Corfu

Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών: Απόκτηση Αποδεικτικών Στοιχείων από Συστήματα Υπολογιστών

Dr. Stylianos Karagiannis (PhD)
Ionian University, Corfu, Greece

NMS.LAB

IONIAN UNIVERSITY

DEPARTMENT OF INFORMATICS
IONIAN UNIVERSITY

</> Stylianos Karagiannis

Corfu, Kozani, Greece Lisbon, Portugal

PhD in Cybersecurity - Post Doc @ Ionian University Department of Informatics, Corfu, Greece
Senior Researcher @ PDMFC, Lisbon, Portugal

Research Interests: Cybersecurity, Privacy, Capture The Flag (CTF) Challenges, Cyber Ranges
Gamification, Incident Handling, Virtual Labs, Game-Based Learning
Social Constructivism, Learning Theories

Email: skaragiannis@ionio.gr, LinkedIn, NMSLab

Συστήματα Υπολογιστών ως Στόχοι

Τα συστήματα υπολογιστών συχνά γίνονται στόχοι κακόβουλων ενεργειών. Μπορούν να χρησιμοποιηθούν ως αρχικός στόχος για πρόσβαση στο δίκτυο ή ως σημείο αναπήδησης (pivot point) για περαιτέρω επιθέσεις. Επίσης, μπορούν να είναι ο τελικός στόχος των επιτιθέμενων.

- **Απόκριση σε Περιστατικά:** Οι αναλυτές απόκρισης σε περιστατικά πρέπει να είναι έτοιμοι να διερευνήσουν τα συστήματα. Κάθε αλλαγή σε αρχεία, εφαρμογές ή λογαριασμούς χρηστών αφήνει ίχνη που μπορούν να αξιολογηθούν.
- **Όγκος Δεδομένων:** Τα σύγχρονα λειτουργικά συστήματα, όπως τα Windows, παρέχουν μεγάλο όγκο δεδομένων. Η αυξανόμενη μνήμη και αποθήκευση σε terabytes καθιστούν διαθέσιμα περισσότερα αποδεικτικά στοιχεία για ανάλυση περιστατικών.
- **Συλλογή Αποδεικτικών Στοιχείων:** Οι αναλυτές πρέπει να είναι έτοιμοι να συλλέξουν διαφορετικούς τύπους στοιχείων από τα συστήματα, προκειμένου να εντοπίσουν την αιτία ενός περιστατικού και να υποστηρίξουν τη διερεύνηση.

Προετοιμασία Αναλυτών

Οι αναλυτές απόκρισης σε περιστατικά πρέπει να διαθέτουν τα απαραίτητα εργαλεία για την απόκτηση αποδεικτικών στοιχείων. Τα εργαλεία αυτά πρέπει να προέρχονται από αξιόπιστες πηγές, να έχουν δοκιμαστεί και να επικυρωθούν πριν από τη χρήση.

- **Εξοπλισμός:** Πέρα από το λογισμικό, απαιτούνται εξωτερικοί σκληροί δίσκοι και επιτραπέζιοι υπολογιστές. Σε εταιρικό περιβάλλον, οι αναλυτές πρέπει να γνωρίζουν τα συνήθη λειτουργικά συστήματα, π.χ. Microsoft ή Linux, ώστε να διαθέτουν τα κατάλληλα εργαλεία.
- **Δικαιώματα και Διαπιστευτήρια:** Πολλά εργαλεία απαιτούν δικαιώματα διαχειριστή. Πρέπει να χρησιμοποιούνται μόνο υπάρχοντες λογαριασμοί, για να διασφαλιστεί η αποδεκτότητα των στοιχείων σε δικαστικές διαδικασίες.
- **Ατομικά Διαπιστευτήρια:** Μια καλή πρακτική είναι η χρήση ειδικών διαπιστευτηρίων που ενεργοποιούνται μόνο κατά τη διάρκεια περιστατικού. Αυτό διαχωρίζει τη νόμιμη από κακόβουλη χρήση και αποτρέπει την αποκάλυψη της ταυτότητας των αναλυτών.

Σειρά Πτητικότητας (Order of Volatility)

Δεν έχουν όλα τα αποδεικτικά στοιχεία την ίδια αξία. Η πτητικότητα (volatility) δείχνει πόσο διατηρούνται τα δεδομένα μετά από ενέργειες όπως αποσύνδεση ή τερματισμό λειτουργίας.

- **Πτητικά Δεδομένα:** Χάνονται αν το σύστημα απενεργοποιηθεί. Περιλαμβάνουν δεδομένα CPU, πίνακες δρομολόγησης, ARP cache και κυρίως τη μνήμη RAM. Η RAM περιέχει κρίσιμα ίχνη κακόβουλου λογισμικού, όπως ιστορικό εντολών και δικτυακές συνδέσεις.
- **Μη Πτητικά Δεδομένα:** Διατηρούνται στον σκληρό δίσκο μετά τον τερματισμό. Περιλαμβάνουν το MFT, δεδομένα μητρώου και αρχεία. Παρέχουν σημαντικές αποδείξεις ακόμη και αν η μνήμη χάθηκε.
- **Συμπέρασμα:** Η σειρά απόκτησης αποδεικτικών στοιχείων πρέπει να λαμβάνει υπόψη την πτητικότητα, δίνοντας προτεραιότητα στα πιο εύθραυστα στοιχεία.

Απόκτηση Αποδεικτικών Στοιχείων (Evidence Acquisition)

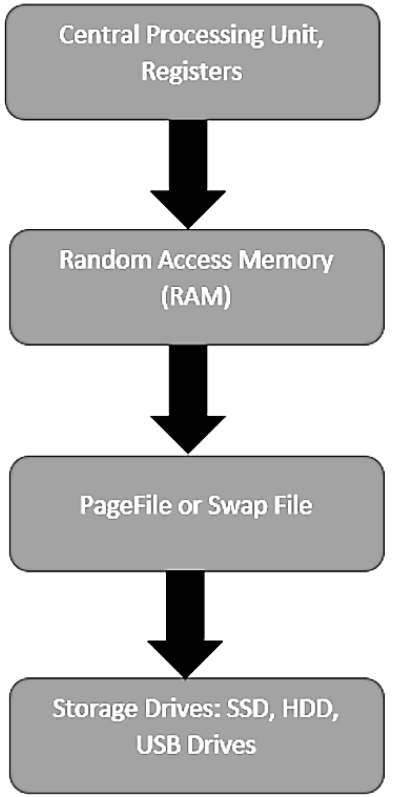
- **Τοπική Απόκτηση (Local):** Πρόσβαση στο σύστημα επιτόπου, όπου οι αναλυτές μπορούν να συλλέξουν δεδομένα άμεσα. Αποτελεί την ιδανική περίπτωση, αλλά δεν είναι πάντα διαθέσιμη.
- **Απομακρυσμένη Απόκτηση (Remote):** Χρησιμοποιούνται εργαλεία και δικτυακές συνδέσεις για συλλογή στοιχείων από απόσταση. Ιδανική όταν υπάρχουν γεωγραφικοί περιορισμοί ή αδυναμία φυσικής πρόσβασης.
- **Ζωντανή Απόκτηση (Live acquisition):** Συλλογή δεδομένων από ενεργό σύστημα. Απαραίτητη για RAM και άλλα πτητικά στοιχεία, καθώς και σε περιβάλλοντα υψηλής διαθεσιμότητας.
- **Εκτός Σύνδεσης (Offline acquisition):** Συλλογή από απενεργοποιημένο σύστημα. Χρησιμοποιείται για σκληρούς δίσκους, αλλά χάνει πτητικά δεδομένα και μπορεί να προκαλέσει καθυστερήσεις >24 ώρες.

Πρακτική Συμβουλή: Συνιστάται εξωτερικός σκληρός δίσκος ή USB με δύο κατατμήσεις: εργαλεία απόκτησης και αποθήκευση αποδεικτικών στοιχείων, για διασφάλιση ακεραιότητας και εύκολη μεταφορά.

Διαδικασίες Συλλογής Αποδεικτικών Στοιχείων

Η ψηφιακή εγκληματολογία ακολουθεί ορθές και τεκμηριωμένες διαδικασίες όπως και άλλες εγκληματολογικές επιστήμες. Οι οργανισμοί πρέπει να εφαρμόζουν επαναλήψιμες πρακτικές για τη συλλογή αποδεικτικών στοιχείων.

- **Φωτογράφιση Συστήματος και Σκηνής:** Η χρήση ψηφιακής κάμερας επιτρέπει την ανακατασκευή γεγονότων σε δικαστικές διαδικασίες. Αποφεύγεται η χρήση κινητών, καθώς ενδέχεται να απαιτηθεί κατάσχεση.
- **Έλεγχος Κατάστασης Συστήματος:** Τα ενεργά συστήματα παραμένουν ενεργά και τα απενεργοποιημένα δεν ενεργοποιούνται. Η αλλαγή κατάστασης μπορεί να αλλοιώσει δεδομένα, ειδικά σε κρυπτογραφημένους δίσκους.
- **Απόκτηση Μνήμης RAM:** Η μνήμη RAM περιέχει κρίσιμες πληροφορίες για διεργασίες, DLLs και δικτυακές συνδέσεις. Η απόκτησή της είναι σημαντική για την ανάλυση κακόβουλου λογισμικού.
- **Απόκτηση Αρχείων Μητρώου και Logs:** Παρέχουν ιστορικό δραστηριοτήτων και βοηθούν στην έρευνα αλλαγών και κακόβουλων ενεργειών. Η άμεση πρόσβαση αυξάνει την αποτελεσματικότητα της ανάλυσης.
- **Αποσύνδεση Παροχής Ρεύματος:** Σε φορητούς υπολογιστές αφαιρείται η μπαταρία, ενώ φωτογραφίζεται το πίσω μέρος με μοντέλο και σειριακό αριθμό για τεκμηρίωση.
- **Φωτογράφιση Σκληρού Δίσκου:** Φωτογραφίζεται το μοντέλο και ο σειριακός αριθμός πριν από οποιαδήποτε αφαίρεση, ώστε να διασφαλίζεται η ακεραιότητα των στοιχείων.
- **Αφαίρεση Σκληρού Δίσκου:** Ο δίσκος τοποθετείται σε αντιστατικό σακουλάκι και σφραγισμένο φάκελο/κουτί. Καταγράφονται αριθμός περιστατικού, αποδεικτικού, ημερομηνία, ώρα και υπεύθυνος.
- **Τεκμηρίωση Ενεργειών:** Καταγράφονται ημερομηνίες, ώρες και υπεύθυνοι για κάθε ενέργεια. Σημειώσεις και φωτογραφίες υποστηρίζουν την ανακατασκευή γεγονότων.



Απόκτηση Πτητικής Μνήμης (Acquiring Volatile Memory)

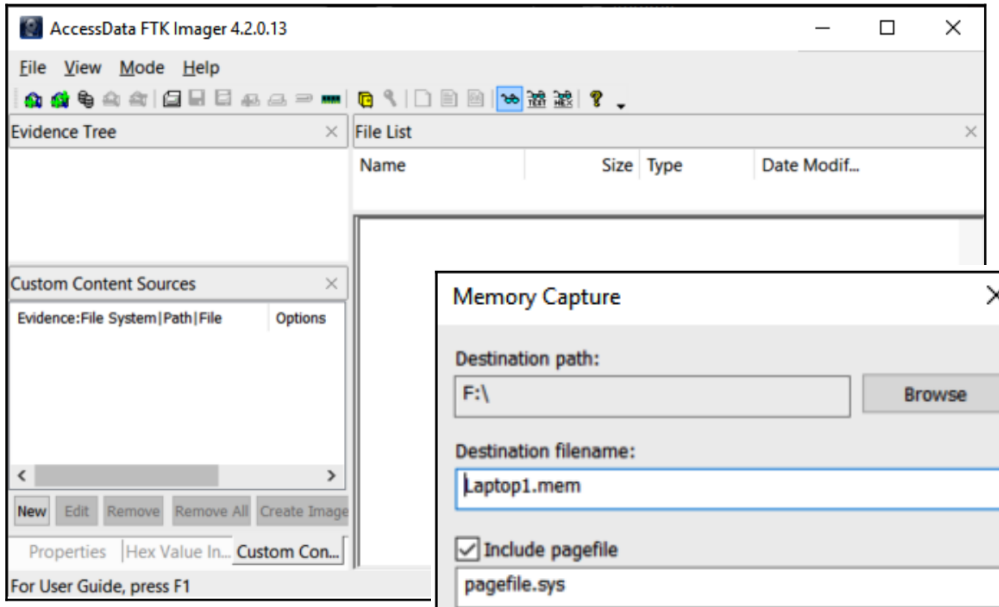
Η παραδοσιακή ψηφιακή εγκληματολογία επικεντρώνεται στον σκληρό δίσκο απενεργοποιημένων συστημάτων. Αυτό καταστρέφει ό,τι υπήρχε στη μνήμη RAM, περιορίζοντας την ανάλυση σε αρχεία εικόνας, έγγραφα ή υπολογιστικά φύλλα.

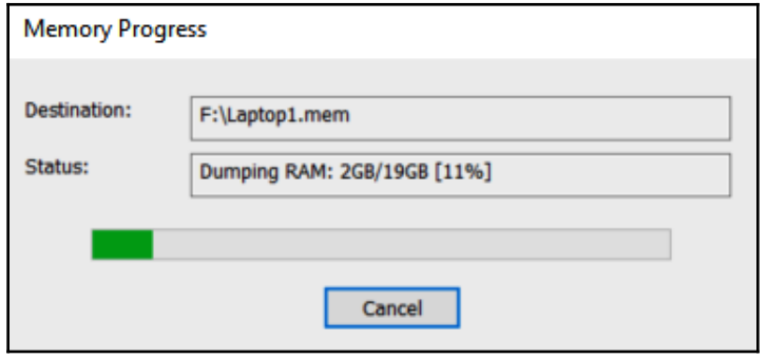
- **Σημασία Πτητικής Μνήμης:** Σε περιστατικά ασφάλειας, η RAM περιέχει κρίσιμα ίχνη κακόβουλου λογισμικού ή εκμετάλλευσης. Η απόκτηση της μνήμης πριν τον τερματισμό του συστήματος είναι απαραίτητη για πλήρη ανάλυση των συμβάντων.
- **Εργαλεία Ανάλυσης Μνήμης:** Υπάρχουν δωρεάν και εμπορικά εργαλεία για την απόκτηση και ανάλυση της μνήμης. Δημοφιλή πλαίσια είναι τα **Rekall** και **Volatility**, που επιτρέπουν λεπτομερή έλεγχο των διεργασιών και συνδέσεων.
- **Τρόποι Απόκτησης Μνήμης:** Η μνήμη μπορεί να αποκτηθεί τοπικά με USB ή άλλο μέσο συνδεδεμένο στο σύστημα, ή απομακρυσμένα μέσω εξειδικευμένου λογισμικού που λειτουργεί μέσω δικτύου.
- **Τοπική Απόκτηση:** Σε φυσική πρόσβαση, η μνήμη και άλλα δεδομένα αποκτώνται με εργαλεία από αφαιρούμενο μέσο. Συχνά συνοδεύεται από κατάσχεση του σκληρού δίσκου. Δημοφιλή εργαλεία: **FTK Imager**, **WinPmem**, **RamCapturer**.
- **Κατάτμηση Εξωτερικού Δίσκου:** Συνιστάται δύο κατατμήσεις: μία για εργαλεία απόκτησης και μία για τα αποδεικτικά αρχεία. Αυτό διασφαλίζει ότι τα εργαλεία δεν αναμειγνύονται με τα στοιχεία απόκρισης.

FTK Imager (AccessData)

Το FTK Imager είναι λογισμικό Windows για απεικόνιση (imaging) και απόκτηση μνήμης συστήματος. Υποστηρίζει τη λήψη της τρέχουσας μνήμης και δημιουργία αρχείων εικόνας για περαιτέρω ανάλυση. Το λογισμικό διατίθεται δωρεάν από την AccessData.

- **Εκκίνηση Εργαλείου:** Μετά τη λήψη, το εκτελέσιμο τοποθετείται στην κατάτμηση Tools του USB και εκτελείται ως διαχειριστής. Απαιτούνται δικαιώματα για χρήση των drivers και πρόσβαση στη μνήμη RAM.
- **Capture Memory:** Στο παράθυρο Capture Memory καθορίζεται η διαδρομή αποθήκευσης, η επιλογή συμπερίληψης pagefile και η μορφή αρχείου (AD1 ή .mem). Πατώντας Capture Memory ξεκινά η διαδικασία απόκτησης.
- **Ολοκλήρωση και Ανάλυση:** Όταν τελειώσει η καταγραφή, δημιουργείται το αρχείο εικόνας μνήμης. Μπορεί να χρησιμοποιηθεί για ανάλυση με εργαλεία όπως Rekall ή Volatility, διατηρώντας κρίσιμα αποδεικτικά στοιχεία.
- **Τεκμηρίωση:** Καταγράφονται η ημερομηνία, ώρα, διαδρομή αποθήκευσης και τυχόν πρόσθετες επιλογές (π.χ. pagefile). Αυτό διασφαλίζει αναπαραγωγιμότητα και ακεραιότητα στη διαδικασία chain of custody.





WinPmem

Το WinPmem είναι εργαλείο απόκτησης μνήμης για Windows, σχεδιασμένο από την ομάδα Rekall. Υποστηρίζει ακατέργαστη μνήμη (raw memory) και είναι συμβατό με Linux και macOS. Η επιλογή εργαλείου εξαρτάται από τα εργαλεία ανάλυσης μνήμης που θα χρησιμοποιηθούν.

- **Μορφή Αρχείου:** Από την έκδοση 2.0.1, η προεπιλεγμένη μορφή είναι AFF4, η οποία οργανώνει πολλαπλές πηγές δεδομένων και ροές εργασίας. Το AFF4 είναι ανοιχτού κώδικα και χρησιμοποιείται για αποδεικτικά στοιχεία στην ψηφιακή εγκληματολογία.
- **Απόκτηση Μνήμης:** Για λήψη μνήμης, ανοίγεται το Command Prompt ως διαχειριστής και εκτελείται η εντολή WinPmem. Η μνήμη αποθηκεύεται στο evidence partition του USB drive σε raw format ή AFF4 container, περιλαμβάνοντας ολόκληρη τη φυσική μνήμη του συστήματος.
- **Μετατροπή σε RAW:** Αν απαιτείται ανάλυση με Volatility, το αρχείο AFF4 πρέπει να μετατραπεί σε raw image. Η μετατροπή γίνεται με εντολή WinPmem που εξάγει την PhysicalMemory από το AFF4 σε raw αρχείο, έτοιμο για ανάλυση.
  - D:\winpmem-2.1.exe D:\Laptop1.aff4 -e PhysicalMemory -o Laptop1.raw

```
D:\>winpmem-2.1.exe --format raw -o e:\Laptop1
Driver Unloaded.
CR3: 0x00001AA000
 7 memory ranges:
Start 0x00001000 - Length 0x0009C000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xBE2FE000
Start 0xBE889000 - Length 0x1BD7E000
Start 0xDA770000 - Length 0x00775000
Start 0xDBAFF000 - Length 0x00001000
Start 0x100000000 - Length 0x31E800000
```

```
Creating output AFF4 Directory structure.
Dumping Range 0 (Starts at 1000, length 9c000)
Dumping Range 1 (Starts at 100000, length 2000)
Dumping Range 2 (Starts at 103000, length be2fe000)
Dumping Range 3 (Starts at be889000, length 1bd7e000)
Dumping Range 4 (Starts at da770000, length 775000)
Dumping Range 5 (Starts at dbaff000, length 1000)
Dumping Range 6 (Starts at 100000000, length 31e800000)
 Reading 0x8000  0MiB / 16272MiB 0MiB/s
 Reading 0x4398000  67MiB / 16272MiB 255MiB/s
 Reading 0x89b0000  137MiB / 16272MiB 275MiB/s
```

Απομακρυσμένη Απόκτηση

Πλεονεκτήματα & Περιορισμοί: Η προτιμώμενη μέθοδος είναι η άμεση επαφή με το ύποπτο σύστημα, καθώς είναι ταχύτερη και πιο αξιόπιστη. Ωστόσο, γεωγραφικοί περιορισμοί μπορούν να κάνουν την απομακρυσμένη απόκτηση αναγκαία σε μεγάλους οργανισμούς.

Εργαλεία & Διαδικασία: Οι αναλυτές χρησιμοποιούν τα ίδια εργαλεία όπως στην τοπική απόκτηση, αλλά απαιτείται απομακρυσμένη τεχνολογία για πρόσβαση στο σύστημα. Η χρήση πρέπει να καταγράφεται για τη διασφάλιση της αλυσίδας γεγονότων και των νόμιμων συνδέσεων.

WinPmem Remote: Το WinPmem μπορεί να εγκατασταθεί σε απομακρυσμένα συστήματα μέσω PsExec ή Remote Desktop. Η έξοδος μπορεί να σταλεί (piped) σε άλλο σύστημα χρησιμοποιώντας NetCat, διασφαλίζοντας συλλογή μνήμης χωρίς φυσική παρουσία.

Παράδειγμα: Η εντολή **C:/winpmem-2.1.exe - | nc 192.168.0.56 4455** εκτελεί τη συλλογή μνήμης στο απομακρυσμένο σύστημα και τη στέλνει στον σταθμό εργασίας του αναλυτή. Μειονέκτημα: απαιτεί εγκατάσταση εργαλείων και πρόσβαση στη γραμμή εντολών.

Εικονικές Μηχανές (Virtual Machines)

Πλεονέκτημα Εικονικών Συστημάτων: Οι αναλυτές μπορούν να διατηρήσουν την τρέχουσα κατάσταση του συστήματος με snapshot ή παύση. Η αντιγραφή ολόκληρου του αρχείου σε USB επιτρέπει μετέπειτα ανάλυση χωρίς να αλλοιωθεί το περιβάλλον.

Ακεραιότητα Δεδομένων: Συνιστάται υπολογισμός hash για κάθε αρχείο πριν και μετά την αντιγραφή, διασφαλίζοντας ότι τα αποδεικτικά στοιχεία παραμένουν ανέπαφα.

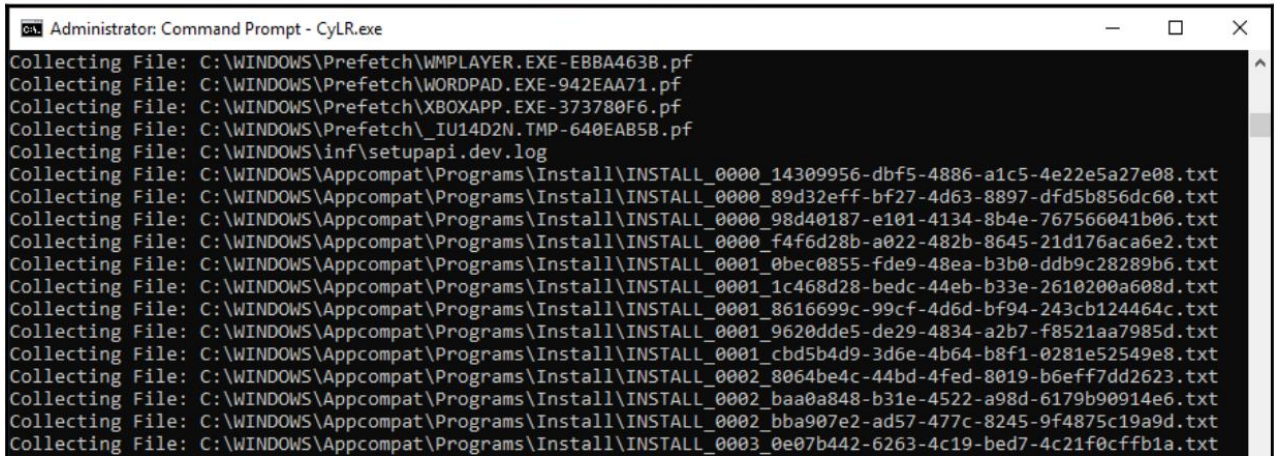
Αρχεία Μνήμης VMware: Η μνήμη της εικονικής μηχανής αποθηκεύεται σε VMEM (RAM) και VMSS (suspended state). Η σωστή διαχείριση αυτών των αρχείων είναι απαραίτητη για πλήρη ανάλυση.

Δημιουργία Αρχείου Ανάλυσης: Μεταφορά των VMEM και VMSS σε USB και χρήση του εργαλείου Vmss2Core.exe για συγχώνευση σε .dmp αρχείο. Εντολή: C:\Program Files (x86)\VMware\VMware Workstation>vmss2core.exe suspect.vmss suspect.vmem

Με αυτόν τον τρόπο δημιουργείται το απαραίτητο .dmp αρχείο για περαιτέρω ανάλυση.

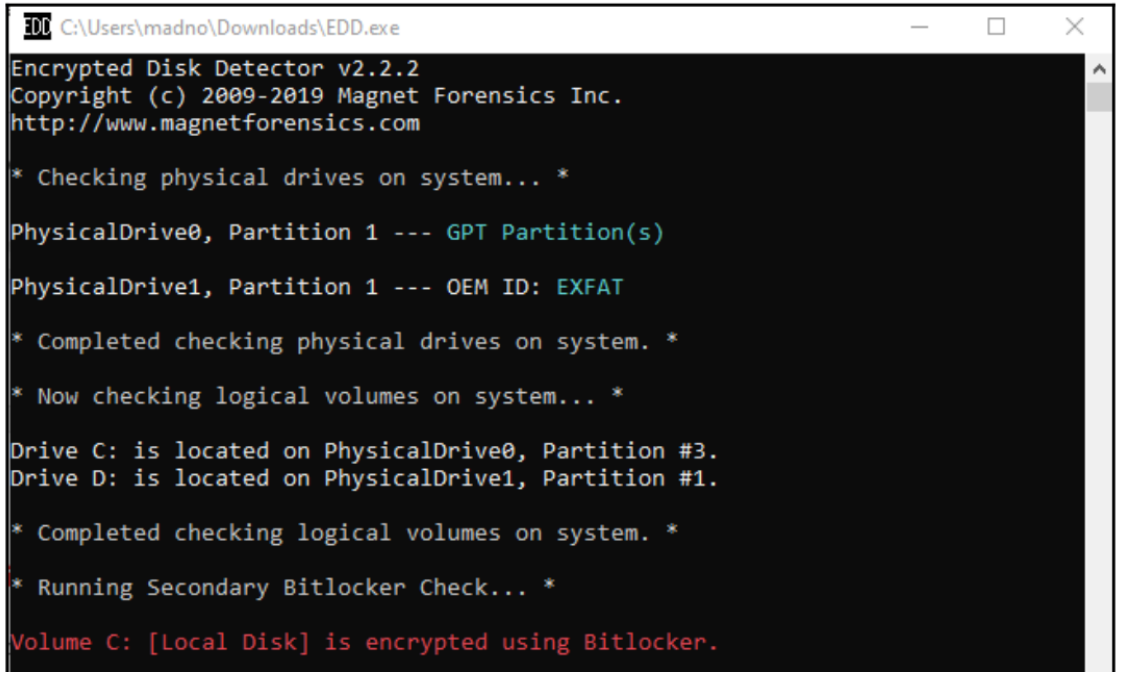
Απόκτηση Μη Πτητικών Δεδομένων

- **Σημασία Σκληρού Δίσκου:** Η απόκτηση δεδομένων από τον σκληρό δίσκο είναι κρίσιμη για την ανάλυση περιστατικών όπως κακόβουλες ενέργειες ή απώλεια δεδομένων. Περιέχει πλούσιο αποδεικτικό υλικό που πρέπει να συλλεχθεί με σωστές διαδικασίες για να είναι αποδεκτό σε δικαστήριο.
- **Registry & Event Logs:** Πριν το κλείσιμο του συστήματος, συνιστάται η εξαγωγή registry keys και event logs, καθώς παρέχουν κρίσιμα στοιχεία για την ανάλυση. Η εντολή wevtutil epl <Log Type> E:\<FileName>.evtx εξάγει τα security, application και system logs.
- **FTK Imager:** Το εργαλείο επιτρέπει απόκτηση registry key settings και προστατευμένων αρχείων, όπως user, system, SAM, NTUSER.DAT. Με κατάλληλη αποθήκευση σε USB, η ανάλυση μπορεί να ξεκινήσει πριν ολοκληρωθεί το πλήρες imaging.
- **CyLR.exe:** Εργαλείο ανοικτού κώδικα που συλλέγει log files, registry και MFT, αποθηκεύοντας τα σε συμπιεσμένο αρχείο. Μπορεί να εκτελεστεί από USB ή απομακρυσμένα, επιτρέποντας γρήγορη προτεραιοποίηση και ασφαλή συλλογή αποδεικτικών στοιχείων.



Έλεγχος για Κρυπτογράφηση (Encryption Check)

- **Ανίχνευση Κρυπτογράφησης:** Οι αναλυτές πρέπει να ελέγχουν για πλήρη κρυπτογράφηση δίσκου (FDE) σε συστήματα Windows, όπως BitLocker, ή εργαλεία όπως VeraCrypt για κρυπτογράφηση αρχείων ή ολόκληρων τόμων.
- **Εργαλεία Ελέγχου:** Το Endpoint Disk Detector της Magnet Forensics εντοπίζει κρυπτογραφημένους τόμους και πληροφορεί για τον τύπο κρυπτογράφησης. Αρκεί η εκτέλεση του εργαλείου ως διαχειριστής για να εμφανιστούν τα αποτελέσματα.
- **Διαχείριση Κλειδιού Κρυπτογράφησης:** Σε περίπτωση BitLocker, ο αναλυτής πρέπει να διασφαλίσει ότι το αντίστοιχο κλειδί είναι διαθέσιμο. Αν δεν είναι, η απόκτηση των λογικών τόμων πρέπει να γίνει όσο το σύστημα είναι ενεργό.
- **Αξιοπιστία Αποδεικτικών Στοιχείων:** Η ορθή εφαρμογή τεχνικών και η τεκμηρίωση των ενεργειών εξασφαλίζουν την εγκυρότητα του υλικού, επιτρέποντας τόσο την ανάλυση της ρίζας του περιστατικού όσο και τη στήριξη σε δικαστικές διαδικασίες.



Εγκληματολογική Εικόνα (Forensic Imaging)

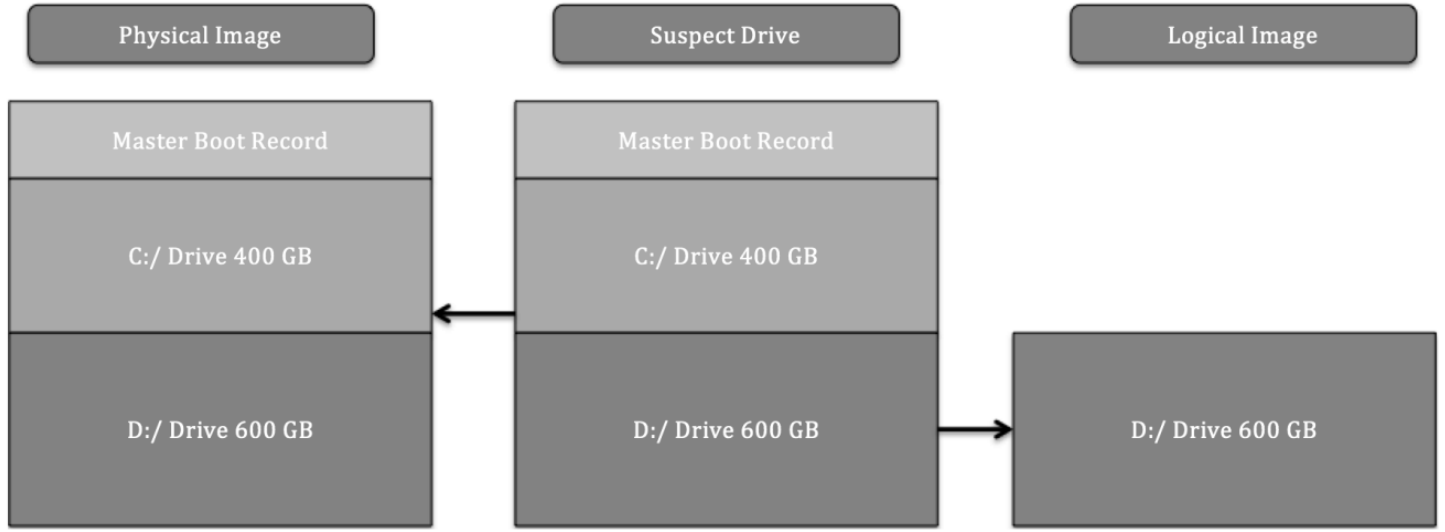
- **Σημασία της Απεικόνισης:** Η δημιουργία εγκληματολογικής εικόνας (imaging) επιτρέπει στους αναλυτές να διατηρούν αποδεικτικά στοιχεία όπως logs, μνήμη και δεδομένα χρήστη, διασφαλίζοντας την ακεραιότητά τους για ανάλυση και δικαστική χρήση.
- **Περιπτώσεις Λεπτομερούς Έρευνας:** Σε περιστατικά όπως απάτη, διαρροή δεδομένων ή βιομηχανική κατασκοπεία, απαιτείται λεπτομερής απόκτηση του δίσκου, περιλαμβάνοντας MFT, αρχεία και συγκεκριμένα δεδομένα χρήστη.
- **Βασικές Αρχές & Προετοιμασία:** Η εγκληματολογική εικόνα απαιτεί κατάλληλα εργαλεία, τεχνικές και τεκμηρίωση. Η προετοιμασία περιλαμβάνει κατανόηση διαδικασίας απεικόνισης, χρήση καθαρών stage drives και write blockers για προστασία των δεδομένων.
- **Εργαλεία & Τεχνικές:** Η επιλογή εργαλείων και τεχνικών απεικόνισης εξαρτάται από το περιστατικό και τη συσκευή. Υπάρχουν υλικοί και λογισμικοί αποκλειστές εγγραφής, ενώ η διαδικασία διασφαλίζει ότι η εικόνα είναι αξιόπιστη για ανάλυση και πιθανή χρήση σε δικαστήριο.

Εγκληματολογική Απεικόνιση (Forensic Imaging)

- **Σημασία γνώσης εργαλείων και διαδικασιών:** Η γνώση εργαλείων, τεχνικών και διαδικασιών διασφαλίζει ότι το αποδεικτικό υλικό χειρίζεται σωστά. Οι αναλυτές αποκτούν εμπιστοσύνη στα στοιχεία και μπορούν να συντάξουν ακριβείς αναφορές ή να καταθέσουν στο δικαστήριο.
- **Διαφορά μεταξύ απεικόνισης και αντιγραφής:** Η απλή αντιγραφή αρχείων περιλαμβάνει μόνο τα δεδομένα, ενώ η απεικόνιση καταγράφει ολόκληρο τον δίσκο. Περιλαμβάνονται περιοχές όπως slack space, unallocated space και διαγραμμένα αρχεία, μαζί με μεταδεδομένα για αναλύσεις χρονογραμμής.
- **Cloning vs Imaging:** Το cloning είναι 1:1 αντιγραφή δίσκου και χρησιμοποιείται για λειτουργικά αντίγραφα ασφαλείας. Η απεικόνιση δημιουργεί αρχείο εικόνας για ανάλυση με εγκληματολογικά εργαλεία, περιλαμβάνοντας όλα τα δεδομένα του δίσκου.
- **Τύποι τόμων προς απεικόνιση:** Φυσικοί τόμοι περιλαμβάνουν ολόκληρο τον σκληρό δίσκο και το master boot record. Λογικοί τόμοι αφορούν συγκεκριμένα partitions και καταγράφουν μόνο τα δεδομένα τους, κατάλληλα για ταχεία ή περιορισμένη απεικόνιση.
- **Επιλογή τύπου απεικόνισης:** Ο τύπος του περιστατικού καθορίζει αν απαιτείται φυσική ή λογική εικόνα. Η λογική απόκτηση είναι χρήσιμη σε περιπτώσεις FDE ή όταν θέλουμε να αποτυπώσουμε μόνο συγκεκριμένα αρχεία χωρίς πλήρη δίσκο.

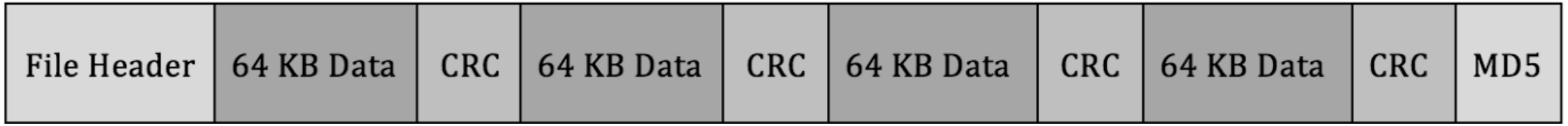
Λογική vs Φυσική Απεικόνιση

- **Πλεονεκτήματα και μειονεκτήματα λογικής εικόνας:** Η λογική εικόνα καταγράφει μόνο τα δεδομένα ενός συγκεκριμένου τόμου ή partition. Δεν περιλαμβάνει μη εκχωρημένα δεδομένα ή διαγραμμένα αρχεία, κάτι που μπορεί να περιορίσει την εγκληματολογική ανάλυση σε υποψίες παραπτωμάτων εργαζομένων.
- **Πλήρης φυσική απεικόνιση:** Η φυσική απεικόνιση καταγράφει ολόκληρο τον δίσκο, συμπεριλαμβανομένων μη εκχωρημένων περιοχών και του master boot record. Χρησιμοποιείται όταν είναι σημαντικό να εντοπιστούν όλα τα ίχνη δραστηριότητας, χωρίς περιορισμούς χρόνου.
- **Ζωντανή απεικόνιση (Live Imaging):** Η ζωντανή απεικόνιση εκτελείται σε ένα σύστημα που λειτουργεί. Είναι χρήσιμη όταν ένα σύστημα δεν μπορεί να απενεργοποιηθεί, όπως σε εξυπηρετητές υψηλής διαθεσιμότητας, και επιτρέπει την απόκτηση λογικών τόμων με πιθανό αποδεικτικό υλικό.
- **Νεκρή απεικόνιση (Dead Imaging):** Η νεκρή απεικόνιση εκτελείται σε απενεργοποιημένο σύστημα με αφαιρεμένο δίσκο. Επιτρέπει την καταγραφή ολόκληρου του δίσκου και όλων των τόμων, διασφαλίζοντας ότι κανένα αποδεικτικό στοιχείο δεν παραμένει ανέλεγκτο.



Τύποι Αρχείων Εικόνας στην Εγκληματολογική Απεικόνιση

- **Ακατέργαστες εικόνες (Raw Images):** Οι ακατέργαστες εικόνες περιέχουν μόνο τα δεδομένα του απεικονισμένου τόμου, χωρίς πρόσθετα μεταδεδομένα. Οι μορφές εξόδου περιλαμβάνουν .raw, .img και .dd, και εργαλεία όπως η εντολή dd στο Linux προσφέρουν ταχύτητα και συμβατότητα με εγκληματολογικά εργαλεία.
- **Αρχεία αποδεικτικών στοιχείων EnCase (E01 / EX01):** Το E01 είναι ιδιόκτητη μορφή αρχείου της OpenText, βασισμένη στο Expert Witness Format (EWF). Περιλαμβάνει μεταδεδομένα για τύπο δίσκου, λειτουργικό σύστημα και χρονικές σημάνσεις. Διαθέτει μηχανισμό CRC που επαληθεύει την ακεραιότητα κάθε 64 KB δεδομένων και hash MD5 στο υποσέλιδο για επιπλέον ασφάλεια. Αυτό το χαρακτηριστικό καθιστά το E01 κατάλληλο για εγκληματολογική ανάλυση και νομικά αποδεκτή τεκμηρίωση.
- **Πλεονεκτήματα του E01:** Το E01 προτιμάται από νομικές και διωκτικές αρχές λόγω της δυνατότητας επαλήθευσης της ακεραιότητας, της υποστήριξης λογισμικού για συμπίεση και της ευρείας συμβατότητας με εργαλεία εγκληματολογικής ανάλυσης.



Εργαλεία Απεικόνισης (Imaging Tools)

Δεν υπάρχει νομική πιστοποίηση για εργαλεία απεικόνισης, αλλά ορισμένα θεωρούνται βέλτιστες πρακτικές. Η επιλογή εξαρτάται από τον οργανισμό, την εμπειρία του αναλυτή και τη συμβατότητα με άλλα εγκληματολογικά εργαλεία.

- **FTK Imager:** Δωρεάν εργαλείο από την Access Data με GUI για λογικούς και φυσικούς τόμους, μνήμη και προστατευμένα αρχεία. Η έκδοση Lite μπορεί να τρέξει από αφαιρούμενο μέσο για ζωντανή απεικόνιση ενεργών συστημάτων.
- **EnCase Imager:** Προσφέρεται από Guidance Software και υποστηρίζει λήψη αποδεικτικών στοιχείων από ποικιλία συστημάτων. Μπορεί να εκτελείται από εξωτερικό δίσκο για ενεργά συστήματα, παρέχοντας παρόμοιες δυνατότητες με το FTK Imager.
- **AFF4 Imager:** Εργαλείο γραμμής εντολών που χρησιμοποιείται για λογικούς και φυσικούς δίσκους, με δυνατότητα απομόνωσης αρχείων κατά χρόνο δημιουργίας. Μειώνει τον χρόνο απεικόνισης και υποστηρίζει συμπίεση.
- **dd (Linux):** Κλασικό εργαλείο Linux για αντιγραφή αρχείων και τόμων, που μπορεί να χρησιμοποιηθεί και για απεικόνιση δίσκων. Συχνά χρησιμοποιείται σε πλατφόρμες εγκληματολογίας βασισμένες σε Linux.
- **Εργαλεία Εικονικοποίησης (Virtualization Tools):** Επιτρέπουν την απόκτηση αποδεικτικών στοιχείων από εικονικά συστήματα. Η απόκτηση μπορεί να γίνει μέσω παύσης του συστήματος, εξαγωγής ολόκληρου φακέλου ή snapshot λειτουργίας.

Πριν την απεικόνιση, διασφαλίζεται ότι το εργαλείο λειτουργεί σωστά, οι αναλυτές είναι εκπαιδευμένοι, και το μέσο προορισμού είναι προετοιμασμένο για την αποθήκευση της εικόνας.

Προετοιμασία Δίσκου Αποθήκευσης (Stage Drive)

Σημασία προετοιμασίας δίσκου: Πριν από μια εγκληματολογική απεικόνιση, είναι κρίσιμο να υπάρχει έτοιμος δίσκος προορισμού για την αποθήκευση της εικόνας. Οι εξωτερικοί δίσκοι USB ή FireWire προσφέρουν φορητότητα και επιτρέπουν τη διερεύνηση περιστατικών εκτός εργαστηρίου.

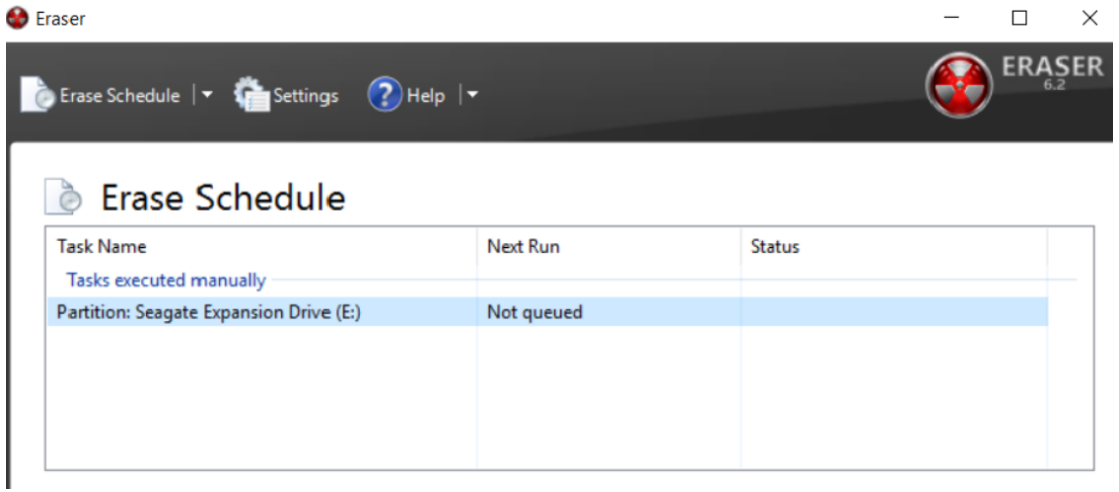
Καθαρισμός δίσκου: Πριν τη χρήση, ο δίσκος πρέπει να είναι κενός και καθαρός. Ακόμη και νέοι δίσκοι μπορεί να περιέχουν προεγκατεστημένα δεδομένα ή λογισμικό, που πρέπει να αφαιρεθούν για να αποφευχθεί επιμόλυνση των αποδεικτικών στοιχείων.

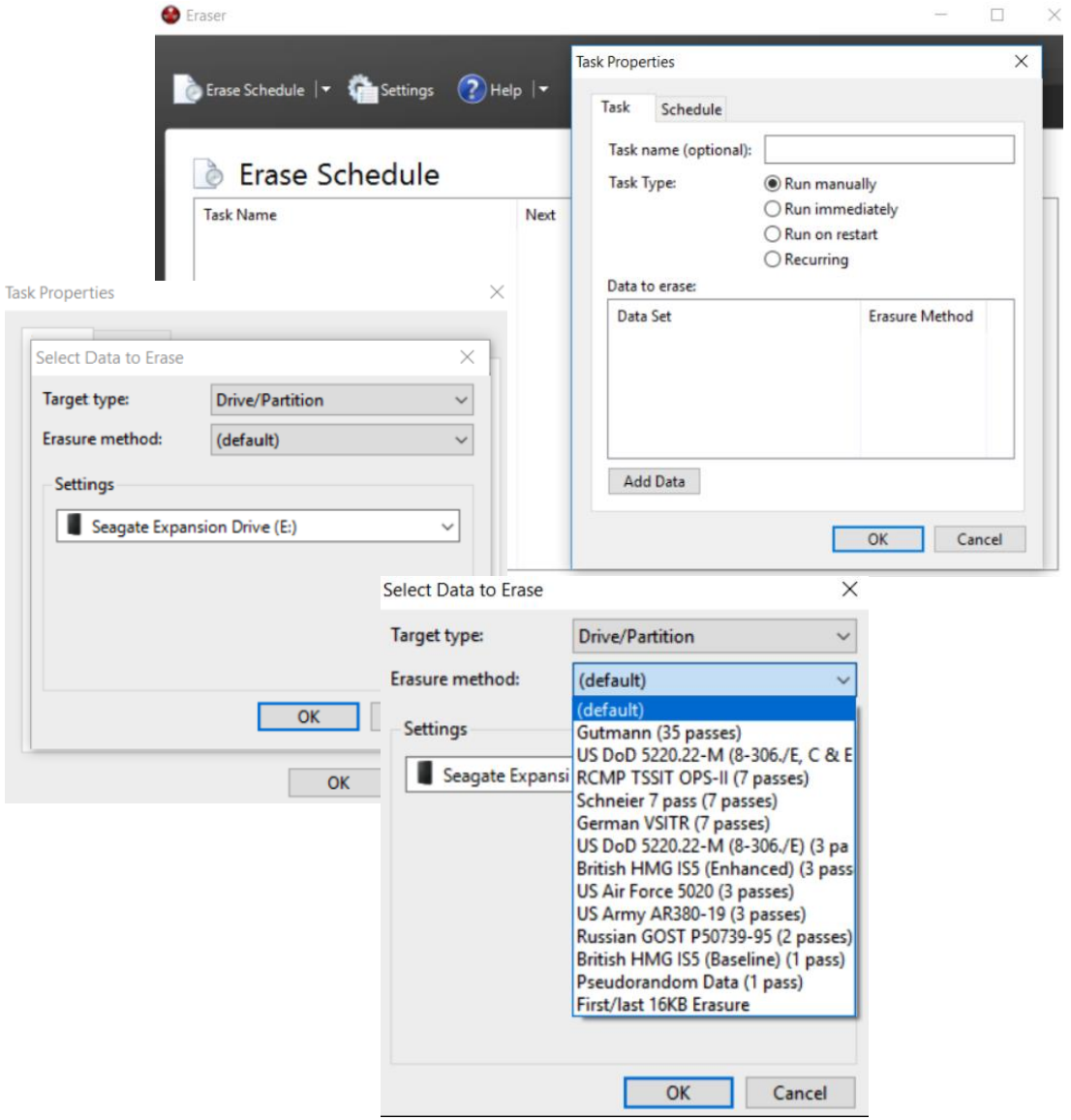
Εργαλεία καθαρισμού: Υπάρχει πληθώρα δωρεάν και εμπορικών εργαλείων για διαγραφή δίσκων. Το πρόγραμμα Eraser (Heidi Computers) υποστηρίζει καθαρισμό αρχείων και ολόκληρων τόμων, εφαρμόζοντας πρότυπα ασφαλούς διαγραφής όπως το US DoD 5220.22-M (3 pass).

Eraser

Βασικά βήματα διαγραφής με Eraser

1. Εκκίνηση Eraser και δημιουργία νέας εργασίας (New Task).
2. Ορισμός ονόματος έργου και προσθήκη δίσκου στόχου (Target type: Drive/Partition).
3. Επιλογή σωστού δίσκου και μεθόδου διαγραφής (π.χ. US DoD 3 Pass).
4. Προγραμματισμός ή άμεση εκτέλεση της εργασίας (Run Now) για ασφαλή καθαρισμό.





Προετοιμασία Δίσκου Αποθήκευσης (Stage Drive)

- **Καταγραφή ολοκλήρωσης καθαρισμού:** Η διαδικασία καθαρισμού δίσκου μπορεί να διαρκέσει ώρες ή ημέρες ανάλογα με το μέγεθος και το σύστημα. Ο αναλυτής πρέπει να καταγράψει στοιχεία που αποδεικνύουν ότι ο δίσκος καθαρίστηκε σωστά, για ένταξη σε εγκληματολογική αναφορά.
- **Διαθεσιμότητα προ-καθαρισμένων δίσκων:** Συνιστάται οι αναλυτές να έχουν αρκετούς καθαρισμένους δίσκους πριν από περιστατικά, ώστε να χρησιμοποιούνται άμεσα και να μην χάνεται χρόνος που είναι κρίσιμος για τη διερεύνηση.
- **Κρυπτογράφηση δίσκου:** Η κρυπτογράφηση του δίσκου αποδεικτικών στοιχείων προστατεύει ευαίσθητες πληροφορίες (π.χ. πιστωτικές κάρτες, ιατρικά δεδομένα). Μπορεί να γίνει με λογισμικό όπως VeraCrypt είτε στον δίσκο είτε στον εγκληματολογικό σταθμό εργασίας.
- **Μέθοδοι κρυπτογράφησης:** Λογισμικό στον σταθμό εργασίας για δίσκους που αφαιρούνται.
- Εγκατάσταση λογισμικού απευθείας στον δίσκο, χωρισμένο σε κατάτμηση εργαλείων και κατάτμηση αποδεικτικών στοιχείων, για ελάχιστες αλλαγές στο σύστημα.
- **Επόμενο βήμα: Write Blockers:** Μόλις ο δίσκος προετοιμαστεί, απαιτείται χρήση write blockers για να διασφαλιστεί ότι δεν θα γίνουν αλλαγές στο ύποπτο σύστημα κατά την απεικόνιση.

Χρήση Write Blockers

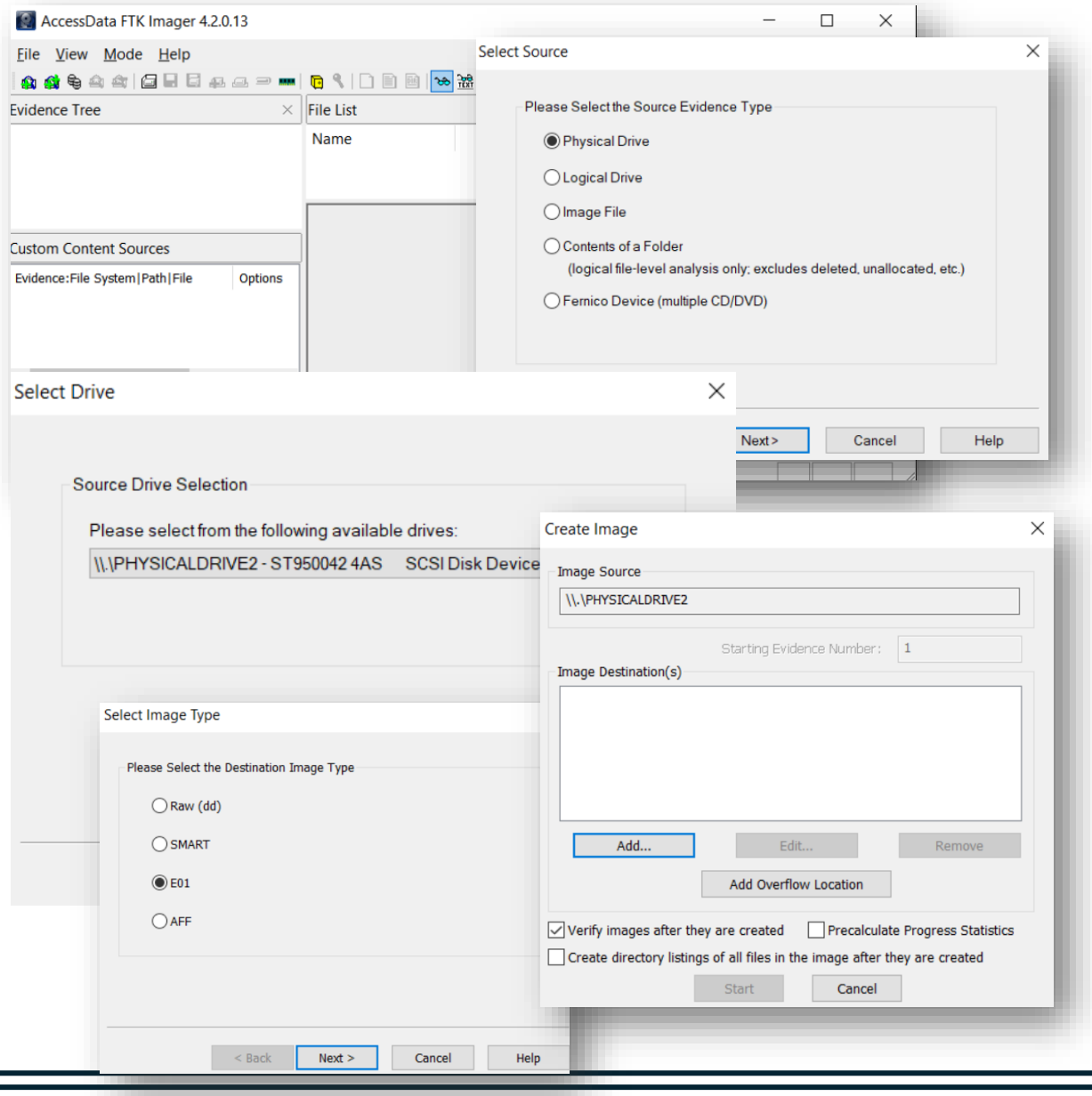
- **Σημασία των Write Blockers:** Η βασική αρχή είναι η διασφάλιση ότι δεν πραγματοποιούνται αλλαγές στα ψηφιακά αποδεικτικά στοιχεία κατά την επεξεργασία. Ακόμη και μικρές αλλαγές μπορούν να αμφισβητήσουν τη διαδικασία ή να αποκλείσουν τα στοιχεία από νομικές διαδικασίες.
- **Λογισμικοί Write Blockers:** Λογισμικό που παρεμβάλλεται μεταξύ λειτουργικού συστήματος και δίσκου, παρέχοντας πρόσβαση μόνο για ανάγνωση. Συχνά περιλαμβάνονται σε εγκληματολογικά εργαλεία όπως το FTK Imager, εξασφαλίζοντας ότι η απόκτηση στοιχείων γίνεται χωρίς εγγραφή.
- **Φυσικοί / Υλικοί Write Blockers:** Συσκευές που τοποθετούνται μεταξύ δίσκου και συστήματος απόκτησης. Επιτρέπουν δεδομένα προς το σύστημα ανάλυσης αλλά όχι αντίστροφα, αποδεικνύοντας ότι τα στοιχεία δεν αλλοιώθηκαν κατά τη φάση της απόκτησης.
- **Επιλογή τύπου Write Blocker:** Η επιλογή εξαρτάται από το είδος της απόκτησης. Οι αναλυτές πρέπει να επιλέγουν εργαλεία και τεχνικές που τεκμηριώνουν ότι έλαβαν όλα τα μέτρα για ακεραιότητα των στοιχείων, μειώνοντας τον κίνδυνο αποκλεισμού από νομικές διαδικασίες.
- **Επόμενο βήμα: Απεικόνιση δίσκων:** Με δίσκο προετοιμασμένο και write blocker ενεργό, οι αναλυτές μπορούν πλέον να προχωρήσουν στην εγκληματολογική απεικόνιση (imaging) των δίσκων αποδεικτικών στοιχείων.

Απεικόνιση με χρήση του FTK Imager

- **Φυσική επιθεώρηση στοιχείων:** Το πρώτο βήμα είναι η επιθεώρηση των αποδεικτικών στοιχείων. Ελέγχεται η φόρμα αλυσίδας διαχείρισης (chain of custody) και συμπληρώνονται τα δικά σας στοιχεία για να τεκμηριωθεί η παραλαβή.
- **Έλεγχος συσκευασίας και σφραγίδων:** Πριν την απεικόνιση, ελέγχεται ότι οι σφραγίδες δεν έχουν παραβιαστεί. Τραβιέται φωτογραφία των στοιχείων στη συσκευασία για τεκμηρίωση της ακεραιότητας.
- **Καταγραφή περιεχομένων μετά το άνοιγμα:** Αφού σπάσει η σφραγίδα, τραβιέται νέα φωτογραφία των περιεχομένων για να αποδειχθεί ότι η ακεραιότητα των στοιχείων διατηρείται και τα δεδομένα ταιριάζουν με τη φόρμα αλυσίδας διαχείρισης.
- **Ρύθμιση φυσικού write blocker:** Χρησιμοποιείται το Tableau TK35u USB 3.0 Forensic IDE/SATA Bridge Kit ως φυσικός write blocker. Ο δίσκος συνδέεται μέσω SATA adapter και FireWire στον υπολογιστή απεικόνισης. Πριν την απεικόνιση, βεβαιωθείτε ότι η συσκευή λειτουργεί σωστά για προστασία της ακεραιότητας.

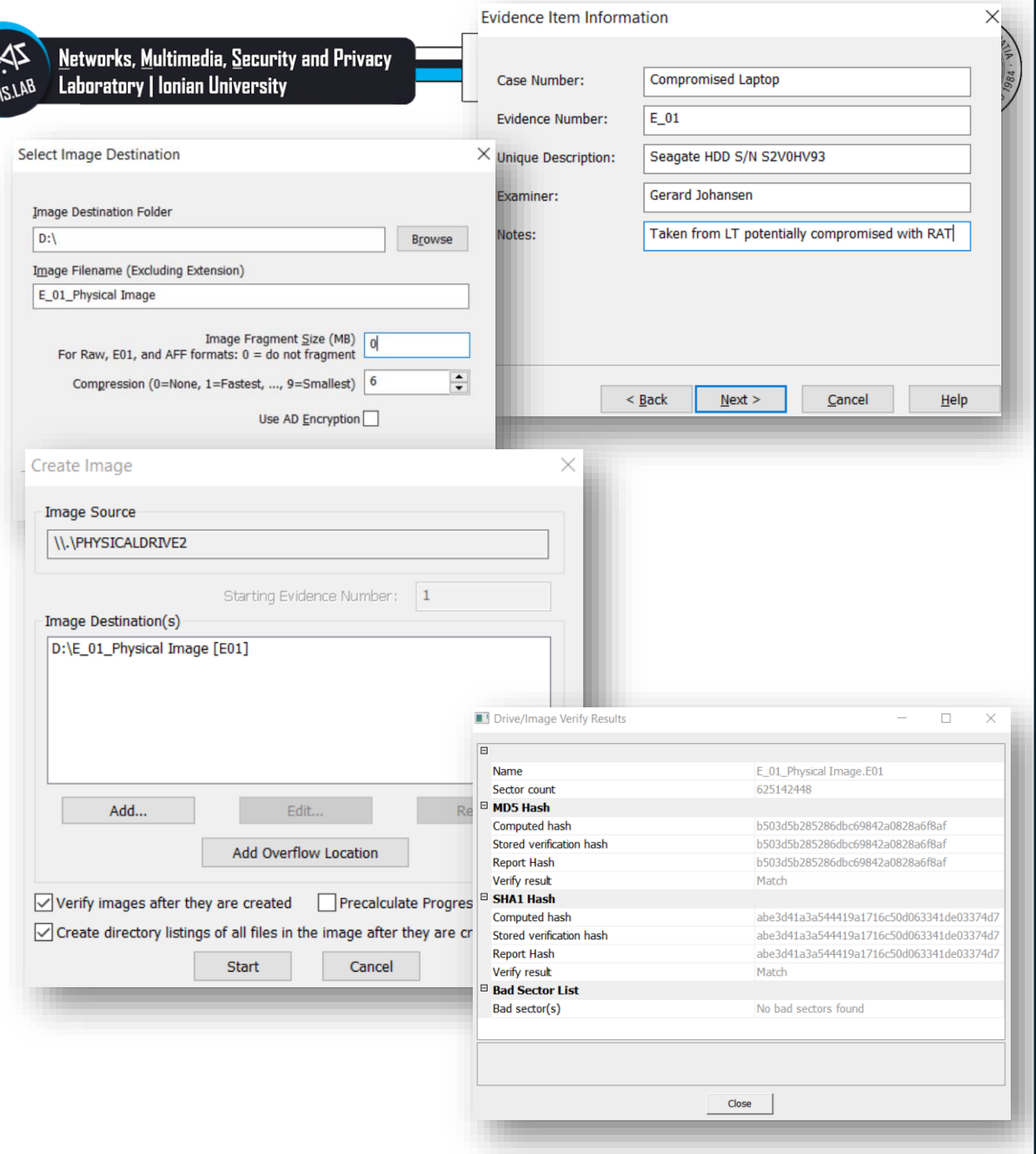
Απεικόνιση με χρήση του FTK Imager

- **Εκκίνηση FTK Imager:** Με τον φυσικό write blocker στη θέση του, ο δίσκος είναι έτοιμος για απεικόνιση. Ανοίξτε την εφαρμογή FTK Imager με δικαιώματα διαχειριστή για να ξεκινήσει η διαδικασία δημιουργίας εικόνας.
- **Δημιουργία εικόνας δίσκου:** Κάντε κλικ στο File → Create Disk Image. Επιλέξτε Physical Drive ως πηγή, ώστε να καταγραφεί ολόκληρος ο δίσκος, συμπεριλαμβανομένου του master boot record, για εγκληματολογική ανάλυση.
- **Επιλογή ύποπτου δίσκου:** Στο επόμενο παράθυρο, επιλέξτε τον σωστό δίσκο προς απεικόνιση. Δώστε προσοχή στις εμφανιζόμενες συσκευές και τον αποθηκευτικό τους χώρο για να διαχωρίσετε τον ύποπτο δίσκο από τον δίσκο προορισμού.
- **Ορισμός δίσκου προορισμού και τύπου αρχείου:** Ορίστε τον δίσκο προορισμού με Add... και επιλέξτε τον τύπο αρχείου εικόνας. Στο παράδειγμα, επιλέγεται E01 για δημιουργία εγκληματολογικά αξιόπιστου αρχείου εικόνας, και στη συνέχεια πατήστε Next.



Απεικόνιση με χρήση του FTK Imager

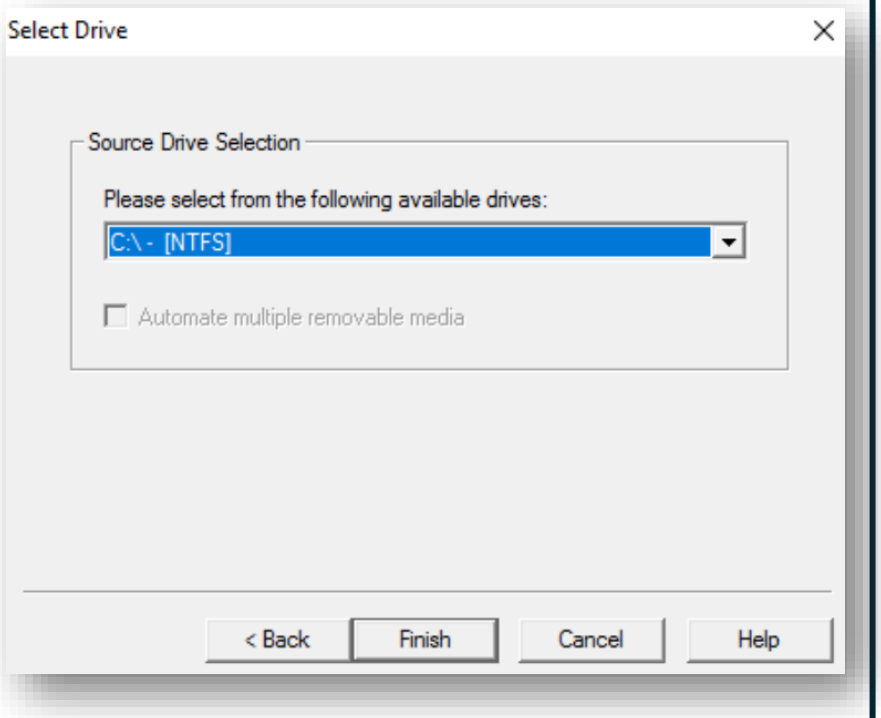
- **Συμπλήρωση πληροφοριών εικόνας:** Στο επόμενο παράθυρο εισάγετε πληροφορίες ειδικές για την εικόνα. Όλες οι λεπτομέρειες θα συμπεριληφθούν στην εγκληματολογική αναφορά. Μετά τη συμπλήρωση, κάντε κλικ στο Next.
- **Επιβεβαίωση ρυθμίσεων δίσκου προορισμού:** Ελέγξτε ότι ο δίσκος προορισμού και τα ονόματα αρχείων είναι σωστά. Ορίστε μέγεθος τεμαχισμού και συμπίεση της εικόνας. Για το παράδειγμα χρησιμοποιούμε τις προεπιλογές και πατάμε Finish.
- **Ρυθμίσεις Create Image:** Στο παράθυρο Create Image υπάρχουν επιλογές ελέγχου της εικόνας μετά τη δημιουργία για διασφάλιση ακεραιότητας και δημιουργίας λίστας αρχείων. Αφού ελεγχθούν, κάντε κλικ στο Start για εκκίνηση της διαδικασίας.
- **Διαδικασία απεικόνισης:** Το FTK Imager ξεκινά την απεικόνιση, που μπορεί να διαρκέσει ώρες ή ημέρες ανάλογα με μέγεθος δίσκου, ταχύτητα συστήματος και τύπο σύνδεσης.
- **Επαλήθευση και αποθήκευση:** Μετά την ολοκλήρωση, ελέγξτε τους υπολογισμένους hashes (MD5 και SHA1). Εάν ταιριάζουν, η διαδικασία ήταν σωστή. Το FTK Imager παρέχει λίστα αρχείων και λεπτομέρειες διαδικασίας για την εγκληματολογική αναφορά.
- **Live vs Dead Imaging:** Η dead imaging παρέχει την εγκληματολογικά πιο αξιόπιστη καταγραφή. Όταν όμως το σύστημα είναι ενεργό, απαιτείται live imaging για τη συλλογή αποδεικτικών στοιχείων χωρίς διακοπή λειτουργίας.



Ζωντανή Απόκτηση Εικόνας (Live Imaging)

Η ζωντανή εικόνα λαμβάνεται από ένα σύστημα που βρίσκεται σε λειτουργία. Το FTK Imager τρέχει από USB, επιτρέποντας τη δημιουργία εικόνας χωρίς να αλλοιώνεται το σύστημα. Αν και ορισμένα αρχεία και ρυθμίσεις μητρώου ενημερώνονται, η βασική ακεραιότητα του συστήματος διατηρείται.

- **Προετοιμασία USB:** Ο αναλυτής πρέπει να έχει προδιαμορφωμένη συσκευή USB με ξεχωριστά partitions για εργαλεία και για στοιχεία απόδειξης. Το partition για τα στοιχεία απόδειξης πρέπει να καθαρίζεται πριν από κάθε χρήση, για να εξασφαλιστεί ότι δεν υπάρχουν προηγούμενα δεδομένα.
- **Χρήση FTK Imager Lite:** Η πλήρης έκδοση FTK Imager μπορεί να παρουσιάσει προβλήματα με DLL σε USB. Η Access Data παρέχει ελαφριά έκδοση FTK Imager Lite, κατάλληλη για live imaging, διαθέσιμη στη διεύθυνση: FTK Imager Lite.
- **Διαδικασία απόκτησης εικόνας:** Συνδέστε το USB στον υπολογιστή στόχο και ξεκινήστε το FTK Imager Lite. Η διαδικασία ακολουθεί τα ίδια βήματα όπως η dead imaging, αλλά μπορεί να εστιάσει σε συγκεκριμένα partitions, π.χ. C:\ [NTFS].
- **Αποτελέσματα και προορισμός:** Ο αναλυτής επιλέγει τον προορισμό (destination drive) για τα στοιχεία απόδειξης, που έχει προδιαμορφωθεί εκ των προτέρων. Η ολοκλήρωση της διαδικασίας παρέχει τις ίδιες πληροφορίες και δυνατότητες ελέγχου ακεραιότητας όπως η νεκρή απεικόνιση.



WinPmem – Απόκτηση Μνήμης

Εγκατάσταση και χρήση: Το WinPmem μπορεί να εγκατασταθεί σε απομακρυσμένα συστήματα μέσω εργαλείων όπως Remote Desktop ή PSExec. Μόλις εγκατασταθεί, η μνήμη του συστήματος μπορεί να καταγραφεί και να σταλεί σε άλλο σύστημα για ανάλυση.

Μεταφορά δεδομένων με NetCat Η έξοδος του WinPmem μπορεί να προωθηθεί μέσω NetCat (piping). Παράδειγμα:

- C:/winpmem-2.1.exe - | nc 192.168.0.56 4455

Η εντολή συλλέγει τη μνήμη και τη στέλνει στον αναλυτή μέσω της θύρας 4455.

Πλεονέκτημα: Απομακρυσμένη συλλογή μνήμης χωρίς φυσική πρόσβαση.

Μειονέκτημα: Απαιτεί πρόσβαση στη γραμμή εντολών, καθώς και εγκατάσταση WinPmem και NetCat. Σε ύποπτα συστήματα, η τεχνική μπορεί να μην είναι ασφαλής ή εφικτή.

https://dfir.it/blog/2015/04/20/memory-acquisition-tools-for-windows/

https://dfir.it/blog/2017/03/29/tekdefense-network-challenge-001-walkthrough/

F-Response – Απομακρυσμένη Απόκτηση Στοιχείων

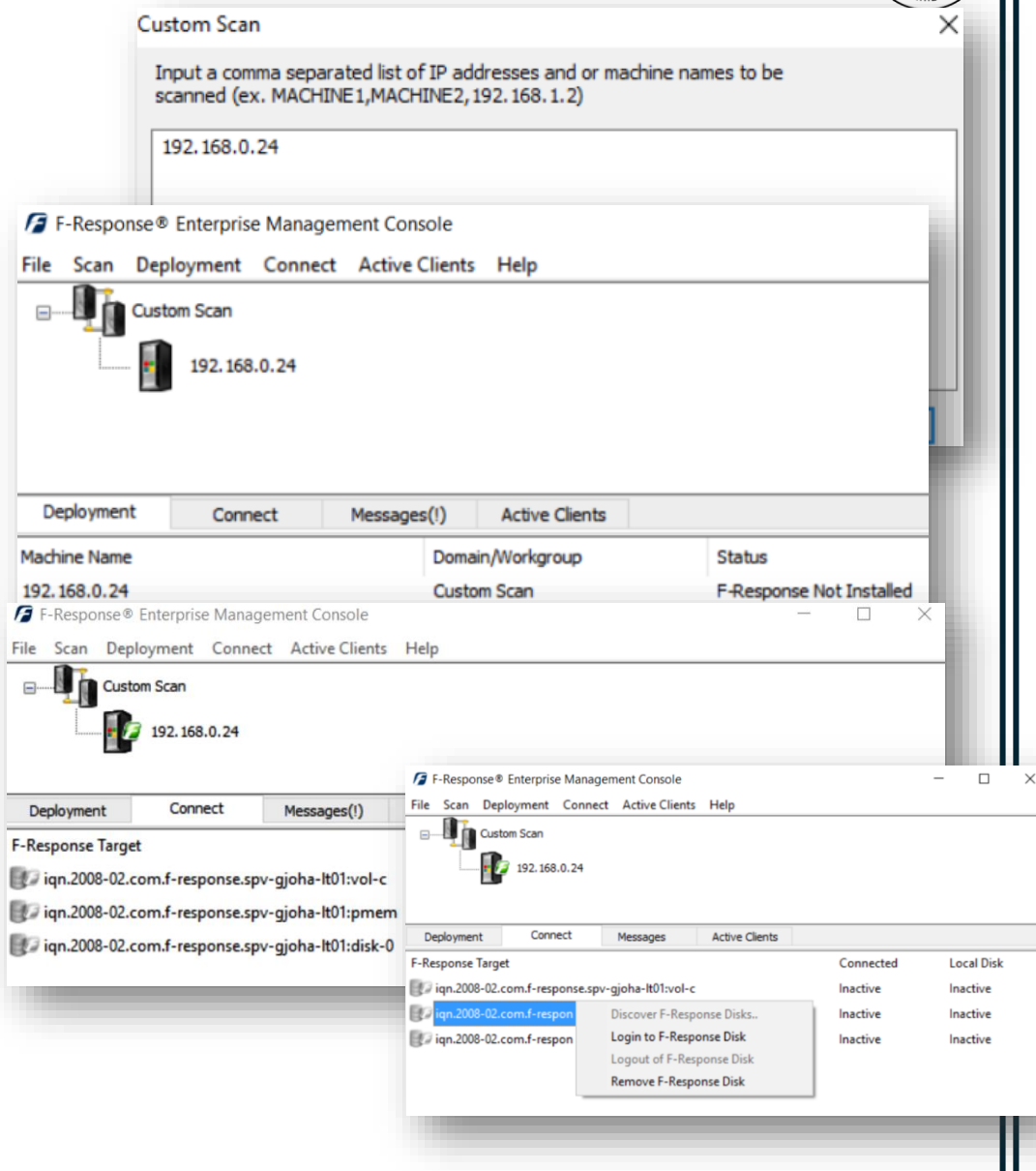
Λογισμικό για απομακρυσμένη πρόσβαση σε αποδεικτικά στοιχεία μέσω δικτύου. Δεν απαιτεί άμεση πρόσβαση μέσω SSH ή RDS. Επιτρέπει χρήση των εργαλείων της προτίμησης του αναλυτή, π.χ. FTK Imager. Περισσότερες πληροφορίες: F-Response

Βήματα χρήσης

1. Εγκατάσταση F-Response Enterprise και επιλογή **Custom Scan**.
2. Εισαγωγή διεύθυνσης IP του ύποπτου συστήματος (π.χ. 192.168.0.24).
3. Επιβεβαίωση σύνδεσης και εγκατάσταση agent στο σύστημα-στόχο (**Install/Start F-Response**).
4. Επιβεβαίωση ότι το σύστημα εμφανίζεται με πράσινο εικονίδιο και διαθέτει:
   - Φυσικό δίσκο (disk-0)
   - Λογικό δίσκο (vol-c)
   - Μνήμη (pmem) – στόχος μας
5. Mount της μνήμης ως φυσικός δίσκος μέσω **Login to F-Response Disk**.: Απόκτηση μνήμης με εργαλεία όπως FTK Imager (RAW image).

Πλεονεκτήματα: Απομακρυσμένη απόκτηση χωρίς φυσική πρόσβαση. Ευελιξία στη χρήση εργαλείων εγκληματολογικής ανάλυσης.

Περιορισμοί: Απαιτεί εγκατάσταση agent στο απομακρυσμένο σύστημα. Η διαδικασία μπορεί να τροποποιήσει ελαφρά το σύστημα κατά την εκτέλεση.



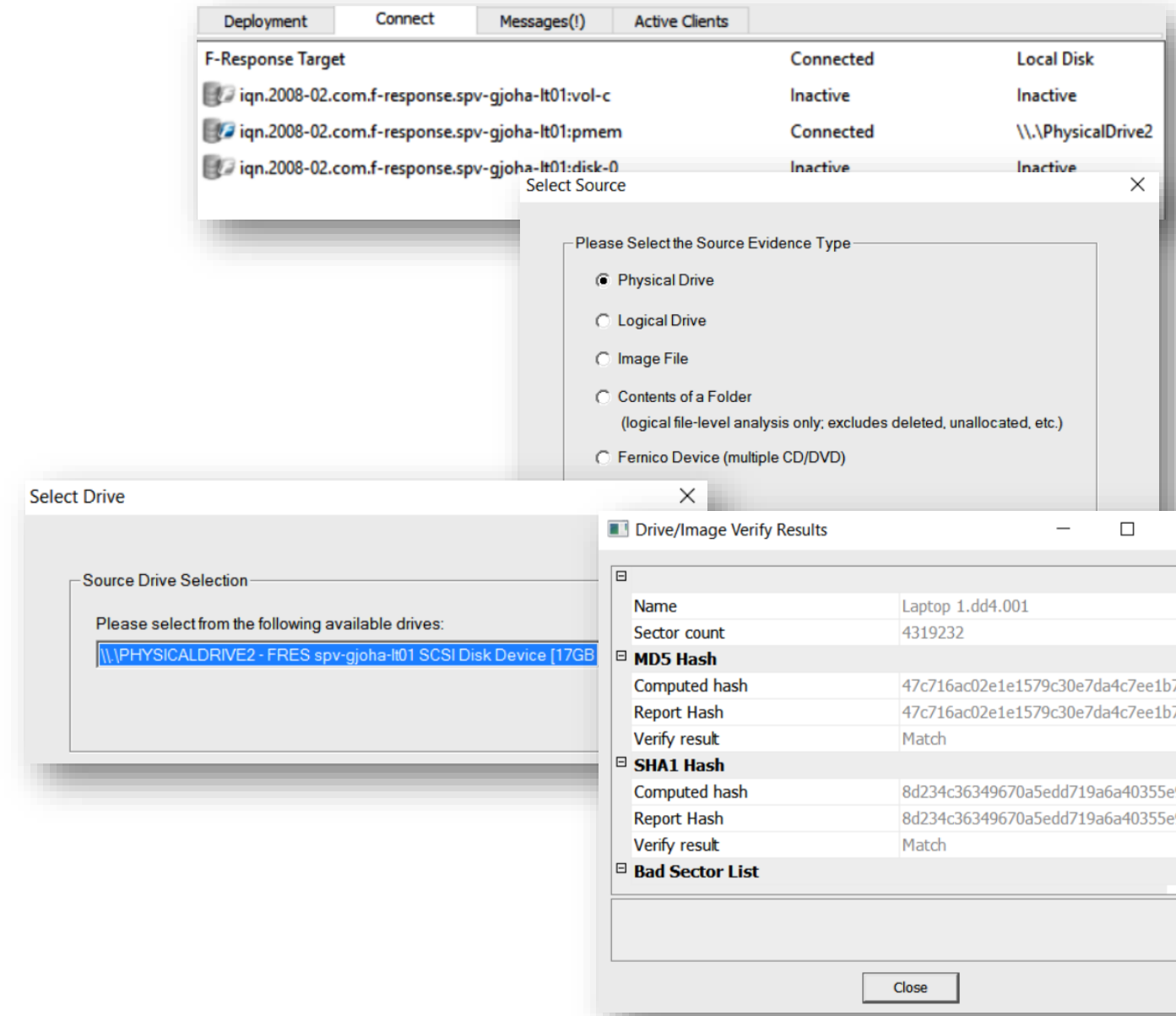
F-Response – Απομακρυσμένη Απόκτηση Στοιχείων

Mount & Ενεργοποίηση Μνήμης: Μόλις γίνει login στο απομακρυσμένο σύστημα, το F-Response εμφανίζει ποιος δίσκος ή μνήμη είναι ενεργός. Η μνήμη μπορεί να mountαριστεί ως φυσικός δίσκος (π.χ. .\PhysicalDrive2) και είναι έτοιμη για απόκτηση μέσω εγκληματολογικών εργαλείων.

FTK Imager – Δημιουργία Εικόνας: Ανοίξτε το FTK Imager, επιλέξτε **File → Create Disk Image** και επιλέξτε **Physical Drive** ως τύπο πηγής. Προσοχή: μην χρησιμοποιήσετε Capture Memory, γιατί θα καταγράψει τη μνήμη τοπικά.

Επιλογή Δίσκου & Imaging: Στη λίστα δίσκων, επιλέξτε τον δίσκο που υποδεικνύει το F-Response (π.χ. .\PHYSICALDRIVE2). Το FTK Imager χειρίζεται τον απομακρυσμένο δίσκο σαν να ήταν τοπικός για τη δημιουργία της εικόνας.

Τεκμηρίωση & Αναφορά: Μετά την ολοκλήρωση, το FTK Imager παρέχει όλα τα δεδομένα και αρχεία που πρέπει να περιληφθούν στην αυτοψία/forensic αναφορά, εξασφαλίζοντας εγκληματολογικά έγκυρη τεκμηρίωση.



Απόκτηση Εικονικών Μηχανών (Virtual Machines)

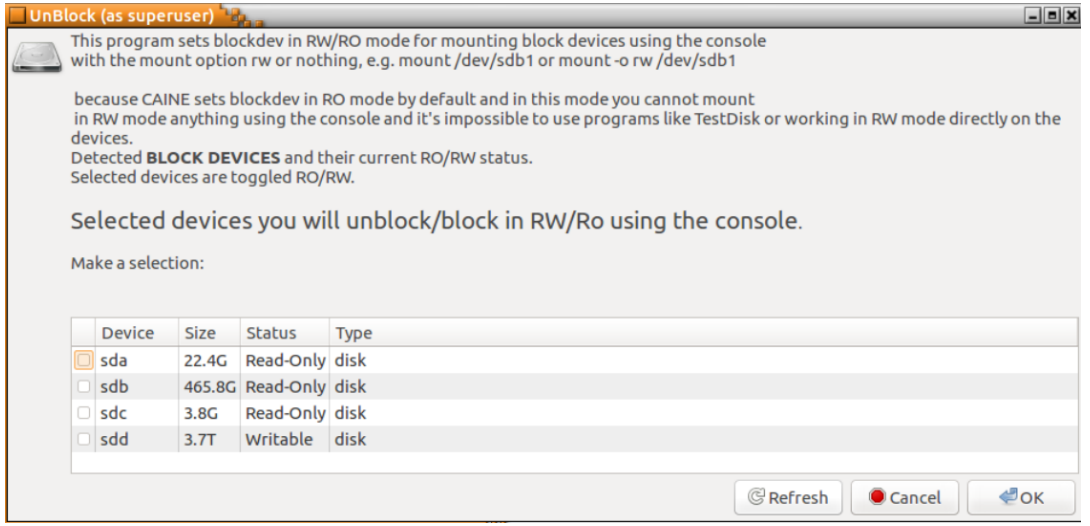
- **Εξαγωγή & Snapshot:** Οι αναλυτές μπορούν να αποκτήσουν εικονικούς διακομιστές ή σταθμούς εργασίας με την εξαγωγή του παγωμένου συστήματος σε αφαιρούμενο δίσκο ή μέσω snapshot. Η σωστή τεκμηρίωση και ο καθαρισμός του δίσκου είναι κρίσιμα για εγκληματολογική εγκυρότητα.
- **Αρχεία Εικονικής Μηχανής:** Το VMware χρησιμοποιεί αρχεία όπως .vmdk (εικόνα δίσκου), .vmem (εικονική μνήμη), .vmss (κατάσταση αναστολής) και .vmsn (snapshot). Κάθε αρχείο παρέχει διαφορετικά στοιχεία για ανάλυση δίσκου και μνήμης.
- **Ανάλυση & Mounting:** Το αρχείο .vmdk μπορεί να φορτώσει για ανάλυση όπως ένας φυσικός δίσκος. Το .vmsn μπορεί να αντιγραφεί για ανακατασκευή του συστήματος χωρίς να επηρεαστεί το πρωτότυπο, επιτρέποντας ασφαλή έρευνα.
- **Συνδυασμός Μνήμης (.vmem + .vmss):** Τα αρχεία μνήμης μπορούν να συνδυαστούν με το εργαλείο **vmss2core.exe** για δημιουργία memory dump. Αυτό επιτρέπει πλήρη ανάλυση της μνήμης του συστήματος και εξαγωγή αποδεικτικών στοιχείων με εγκληματολογική εγκυρότητα.
  - C:\VirtualTools\vmss2core.exe -W "InfectedServer.vmss" "InfectedServer.vmem"

Η παραπάνω εντολή θα παράγει ένα memory dump στον κατάλογο που περιέχει τα δύο αρχεία.

Linux Imaging για Αποτύπωση Δίσκων

- **Εκκινήσιμη USB & Ταυτόχρονη Αποτύπωση:** Η χρήση μιας bootable Linux διανομής, όπως το CAINE, επιτρέπει στους αναλυτές να αποτυπώσουν πολλαπλά συστήματα ταυτόχρονα, ακόμη κι αν υπάρχει μόνο ένας write blocker. Κάθε πηγή απαιτεί USB και δίσκο αποδεικτικών στοιχείων.
- **Αναγνώριση Δίσκων**: Μετά την εκκίνηση του CAINE, η εντολή fdisk -l εμφανίζει όλες τις κατατμήσεις. Ο αναλυτής πρέπει να αναγνωρίσει τον σωστό δίσκο-στόχο (/dev/sdb) και τον δίσκο αποδεικτικών στοιχείων (/dev/sdd), ώστε να αποφευχθούν λάθη στην αποτύπωση.
- **Χρήση Write Blocker**: Το CAINE OS διαθέτει λογισμικό write blocker ("Block on/off") που εμποδίζει την εγγραφή στα συστήματα-στόχους. Οι δίσκοι εκτός του δίσκου αποδεικτικών στοιχείων ορίζονται ως read-only, εξασφαλίζοντας ότι δεν τροποποιούνται δεδομένα κατά τη διαδικασία.
- **Τεκμηρίωση:** Συνιστάται να τραβηχτούν στιγμιότυπα οθόνης των ρυθμίσεων write blocker και της λίστας δίσκων. Αυτό εξασφαλίζει πλήρη τεκμηρίωση για την εγκληματολογική αναφορά και τη διατήρηση της ακεραιότητας των στοιχείων.

```
Disk /dev/sdb: 465.8 GiB, 500107862016 bytes, 976773168 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x345601e6

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sdb1  *         2048   1026047   1024000   500M  7 HPFS/NTFS/exFAT
/dev/sdb2         1026048 975847423 974821376 464.9G  7 HPFS/NTFS/exFAT
/dev/sdb3       975847424 976769023    921600   450M 27 Hidden NTFS WinRE


Disk /dev/sdc: 3.8 GiB, 4060086272 bytes, 7929856 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000f1d04

Device     Boot Start     End Sectors  Size Id Type
/dev/sdc1  *     2048 7929855 7927808  3.8G  c W95 FAT32 (LBA)


Disk /dev/sdd: 3.7 TiB, 4000787029504 bytes, 7814037167 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 33553920 bytes
Disklabel type: gpt
Disk identifier: 30B0BF34-42D8-41E5-A90C-E5735893CFB6

Device      Start        End    Sectors  Size Type
/dev/sdd1      34     262177     262144  128M Microsoft reserved
/dev/sdd2  264192 7814035455 7813771264  3.7T Microsoft basic data
```



Linux Imaging για Αποτύπωση Δίσκων

Αποτύπωση Δίσκου με dc3dd: Το dc3dd είναι εργαλείο εγκληματολογικής απόκτησης που επεκτείνει την εντολή dd, παρέχοντας αναφορές σφαλμάτων και hash on-the-fly. Η εντολή dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt αποτυπώνει τον δίσκο-στόχο, υπολογίζει το MD5 hash και δημιουργεί αρχείο log για τεκμηρίωση.

Παρακολούθηση Διαδικασίας: Η διαδικασία μπορεί να διαρκέσει ώρες, ανάλογα με το μέγεθος του δίσκου. Ο αναλυτής μπορεί να παρακολουθεί την πρόοδο και στο τέλος να ελέγχει τους τομείς που χρησιμοποιήθηκαν και το hash για επαλήθευση της ακεραιότητας της εικόνας.

Αρχεία και Τεκμηρίωση: Τα δημιουργημένα αρχεία εικόνας και log πρέπει να εξεταστούν σε σύστημα Windows. Το log περιέχει λεπτομέρειες όπως το μέγεθος δίσκου, αριθμό τομέων, σφάλματα και hash, που είναι κρίσιμες για την εγκληματολογική αναφορά.

Κλιμάκωση & Βιωσιμότητα Linux: Το Linux επιτρέπει παράλληλη απόκτηση δεδομένων από πολλαπλά συστήματα χρησιμοποιώντας πολλαπλές USB συσκευές και write blockers. Η σωστή τεκμηρίωση και συστηματική διαδικασία διασφαλίζει την εγκυρότητα των αποδεικτικών στοιχείων για δικαστική χρήση.

```
dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
device size: 976773168 sectors (probed),   500,107,862,016 bytes
sector size: 512 bytes (probed)
500107862016 bytes ( 466 G ) copied ( 100% ), 5854 s, 81 M/s

input results for device `/dev/sdb':
   976773168 sectors in
   0 bad sectors replaced by zeros
   d48a7ccafaead6fab7d284b4be300bd8 (md5)

output results for file `ideapad.img':
   976773168 sectors out

dc3dd completed at 2017-04-02 20:56:09 +0100
```

dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100

compiled options:

command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5

log=dc3ddlog.txt

device size: 976773168 sectors (probed), 500,107,862,016 bytes

sector size: 512 bytes (probed)

500107862016 bytes (466 G) copied (100%), 5854.43 s, 81 M/s

input results for device `/dev/sdb': 976773168 sectors in

0 bad sectors replaced by zeros d48a7ccafaead6fab7d284b4be300bd8

(md5)

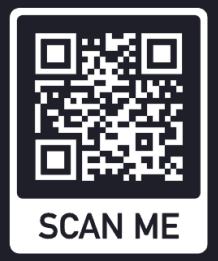
output results for file `ideapad.img': 976773168 sectors out

dc3dd completed at 2017-04-02 20:56:09 +0100

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr