

Module 03

Cybersecurity 3

Modèle de Journal d'Analyse Forensique

Informations Générales

Élément	Valeur
Analyste	[Nom, prénom]
Date de l'analyse	[JJ/MM/AAAA]
Heure de début	[HH:MM]
Heure de fin	[HH:MM]
Numéro de dossier / Référence	[EX : CASE-2025-07-001]
Support analysé	[Disque dur / Clé USB / Image disque (ex : .E01, .dd)]
Nom du fichier/image analysé	[Ex : suspect01.E01]
Outils utilisés	[Autopsy, Sleuth Kit, Volatility, etc.]
Localisation de l'image analysée [Chemin absolu vers le fichier ou stockage]	

Objectif de l'analyse

(Ex : Rechercher des documents supprimés, identifier l'exfiltration de données, détecter un malware, etc.)

Étapes d'analyse effectuées

Heure	Action réalisée	Outil utilisé	Commentaire / Résultat
09:12	Monté l'image disque suspect01.E01	Autopsy	Image montée avec succès

Heure	Action réalisée	Outil utilisé	Commentaire / Résultat
09:15	Analyse du MFT (Master File Table)	Sleuth Kit (fls/mactime)	Liste des fichiers récupérée, timeline générée
09:50	Recherche de fichiers récemment supprimés	Autopsy	4 fichiers supprimés retrouvés dans la corbeille
10:30	Extraction des fichiers suspects (.exe et .docx)	Autopsy	Sauvegardés dans dossier /mnt/investigation/extractions
11:00	Recherche de présence de clé USB insérée récemment	Sleuth Kit / RegRipper	Présence d'un périphérique USB le 12/07/2025 à 23h12
11:45	Export de l'historique du navigateur (Chrome)	Autopsy	Navigation vers mega.nz, possible exfiltration détectée
12:15	Génération de hash SHA256 des fichiers suspects	Autopsy / sha256sum	Hashs générés, consignés ci-dessous

Hachages des fichiers extraits

Nom du fichier	Chemin local	SHA256
trojan.exe	/mnt/extraction/trojan.exe	e3b0c44298fc1c14 ...
rapport_confidentiel.docx	/mnt/extraction/rapport_confidentiel.docx	9f86d081884c7d65 ...

Captures / Exportations

- **Timeline MFT exportée** : /mnt/report/timeline_mft.csv
- **Captures d'écran de la navigation suspecte** : /mnt/report/screenshots/
- **Rapport Autopsy HTML** : /mnt/report/autopsy_case01.html

Observations personnelles

(Notez tout comportement suspect, difficulté technique, ou point nécessitant validation supplémentaire.)

☒ **Signature de l'analyste**

Nom : _____

Signature : _____

Date : _____