Corfu

Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών: Βασικά Στοιχεία Digital Forensics

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

</> 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

Ψηφιακή Εγκληματολογία και Incident Response

Η ψηφιακή διερμηνεία αποτελεί κρίσιμο στοιχείο της αντίδρασης σε περιστατικά, καθώς επιτρέπει στους αναλυτές: Να κατανοήσουν την αλληλουχία γεγονότων που οδήγησαν σε παραβίαση ή κακόβουλη δραστηριότητα. Να εντοπίσουν υπευθύνους σε περιπτώσεις εσωτερικής απάτης ή κακόβουλης ενέργειας χρηστών. Η διαδικασία ψηφιακής διερμηνείας παρέχει πλαίσιο και μεθοδολογία, διασφαλίζοντας ότι τα ψηφιακά αποδεικτικά στοιχεία είναι έγκυρα και αξιοποιήσιμα. **Διαδικασία Ψηφιακής Διερμηνείας (DFRWS Framework):** Η διαδικασία περιλαμβάνει **έξι βασικά στάδια:**

1. **Ταυτοποίηση (Identification):** Εντοπισμός πιθανών ψηφιακών αποδεικτικών στοιχείων που σχετίζονται με το περιστατικό.
2. **Διατήρηση (Preservation):** Ασφάλιση των στοιχείων ώστε να διατηρηθεί η ακεραιότητά τους και η αλυσίδα τεκμηρίωσης (chain of custody).
3. **Συλλογή (Collection):** Συστηματική και τεκμηριωμένη λήψη των αποδεικτικών στοιχείων από τα συστήματα και τα δίκτυα.
4. **Εξέταση (Examination):** Ανάλυση των αποδεικτικών στοιχείων για τον εντοπισμό ύποπτων ή μη φυσιολογικών ενεργειών.
5. **Ανάλυση (Analysis):** Συνεκτική αξιολόγηση των δεδομένων για την κατανόηση της αλληλουχίας γεγονότων και των επιπτώσεων.
6. **Παρουσίαση (Presentation):** Παρουσίαση των ευρημάτων σε ανώτερα στελέχη ή αρμόδιες αρχές, διατηρώντας την εγκυρότητα και αξιοπιστία των αποδεικτικών στοιχείων.

Σημαντικές Ισορροπίες: Το προσωπικό CSIRT συνήθως δεν κατασχέσει δίκτυα ή κρίσιμα συστήματα εκτός αν υπάρχει επαρκής λόγος. Η ψηφιακή διερεύνηση μπορεί να είναι χρονοβόρα (μήνες), αλλά πρέπει να ισορροπεί με την ανάγκη επανέναρξης ή συνέχισης των κανονικών λειτουργιών του οργανισμού.

Ταυτοποίηση (Identification)

Η ταυτοποίηση αποτελεί το πρώτο και θεμελιώδες στάδιο της ψηφιακής διερμηνείας, όπου εντοπίζονται πιθανά ψηφιακά αποδεικτικά στοιχεία που σχετίζονται με ένα περιστατικό. Η διαδικασία αυτή καθοδηγείται από αρχές της εγκληματολογίας, όπως η αρχή ανταλλαγής του Locard.

- **Αρχή Locard:** Όταν δύο αντικείμενα έρχονται σε επαφή, αφήνουν ίχνη το ένα στο άλλο. **Παράδειγμα φυσικού κόσμου:** Οι ίνες ενός χαλιού κολλάνε στα παπούτσια. **Παράδειγμα ψηφιακού κόσμου:** Ένα σύστημα που επισκέπτεται έναν ιστότοπο αφήνει ίχνη, όπως διεύθυνση IP καταγεγραμμένη στο server ή cookie στο laptop.

Εφαρμογή στον ψηφιακό χώρο

1. **Εντοπισμός πηγών αποδεικτικών στοιχείων:** Αναλύεται το μολυσμένο σύστημα ή οι εμπλεκόμενοι υπολογιστές. Παρατηρούνται logs από firewalls, web proxies ή εφαρμογές για εξερχόμενη ή εισερχόμενη κίνηση.
2. **Ανάλυση δικτύου και επικοινωνιών:** Για malware που επικοινωνεί με C2 servers, η ανασκόπηση των IP διευθύνσεων μπορεί να αποκαλύψει: α) Τον C2 server. β) Πιθανές παραλλαγές του malware. γ) Δικτυακές διαδρομές και ενδεχόμενες επιπλέον μολύνσεις.
3. **Επιβεβαίωση στοιχείων:** Τα ψηφιακά στοιχεία μπορεί να παραποιηθούν εύκολα.Η αξιοπιστία ενός μόνο αποδεικτικού στοιχείου πρέπει να επαληθεύεται με άλλα ανεξάρτητα στοιχεία πριν θεωρηθεί αξιόπιστο.

Σημαντικά σημεία: Η ταυτοποίηση παρέχει την αρχική εικόνα των συστημάτων, δικτύων και δεδομένων που επηρεάστηκαν. Αποτελεί τη βάση για τα επόμενα στάδια: διατήρηση (preservation), συλλογή (collection) και ανάλυση (analysis). Η αρχή ανταλλαγής του Locard στον ψηφιακό χώρο βοηθά στον καθορισμό πιθανών σημείων συλλογής αποδεικτικών στοιχείων και στην κατανόηση της αλληλεπίδρασης συστημάτων.

Διατήρηση (Preservation)

Η διατήρηση αποτελεί το δεύτερο στάδιο της ψηφιακής διερμηνείας και αφορά την προστασία των ψηφιακών αποδεικτικών στοιχείων από οποιαδήποτε τροποποίηση, διαγραφή ή αλλοίωση. Η σωστή διατήρηση εξασφαλίζει ότι τα στοιχεία παραμένουν αξιόπιστα για περαιτέρω εξέταση και πιθανή χρήση σε νομικό ή διοικητικό πλαίσιο. **Κύρια μέτρα διατήρησης:**

1. **Προστασία αρχείων καταγραφής (logs):** Ενεργοποίηση μηχανισμών ελέγχου που αποτρέπουν την τροποποίηση ή διαγραφή.Χρήση write-once/read-many (WORM) συστημάτων ή προστατευμένων βάσεων δεδομένων για logs.
2. **Απομόνωση συστημάτων:** Απομόνωση υπολογιστών ή servers από το δίκτυο για να αποφευχθεί η μετάδοση κακόβουλου λογισμικού ή η αλλοίωση δεδομένων. Χρήση φυσικών αποσυνδέσεων (π.χ. αποσύνδεση καλωδίων δικτύου) ή λογικών ελέγχων (VLAN isolation, firewall rules). Περιορισμός πρόσβασης χρηστών σε ύποπτα συστήματα για την αποφυγή εκ προθέσεως ή ακούσιας τροποποίησης.
3. **Ασφάλεια πρόσβασης:** Εφαρμογή κανόνων πρόσβασης βάσει ρόλων (RBAC) για την ελαχιστοποίηση της αλληλεπίδρασης με τα κρίσιμα στοιχεία. Καταγραφή κάθε προσπάθειας πρόσβασης για περαιτέρω διερεύνηση.
4. **Χρήση εικονικών πλατφορμών:** Δημιουργία snapshots των εικονικών μηχανών για καταγραφή της κατάστασης των συστημάτων σε συγκεκριμένη χρονική στιγμή. Αποθήκευση των snapshots σε μη πτητικά μέσα (non-volatile storage) για προστασία από απώλεια δεδομένων. Δυνατότητα επαναφοράς σε γνωστή καλή κατάσταση για ανάλυση χωρίς κίνδυνο αλλοίωσης.

Σημαντικά σημεία: Η διατήρηση είναι κρίσιμη για τη διασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων.Η απομόνωση συστημάτων δεν πρέπει να εμποδίζει την ανάλυση, αλλά να περιορίζει την περαιτέρω εξάπλωση του περιστατικού.Τα εικονικά περιβάλλοντα προσφέρουν ευελιξία και δυνατότητα ασφαλούς διατήρησης, ιδιαίτερα σε μεγάλα ή κατανεμημένα περιβάλλοντα.

Συλλογή (Collection)

Η συλλογή αποτελεί το στάδιο όπου οι αναλυτές ψηφιακής εγκληματολογίας αποκτούν και καταγράφουν τα ψηφιακά αποδεικτικά στοιχεία. Η σωστή συλλογή είναι κρίσιμη για τη διασφάλιση της εγκυρότητας και της ακεραιότητας των στοιχείων.

Μεταβλητότητα ψηφιακών στοιχείων: Μερικά αποδεικτικά στοιχεία είναι μεταβλητά, δηλαδή μπορούν να χαθούν εάν το σύστημα απενεργοποιηθεί ή αλλοιωθεί. Ο σωστός προσδιορισμός αυτών των στοιχείων καθορίζει τη σειρά με την οποία πρέπει να συλλεχθούν. **Παράδειγμα μεταβλητών στοιχείων: α) Δίκτυα και routers:** ενεργές συνδέσεις, καταχωρητές (routing tables), cache ARP, στατιστικά πυρήνα. **β) Υπολογιστές (laptops/desktops):** μνήμη RAM, cache ARP, πίνακες διεργασιών. **γ) Συστήματα αρχείων:** προσωρινά αρχεία και caches.

Σειρά μεταβλητότητας (RFC 3227 – IETF): Το έγγραφο RFC 3227 – Guidelines for Evidence Collection and Archiving καθορίζει τη σειρά συλλογής στοιχείων με βάση τη μεταβλητότητά τους:

1. Καταχωρητές και cache: πίνακας δρομολόγησης, ARP cache, πίνακας διεργασιών, στατιστικά πυρήνα, μνήμη RAM.
2. Προσωρινά συστήματα αρχείων (temporary files, volatile storage).
3. Δίσκος (persistent storage).
4. Απομακρυσμένα logs και δεδομένα παρακολούθησης (π.χ., syslog servers, cloud logs).
5. Φυσική διαμόρφωση και τοπολογία δικτύου (physical layout, network devices).
6. Αρχειακά μέσα (tapes, offline storage, backups).

Κατευθύνσεις για συλλογή: α) Συλλογή μεταβλητών στοιχείων πρώτα: διασφαλίζει ότι δεν χάνονται κρίσιμες πληροφορίες που δεν μπορούν να ανακτηθούν μετά το κλείσιμο ή επανεκκίνηση συστήματος. β) Μεταφορά σε μη πτητικά μέσα: χρησιμοποιούνται εξωτερικοί σκληροί δίσκοι, write-once media ή ελεγχόμενα αποθηκευτικά μέσα. γ) Τεκμηρίωση: κάθε βήμα συλλογής πρέπει να καταγράφεται για να διασφαλιστεί η ακεραιότητα και η εγκυρότητα των στοιχείων. δ) Ασφάλεια πρόσβασης: περιορισμός πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό για αποφυγή αλλοίωσης.

Σωστή Διαχείριση Αποδεικτικών Στοιχείων (Evidence Handling)

Η σωστή διαχείριση των αποδεικτικών στοιχείων είναι κρίσιμη για να διασφαλιστεί ότι τα στοιχεία παραμένουν εγκληματολογικά αξιόπιστα και μπορούν να χρησιμοποιηθούν σε νομικές διαδικασίες. Λάθη στη συλλογή ή αποθήκευση μπορούν να οδηγήσουν σε αλλοίωση ή ακύρωση των αποδεικτικών στοιχείων σε ποινικές ή αστικές δίκες. Βασικές αρχές διαχείρισης αποδεικτικών στοιχείων:

1. **Αποφυγή αλλοίωσης των αρχικών στοιχείων:** Οι ενέργειες των αναλυτών δεν πρέπει να τροποποιούν τα πρωτογενή δεδομένα. **Παραδείγματα:** α) Μη πρόσβαση σε λειτουργικό σύστημα χωρίς σοβαρό λόγο. β) Χρήση εργαλείων που δημιουργούν αντίγραφα για ανάλυση αντί των πρωτοτύπων. γ) Τεκμηρίωση κάθε ενέργειας μειώνει την πιθανότητα τα στοιχεία να θεωρηθούν αλλοιωμένα.
2. **Τεκμηρίωση:** Κάθε βήμα συλλογής, ανάλυσης και αποθήκευσης πρέπει να καταγράφεται. Τεκμηρίωση μπορεί να περιλαμβάνει: α) Λεπτομερείς σημειώσεις για κάθε ενέργεια. β) Διαγράμματα και σχήματα που απεικονίζουν τη ροή δεδομένων. γ) Φωτογραφική τεκμηρίωση (π.χ. snapshots φυσικών ή εικονικών συστημάτων). **Στόχος:** να ανακατασκευαστεί η αλληλουχία γεγονότων αν τεθεί υπό αμφισβήτηση η ακεραιότητα των στοιχείων.
3. **Εφαρμογή καλών πρακτικών από τις αρχές επιβολής του νόμου:** Υπάρχουν καθιερωμένα έγγραφα και οδηγίες για τη σωστή διαχείριση ψηφιακών στοιχείων: Seizing Electronic Evidence, Digital Evidence Guidelines – NCJRS, Digital Evidence Booklet – IACP.

Συνοπτικά: α) Η ακεραιότητα των στοιχείων είναι θεμέλιο της ψηφιακής εγκληματολογίας. β) Κάθε βήμα πρέπει να τεκμηριώνεται λεπτομερώς. γ) Χρήση αντιγράφων εργασίας (forensic copies) για ανάλυση αντί των πρωτοτύπων. δ) Εφαρμογή καλών πρακτικών και οδηγών από τις αρχές για ασφάλεια και εγκυρότητα των στοιχείων.

Αλυσίδα Κηδεμονίας (Chain of Custody)

Η αλυσίδα κηδεμονίας περιγράφει τη διαδικασία τεκμηρίωσης και παρακολούθησης ενός αποδεικτικού στοιχείου καθ' όλη τη διάρκεια ζωής του – από τη στιγμή που το στοιχείο εντοπίζεται μέχρι την τελική διαχείριση του περιστατικού (επιστροφή ή καταστροφή).

Η διατήρηση σωστής αλυσίδας κηδεμονίας είναι κρίσιμη, καθώς οποιοδήποτε κενό μπορεί να οδηγήσει στον αποκλεισμό του στοιχείου σε νομική διαδικασία. Τρόποι καταγραφής της αλυσίδας κηδεμονίας:

1. **Ηλεκτρονικά:** Χρήση λογισμικού και υλικού που αυτοματοποιεί την αλυσίδα κηδεμονίας. Τα αποδεικτικά στοιχεία επισημαίνονται με μοναδικούς γραμμωτούς κώδικες. Σαρωτές καταγράφουν ηλεκτρονικά κάθε μετακίνηση ή αλλαγή κατάστασης.
2. **Μέθοδος χαρτιού και στυλό**: Χρήση έντυπων φορμών για καταγραφή πληροφοριών. Απαιτεί προσοχή για να προστατευτεί από καταστροφή ή χειραγώγηση. Οικονομική λύση για μικρότερες ομάδες CSIRT χωρίς αυτοματοποιημένα συστήματα.

Σημείωση:

- Η λεπτομέρεια στην καταγραφή εξασφαλίζει ότι:
- Κάθε αποδεικτικό στοιχείο παρακολουθείται σωστά.
- Η ακεραιότητα και αυθεντικότητα των στοιχείων διατηρείται.
- Οι διαδικασίες μπορούν να υποστηρίξουν πιθανές νομικές ενέργειες χωρίς αμφισβήτηση.

Αλυσίδα Κηδεμονίας (Chain of Custody): Περιγραφή Αντικειμένου

Η πρώτη ενότητα περιλαμβάνει λεπτομερή περιγραφή του αντικειμένου. Στην ψηφιακή εγκληματολογία, η ακρίβεια είναι καθοριστική, καθώς οι λεπτομέρειες εξασφαλίζουν την αυθεντικότητα και αφαιρούν κάθε αμφιβολία για το αποδεικτικό στοιχείο.

Electronic Media Details

Item Number:	Description:		
1	Western Digital WD01EURS Hard Drive		
Manufacturer:		Model#	Serial Number:
Western Digital		WD01EURS	WMAV1234567

- **Αριθμός Αντικειμένου (Item Number):** Κάθε στοιχείο λαμβάνει έναν μοναδικό αριθμό. Εάν υπάρχουν πολλαπλά αντικείμενα, καταγράφονται σε ξεχωριστά έντυπα αλυσίδας κηδεμονίας.
- **Περιγραφή (Description):** Γενική καταγραφή του αντικειμένου, π.χ. «500 GB SATA HDD». Η απλή περιγραφή διευκολύνει την άμεση αναγνώριση.
- **Κατασκευαστής (Manufacturer):** Η αναφορά του κατασκευαστή είναι σημαντική όταν υπάρχουν πολλά αντικείμενα διαφορετικής προέλευσης.
- **Μοντέλο (Model):** Ο αριθμός μοντέλου παρέχει επιπλέον τεχνικές λεπτομέρειες που ενισχύουν την ακρίβεια της ταυτοποίησης.
- **Σειριακός Αριθμός (Serial Number):** Κρίσιμο στοιχείο σε περιπτώσεις όπου πολλά συστήματα έχουν πανομοιότυπη διαμόρφωση. Εξασφαλίζει ότι κάθε αντικείμενο μπορεί να αντιστοιχηθεί με την σωστή αλυσίδα κηδεμονίας.

Αλυσίδα Κηδεμονίας (Chain of Custody): Αρχεία / Εικόνες

Μια εναλλακτική ενότητα χρησιμοποιείται όταν τα αποδεικτικά στοιχεία είναι αρχεία καταγραφής ή εικόνες που συλλέχθηκαν κατά τη διάρκεια της έρευνας. Η ενότητα αυτή περιλαμβάνει τα βασικά στοιχεία που χρειάζονται για την πλήρη τεκμηρίωση και την επαλήθευση των αποδεικτικών στοιχείων.

Image or File Details

Date / Time Acquired:	Created By:	Method:	Storage Drive:
5/30/19 1224 UTC	Gerard Johansen	Wireshark	USB Drive 1
File/Image Name:		Hash:	
EdgeFirewallCapture.PCAP / Packet Capture		1ceaa2393357d2ed88f81bec1e647af0	

- **Ημερομηνία/Ώρα Απόκτησης (Date/Time Acquired):** Καθορίζει με ακρίβεια την ημερομηνία και την ώρα κατά την οποία αποκτήθηκαν τα στοιχεία. Η σωστή χρονοσήμανση είναι κρίσιμη για την ανακατασκευή των γεγονότων του περιστατικού.
- **Περιγραφή (Description):** Σύντομη περιγραφή του μέσου ή του αρχείου, όπως «Firewall log file» ή «Disk image». Βοηθά στην ταυτοποίηση του αντικειμένου χωρίς να χρειάζεται να ανοίξει.
- **Μέθοδος (Method):** Αναφέρεται το εργαλείο ή η διαδικασία που χρησιμοποιήθηκε για την απόκτηση των στοιχείων. Σε άλλες περιπτώσεις μπορεί να περιγράφεται η απλή αντιγραφή σε εξωτερικό μέσο.
- **Μονάδα Αποθήκευσης (Storage Drive):** Καταγράφεται η συσκευή όπου αποθηκεύτηκε το στοιχείο, π.χ. «External HDD 1TB». Η σωστή καταγραφή εξασφαλίζει ότι τα στοιχεία παραμένουν ασφαλή και προσβάσιμα.
- **Όνομα Αρχείου/Εικόνας (File/Image Name):** Καταχωρείται το μοναδικό όνομα του αρχείου ή της εικόνας για εύκολη αναφορά και ταυτοποίηση μέσα στη διαδικασία. Αλυσίδα Ελέγχου (Hash): Για κάθε αρχείο υπολογίζεται μια μοναδική τιμή hash (π.χ. SHA-256) ώστε να επαληθεύεται η ακεραιότητα και η αυθεντικότητα του στοιχείου.

Αλυσίδα Κηδεμονίας (Chain of Custody): Αρχεία / Εικόνες

Μια εναλλακτική ενότητα χρησιμοποιείται όταν τα αποδεικτικά στοιχεία είναι αρχεία καταγραφής ή εικόνες που συλλέχθηκαν κατά τη διάρκεια της έρευνας. Η ενότητα αυτή περιλαμβάνει τα βασικά στοιχεία που χρειάζονται για την πλήρη τεκμηρίωση και την επαλήθευση των αποδεικτικών στοιχείων.

Image or File Details

Date / Time Acquired:	Created By:	Method:	Storage Drive:
5/30/19 1224 UTC	Gerard Johansen	Wireshark	USB Drive 1
File/Image Name:		Hash:	
EdgeFirewallCapture.PCAP / Packet Capture		1ceaa2393357d2ed88f81bec1e647af0	

- **Ημερομηνία/Ώρα Απόκτησης (Date/Time Acquired):** Καθορίζει με ακρίβεια την ημερομηνία και την ώρα κατά την οποία αποκτήθηκαν τα στοιχεία. Η σωστή χρονοσήμανση είναι κρίσιμη για την ανακατασκευή των γεγονότων του περιστατικού.
- **Περιγραφή (Description):** Σύντομη περιγραφή του μέσου ή του αρχείου, όπως «Firewall log file» ή «Disk image». Βοηθά στην ταυτοποίηση του αντικειμένου χωρίς να χρειάζεται να ανοίξει.
- **Μέθοδος (Method):** Αναφέρεται το εργαλείο ή η διαδικασία που χρησιμοποιήθηκε για την απόκτηση των στοιχείων. Σε άλλες περιπτώσεις μπορεί να περιγράφεται η απλή αντιγραφή σε εξωτερικό μέσο.
- **Μονάδα Αποθήκευσης (Storage Drive):** Καταγράφεται η συσκευή όπου αποθηκεύτηκε το στοιχείο, π.χ. «External HDD 1TB». Η σωστή καταγραφή εξασφαλίζει ότι τα στοιχεία παραμένουν ασφαλή και προσβάσιμα.
- **Όνομα Αρχείου/Εικόνας (File/Image Name):** Καταχωρείται το μοναδικό όνομα του αρχείου ή της εικόνας για εύκολη αναφορά και ταυτοποίηση μέσα στη διαδικασία. Αλυσίδα Ελέγχου (Hash): Για κάθε αρχείο υπολογίζεται μια μοναδική τιμή hash (π.χ. SHA-256) ώστε να επαληθεύεται η ακεραιότητα και η αυθεντικότητα του στοιχείου.

Αλυσίδα Κηδεμονίας (Chain of Custody): Βήματα Κύκλου Ζωής

Η ενότητα αυτή περιγράφει τα βήματα που ακολουθεί το αποδεικτικό στοιχείο κατά τον κύκλο ζωής του. Σε κάθε στάδιο καταγράφονται συγκεκριμένα δεδομένα, ώστε να διασφαλιστεί η διαφάνεια και η ιχνηλασιμότητα.

Chain of Custody

Tracking No:	Date/Time:	FROM:	TO:	Reason:
1	Date: 5/30/19	Name/Org: Carol Davies Global Services Corp.	Name/Org: Gerard Johansen IRProactive	Evidence Acquisition
	Time: 1224 UTC	Signature: *Carol Davies*	Signature: *Gerard T Johansen*	
2	Date: 5/30/19	Name/Org: G Johansen IRProactive	Name/Org: David Michell ACME Forensics	Analysis
	Time: 1305 UTC	Signature: *Gerard T Johansen*	Signature: *David Michell*	

- **Αριθμός Παρακολούθησης (Tracking No):** Υποδεικνύει τη θέση του αποδεικτικού στοιχείου στον κύκλο ζωής. Κάθε ενέργεια λαμβάνει το δικό της αριθμό για ευκολότερη παρακολούθηση.
- **Ημερομηνία/Ώρα (Date/Time):** Καταγράφεται για κάθε βήμα που εκτελείται. Έτσι μπορεί να ανακατασκευαστεί με ακρίβεια η πορεία του αποδεικτικού στοιχείου λεπτό προς λεπτό.
- **Από και Προς (FROM – TO):** Δείχνει ποιος ή ποιος χώρος είχε στην κατοχή του το στοιχείο. Όλες οι μεταφορές καταγράφονται και, όπου απαιτείται, υπογράφονται για να διασφαλιστεί υπευθυνότητα.
- **Λόγος (Reason):** Κάθε μετακίνηση πρέπει να αιτιολογείται. Ο λόγος καταγράφεται ώστε να είναι ξεκάθαρο γιατί έγινε το συγκεκριμένο βήμα.

Καταγραφή Μετακινήσεων Αποδεικτικών Στοιχείων

- Κάθε μετακίνηση καταγράφεται λεπτομερώς στο έντυπο αλυσίδας κηδεμονίας. Η πρώτη μετακίνηση αφορά συνήθως την κατάσχεση (π.χ. ενός σκληρού δίσκου από το data center). Σε αυτό το στάδιο δεν ορίζεται φύλακας, καθώς το στοιχείο μόλις αφαιρείται από το περιβάλλον του.
- Ο υπεύθυνος καταγραφής θεωρείται διαχειριστής του στοιχείου μέχρι τη μεταβίβασή του στον επόμενο φύλακα (π.χ. στον David Michell της ACME Forensics για ανάλυση).
- Η αλυσίδα κηδεμονίας πρέπει να παραμένει ενεργή σε όλο τον κύκλο ζωής του αποδεικτικού στοιχείου. Ακόμη και η καταστροφή ή η επιστροφή του καταγράφεται ως εγγραφή στο έντυπο.
- Τα έντυπα της αλυσίδας φυλάσσονται μαζί με όλο το παραγόμενο υλικό του περιστατικού και ενσωματώνονται σε οποιαδήποτε μεταγενέστερη αναφορά.

Ανάλυση (Analysis)

Μετά την εξαγωγή πιθανών σχετικών δεδομένων στη φάση της εξέτασης, ακολουθεί η **ανάλυση**. Ο αναλυτής ψηφιακής εγκληματολογίας εξετάζει τα δεδομένα αυτά σε συνδυασμό με άλλες πηγές που έχουν συλλεχθεί, προκειμένου να εξαχθούν **συμπεράσματα** και να κατανοηθεί η φύση του περιστατικού.

Παράδειγμα διαδικασίας:

- Εντοπισμός ενεργής σύνδεσης παραβιασμένου υπολογιστή με εξωτερική διεύθυνση **IP**.
- Συσχέτιση του ευρήματος με την ανάλυση καταγραφών πακέτων δικτύου.
- Απομόνωση της σχετικής κίνησης και αναγνώριση beaconing προς **C2 (Command & Control) server**.
- Διασταύρωση με επιπλέον πηγές για την ταυτοποίηση του συγκεκριμένου τρόπου επίθεσης που σχετίζεται με τη διεύθυνση **IP**.

Στόχος της ανάλυσης: Η **συσχέτιση και ερμηνεία** των αποδεικτικών στοιχείων ώστε να προσδιοριστεί η μέθοδος επίθεσης, η πηγή της απειλής και οι επιπτώσεις για το σύστημα ή τον οργανισμό.

Παρουσίαση (Presentation)

Η φάση της παρουσίασης αφορά τη **σύνταξη και κοινοποίηση των ευρημάτων** της ψηφιακής εγκληματολογικής έρευνας. Η αναφορά πρέπει να είναι **σαφής, ακριβής και αντικειμενική**, περιλαμβάνοντας όλα τα βήματα που ακολουθήθηκαν και τα κρίσιμα δεδομένα που συλλέχθηκαν. Στόχος είναι η τεκμηρίωση της διαδικασίας και η εξαγωγή **αξιόπιστων συμπερασμάτων** που θα υποστηρίξουν την έρευνα.

Κύρια σημεία:

- Σύνταξη **λεπτομερούς γραπτής αναφοράς** χωρίς προσωπικές απόψεις ή προκαταλήψεις.
- Ενσωμάτωση της αναφοράς στο πλαίσιο της συνολικής διερεύνησης του περιστατικού.
- Υποστήριξη στον εντοπισμό της **βασικής αιτίας** και των επιπτώσεων.

Συμμετοχή σε νομικές διαδικασίες: Ο αναλυτής ενδέχεται να κληθεί να καταθέσει σε **ποινικές ή αστικές υποθέσεις**. Σε αυτήν την περίπτωση:

- Παρουσιάζει τα γεγονότα με ακρίβεια και αντικειμενικότητα.
- Περιορίζεται σε **τεκμηριωμένες παρατηρήσεις** και όχι σε προσωπικές κρίσεις.
- Αν διαθέτει τον απαιτούμενο βαθμό εμπειρίας, μπορεί να λειτουργήσει και ως **μάρτυρας-ειδικός**, παρέχοντας εμπεριστατωμένη γνώμη.

Τι χρειαζόμαστε;

- **Εργαστήριο Ψηφιακής Εγκληματολογίας:** Η ψηφιακή εγκληματολογία απαιτεί ειδικά εργαλεία, τεχνικές και γνώσεις για την εξαγωγή αποδεικτικών στοιχείων. Χρειάζεται ξεχωριστός χώρος από τις κανονικές επιχειρησιακές δραστηριότητες ώστε να διασφαλίζεται η ιδιωτικότητα των αναλυτών και η ακεραιότητα των δεδομένων.
- **Φυσική Ασφάλεια:** Η πρόσβαση στο εργαστήριο πρέπει να ελέγχεται αυστηρά και να δίνεται μόνο σε άτομα με νόμιμη ανάγκη. Ο χώρος παραμένει κλειδωμένος και η πρόσβαση γίνεται ιδανικά με κάρτες ή fobs για πλήρη ιχνηλασιμότητα. Τα αποδεικτικά φυλάσσονται σε κλειδωμένες ντουλάπες, κατά προτίμηση ξεχωριστές ανά περιστατικό.
- **Εργαλεία:** Το εργαστήριο πρέπει να διαθέτει βασικά χειροκίνητα εργαλεία για φυσική πρόσβαση σε συσκευές, κουτιά ασφαλούς φύλαξης για αποδεικτικά, καθώς και σακούλες Faraday. Οι σακούλες επιτρέπουν την απομόνωση smartphones ή tablets από δίκτυα, διατηρώντας παράλληλα την τροφοδοσία τους.
- **Forensic Workstations:** Ισχυροί υπολογιστές με τουλάχιστον **32 GB RAM**, δύο δίσκους (OS/λογισμικό & αποδεικτικά ≥2TB). Χρησιμοποιούνται για imaging και ανάλυση μεγάλων όγκων δεδομένων.
- **Δευτερεύων Υπολογιστής:** Συνδεδεμένος στο διαδίκτυο για αναζήτηση και σύνταξη αναφορών. Η forensic workstation παραμένει offline για μέγιστη ασφάλεια.
- **Write Blockers & Imaging Stations:** Οι write blockers αποτρέπουν την εγγραφή σε αποδεικτικά μέσα. Προαιρετικά εγκαθίσταται ειδικός σταθμός forensic imaging για ταχύτερη αντιγραφή δίσκων.
- **Αποθηκευτικά Μέσα:** Εξωτερικοί USB δίσκοι 2–3 TB (≥6 τεμάχια) για αποθήκευση εικόνων. Χρήσιμοι και μικρότεροι USB 3.0 για log files & memory dumps.
- **Φορητός Εξοπλισμός:** Σκληρές θήκες για ασφαλή μεταφορά εργαλείων και forensic laptop. Εξασφαλίζεται προστασία από φθορά σε επιτόπιες εξετάσεις.

Λογισμικό (Software)

Βασικές Λειτουργίες: Το εργαστήριο πρέπει να διαθέτει λογισμικό για imaging δίσκων, ανάλυση εικόνων, ανάλυση μνήμης και σύνταξη αναφορών. Απαραίτητη η ύπαρξη εναλλακτικών εργαλείων για διασταύρωση αποτελεσμάτων.

Κύριες Εφαρμογές

- **Autopsy:** Ανοιχτού κώδικα, με αυτοματοποιημένα εργαλεία.
- **EnCase:** Εμπορικό, πλήρης ανάλυση και αναφορές.
- **FTK:** Ευρέως χρησιμοποιούμενο, εναλλακτική του EnCase.
- **X-Ways:** Ισχυρό, χαμηλότερου κόστους, χωρίς ανάγκη για δίκτυο.
- **Linux Εργαλεία**
- **DEFT Zero:** Ασφαλής απόκτηση δεδομένων.
- **Paladin:** Εργαλεία για malware, hashing και imaging.
- **SIFT:** Imaging, μνήμη, timelines, δωρεάν.
- **CAINE:** Πλήρης forensic διανομή Linux.

Επισκόπηση των δικτυακών αποδεικτικών στοιχείων

- **Πηγές Δικτυακών Αποδεικτικών:** Κάθε συσκευή δικτύου παρέχει διαφορετικά αποδεικτικά στοιχεία ανάλογα με τον κατασκευαστή και το μοντέλο. Το προσωπικό CSIRT πρέπει να γνωρίζει τον τρόπο πρόσβασης στα logs ή να έχει καθιερωμένες διαδικασίες με το IT για τη συλλογή στοιχείων κατά τη διάρκεια περιστατικού.
- **Switches:** Τα core και edge switches διαχειρίζονται τη ροή κυκλοφορίας. Παρέχουν: α) CAM tables για εντοπισμό μη εξουσιοδοτημένων συσκευών. β) Καταγραφή κυκλοφορίας για διερεύνηση περιστατικών.
- **Routers & Firewalls:** α) Routers: Routing tables, NetFlow δεδομένα και έλεγχος επιτρεπόμενων ροών. β) Firewalls: Ανίχνευση και πρόληψη εισβολών, λεπτομερή logs και ειδοποιήσεις.
- **Άλλες Συσκευές:** α) IDS/IPS: Εντοπίζουν ή μπλοκάρουν κακόβουλη δραστηριότητα. β) Web proxies: Καταγραφή πρόσβασης σε ιστότοπους και ειδοποιήσεις για C2 servers. γ) Domain controllers/DHCP/Application servers: Παρέχουν πληροφορίες για συνδέσεις, εκχωρήσεις IP και απομακρυσμένες συνδέσεις.

Προετοιμασία

Σημασία Προετοιμασίας: Η δυνατότητα απόκτησης στοιχείων δικτύου εξαρτάται από την προετοιμασία πριν από το περιστατικό. Χωρίς σωστά μέτρα ασφάλειας υποδομών, κρίσιμα στοιχεία μπορεί να χαθούν ή να μην είναι διαθέσιμα εγκαίρως στην ομάδα CSIRT.

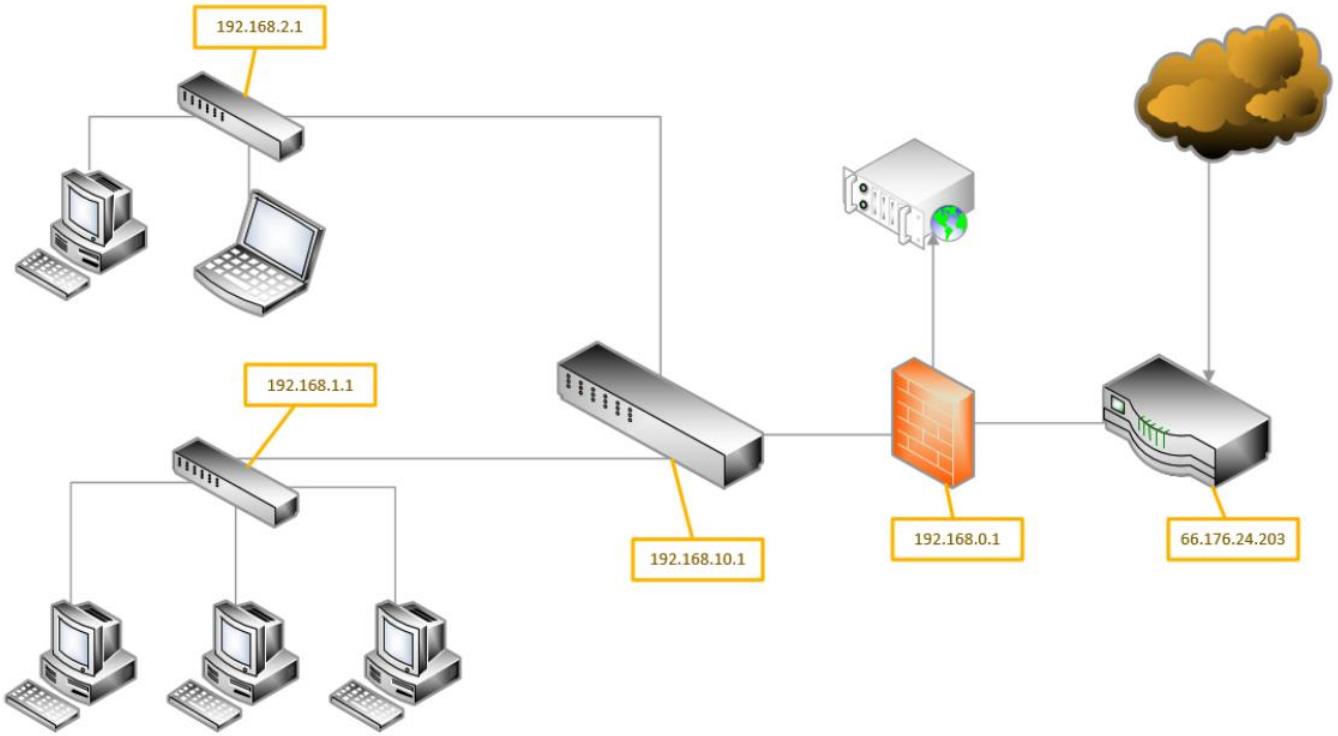
Τεχνικά Μέτρα Προετοιμασίας. Οι οργανισμοί πρέπει να διασφαλίσουν:

- Τεκμηρίωση του δικτύου (network documentation).
- Ενημερωμένες ρυθμίσεις συσκευών δικτύου.
- Κεντρική λύση διαχείρισης αρχείων καταγραφής (central log management).

Νομική Συμμόρφωση: Τα μέλη CSIRT πρέπει να γνωρίζουν κανονιστικά θέματα για τη συλλογή στοιχείων. Η παρακολούθηση κυκλοφορίας μπορεί να θεωρηθεί παραβίαση ιδιωτικότητας, εκτός αν υπάρχει σαφής πολιτική παρακολούθησης που ενημερώνει όλους τους υπαλλήλους πριν από τη συλλογή στοιχείων.

Διάγραμμα Δικτύου

- **Σημασία Διαγράμματος:** Οι ανακριτές περιστατικών χρειάζονται σαφή κατανόηση της δομής του δικτύου για τον εντοπισμό πιθανών πόρων στοιχείων. Ένα ενημερωμένο διάγραμμα δικτύου παρέχει γρήγορη αναγνώριση επιμέρους στοιχείων και πηγών αποδεικτικών στοιχείων.
- **Στοιχεία Διαγράμματος.** Το διάγραμμα πρέπει να περιλαμβάνει:
  - Switches, routers, wireless access points
  - Εσωτερικές διευθύνσεις IP για άμεση πρόσβαση στα συστήματα



- **Παράδειγμα Χρήσης:** Η κυκλοφορία από έναν φορητό υπολογιστή που επικοινωνεί με έναν C2 server μπορεί να εντοπιστεί ακολουθώντας τη διαδρομή της μέσα από switches, firewall και δρομολογητή προς το διαδίκτυο.
- **Διαμόρφωση Συσκευών:** Η διατήρηση τυπικών αποθηκευμένων διαμορφώσεων για switches και routers επιτρέπει την εύκολη ανίχνευση μη εξουσιοδοτημένων αλλαγών και υποστηρίζει ανάκτηση σε περίπτωση περιστατικού.

Συλλογή Δικτυακών Αποδεικτικών Στοιχείων

Firewalls & Proxy Logs: Τα firewalls και τα proxy logs παρέχουν κρίσιμες πληροφορίες για την κυκλοφορία εισόδου/εξόδου του δικτύου. Η πρόσβαση στο διαδίκτυο από κακόβουλο λογισμικό ή για εγκαθίδρυση C2 servers περνά από αυτά τα σημεία, καθιστώντας τα σημαντική πηγή αποδεικτικών στοιχείων.

Firewalls: Τα firewalls επόμενης γενιάς συνδυάζουν κανόνες allow/deny με IDS/IPS και έλεγχο εφαρμογών. Παρέχουν λεπτομερή εικόνα για συνδέσεις εισόδου και εξόδου, επιτρέποντας την ανίχνευση πιθανών παραβιάσεων ή ύποπτης δραστηριότητας.

Αρχεία Καταγραφής (Logs):

- **Connection logs:** Καταγράφουν διευθύνσεις IP και πρωτόκολλα για όλες τις συνδέσεις, περιλαμβάνοντας απορρίψεις που μπορεί να υποδηλώνουν αναγνώριση θυρών από επιτιθέμενους.
- **Remote access logs:** Δείχνουν ποιες συσκευές συνδέονται μέσω VPN ή απομακρυσμένης πρόσβασης και πότε, βοηθώντας στον εντοπισμό πηγής μόλυνσης και συσχέτιση δραστηριοτήτων.

Δικτυακά Αποδεικτικά Στοιχεία – Μέθοδοι & Εργαλεία

- **Ροές Δικτύου (NetFlow):** Μεταδεδομένα ροών κίνησης δικτύου καταγράφουν πηγή, προορισμό, όγκο και διαδρομή της κυκλοφορίας, χωρίς πλήρες περιεχόμενο πακέτων. Χρήσιμη για συνολική εικόνα δραστηριότητας. **Εργαλεία:** Silk, Nfsen, Nfdump
- **Συλλογή Πακέτων (Packet Capture):** Καταγραφή πακέτων σε πραγματικό χρόνο για ανάλυση περιεχομένου επικοινωνιών, troubleshooting και εντοπισμό επιθέσεων. **Εργαλεία:** Arkime (Moloch), Tcpdump, Wireshark, Tshark
- **NIDS (Network IDS):** Παρακολουθεί την κυκλοφορία του δικτύου και εντοπίζει κακόβουλη δραστηριότητα, χρησιμοποιώντας promiscuous mode. **Εργαλεία:** Snort, Suricata, Bro (Zeek), εμπορικά NIDS προϊόντα
- **Proxy Logs:** Καταγράφουν όλα τα αιτήματα προς το διαδίκτυο από χρήστες και εφαρμογές. Χρήσιμα για έλεγχο χρήσης και ανίχνευση ύποπτων αιτημάτων. **Εργαλεία:** Squid, εμπορικά Proxy προϊόντα
- **DNS Logs:** Παρακολούθηση αιτημάτων DNS για ανίχνευση εξαγωγής δεδομένων, επικοινωνιών C2 ή DNS tunneling. Συλλέγονται από servers, δίκτυο, endpoints ή passive DNS.

Σύνοψη:
NetFlow: Εικόνα ροής κυκλοφορίας
Packet Capture: Ανάλυση περιεχομένου πακέτων
NIDS: Ανίχνευση εισβολών
Proxy Logs: Έλεγχος αιτημάτων χρηστών/εφαρμογών
DNS Logs: Ανίχνευση επιθέσεων βασισμένων σε DNS

Web Proxy Server – Συλλογή Δικτυακών Αποδεικτικών Στοιχείων

Λειτουργία: Οι web proxy servers καταγράφουν όλα τα HTTP/HTTPS αιτήματα των συστημάτων στο εσωτερικό δίκτυο. Παρέχουν στοιχεία για ιστοσελίδες και URLs που προσπελάστηκαν. **Απειλή:** Οι επιτιθέμενοι χρησιμοποιούν scripting (VB, PowerShell) για λήψη κακόβουλου λογισμικού ή exploit μέσω URLs αντί για στατικές IP, ώστε να αλλάζουν εύκολα υποδομές.

Αξιοποίηση Logs:

- Εντοπισμός θέσης και κακόβουλου λογισμικού
- Ανίχνευση δραστηριότητας C2
- Ανάλυση ιστορικών δεδομένων εβδομάδων ή μηνών
- Στοιχεία: ημερομηνίες, ώρες, συστήματα και URLs

Σημείωση: Η ανάλυση web proxy logs είναι κρίσιμη για τη διατήρηση αποδεικτικών στοιχείων και την ανακατασκευή της αλυσίδας επίθεσης.

NetFlow – Παρακολούθηση Δικτυακής Κυκλοφορίας

Ορισμός: Λειτουργία που υπάρχει σε switches και routers για παρακολούθηση της κυκλοφορίας. Αποστέλλει δεδομένα σε NetFlow Collector μέσω UDP.

Χρήση σε Ασφάλεια: Αναλυτές περιστατικών αποκτούν εικόνα της εσωτερικής κυκλοφορίας (east-west traffic).

- Εντοπισμός κινήσεων επιτιθέμενων μεταξύ υποδικτύων και συστημάτων.
- Συλλογή πληροφοριών: διευθύνσεις IP, πρωτόκολλα, μέγεθος δεδομένων.

Πλεονεκτήματα:

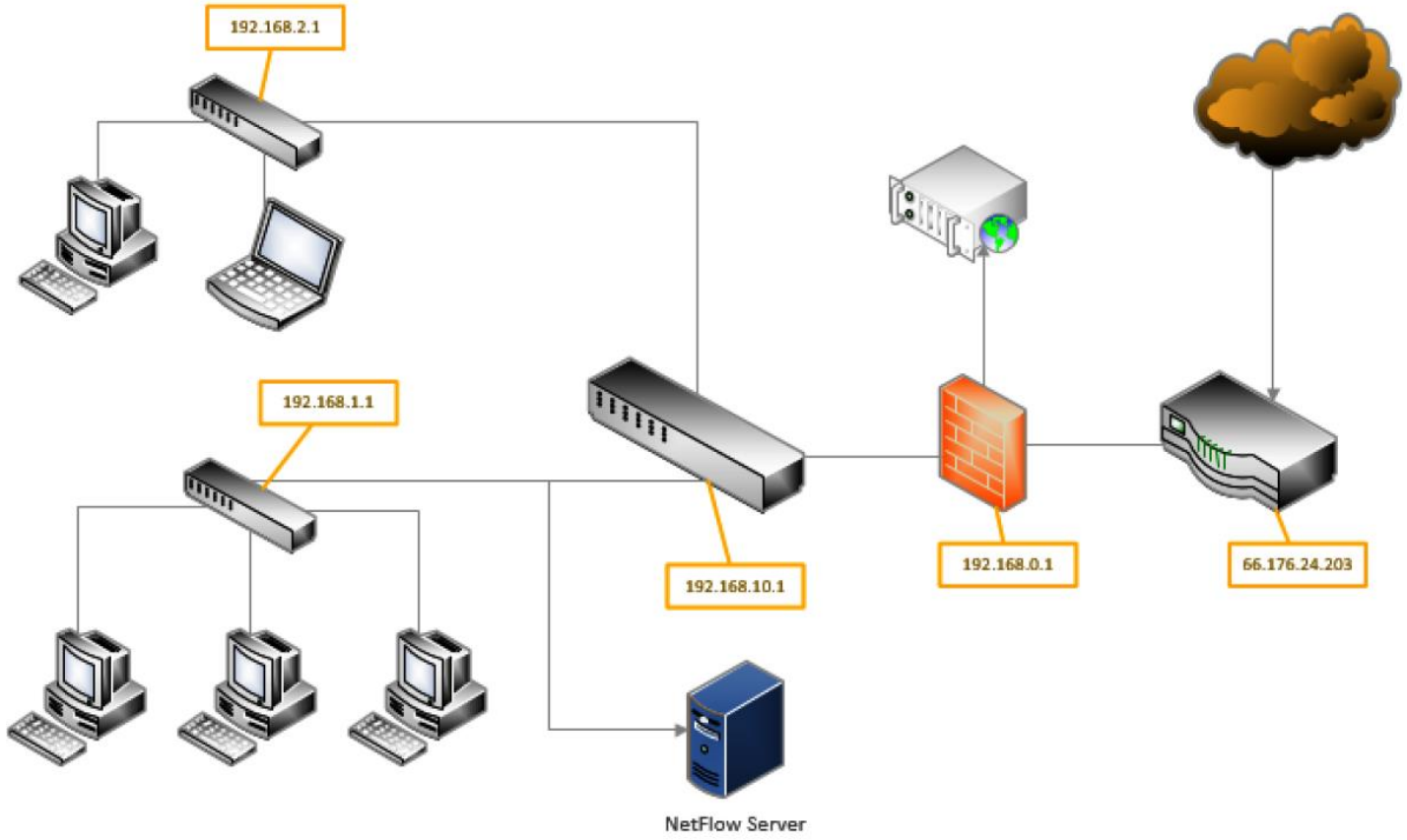
- Παρέχει δεδομένα για την απόκριση περιστατικών.
- Χρήσιμη και για καθημερινή λειτουργία δικτύου (ανίχνευση καθυστερήσεων, προβλημάτων).
- Ευέλικτη διαμόρφωση ανά τύπο συσκευής και προϋπολογισμό.

Σημείωση: Η ενσωμάτωση NetFlow στις λειτουργίες δικτύου διευκολύνει ανάλυση συμβάντων και συντήρηση δικτύου ταυτόχρονα.

Καταγραφές Πακέτων (Packet Captures)

Σκοπός: Παρακολούθηση και ανάλυση δικτυακής κυκλοφορίας για: α) Εντοπισμό επικοινωνίας με C2 servers. β) Ανίχνευση πιθανής εξαγωγής δεδομένων (exfiltration).

- **Network Tap:** Τοποθετείται ανάμεσα στον υπολογιστή και το switch για άμεση καταγραφή πακέτων.
- **Switched Port Analyzer (SPAN / Port Mirroring):** Καθρεφτίζει την κυκλοφορία μιας θύρας σε άλλη για συλλογή δεδομένων.
- Ενσωματωμένα εργαλεία σε συσκευές: π.χ. tcpdump για άμεση καταγραφή και ανάλυση.



Πλεονεκτήματα: Πλήρης εικόνα επικοινωνίας δικτύου. Μπορεί να γίνει απομακρυσμένα (σε περίπτωση εργαλείων στο switch). **Μειονεκτήματα:** Περιορισμένη χωρητικότητα αποθήκευσης σε switch.Υψηλή φόρτιση μπορεί να οδηγήσει σε απώλεια πακέτων.

Tcpdump – Packet Capture

Περιγραφή:

- Εργαλείο γραμμής εντολών για packet capture.
- Διαθέσιμο σε Linux και σε πολλές συσκευές δικτύου.
- Απαιτεί συχνά δικαιώματα root για πλήρη πρόσβαση στην κυκλοφορία.
- Τεκμηρίωση: tcpdump.org

Capture πακέτων από συγκεκριμένη πηγή IP:

- **sudo tcpdump -i ens33 src host 192.168.10.54**

Capture πακέτων προς συγκεκριμένο προορισμό IP:

- **sudo tcpdump -i ens33 dst host 162.4.5.23**

```
File  Edit  View  Search  Terminal  Help
(1), length 84)
    ubuntu > dns.google: ICMP echo request, id 40024, seq 47, length 64
08:31:08.437340 IP (tos 0x0, ttl 128, id 43477, offset 0, flags [none], proto IC
MP (1), length 84)
    dns.google > ubuntu: ICMP echo reply, id 40024, seq 47, length 64
08:31:09.420894 IP (tos 0x0, ttl 64, id 54227, offset 0, flags [DF], proto ICMP
(1), length 84)
    ubuntu > dns.google: ICMP echo request, id 40024, seq 48, length 64
08:31:09.440265 IP (tos 0x0, ttl 128, id 43478, offset 0, flags [none], proto IC
MP (1), length 84)
```

Βασικές εντολές

1. Βοήθεια: tcpdump -h
2. Προβολή διαθέσιμων διεπαφών: tcpdump -D
3. Βασική καταγραφή σε Ethernet διεπαφή ens33:
   - **sudo tcpdump -i ens33 -v**

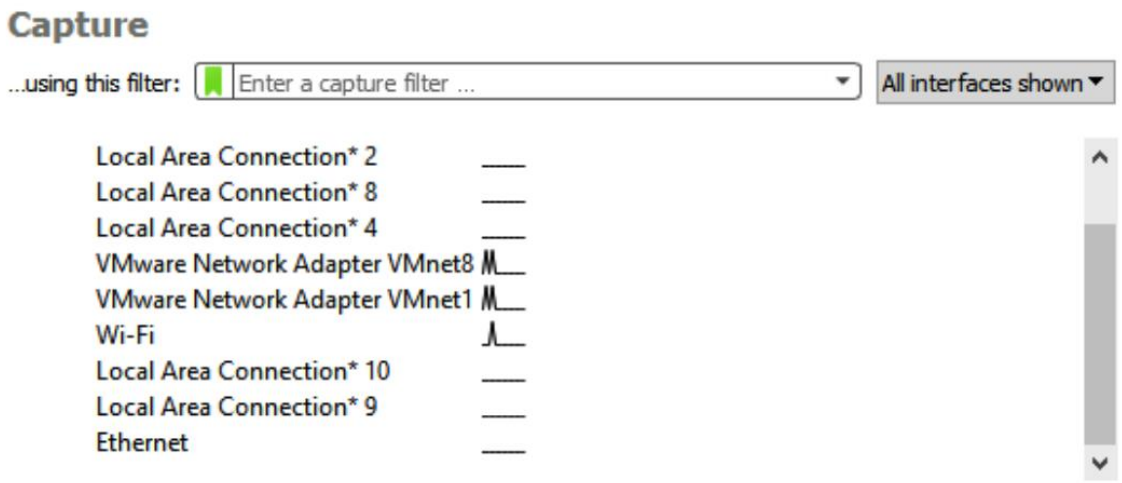
   -i: ορίζει τη διεπαφή για capture

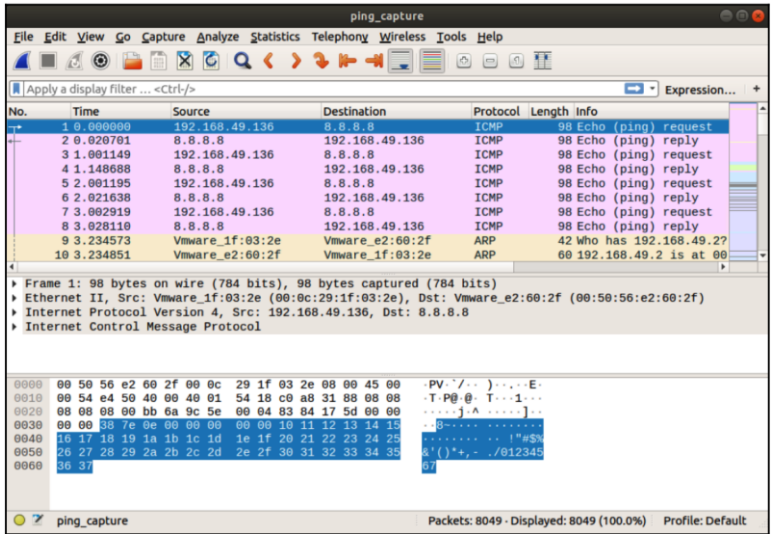
   -v: καθορίζει λεπτομέρεια καταγραφής (verbosity)

   Για περισσότερη λεπτομέρεια: -vvv

Wireshark

- **Εισαγωγή:** Το Wireshark είναι εργαλείο GUI για Unix και Windows, σχεδιασμένο για καταγραφή και ανάλυση πακέτων. Διαφέρει από εργαλεία γραμμής εντολών όπως το tcpdump, καθώς προσφέρει πλήθος λειτουργιών για λεπτομερή ανάλυση κυκλοφορίας.
- **Εγκατάσταση & Εκτέλεση:** Η ανάπτυξη του Wireshark σε περιστατικά μπορεί να καθυστερήσει, αφού απαιτεί εγκατάσταση. Υποστηρίζεται κυρίως σε Windows και macOS, ενώ σε Linux χρειάζεται επιπλέον προσπάθεια. Το εργαλείο μπορεί να εκτελεστεί και από USB drive.
- **Καταγραφή Πακέτων:** Οι αναλυτές επιλέγουν διεπαφή (π.χ. Wi-Fi) για καταγραφή. Κάνοντας διπλό κλικ, ξεκινά η καταγραφή και εμφανίζεται σε πραγματικό χρόνο για άμεση ανάλυση.
- **Αποθήκευση & Τερματισμός:** Για να σταματήσει η καταγραφή, πατάμε το κόκκινο κουμπί πάνω αριστερά. Το αρχείο μπορεί να αποθηκευτεί για περαιτέρω ανάλυση και διερεύνηση περιστατικών.





Mergecap – Συνδυασμός Αρχείων Πακέτων

Το mergecap είναι εργαλείο γραμμής εντολών που συνοδεύει το Wireshark. Επιτρέπει τον **συνδυασμό πολλαπλών αρχείων καταγραφής** πακέτων από Wireshark, tcpdump ή RawCap. Είναι χρήσιμο όταν οι αναλυτές έχουν συλλέξει δεδομένα από πολλές πηγές.

Χρήση: Με το mergecap, οι αναλυτές μπορούν να ελέγξουν την κυκλοφορία προς συγκεκριμένο υπολογιστή. Αυτό διευκολύνει την ανάλυση πολυπληθών αρχείων καταγραφής χωρίς χειροκίνητο έλεγχο κάθε αρχείου ξεχωριστά.

Παράδειγμα Εντολής - Για βοήθεια

- **mergecap –help**

Για συγχώνευση:

- **mergecap -w switches.pcap switch1.pcap switch2.pcap switch3.pcap**

Πλεονέκτημα:Ο συνδυασμός πολλαπλών καταγραφών επιτρέπει στους αναλυτές να εξετάσουν ευρύτερο φάσμα δραστηριοτήτων δικτύου. Είναι ιδιαίτερα χρήσιμο για αναγνώριση κυκλοφορίας προς ύποπτες IP ή εξωτερικούς C2 servers.

Συλλογή Δικτυακών Αποδεικτικών Στοιχείων

Για σωστή ανάλυση αρχείων καταγραφής και πακέτων, τα δεδομένα συχνά μετακινούνται εκτός σύνδεσης. Η προσεκτική διαχείριση είναι απαραίτητη ώστε να αποφευχθεί καταστροφή ή τροποποίηση. Μια κοινή πρακτική είναι η μεταφορά σε USB drive και η δημιουργία hash πριν από οποιαδήποτε ανάλυση.

Τεκμηρίωση: Η συλλογή αποδεικτικών στοιχείων πρέπει να καταγράφεται με ακρίβεια. Κάθε αρχείο πρέπει να μπορεί να αναχθεί στην πηγή, στην ημερομηνία και στην ώρα συλλογής του. Αυτό βοηθά στη διατήρηση της αξιοπιστίας των στοιχείων για μελλοντική ανάλυση.

Φύλλο Καταγραφής: Το φύλλο περιλαμβάνει στοιχεία όπως: Όνομα Αρχείου, Περιγραφή, Τοποθεσία, Ημερομηνία και Ώρα, Συλλέχθηκε από, MD5 Hash. Το hash παρέχει ψηφιακό αποτύπωμα για να διασφαλιστεί η ακεραιότητα του αρχείου.

Υπολογισμός Hash: Το MD5 hash μπορεί να υπολογιστεί με το πρόγραμμα md5sum σε Linux:

- md5sum ping_capture

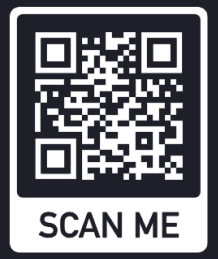
Μετά τη συλλογή, τα αρχεία αποθηκεύονται σε μέσο αποθήκευσης και συμπληρώνεται η φόρμα αλυσίδας φύλαξης (chain of custody) πριν από την ανάλυση.

File Name	Description	Location	Date	Time	Collected By	MD5 Hash
Ping_capture	Packet Capture of Ping activity	192.168.2.1	6/26/19	1642	GTJ	7e559dc8eeeb66115566d93f96e7dfb8

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr