιούνται στο μέλλον, θα πρέπει να παρέχουν εφαρμογές για την αυτόματη εκκαθάριση δίσκου **[9]**.
- Οι προμηθευτές σκληρών δίσκων θα πρέπει να εξοπλίσουν τους δίσκους με ειδικούς τρόπους γρήγορης διαγραφής των δεδομένων των δίσκων. Για παράδειγμα, θα μπορούσαν να εξοπλίσουν έναν δίσκο με κρυπτογραφικό υποσύστημα, το οποίο θα κρυπτογραφεί αυτόματα κάθε κομμάτι του δίσκου όταν αυτό θα γράφεται και θα το αποκρυπτογραφεί όταν θα διαβάζεται. Έπειτα οι χρήστες θα μπορούν να καθιστούν τα δεδομένα μη προσβάσιμα σε οποιονδήποτε άλλον διαγράφοντας το κλειδί **[9]**.

2. ΕΡΕΥΝΑ

Στο κεφάλαιο που ακολουθεί παρουσιάζεται το ερευνητικό κομμάτι της εργασίας.

Τα υποκεφάλαια που αναπτύσσονται είναι:

2.1 Σκοπός:
Περιγραφή του σκοπού της έρευνας, καθώς και περιληπτική αναφορά των μεθόδων που θα χρησιμοποιηθούν.

2.2 Γιατί μια τέτοια έρευνα είναι χρήσιμη στην Ελλάδα:
Μια αναφορά στην κατάσταση που επικρατεί στην Ελλάδα, όπως φαίνεται από ελληνικά άρθρα.

2.3 Ερωτηματολόγιο:
Περιγραφή του σκοπού του ερωτηματολογίου που χρησιμοποιήθηκε, γενικές πληροφορίες για αυτό, τα αποτελέσματα όπως προέκυψαν από την στατιστική ανάλυση και τα συμπεράσματα που εξήχθησαν.

2.4 Συμβουλές για τον ελλαδικό χώρο:
Στο υποκεφάλαιο αυτό προτείνονται κάποια βήματα που μπορούν να ληφθούν για να μειωθεί η πιθανότητα να ανακτηθούν ευαίσθητα προσωπικά δεδομένα από κακόβουλους χρήστες στην Ελλάδα.

2.5 Μελλοντική έρευνα:
Στο υποκεφάλαιο αυτό προτείνονται κάποια ερευνητικά θέματα που μπορούν να μελετηθούν μελλοντικά για την Ελλάδα σχετικά με το θέμα της ασφαλούς απόσυρσης δεδομένων από μαγνητικά μέσα.

2.1 ΣΚΟΠΟΣ

Σκοπός της εργασίας είναι να διεξαχθεί μια πιλοτική έρευνα για να διαπιστωθεί αν υπάρχει πρόβλημα στην Ελλάδα με την απόσυρση των δίσκων, από την πλευρά των οικιακών χρηστών.

Αποφασίστηκε να μη ακολουθηθεί η μεθοδολογία που προτείνεται από τα ξένα άρθρα αλλά να δοθεί ένα ερωτηματολόγιο ώστε να εκτιμηθούν αρχικά κάποια στατιστικά στοιχεία που να αφορούν τους οικιακούς χρήστες.

Το ερωτηματολόγιο μοιράστηκε σε οικιακούς χρήστες για να φανεί η ευαισθητοποίηση τους στο θέμα. Σκοπός του ερωτηματολογίου είναι να ελέγξει τη συμπεριφορά του χρήστη όσον αφορά στα δεδομένα που κρατάει στον προσωπικό του υπολογιστή, καθώς και η εμπιστοσύνη του στους φορείς που επεξεργάζονται τα προσωπικά δεδομένα του.

2.2 ΓΙΑΤΙ ΜΙΑ ΤΕΤΟΙΑ ΕΡΕΥΝΑ ΕΙΝΑΙ ΧΡΗΣΙΜΗ ΣΤΗΝ ΕΛΛΑΔΑ

Όπως παρουσιάστηκε σε παραπάνω υποκεφάλαιο, υπάρχουν νομοθετικά πλαίσια που καλύπτουν το ζήτημα της απόσυρσης αποθηκευτικών μέσων με ασφαλή τρόπο, καθώς και οδηγίες που προτείνουν τις μεθόδους απόσυρσης δεδομένων που θεωρούνται πιο ασφαλείς. Επίσης τονίζεται από τον νόμο 2472/1997 ότι οι οργανισμοί που δε θα ακολουθήσουν τις οδηγίες αυτές θεωρούνται υπεύθυνοι και πως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει το δικαίωμα να επιβάλει πρόστιμα.

Η αγορά αποσυρμένων δίσκων δεν είναι διαδεδομένη στην Ελλάδα. Στο Ebay δεν υπάρχουν αποσυρμένοι δίσκοι από την Ελλάδα. Έτσι, δεν είναι διαδεδομένο πρόβλημα προς το παρόν η διαρροή δεδομένων από αποσυρμένους δίσκους.

Έπειτα από μια έρευνα σε άρθρα από ελληνικές εφημερίδες που να αφορούν το ζήτημα φαίνεται πως το πρόβλημα δεν αναγνωρίζεται καν. Οι αποσυρμένοι σκληροί δίσκοι αναφέρονται μόνο σε σχέση με τη περιβαλλοντική καταστροφή που προκαλούν και όχι σε σχέση με τους πιθανούς κίνδυνους από την διαρροή των πληροφοριών που βρίσκονται σε αυτούς. Επίσης υπάρχουν ελάχιστες αναφορές στο ζήτημα. Για παράδειγμα στο περιοδικό PC World αναφέρεται στο άρθρο «Θησαυροί στα σκουπίδια» πως «Θεωρητικά όλο το περιεχόμενο των σκληρών δίσκων σβήνεται και τα χαμένα αντικείμενα επιστρέφονται στους νόμιμους ιδιοκτήτες τους. Θεωρητικά…» **[26]**. Σε ένα άλλο άρθρο στο περιοδικό Computer Act!ve με θέμα «Κλεμμένη ταυτότητα!» αναφέρεται ότι μπορούν να βρεθούν επαρκή δεδομένα σε αποθηκευτικά μέσα, ώστε να οδηγήσουν σε κλοπή ταυτότητας και πως οι «επαγγελματίες» μπορούν να τα αποκτήσουν ψάχνοντας στα σκουπίδια (dumpster diving). Μάλιστα προτείνεται η φυσική καταστροφή του σκληρού δίσκου για να αποφευχθεί αυτό το ενδεχόμενο **[30]**.

Από την άλλη πλευρά φαίνεται πως το ζήτημα της διαρροής προσωπικών δεδομένων από έγγραφα που βρίσκονται στα σκουπίδια των οργανισμών είναι πολύ σημαντικό. Έχουν σημειωθεί αρκετά κρούσματα διαρροής προσωπικών δεδομένων από οργανισμούς μέσω αρχείων που βρίσκονται πεταμένα στα σκουπίδια. Μέσω των στοιχείων αυτών έγινε δυνατό να πραγματοποιηθεί κλοπή ταυτότητας και αθώα άτομα να χρεωθούν υπέρογκα ποσά **[31]**. Πρέπει να τονιστεί το γεγονός ότι μεγάλοι οργανισμοί βρίσκονται υπότροποι στην παραβίαση του νόμου 2472/1997, δηλαδή συνεχίζουν να τον παραβιάζουν και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει επιβάλει πρόστιμα **[27] [28] [29]**.

Παρόλο που το πρόβλημα διαρροής δεδομένων από αποσυρμένους δίσκους δεν είναι προς το παρόν διαδεδομένο στην Ελλάδα, πρέπει να γίνει γνωστός ο κίνδυνος έτσι ώστε να προετοιμαστούν τόσο οι εταιρείες όσο και οι απλοί χρήστες. Είναι αρκετά ανησυχητικό το γεγονός ότι υπάρχουν κρούσματα κλοπής ταυτότητας και πως οι «επαγγελματίες» του είδους γνωρίζουν ότι

μπορούν να βρουν τέτοια στοιχεία στα σκουπίδια, έστω και αν πρόκειται για έγγραφα. Αυτό σημαίνει ότι είναι θέμα χρόνου προτού στραφούν και σε μαγνητικά αποθηκευτικά μέσα όπως οι σκληροί δίσκοι. Επίσης πολύ ανησυχητικό είναι το γεγονός ότι οι οργανισμοί φαίνεται πως δεν ακολουθούν στο έπακρο τον νόμο 2472/1997 για την προστασία των Προσωπικών Δεδομένων.

2.3 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

2.3.1 Γενικά

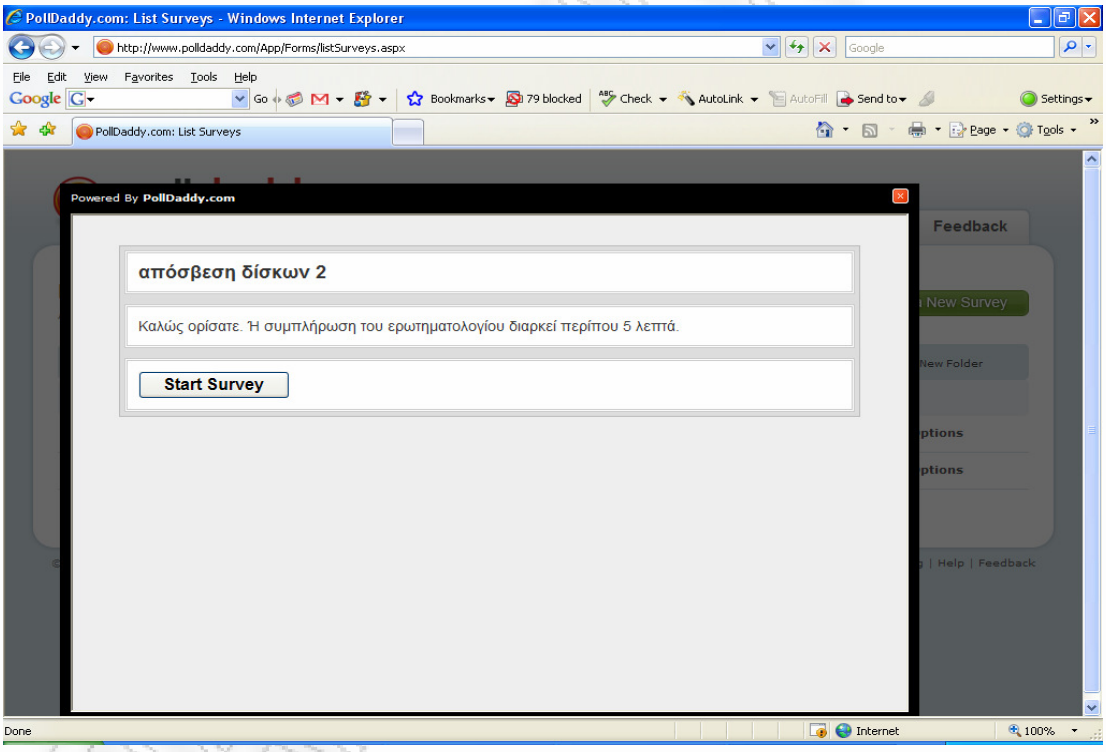
Σκοπός του ερωτηματολογίου είναι φανεί η ευαισθητοποίηση των οικιακών χρηστών όσον αφορά στο θέμα της ασφαλούς απόσυρσης των προσωπικών τους δεδομένων από δίσκους.

Οι ερωτήσεις χωρίζονται σε δύο βασικές κατηγορίες, αυτές που έχουν σκοπό να καθορίσουν τη συμπεριφορά του χρήστη όσον αφορά στα δεδομένα που κρατάει στον προσωπικό του υπολογιστή, και σε αυτές που προσπαθούν να εξακριβώσουν το κατά πόσο είναι ενήμερος σχετικά με τα δικαιώματά του ως προς τη φύλαξη των προσωπικών του στοιχείων από τρίτους και εάν εμπιστεύεται τους φορείς που επεξεργάζονται τα προσωπικά του δεδομένα.
Έτσι υπάρχουν ερωτήσεις που αφορούν στη γνώση του προβλήματος από τον χρήστη, τα βήματα που παίρνει για να προστατεύσει τα προσωπικά του δεδομένα που φυλάει στον προσωπικό του υπολογιστή, άλλα και τη γνώση των δικαιωμάτων του, όπως αυτά αναφέρονται στους αντίστοιχους νόμους και κατά πόσο εμπιστεύεται του φορείς ως προς τη φύλαξη των προσωπικών τους στοιχείων και κυρίως ως προς την απόσυρση των στοιχείων αυτών.

Το ερωτηματολόγιο όπως προέκυψε μετά από πιλοτικό test σε μια ομάδα 13 ατόμων, φαίνεται στο παράρτημα Α.

Δείγμα Ερωτηθέντων

Αποφασίστηκε για τις ανάγκες της έρευνας να μοιραστεί το ερωτηματολόγιο σε δύο διαφορετικές ομάδες ατόμων, σε φοιτητές με τομέα σπουδών την επιστήμη πληροφορικής και σε φοιτητές με διαφορετικό τομέα σπουδών. Το ερωτηματολόγιο αναρτήθηκε στο διαδίκτυο με δύο διαφορετικές ηλεκτρονικές διευθύνσεις, ανάλογα με την ομάδα που άνηκε ο κάθε φοιτητής.
Η ηλεκτρονική διεύθυνση για τους φοιτητές πληροφορικής είναι:
http://www.polldaddy.com/s/5CE49D58C0AB914B/
και η ηλεκτρονική διεύθυνση για τους υπόλοιπους φοιτητές είναι:
http://www.polldaddy.com/s/F3EEDE6951628C27/



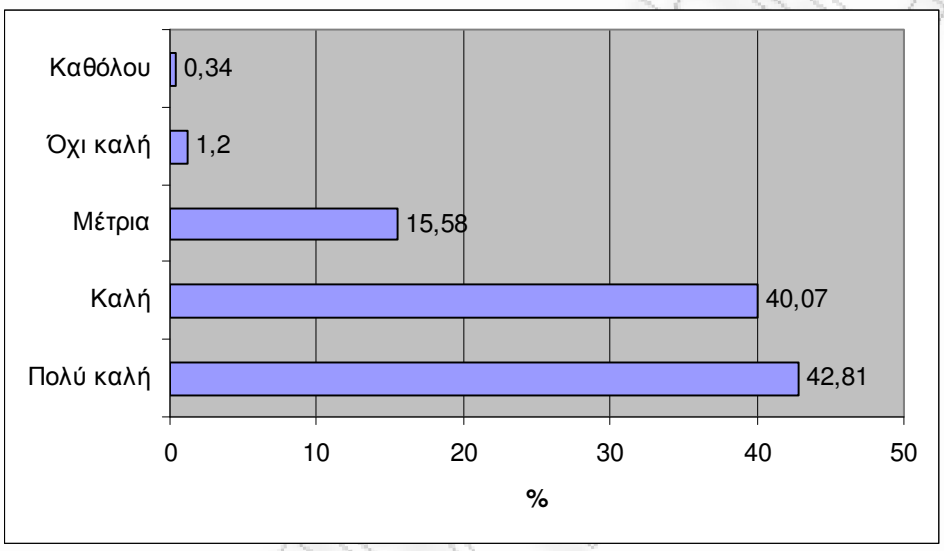
Το ερωτηματολόγιο συμπληρώθηκε από 582 φοιτητές πληροφορικής και 61 φοιτητές άλλων κατευθύνσεων. Υπάρχει μεγάλη διαφορά στον αριθμό των φοιτητών και δεν είναι δυνατή η σύγκριση των αποτελεσμάτων των δύο ομάδων. Επίσης δεν είναι στατιστικά ασφαλές να υπολογιστούν συσχετίσεις

για τη δεύτερη ομάδα και πιθανότατα τα αποτελέσματα δεν είναι αντιπροσωπευτικά του συνόλου.

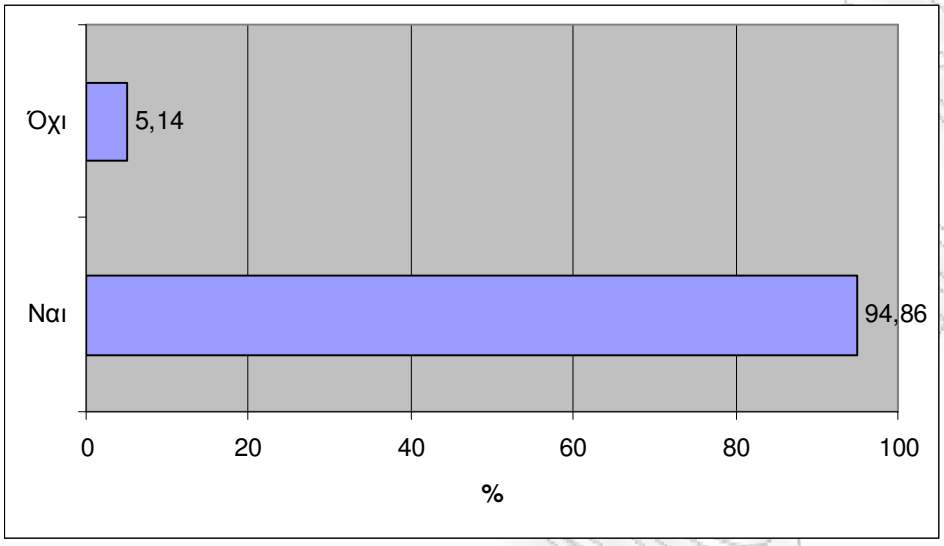
2.3.2 Αποτελέσματα

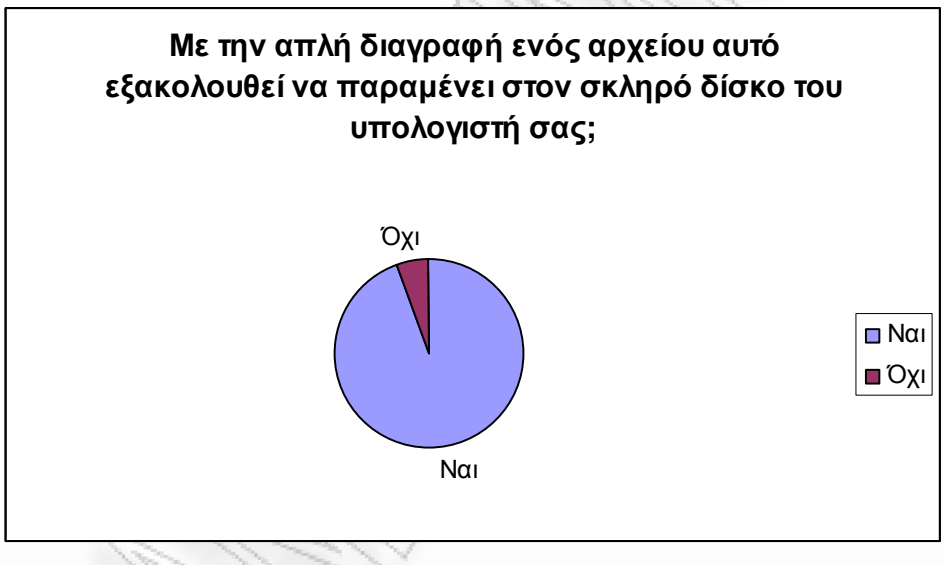
2.3.2.1 Αποτελέσματα από φοιτητές πληροφορικής:

1. Θεωρείτε πως έχετε καλή γνώση ηλεκτρονικών υπολογιστών;



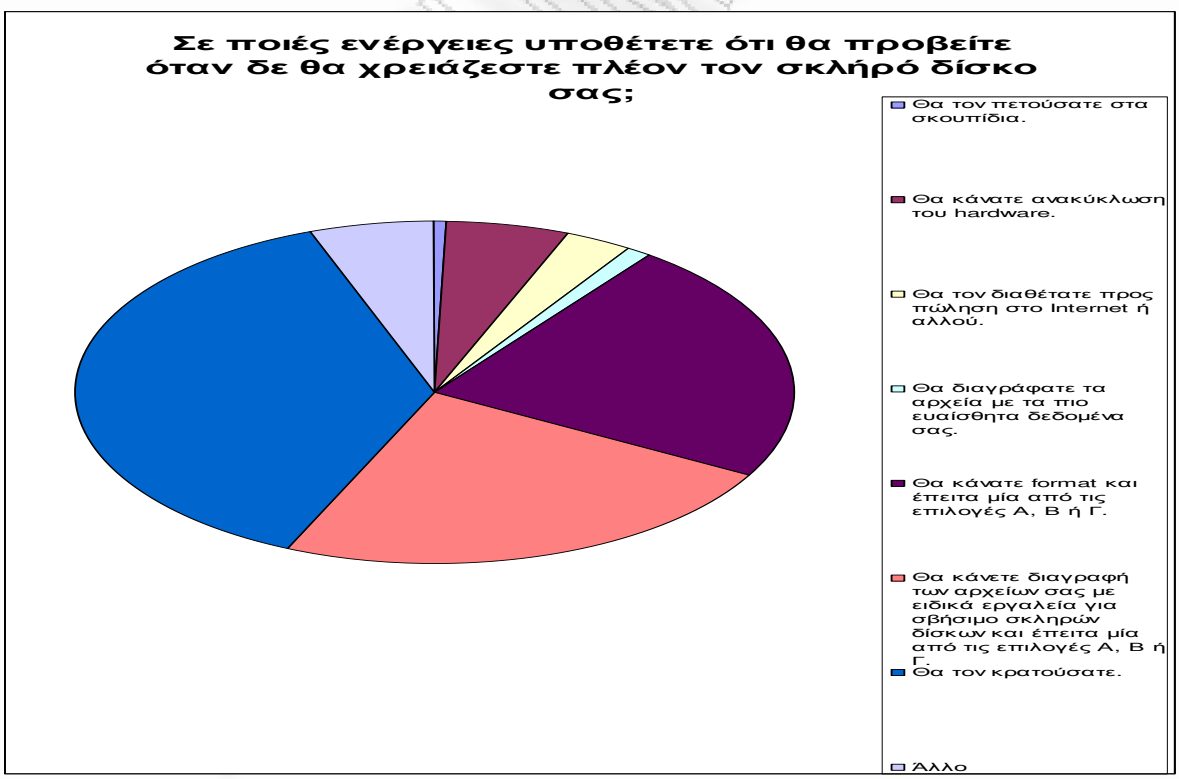
2. Με την απλή διαγραφή ενός αρχείου αυτό εξακολουθεί να παραμένει στον σκληρό δίσκο του υπολογιστή σας;



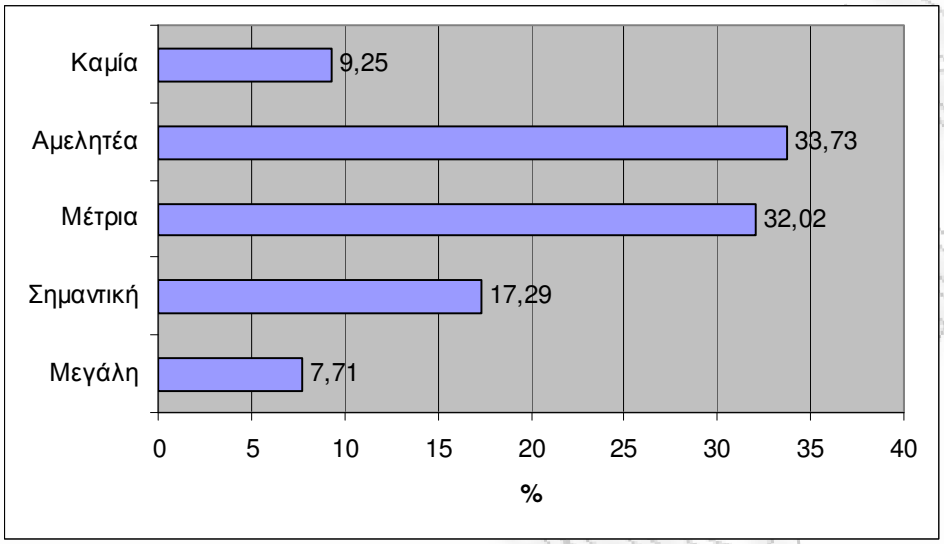


3. Σε ποιές ενέργειες υποθέτετε ότι θα προβείτε όταν δε θα χρειάζεστε πλέον τον σκληρό δίσκο σας:

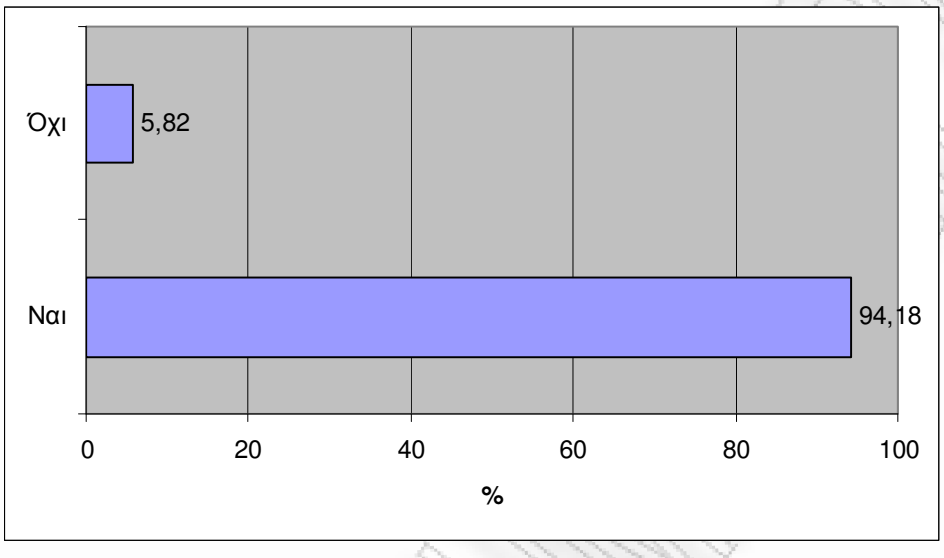
Θα διαγράφατε τα αρχεία με τα πιο ευαίσθητα δεδομένα σας.	7 (1%)
Θα τον πετούσατε στα σκουπίδια.	4 (1%)
Other Option...	33 (6%)
Θα κάνατε ανακύκλωση του hardware.	32 (5%)
Θα τον κρατούσατε.	219 (38%)
Θα τον διαθέτατε προς πώληση στο Internet ή και αλλού	17 (3%)
Θα κάνετε διαγραφή των αρχείων σας με ειδικά εργαλεία για σβήσιμο σκληρών δίσκων και έπειτα μία από τις επιλογές Α, Β ή Γ.	137 (24%)
Θα κάνατε format και έπειτα μία από τις επιλογές Α, Β ή Γ.	133 (23%)

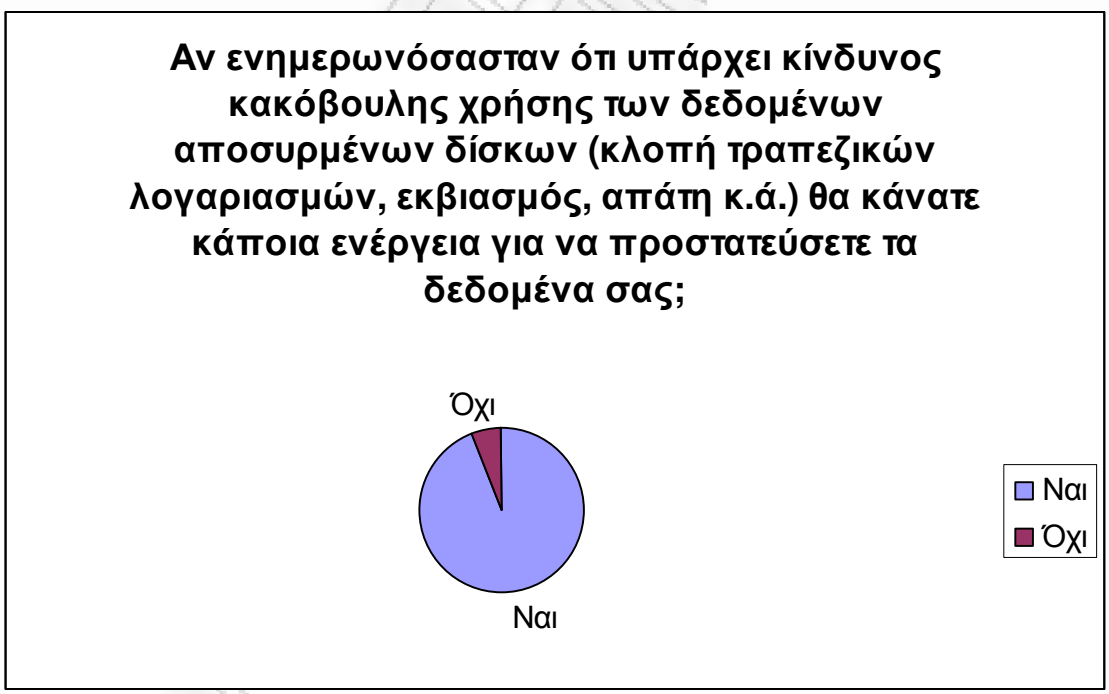


4. Υπάρχει πιθανότητα να ενδιαφερθεί κάποιος για τα δεδομένα του παλιού σας σκληρού δίσκου με κακόβουλο σκοπό;

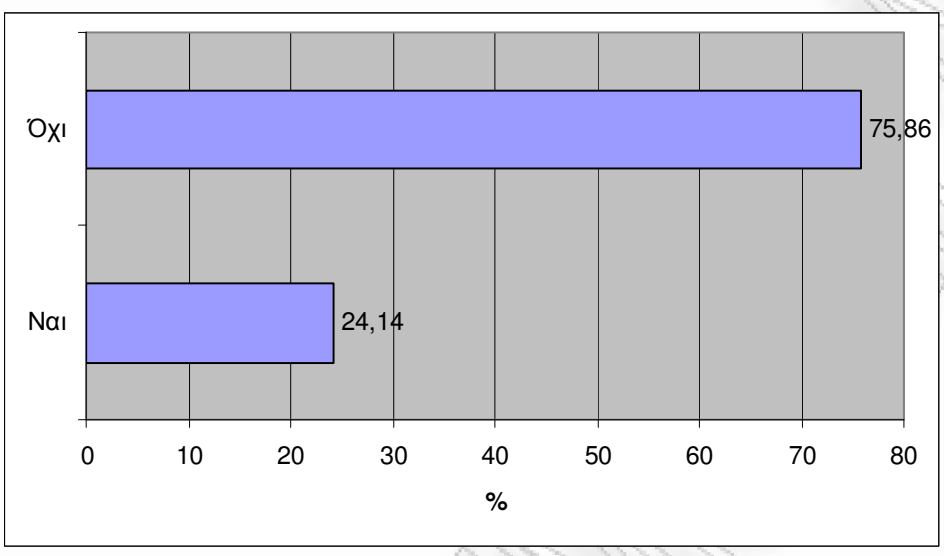


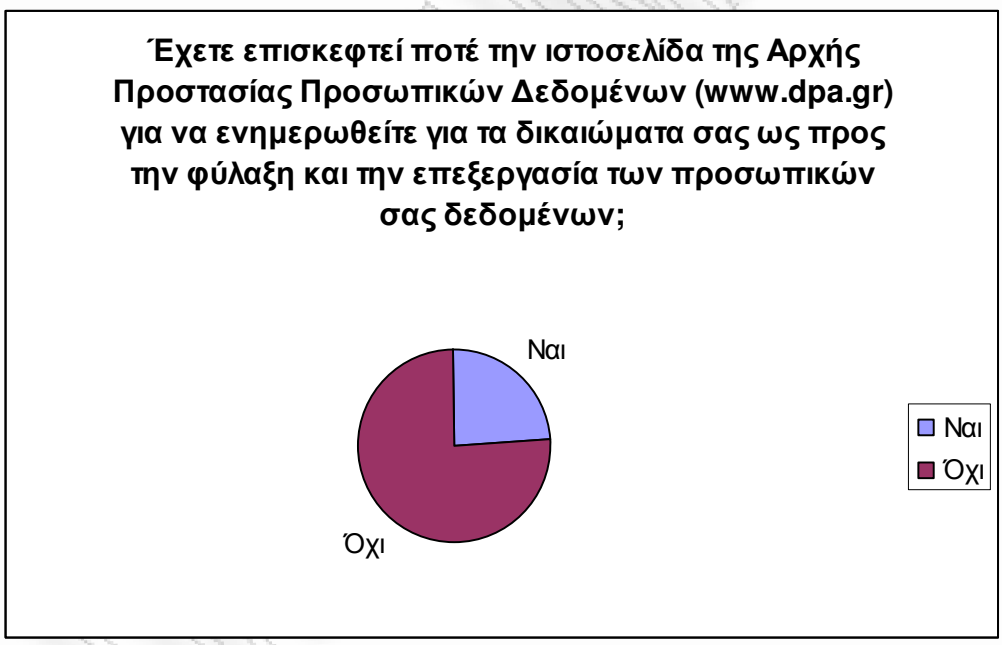
5. Αν ενημερωνόσασταν ότι υπάρχει κίνδυνος κακόβουλης χρήσης των δεδομένων αποσυρμένων δίσκων (κλοπή τραπεζικών λογαριασμών, εκβιασμός, απάτη κ.ά.) θα κάνατε κάποια ενέργεια για να προστατεύσετε τα δεδομένα σας;



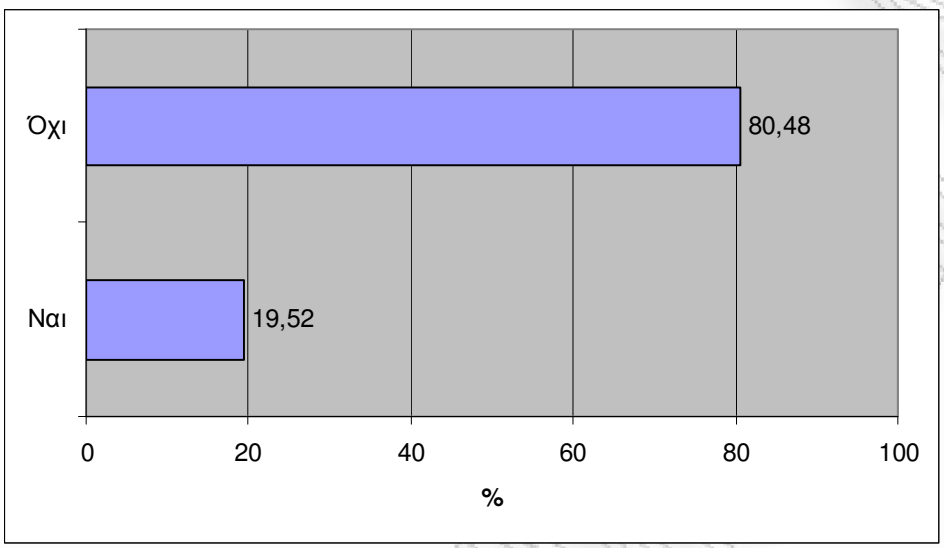


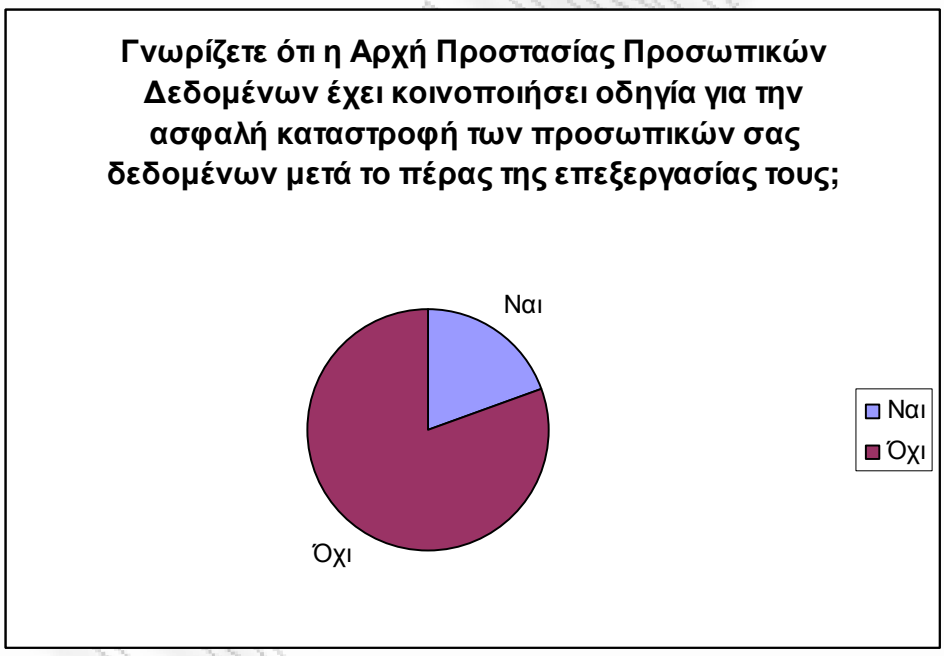
6. Έχετε επισκεφτεί ποτέ την ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων (www.dpa.gr) για να ενημερωθείτε για τα δικαιώματα σας ως προς την φύλαξη και την επεξεργασία των προσωπικών σας δεδομένων;



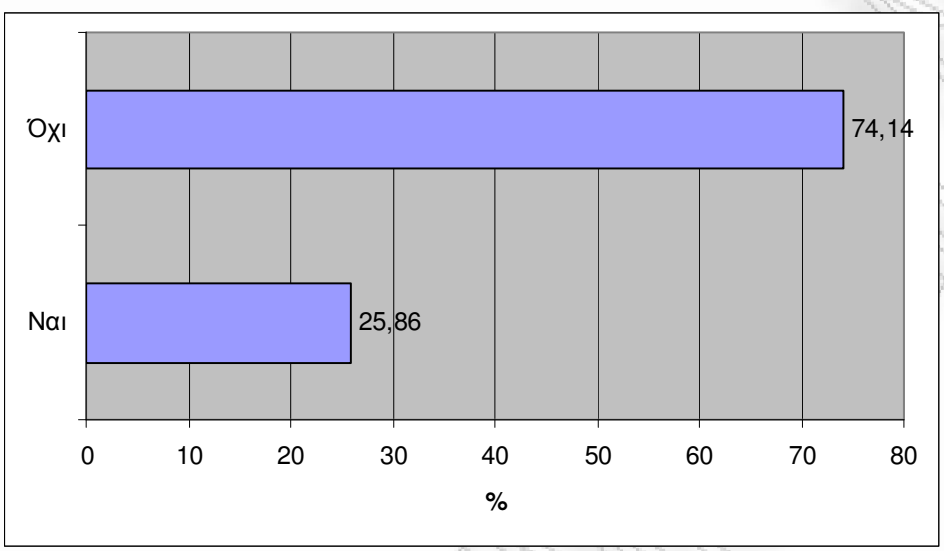


7. Γνωρίζετε ότι η Αρχή Προστασίας Προσωπικών Δεδομένων έχει κοινοποιήσει οδηγία για την ασφαλή καταστροφή των προσωπικών σας δεδομένων μετά το πέρας της επεξεργασίας τους;



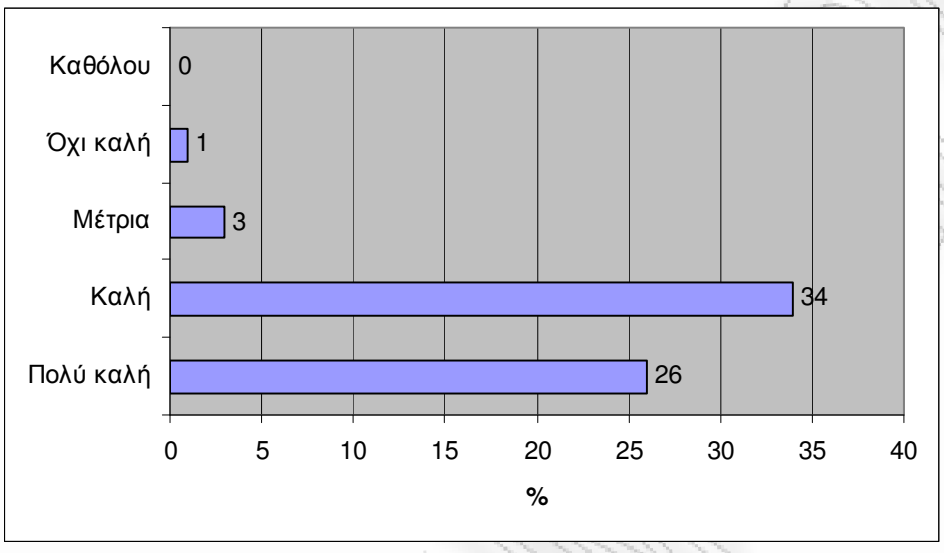


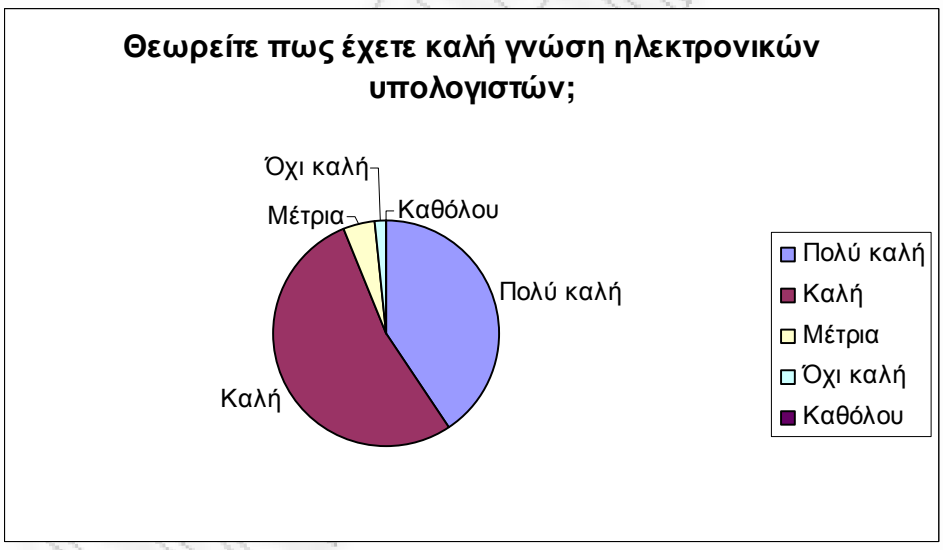
8. Θεωρείτε ότι οι φορείς (π.χ. Τράπεζες, Εταιρείες Τηλεπικοινωνίας, Δημόσιοι Φορείς) που επεξεργάζονται τα προσωπικά σας στοιχεία τηρούν τις οδηγία αυτή;



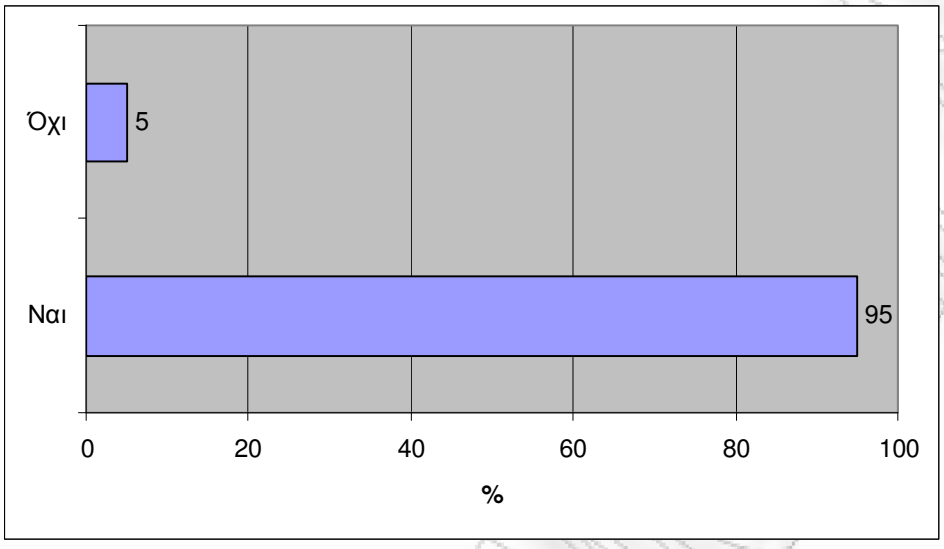
2.3.2.2 Αποτελέσματα από τους υπόλοιπους φοιτητές:

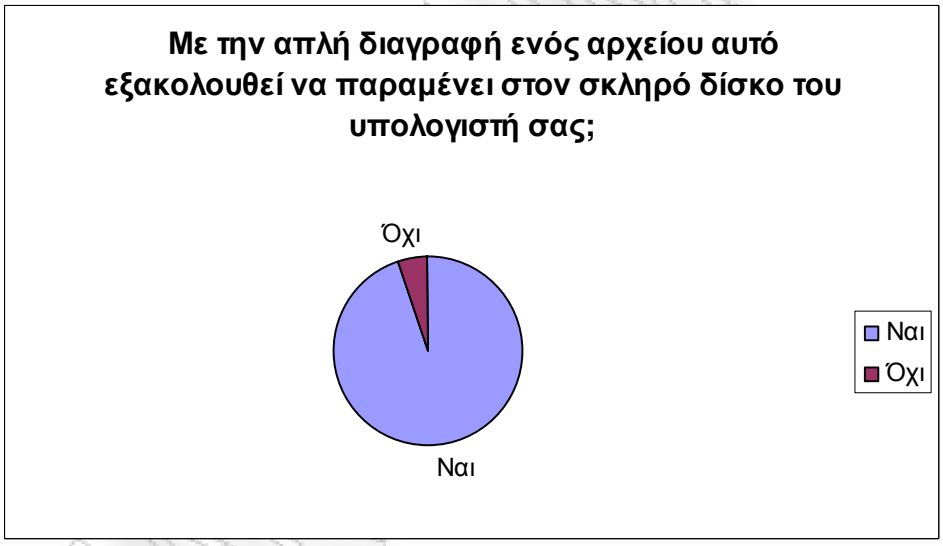
1. Θεωρείτε πως έχετε καλή γνώση ηλεκτρονικών υπολογιστών;





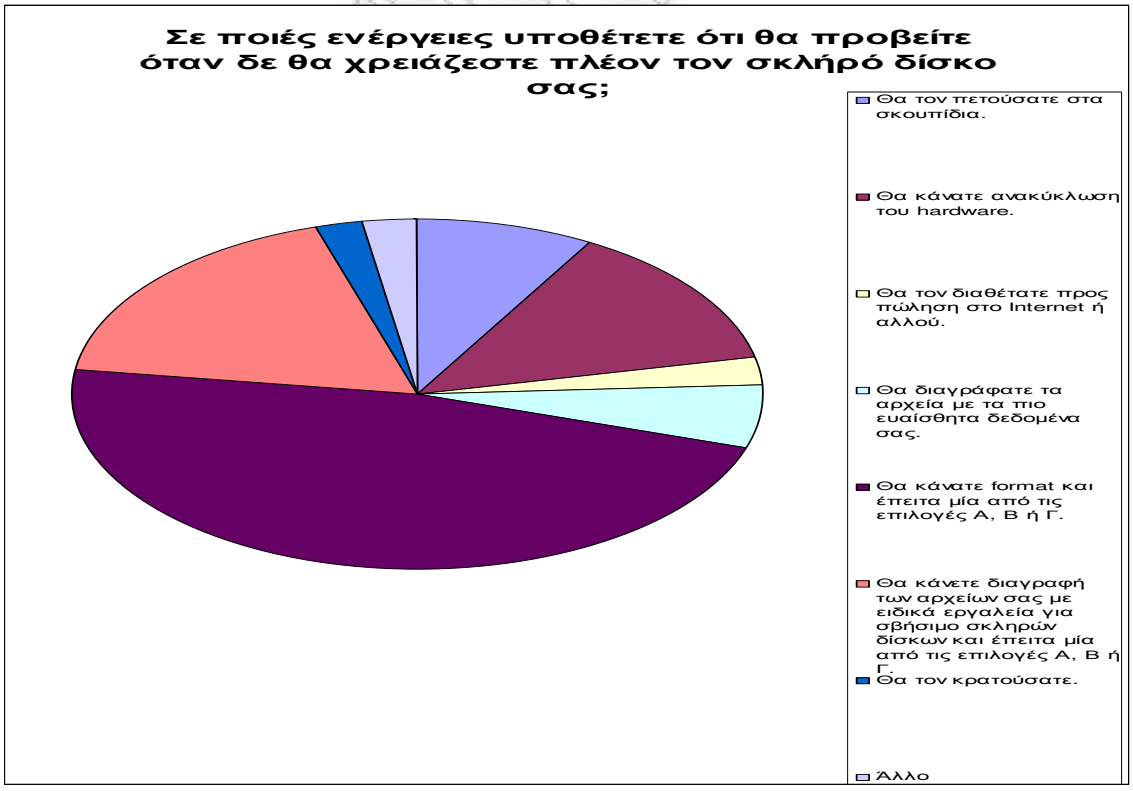
2. Με την απλή διαγραφή ενός αρχείου αυτό εξακολουθεί να παραμένει στον σκληρό δίσκο του υπολογιστή σας;



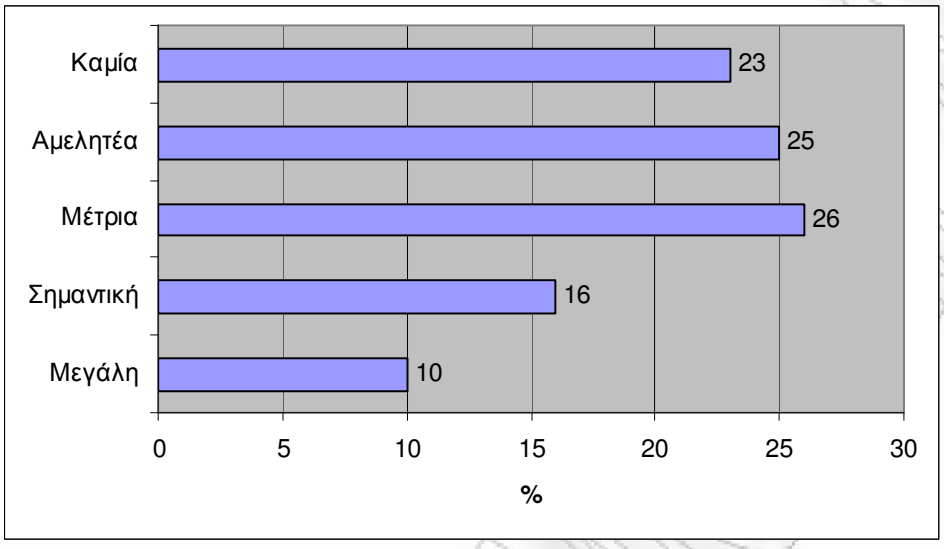


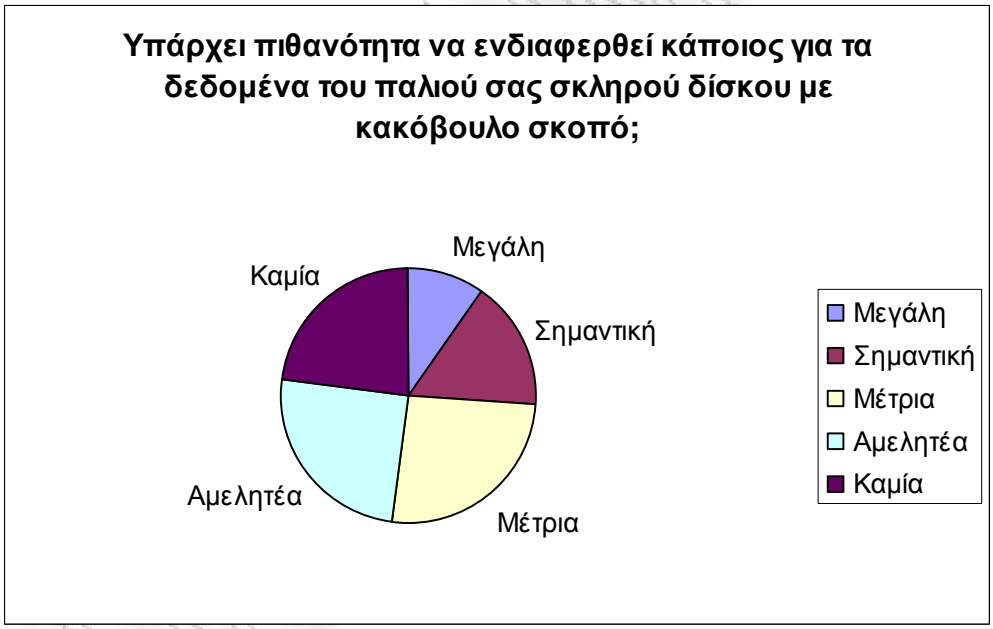
3. Σε ποιές ενέργειες υποθέτετε ότι θα προβείτε όταν δε θα χρειάζεστε πλέον τον σκληρό δίσκο σας:

Θα κάνετε διαγραφή των αρχείων σας με ειδικά εργαλεία για σβήσιμο σκληρών δίσκων και έπειτα μία από τις επιλογές Α, Β ή Γ.	9 (15%)
Θα κάνατε ανακύκλωση του hardware.	7 (11%)
Θα τον πετούσατε στα σκουπίδια.	4 (7%)
Θα διαγράφατε τα αρχεία με τα πιο ευαίσθητα δεδομένα σας.	3 (5%)
Θα κάνατε format και έπειτα μία από τις επιλογές Α, Β ή Γ.	24 (39%)
Θα τον κρατούσατε.	12 (20%)
Other Option...	1 (2%)
Θα τον διαθέτατε προς πώληση στο Internet ή και αλλού.	1 (2%)

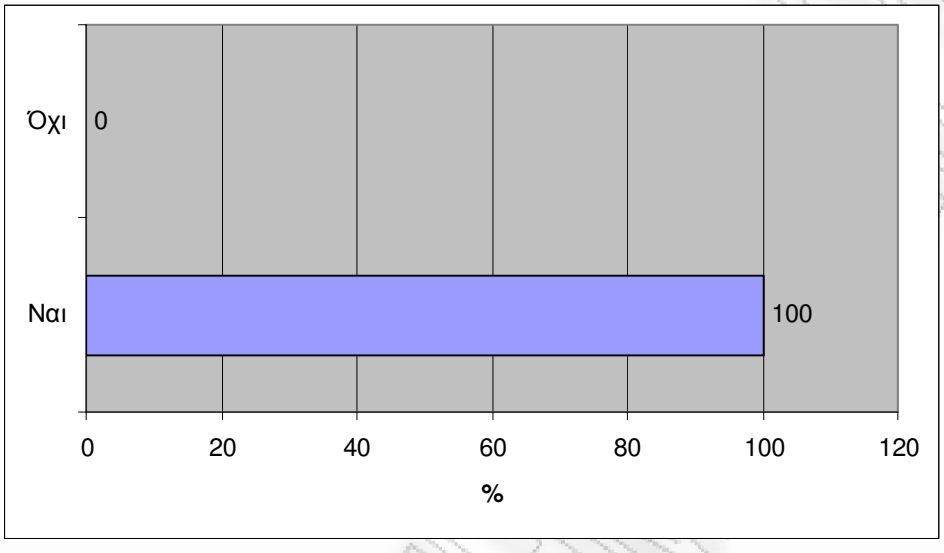


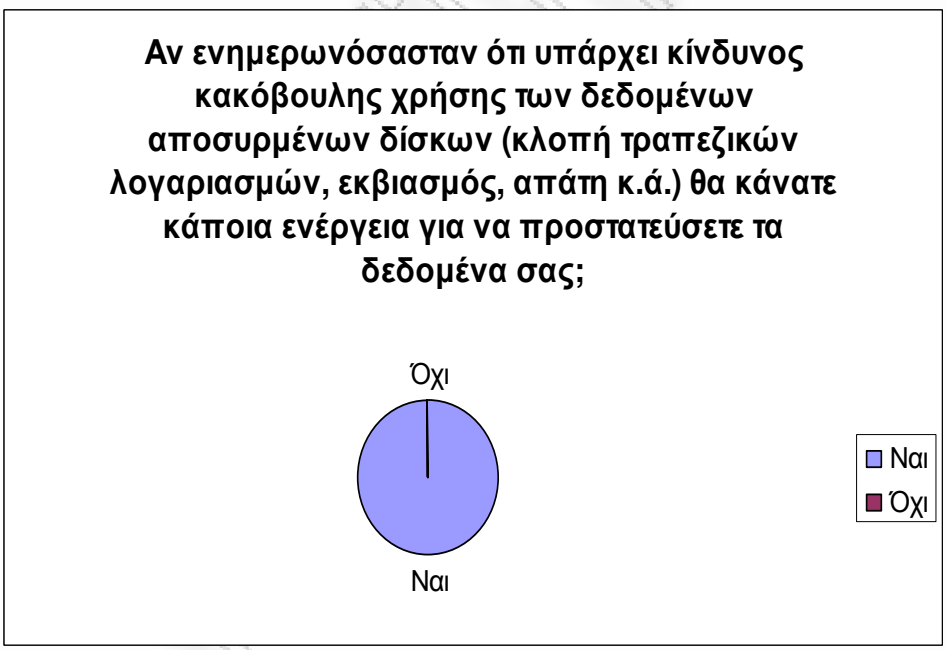
4. Υπάρχει πιθανότητα να ενδιαφερθεί κάποιος για τα δεδομένα του παλιού σας σκληρού δίσκου με κακόβουλο σκοπό;



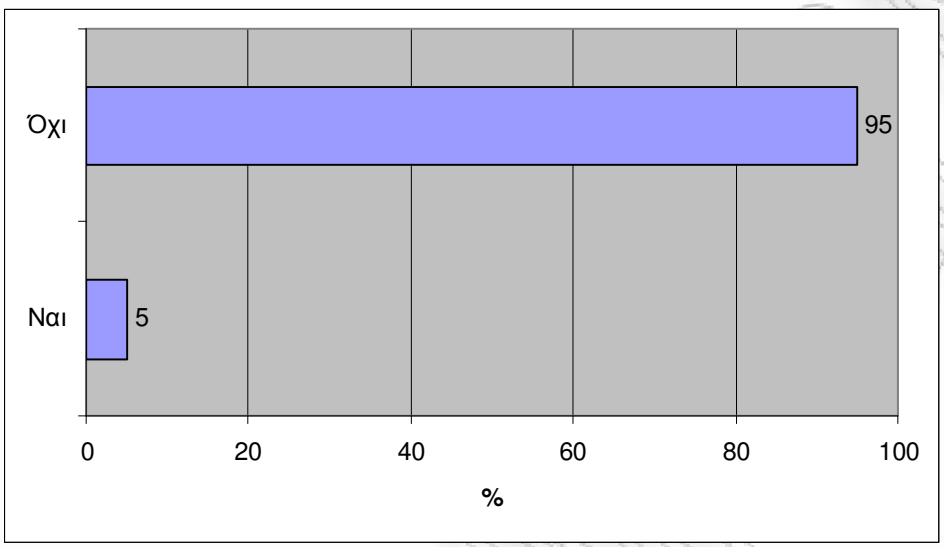


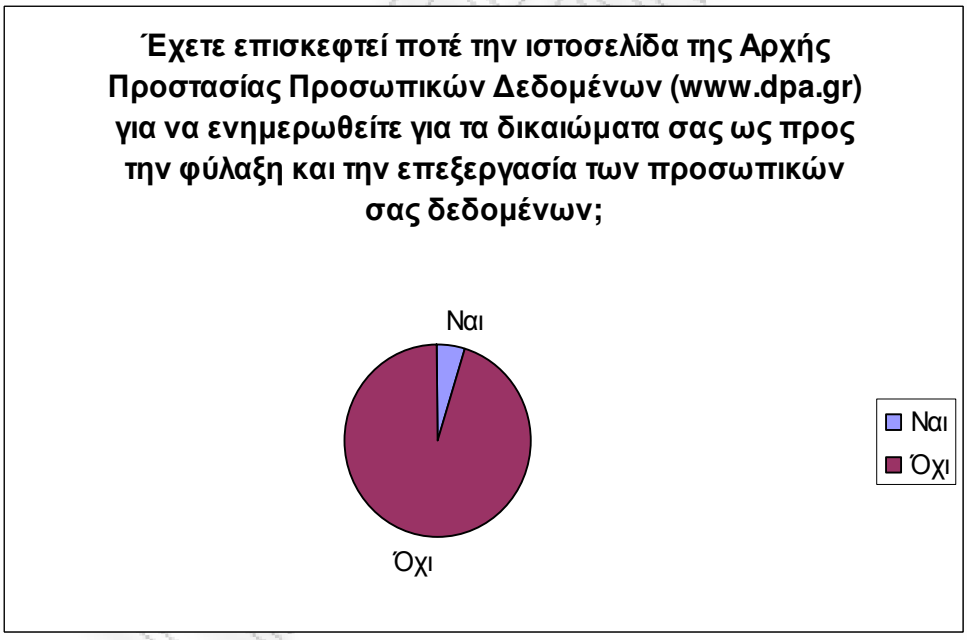
5. Αν ενημερωνόσασταν ότι υπάρχει κίνδυνος κακόβουλης χρήσης των δεδομένων αποσυρμένων δίσκων (κλοπή τραπεζικών λογαριασμών, εκβιασμός, απάτη κ.ά.) θα κάνατε κάποια ενέργεια για να προστατεύσετε τα δεδομένα σας;



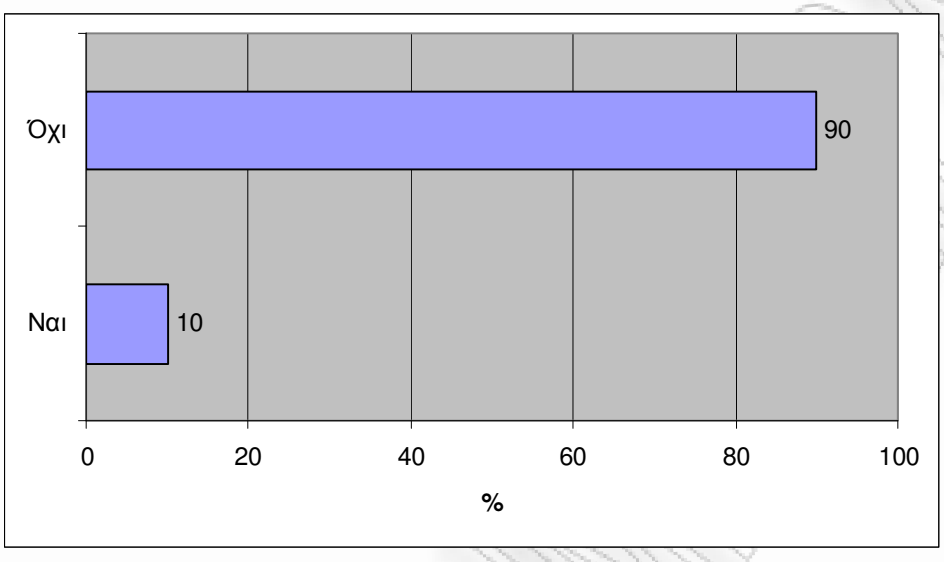


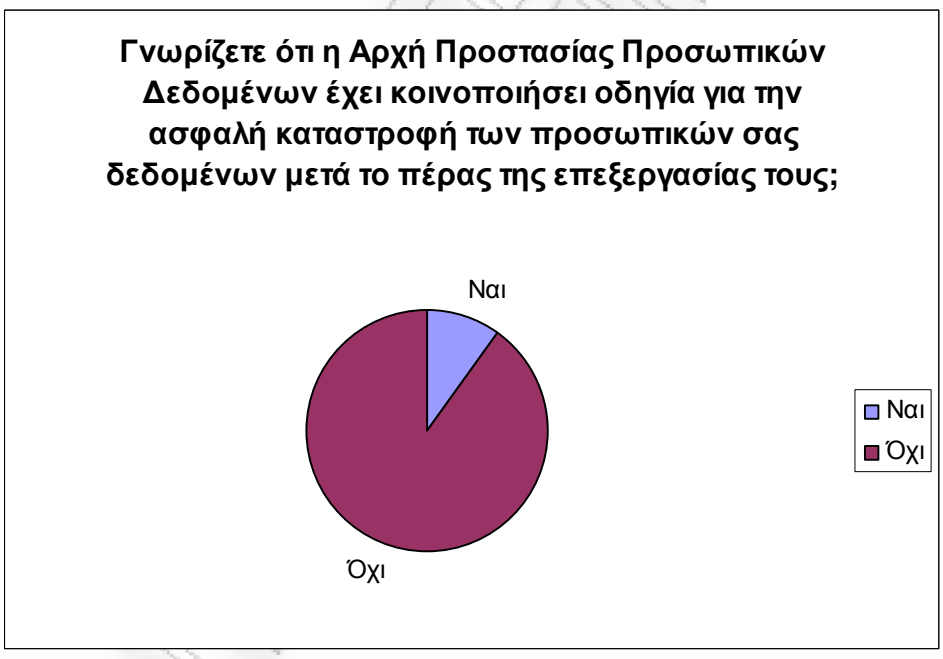
6. Έχετε επισκεφτεί ποτέ την ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων (www.dpa.gr) για να ενημερωθείτε για τα δικαιώματα σας ως προς την φύλαξη και την επεξεργασία των προσωπικών σας δεδομένων;



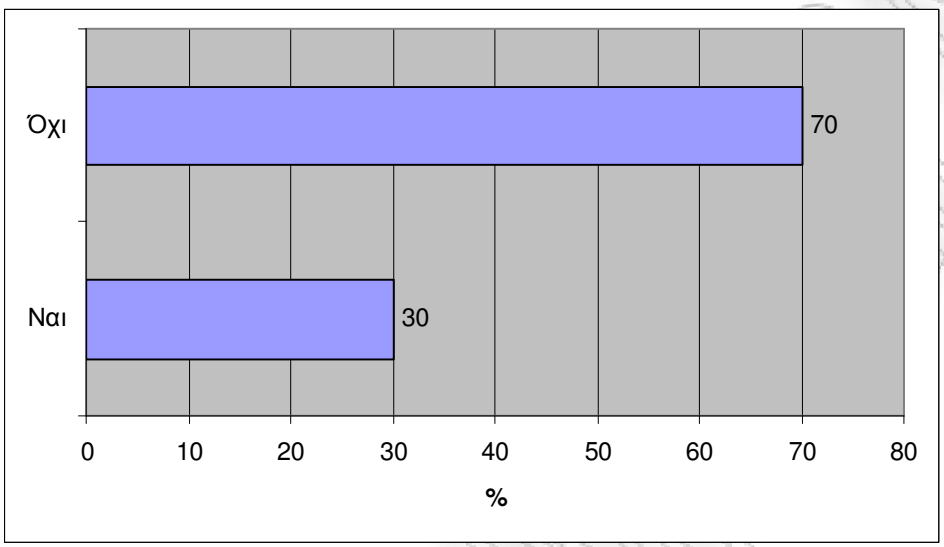


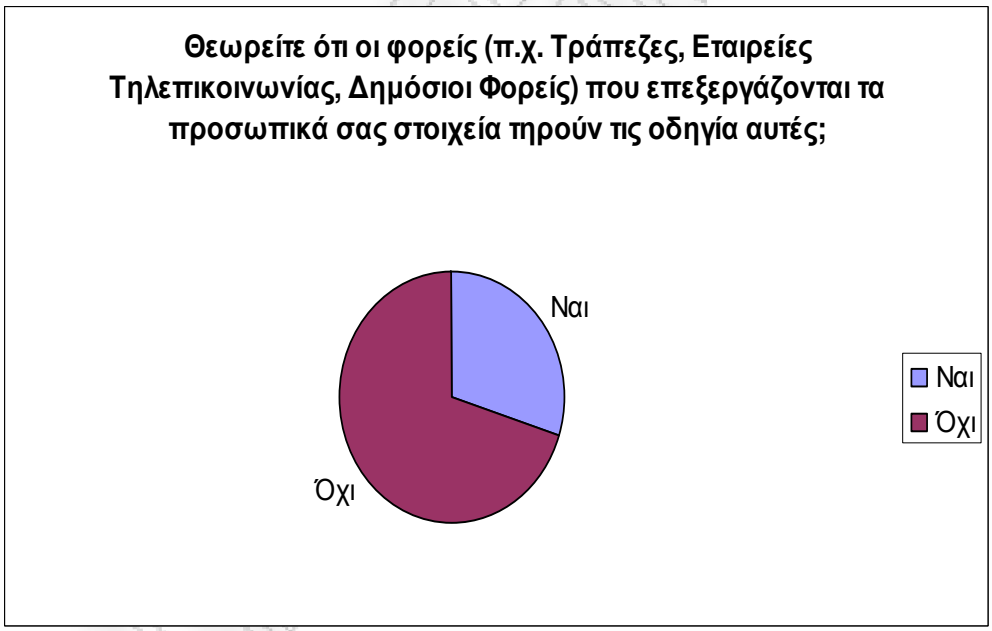
7. Γνωρίζετε ότι η Αρχή Προστασίας Προσωπικών Δεδομένων έχει κοινοποιήσει οδηγία για την ασφαλή καταστροφή των προσωπικών σας δεδομένων μετά το πέρας της επεξεργασίας τους;





8. Θεωρείτε ότι οι φορείς (π.χ. Τράπεζες, Εταιρείες Τηλεπικοινωνίας, Δημόσιοι Φορείς) που επεξεργάζονται τα προσωπικά σας στοιχεία τηρούν τις οδηγία αυτή;





2.3.3 Συμπεράσματα

2.3.3.1 Για φοιτητές πληροφορικής:

Από τα αποτελέσματα του ερωτηματολογίου που κατανεμήθηκε στους φοιτητές πληροφορικής προκύπτουν τα εξής συμπεράσματα:

- Το μεγαλύτερο ποσοστό των ερωτηθέντων (94,86%) δηλώνει ότι γνωρίζει ότι ένα διαγραμμένο αρχείο εξακολουθεί να βρίσκεται στο σκληρό δίσκο. Αυτό ήταν κάτι αναμενόμενο από τη στιγμή που, όπως προκύπτει και από το ερωτηματολόγιο το μεγαλύτερο ποσοστό (98,39%) των ερωτηθέντων έχει γνώση πληροφορικής περισσότερη από την μέτρια.
- Στην ερώτηση που αφορά στις ενέργειες που προβαίνει ο χρήστης όταν δε χρειάζεται πλέον τον υπολογιστή του, το 61,17% έχει επιλέξει ενέργειες που είναι πιο ασφαλείς για την ασφάλεια των προσωπικών του δεδομένων (το 22,85% θα χρησιμοποιούσε εξειδικευμένο εργαλείο διαγραφής δεδομένων και το 37,63% θα κρατούσε τον σκληρό δίσκο). Είναι πολύ σημαντικό να τονιστεί ότι μόλις το 3% θα διέθετε τον υπολογιστή του για πώληση.
- Στην ερώτηση που αφορά την άποψη του ερωτηθέντος αν κινδυνεύουν τα δεδομένα του, το μεγαλύτερο ποσοστό δε θεωρεί τον κίνδυνο σημαντικό (42,98%), ένα μεγάλο ποσοστό τον θεωρεί μέτριο (32,02%) και ένα σημαντικό ποσοστό τον θεωρεί σημαντική απειλή (25%). Φαίνεται λοιπόν ότι ένα μεγάλο ποσοστό θεωρεί ότι κινδυνεύει παρόλο που το πρόβλημα δεν είναι ευρέως γνωστό. Πιθανότατα αυτό το γεγονός οφείλεται στο ότι οι ερωτηθέντες είναι φοιτητές Πληροφορικής.
- Όσον αφορά στις ερωτήσεις που αποσκοπούν στο να διαπιστώσουν αν ο ερωτώμενος γνωρίζει τα δικαιώματα του για την επεξεργασία των προσωπικών του δεδομένων, όπως αυτά αναφέρονται στον νόμο 2472/1997, προκύπτει ότι η μεγάλη πλειοψηφία δε τα γνωρίζει

(80,48%) και δεν έχει επισκεφτεί την ιστοσελίδα της Αρχής Προστασίας Προσωπικών δεδομένων για να ενημερωθεί για αυτά (75,86%).

- Από την άλλη πλευρά, το μεγαλύτερο ποσοστό (74,15%) θεωρεί ότι δε εφαρμόζουν σωστά τον νόμο για τα προσωπικά του στοιχεία οι φορείς που επεξεργάζονται τα προσωπικά του δεδομένα. Αυτό είναι αξιοσημείωτο, ειδικά από τη στιγμή που δε γνωρίζουν τον νόμο (αρνητική συσχέτιση μεταξύ των ερωτήσεων).
- Προκύπτει επίσης, ότι εφόσον ενημερωθεί ο χρήστης πως υπάρχει κίνδυνος για τα προσωπικά του δεδομένα στους δίσκους που αποσύρει είναι πρόθυμος να προβεί σε κατάλληλες ενέργειες, ώστε να διασφαλίσει την προστασία τους (ερώτηση 5, θετική απάντηση 94,18%).
- Τέλος, φαίνεται ότι οι χρήστες προβαίνουν σε αρκετά ασφαλείς ενέργειες για να διασφαλίσουν τα προσωπικά τους δεδομένα, ενώ δεν εμπιστεύονται ότι θα προβούν σε αντίστοιχες ενέργειες οι διάφοροι φορείς (αρνητική συσχέτιση μεταξύ ερωτήσεων 3 και 8).

2.3.3.2 Για τους υπόλοιπους φοιτητές:

Από τα αποτελέσματα του ερωτηματολογίου που κατανεμήθηκε στους υπόλοιπους φοιτητές, οι οποίοι δε σπουδάζουν πληροφορική, προκύπτουν τα παρακάτω συμπεράσματα. Ωστόσο επειδή απάντησε μικρός αριθμός ατόμων, δεν είναι ασφαλές να θεωρηθεί ότι τα συμπεράσματα αυτά ισχύουν για όλο τον πληθυσμό:

- Το μεγαλύτερο ποσοστό των ερωτηθέντων (95%) δηλώνει ότι γνωρίζει ότι ένα διαγραμμένο αρχείο εξακολουθεί να βρίσκεται στο σκληρό δίσκο. Από ότι φαίνεται στο 1^{ο} κεφάλαιο αυτή δεν είναι μια γνώση που είναι αναμενόμενο να κατέχει ένας απλός χρήστης. Ωστόσο στη συγκεκριμένη περίπτωση μπορεί να οφείλεται στο ότι όπως δηλώνεται και στο ερωτηματολόγιο, τα περισσότερα άτομα έχουν πάνω από μέτρια γνώση ηλεκτρονικών υπολογιστών (60%). Φυσικά πρέπει να τονιστεί

ότι από τη στιγμή που το ερωτηματολόγιο είχε αναρτηθεί στο internet, είναι αναμενόμενο που δεν απαντήθηκε από περισσότερα άτομα με λιγότερη γνώση ηλεκτρονικών υπολογιστών.

- Στην ερώτηση που αφορά στις ενέργειες που προβαίνει ο χρήστης όταν δε χρειάζεται πλέον τον υπολογιστή του, το 17% μόνο έχει επιλέξει ενέργειες που είναι πιο ασφαλείς για την ασφάλεια των προσωπικών του δεδομένων (το 15% θα χρησιμοποιούσε εξειδικευμένο εργαλείο διαγραφής δεδομένων και μόλις το 2% θα κρατούσε τον σκληρό δίσκο). Επίσης είναι πολύ σημαντικό να τονιστεί ότι μόνο το 2% θα διέθετε τον υπολογιστή του προς πώληση. Η μεγάλη πλειοψηφία των ερωτηθέντων επιλέγει να κάνει format (39%), θεωρώντας λανθασμένα ότι με αυτόν τον τρόπο τα δεδομένα τους είναι ασφαλή.
- Στην ερώτηση που αφορά στην άποψη του ερωτηθέντος αν κινδυνεύουν τα δεδομένα του, το μεγαλύτερο ποσοστό θεωρεί τον κίνδυνο μικρότερο από μέτριο (74%) και είναι σημαντικό ότι ένα μεγάλο ποσοστό τον θεωρεί μηδενικό (23%).
- Όσον αφορά στις ερωτήσεις που αποσκοπούν να διαπιστώσουν αν ο ερωτώμενος γνωρίζει τα δικαιώματα του για την επεξεργασία των προσωπικών του δεδομένων, όπως αυτά αναφέρονται στον νόμο 2472/1997, προκύπτει ότι η μεγάλη πλειοψηφία δε τα γνωρίζει (90%) και δεν έχει επισκεφτεί την ιστοσελίδα της Αρχής Προστασίας Προσωπικών δεδομένων για να ενημερωθεί για αυτά (95%).
- Από την άλλη πλευρά, το μεγαλύτερο ποσοστό (70%) θεωρεί ότι οι φορείς που επεξεργάζονται τα προσωπικά του δεδομένα, δε εφαρμόζουν σωστά τον νόμο που αφορά την προστασία των προσωπικών του στοιχείων.
- Προκύπτει επίσης, ότι εφόσον ενημερωθούν πως υπάρχει κίνδυνος για τα προσωπικά του δεδομένα στους δίσκους που αποσύρουν, όλοι οι ερωτηθέντες είναι πρόθυμοι να προβούν σε κατάλληλες ενέργειες, ώστε να διασφαλίσουν την προστασία τους (ερώτηση 5, θετική απάντηση 100%).

2.4 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ

Στο υποκεφάλαιο αυτό προτείνονται κάποιες συμβουλές για βήματα που μπορούν να ληφθούν στην Ελλάδα ώστε να υπάρχει πρόληψη για το πρόβλημα. Από ότι φαίνεται από τα άρθρα που έχουν δημοσιευτεί στην Ελλάδα, το πρόβλημα κλοπής προσωπικών δεδομένων από αποσυρμένους δίσκους δε βρίσκεται σε έξαρση και μάλλον τα κρούσματα είναι λίγα. Ωστόσο, είναι θεμιτό να ληφθούν προληπτικά μέτρα.

Κάποια μέτρα που μπορούν να ληφθούν είναι:

- Να ενημερωθεί το κοινό για τον κίνδυνο που μπορεί να προκύψει από μη ασφαλή απόσυρση των παλιών δίσκων ώστε να αυξηθεί η ευαισθητοποίηση του για το ζήτημα, καθώς και για τον τρόπο που μπορεί να τους αποσύρει με ασφαλή τρόπο. Η ενημέρωση του κοινού μπορεί να γίνει από τα μέσα μαζικής ενημέρωσης σε συνδυασμό με τη κυβέρνηση. Όπως φάνηκε από το ερωτηματολόγιο η πλειοψηφία των ερωτηθέντων είναι πρόθυμη να προβεί στα αντίστοιχα βήματα ώστε να διασφαλίσει τα προσωπικά δεδομένα της.
- Οι οργανισμοί και οι εταιρείες πρέπει να καθορίσουν τον βαθμό ασφάλειας που παρέχουν και να διασφαλίζουν με αυστηρές διαδικασίες ότι τηρούνται ο νόμος 2472/1997 και η οδηγία ΑΡ.1/2005 για την απόσυρση των δεδομένων γενικά. Επίσης πρέπει να εκπαιδεύουν το προσωπικό τους ώστε οι διαδικασίες να εφαρμόζονται πιστά. Η Αρχή Προστασίας Προσωπικών δεδομένων μπορεί να διασφαλίζει την τήρηση τους με συχνούς ελέγχους και αυστηρές ποινές στους παραβάτες.
- Οι εταιρείες κατά κύριο λόγο, αλλά και οι χρήστες μπορούν να κρυπτογραφούν τους δίσκους τους, ώστε να είναι πιο δύσκολο να ανακτηθούν τα δεδομένα. Ειδικά για τις εταιρείες θα μπορούσε να ισχύσει κάτι τέτοιο μέσω μιας οδηγίας που θα εξέδιδε η Αρχή Προστασίας Προσωπικών Δεδομένων.

2.5 ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Στο υποκεφάλαιο αυτό προτείνονται κάποια θέματα που μπορούν να μελετηθούν μελλοντικά για την Ελλάδα.

Ένας τομέας που μπορεί να μελετηθεί περισσότερο στο μέλλον είναι οι απόψεις και η συμπεριφορά των οικιακών χρηστών. Μπορεί να ξαναγίνει έρευνα μέσω ερωτηματολογίου, αλλά αυτή τη φορά να στοχεύει σε άτομα με μικρότερη γνώση για τους ηλεκτρονικούς υπολογιστές. Επιπρόσθετα, μπορούν να αναλυθούν αποτελέσματα που προέρχονται από δίσκους που ανήκουν σε οικιακούς χρήστες.

Επίσης, είναι δυνατόν να χρησιμοποιηθεί η μεθοδολογία ανάκτησης δεδομένων από αποσυρμένους σκληρούς δίσκους εταιρειών ή και οικιακών χρηστών. Θα μπορούσε να χρησιμοποιηθεί κάποια εταιρεία που αναλαμβάνει την διαδικασία απόσυρσης δίσκων. Μια τέτοια έρευνα είναι απαραίτητη για να προκύψουν στατιστικά αποτελέσματα για τα δεδομένα που παραμένουν στους δίσκους, ώστε να εξεταστεί κατά πόσο οι εταιρείες τηρούν τον νόμο 2472/1997 και την οδηγία ΑΡ.1/2005 και το μέγεθος του προβλήματος στην Ελλάδα. Στο παράρτημα Γ παρουσιάζεται ένα ενδεικτικό φύλλο αποτελεσμάτων ανά δίσκο για αυτού του είδους την ανάλυση.

Άλλα θέματα που μπορούν να εξεταστούν είναι συγκρίσεις των διάφορων εργαλείων απόσυρσης, μια έρευνα που ενδιαφέρει κυρίως τις εταιρείες, ώστε να αποφασίσουν τα εργαλεία που θα χρησιμοποιούν. Επίσης μπορούν να γίνουν συγκρίσεις διάφορων εργαλείων ανάκτησης δεδομένων. Τέλος, ένα θέμα που θα ήταν ενδιαφέρον να ερευνηθεί είναι τα δεδομένα που μπορούν να ανακτηθούν από Flash μνήμες.

3. ΠΑΡΑΡΤΗΜΑΤΑ

Τα παραρτήματα που περιέχονται είναι:

3.1 Παράρτημα Α:

Παρουσιάζονται οι Κατηγορίες Προσωπικών Δεδομένων όπως προκύπτουν από τον νόμο. Χωρίζονται σε μη Ευαίσθητα και Ευαίσθητα Προσωπικά Δεδομένα.

3.2 Παράρτημα Β:

Περιέχεται το ερωτηματολόγιο που απαντήθηκε από τους φοιτητές για το ερευνητικό κομμάτι της πτυχιακής.

3.3 Παράρτημα Γ:

Παρουσιάζεται ένα ενδεικτικό φύλλο αποτελεσμάτων ανά δίσκο για ανάλυση δίσκων.

ΠΑΡΑΡΤΗΜΑ Α

Κατηγορίες Προσωπικών Δεδομένων

Προσωπικά Δεδομένα μη Ευαίσθητα:

1. Στοιχεία Αναγνώρισης
    a. Προσωπικά Στοιχεία
    b. Επίσημα στοιχεία Ληξιαρχείου
    c. Καταγωγή
    d. Στοιχεία Ταυτότητας (πχ Υπηκοότητα)
    e. Λοιπά στοιχεία αναγνώρισης
2. Προσωπικά Χαρακτηριστικά
    a. Φυσικά χαρακτηριστικά
    b. Ενδιαφέροντα, συνήθειες
    c. Μετακινήσεις – Ταξίδια
    d. Στοιχεία προσωπικότητας
    e. Λοιπά στοιχεία προσωπικών χαρακτηριστικών
3. Οικογενειακές συνθήκες
    a. Έγγαμος βίος
    b. Οικογενειακή κατάσταση
    c. Κοινωνικές επαφές
    d. Λοιπά στοιχεία οικογενειακών συνθηκών
4. Εκπαίδευση
    a. Δεδομένα ακαδημαϊκής δραστηριότητας
    b. Τομείς ειδίκευσης και πιστοποιητικά
    c. Σπουδαστικό / Μαθητικό Αρχείο
    d. Εγγραφή σε επιτροπές
    e. Επαγγελματική ειδίκευση
    f. Λοιπά στοιχεία
5. Οικονομική κατάσταση

a. Έσοδα, περιουσιακά στοιχεία, επενδύσεις
b. Απολογισμός εξόδων
c. Δάνεια, υποθήκες, πιστώσεις
d. Επιδόματα, εργασιακά προνόμια, επιχορηγήσεις
e. Δεδομένα ασφάλισης, συντάξεις γήρατος
f. Αγαθά και υπηρεσίες που προσφέρονται στο άτομο
g. Αγαθά και υπηρεσίες που προσφέρει το άτομο
h. Τραπεζικοί Λογαριασμοί, πιστωτικές κάρτες
i. Κληρονομιά
j. Αποζημίωση
k. Λοιπά στοιχεία οικονομικής κατάστασης

6. Εργασία
   a. Παρούσα Εργασία
   b. Δεδομένα Πρόσληψης
   c. Ιστορικό Εργασίας
   d. Εργασιακή συμπεριφορά
   e. Περιγραφή Εργασίας
   f. Αξιολόγηση εργασίας
   g. Εκπαιδευτικό αρχείο
   h. Δεδομένα ασφαλείας
   i. Αμοιβές και κρατήσεις
   j. Εργασιακές παροχές
   k. Λοιπά στοιχεία εργασίας

Ευαίσθητα προσωπικά δεδομένα:

1. Φυλετική ή Εθνική προέλευση:
    a. Εθνική καταγωγή
    b. Μειονότητες
    c. Φυλετική προέλευση
2. Πολιτικά Φρονήματα:
    a. Δεδομένα πολιτικών πεποιθήσεων
3. Θρησκευτικές Πεποιθήσεις
    a. Δεδομένα θρησκευτικής πίστης
4. Φιλοσοφικές πεποιθήσεις
    a. Δεδομένα φιλοσοφικών πεποιθήσεων
5. Συμμετοχή σε ενώσεις / σωματεία
    a. Επιστημονικά σωματεία
    b. Πολιτιστικοί φορείς
    c. Φιλανθρωπικές οργανώσεις
6. Συνδικαλιστική δράση
    a. Επαγγελματικά σωματεία – Επιμελητήρια
    b. Συνδικαλιστική Δραστηριότητα
7. Υγεία
    a. Φυσική κατάσταση
    b. Πνευματική κατάσταση
    c. Ανικανότητες ή αναπηρίες
    d. Διαιτητικές ή άλλες σχετικές ανάγκες
    e. Ιατρικό ιστορικό ασθενούς
    f. Χορήγηση φαρμάκων
    g. Λοιπά στοιχεία υγείας
8. Κοινωνική πρόνοια (για φορείς με συναφές αντικείμενο)
    a. Ασφάλιση
    b. Σύνταξη
9. Ερωτική ζωή
    a. Σεξουαλική ζωή

10. Ποινικές Διώξεις
    a. Καταγγελίες
    b. Διώξεις
    c. Διοικητικά μέτρα
    d. Διοικητικές ποινές
    e. Παραβιάσεις κώδικα Οδικής Κυκλοφορίας
    f. Δεδομένα Ποινικού Μητρώου
11. Καταδίκες
    a. Αποφάσεις δικαστηρίων
    b. Ποινικό Μητρώο

ΠΑΡΑΡΤΗΜΑ Β

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. Θεωρείτε πως έχετε καλή γνώση ηλεκτρονικών υπολογιστών;

Καθόλου	**Όχι καλή**	**Μέτρια**	**Καλή**	**Πολύ Καλή**
☐	☐	☐	☐	☐

2. Με την απλή διαγραφή ενός αρχείου αυτό εξακολουθεί να παραμένει στο σκληρό δίσκο του υπολογιστή σας;

☐ Ναι ☐ Όχι

3. Σε ποιες ενέργειες υποθέτετε ότι θα προβείτε όταν δεν θα χρειάζεστε πλέον τον σκληρό δίσκο σας:

Α. Θα τον πετούσατε στα σκουπίδια.
Β. Θα κάνατε ανακύκλωση του hardware.
Γ. Θα τον διαθέτατε προς πώληση στο Internet ή αλλού.
Δ. Θα διαγράφατε τα αρχεία με τα πιο ευαίσθητα δεδομένα σας.
Ε. Θα κάνατε format και έπειτα μία από τις επιλογές Α, Β ή Γ.
ΣΤ. Θα κάνετε διαγραφή των αρχείων σας με ειδικά εργαλεία για σβήσιμο σκληρών δίσκων και έπειτα μία από τις επιλογές Α, Β ή Γ.
Ζ. Θα τον κρατούσατε.
Η. Άλλο

Αν απαντήσατε την επιλογή (Η) συμπληρώστε την ενέργεια σας:
……
……
……..

4. Υπάρχει πιθανότητα να ενδιαφερθεί κάποιος για τα δεδομένα του παλιού σας σκληρού δίσκου με κακόβουλο σκοπό;

Καμία	**Αμελητέα**	**Μέτρια**	**Σημαντική**	**Μεγάλη**
☐	☐	☐	☐	☐

5. Αν ενημερωνόσασταν ότι υπάρχει κίνδυνος κακόβουλης χρήσης των δεδομένων αποσυρμένων δίσκων (κλοπή τραπεζικών λογαριασμών, εκβιασμός, απάτη κ.ά.) θα κάνατε κάποια ενέργεια για να προστατεύσετε τα δεδομένα σας;

☐ Ναι ☐ Όχι

6. Έχετε επισκεφτεί ποτέ την ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων (*www.dpa.gr*) για να ενημερωθείτε για τα δικαιώματα σας ως προς την φύλαξη και την επεξεργασία των προσωπικών σας δεδομένων;

☐ Ναι ☐ Όχι

7. Γνωρίζετε ότι η Αρχή Προστασίας Προσωπικών Δεδομένων έχει κοινοποιήσει οδηγία για την ασφαλή καταστροφή των προσωπικών σας δεδομένων μετά το πέρας της επεξεργασίας τους;

☐ Ναι ☐ Όχι

8. Θεωρείτε ότι οι φορείς (π.χ. Τράπεζες, Εταιρείες Τηλεπικοινωνίας, Δημόσιοι Φορείς) που επεξεργάζονται τα προσωπικά σας στοιχεία τηρούν τις οδηγία αυτή;

☐ Ναι ☐ Όχι

ΠΑΡΑΡΤΗΜΑ Γ

Παράδειγμα Φύλλου Ανάλυσης Δίσκου

Λεπτομέρειες από την αντιγραφή των περιεχομένων του Δίσκου (Imaging)

Αριθμος Δισκου			
Ημερομηνια			
Σειριακος Αριθμος Δισκου			
Προελευση δισκου			
Χωρητικοτητα (σε MB/GB)			
Αποτελεσμα Διαδικασιας->	Επιτυχης	Αντιγραφη με λαθη	Αποτυχια αναγνωσης δισκου

Ανάλυση Δίσκου

Εργαλεια / Διαδικασιες που χρησιμοποιηθηκαν:	

Ύπαρξη ονοματος χρηστη / προσωπικων δεδομενων (πχ. Αριθμοι τηλεφωνων)	(επιλεξτε ενα)	ΝΑΙ	ΟΧΙ
Αν ναι, παραθεστε συντομα παραδειγματα:			

Τυπος προηγουμενου ιδιοκτητη	(επιλεξτε ενα η και τα δυο αν ειναι ασαφες)	Εταιρικο	Προσωπικο
Συντομα παραδειγματα:			

Ύπαρξη ημερομηνιων	(επιλεξτε ενα)	ΝΑΙ	ΟΧΙ
Συντομα παραδειγματα:			

Συνέχεια παρακάτω…

Συνέχεια…

Ύπαρξη email	(επιλέξτε ένα)	ΝΑΙ	ΟΧΙ
Σύντομα παραδείγματα:			

Ενέργειες διαγραφής που έχουν γίνει	(επιλέξτε ένα)	ΝΑΙ	ΟΧΙ
	Διαγραφη	Format	Επανεγκατασταση Λειτουργικου
	Μερικη Επικαλυψη	Διαγραφη δεδομενων με χρηση εργαλειου	Άλλο
Αν χρησιμοποιηθηκε εργαλειο διαγραφης, συμπληρωστε ποιο:			

Ύπαρξη πορνογραφικού υλικού	(επιλέξτε ένα)	ΝΑΙ	ΟΧΙ
Αν ΝΑΙ, περιγραφη			

Παρουσία συνθηματικών / Δεδομένα ασφαλείας	(επιλέξτε ένα)	ΝΑΙ	ΟΧΙ
Σύντομα παραδείγματα:			

Δεδομένα δικτύου	(επιλέξτε ένα)	ΝΑΙ	ΟΧΙ
Σύντομα παραδείγματα:			

Συμπληρωματικές πληροφορίες/ χαρακτηριστικά κλειδια	

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Jones A, Mee V, Meyler C, Gooch J. Analysis of data recovered from computer disks released for resale by organizations. J Inform Warfare 2005

2. Fellows G. The joys of complexity and the deleted file. Digital Investigation 2 (2005)

3. Jones A. and Meyler C. What evidence is left after disk cleaners? Digital Investigation 2(2004)

4. Thomas, P. and Tryfonas, T. (2007), "Hard-drive Disposal and Identity Fraud", in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), paper at the Security and Control of Identity in Society Workshop (SCITS 4), IFIP/SEC 2007, Johannesburg, South Africa, pp. 461-466.

5. Tryfonas, T. Hard-drive Disposal & Identity Fraud Information Security Research Group, *Dept. of Electronics & Computer Systems, Engineering Faculty of Advanced Technology,niversity of Glamorgan, Wales, United Kingdom*

6. Fragkos G., Xynos K., Angelopoulou O., Mee V., An empirical methodology derived from the analysis of information remaining on second hand hard disks, European Conference on Computer Network Defence, University of Glamorgan 2006

7. Information Commissioner's Office (ICO) (2007) Banks in unacceptable data protection breach http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf

8. Jones A, Valli C, Sutherland I, Thomas P. The 2006 analysis of information remaining on disks offered for sale on the second hand market. J Digit Forensics Secur Law 2006;1(3):23-36.

9. "Remembrance of Data Passed: A Study of Disk Sanitization Practices," Simson L. Garfinkel and Abhi Shelat, IEEE Security & Privacy, Jan/Feb 2003, pp. 17-27: http://csdl.computer.org/dl/mags/sp/2003/01/j1017.htm

10. Perlman R. The Ephemerizer: Making Data Disappear for Sun Microsystems (2005)

11. Mee V. An Empirical Methodology derived from the Analysis of Information remaining on second hand hard disks Faculty of Advanced Technology, University of Glamorgan

12. Dawson E. How James Bond would wipe his hard drive for Australian PC Authority (2007) http://www.pcauthority.com.au/print.aspx?CIID=73076&SIID=10

13. Brown J. (2005), Protect yourself against the identity theft epidemic, The Sunday Times, 6th February 2005.

14. P. Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, Proc. Sixth Usenix Security Symp., Usenix Assoc., (1996) www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

15. Forensic science from Wikipedia, http://en.wikipedia.org/wiki/Forensic

16. ΝΟΜΟΣ 2472/1997 ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΤΟΜΟΥ ΑΠΟ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/2472_1997.PDF

17. ΟΔΗΓΙΑ ΑΡ.1/2005 Οδηγία για την ασφαλή καταστροφή προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/1_2005.DOC

18. Villano M., "Hard-Drive Magic: Making Data Disappear Forever," New York Times, 2 May 2002. http://query.nytimes.com/gst/fullpage.html?res=9F07E5DC1531F931A35756C0A9649C8B63

19. Tryfonas T., Thomas P., Owen P. (2006), "ID Theft: Fraudsters' techniques for Personal Data Collection, the Related digital Evidence and Investigation Issues", Information Systems Control Journal, (JOnline) Vol. 1.

20. Valli, C. and Jones, A. (2005). A UK and Australian Study of Hard Disk Disposal, Proceedings of the 3rd Australian Computer, Network and Information Forensics Conference, Edith Cowan University, Perth, 29th September, 2005 http://scissec.scis.ecu.edu.au/conference_proceedings/2005/forensics/valli2.pdf

21. Valli, C. (2004), "Throwing out the Enterprise with the Hard Disk", In *Proceedings of 2nd Australian Computer, Information and Network Forensics Conference,* We-BCentre.COM, Fremantle Western Australia. http://scissec.scis.ecu.edu.au/publications/forensics04/Valli-2.pdf

22. Defense (1997). DoD 5220.22-M: National Industrial Security Program Operating Manual, Department of Defense. http://cryptome.org/nispom/nispom.htm

23. Monroe, J. (2003). Forecast: hard disk drives, worldwide, 1999-2008 (executive summary), Gartner. http://www.gartner.com/DisplayDocument?id=492870&ref=g_sitelink

24. Valli, C. and Patak, P. (2005) *An investigation into the efficiency of forensic erasure tools for hard disk mechanisms,* Paper accepted for *3rd Australian Computer, Networks & Information Forensics Conference,* School of Computer and Information Science, Edith Cowan University, Perth, Western Australia http://scissec.scis.ecu.edu.au/conference_proceedings/2005/forensics/valli3.pdf

25. Valli, C. & Woodward, A. (2007). Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks. In Proceedings of the 5th Australian Digital Forensics Conference, School of Computer and, Information Science, Edith Cowan University, Perth, Western Australia 3rd December http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/24%20-Valli%20&%20Woodward%20oops%20they%20did%20it%20again%202007%20HDD%20study.pdf

26. Περιοδικό PC WORLD, «Θησαυροί μέσα στα σκουπίδια» 13-12-2005, http://www.pcw.gr/default.php?pid=6&art_id=1016

27. ΕΛΕΥΘΕΡΟΤΥΠΙΑ, Φύλλο Παρασκευής 10/08/2007 «Προσωπικά δεδομένα στα σκουπίδια» http://www.enet.gr/online/online_text/c=112,dt=10.08.2007,id=70113064

28. ΚΑΘΗΜΕΡΙΝΗ, Φύλλο Παρασκευής 13/04/2007 «Πρόστιμα για τα προσωπικά δεδομένα στα σκουπίδια» http://news.kathimerini.gr/4dcgi/_w_articles_economyepix_1_13/04/2007_223093

29. ΕΛΕΥΘΕΡΟΤΥΠΙΑ, Φύλλο Παρασκευής 13/04/2007 «ΠΡΟΣΤΙΜΑ ΑΠΟ ΤΗΝ ΑΡΧΗ Στα σκουπίδια ευαίσθητα προσωπικά δεδομένα» http://www.enet.gr/online/online_text/c=112,dt=13.04.2007,id=19349636

30. Περιοδικό Computer act!ve, «Κλεμμένη ταυτότητα!», 27/04/2007 http://www.computeractive.gr/default.php?pid=6&art_id=2278&nologin=1

31. ΠΡΩΤΟ ΘΕΜΑ, 13/12/2007, «Προσωπικά δεδομένα στα σκουπίδια», της Χρυσάνθης Λαμπροπούλου, http://www.prototothema.gr/content.php?id=544

32. Altheide C. (2004), Forensic analysis of Windows hosts using UNIX-based tools, Digital Investigation, 2004 – Elsevier