

Corrigé complet - Lab 01

Analyse forensique du volume NTFS ntfs1-gen2.E01

Élément	Valeur
Source analysée	L01-ntfs1-gen2(2).E01
Nature réelle	Image de test NTFS autonome, sans installation Windows complète
Support	Corrigé apprenant avec réponses attendues
Date de production	6 août 2026

Conclusion principale - Le fichier fourni ne contient pas un poste Windows compromis. Il contient un volume NTFS de démonstration structuré autour de trois répertoires - RAW, Compressed et Encrypted - et de fichiers de test. Le corrigé adapte donc honnêtement le scénario aux preuves observables.

1. Objet et périmètre

Ce document complète le Lab 01 à partir de l'image E01 réellement fournie. Il distingue les résultats prouvés, les commandes à exécuter par les apprenants et les limites du jeu de données.

Règle forensique - On ne déduit jamais une compromission à partir du seul intitulé du laboratoire. Toute conclusion doit être reliée à un artefact observé, un horodatage, un chemin ou une empreinte.

2. Vérification de la preuve

Contrôle	Résultat
Taille du conteneur E01	36,083,007 octets
MD5 du fichier E01	5e28d70f86f8e105fec78a89b0cbea63
SHA-256 du fichier E01	2badead91bef56c80155d7731671ad1d93c08f32cd4ce17566fdf02d5769feea
MD5 du média logique exporté	27a9053e35aac74608493e755353cb95
Taille du média logique	516 554 752 octets (1 008 896 secteurs x 512)

```
sha256sum 'L01-ntfs1-gen2(2).E01'
```

```
md5sum 'L01-ntfs1-gen2(2).E01'
```

Résultat attendu : les empreintes doivent rester identiques avant et après l'analyse. L'empreinte du conteneur E01 et celle du média logique sont deux objets différents.

3. Préparation de l'environnement

3.1 Correction de la copie du fichier

```
mkdir -p ~/cyberlab/data
```

```
cp 'L01-ntfs1-gen2(2).E01' ~/cyberlab/data/ntfs1-gen2.E01
```

```
cd ~/cyberlab
```

Le renommage évite les espaces, parenthèses et incohérences entre le nom du sujet et le nom effectivement fourni.

3.2 Docker Compose corrigé

```
services:
  sleuthkit:
    image: sleuthkit/tsk
    volumes:
      - ./data:/data:ro
    stdin_open: true
    tty: true
  autopsy:
    image: fkiedad/autopsy
    ports:
      - "9999:9999"
    volumes:
      - ./data:/data:ro
```

Correction importante - Le suffixe :ro monte la preuve en lecture seule. Le champ version: "3.8" est aujourd'hui facultatif avec Docker Compose moderne.

4. Analyse initiale du volume

4.1 Export ou montage E01

```
mkdir -p /mnt/ewf
```

```
ewfmount /data/ntfs1-gen2.E01 /mnt/ewf
```

```
ls -lh /mnt/ewf/ewf1
```

Dans ce jeu de données, le média logique est un volume NTFS direct : il n'existe pas de table de partitions MBR/GPT à traverser.

4.2 Résultat attendu de fsstat

```
fsstat /mnt/ewf/ewf1
```

Paramètre	Valeur observée
Système de fichiers	NTFS
Octets par secteur	512
Secteurs par cluster	1
Taille de cluster	512 octets
Nombre total de secteurs	1 008 896
Taille logique	516 554 752 octets
Cluster de départ de la \$MFT	336 298
Taille d'un enregistrement MFT	1 024 octets
Taille de la \$MFT	98 304 octets, soit 96 enregistrements

5. Inventaire réel des artefacts

Les entrées utiles sont les enregistrements MFT 27 à 49. Aucun profil C:\Users, aucun registre Windows, aucun Prefetch et aucun journal EVTXT n'est présent.

MFT	État	Chemin	Taille
27	Alloué	/RAW	Dossier
28	Alloué	/Compressed	Dossier
29	Alloué	/Encrypted	Dossier
31-33	Alloué	NIST_logo.jpg dans les trois dossiers	2 205 octets
34-36	Alloué	NISTSP800-88_rev1.pdf dans les trois dossiers	554 121 octets

37-39	Alloué	report02-3.pdf dans les trois dossiers	1 421 998 octets
40-42	Alloué	20076517123273.pdf dans les trois dossiers	1 001 647 octets
43	Alloué	/EFS-key-no-password.pfx	1 730 octets
44	Alloué	/EFS-key-password.pfx	1 730 octets
45	Alloué	/EFS-key-password-strong-protection.pfx	1 734 octets
46	Alloué	/EFS-key-info.txt	57 octets
47-49	Alloué	logfile1.txt dans RAW, Compressed, Encrypted	Données NTFS particulières

Interprétation - La structure est conçue pour comparer le stockage NTFS normal, compressé et chiffré EFS. Les fichiers PFX sont des clés/certificats de test. Ils ne constituent pas, à eux seuls, un indicateur de compromission.

6. Corrigé ligne par ligne du sujet

Étape 1 - Préparation

Ligne du lab	Corrigé attendu	Explication
mkdir -p ~/cyberlab/data	Correct	Crée l'arborescence sans erreur si elle existe déjà.
cp ntfs1-gen2.E01 ~/cyberlab/data/	À adapter au nom reçu	Renommer le fichier évite les caractères spéciaux.
cd ~/cyberlab	Correct	Place le terminal au niveau du compose et du dossier data.
docker compose up -d	Correct après création du YAML	Lance les services en arrière-plan.

Étape 2 - Analyse initiale

Ligne du lab	Correction	Résultat attendu
docker run -it --rm -v \$(pwd)/data:/data sleuthkit/tsk bash	Ajouter :ro	La preuve est accessible sans écriture.
ewfmount /data/ewf1.E01 /mnt/ewf	Nom incorrect	Utiliser /data/ntfs1-gen2.E01.
fsstat /mnt/ewf/ewf1.raw	Nom possiblement incorrect	ewfmount crée généralement ewf1, pas ewf1.raw.
fls -r -m / /mnt/ewf/ewf1 > /data/bodyfile.txt	Correct	Produit un bodyfile récursif.
Identifier l'utilisateur principal	Non applicable	Aucun dossier Users ni profil Windows dans cette image.

Étape 3 - Analyse des artefacts

```
fls -r -p /mnt/ewf/ewf1
fls -r -d -p /mnt/ewf/ewf1
istat /mnt/ewf/ewf1 43
icat /mnt/ewf/ewf1 46 > /data/EFS-key-info.txt
```

Réponse attendue : les dossiers à inspecter sont /RAW, /Compressed, /Encrypted et la racine contenant les clés PFX. La recherche d'applications installées est impossible, car l'image ne contient pas une installation Windows.

Étape 4 - Timeline

```
fls -r -m / /mnt/ewf/ewf1 > /data/bodyfile.txt
mactime -b /data/bodyfile.txt -d > /data/timeline.csv
```

Amélioration - L'option -d produit un CSV plus exploitable. Il faut documenter le fuseau horaire du poste d'analyse et ne pas convertir silencieusement les timestamps.

Étape 5 - Interprétation

Question du sujet	Réponse fondée sur la preuve
Point d'entrée : EXE douteux ?	Aucun fichier EXE observé.
Autorun ou clé de registre modifiée ?	Non vérifiable : aucune ruche de registre.
Accès réseau ou exfiltration ?	Non vérifiable : aucun PCAP, historique navigateur ou journal réseau.
Programme en autostart ?	Non vérifiable.
Corrélation via timeline ?	Oui, mais uniquement pour les opérations sur les fichiers de test NTFS.
Compromission confirmée ?	Non. Le jeu de données ne fournit aucun élément suffisant pour l'affirmer.

7. Construction et lecture de la timeline

Horodatage principal	Événement interprétable
31/12/2008 22:44:17	Création du dossier RAW.
31/12/2008 22:44:33	Création du dossier Compressed.
31/12/2008 22:44:43	Création du dossier Encrypted.
31/12/2008 23:03:26 à 23:03:36	Copie de NIST_logo.jpg dans les trois variantes.
31/12/2008 23:06:17 à 23:06:24	Copie de NISTSP800-88_rev1.pdf dans les trois variantes.
31/12/2008 23:09:31 à 23:09:38	Copie de report02-3.pdf dans les trois variantes.
31/12/2008 23:16:20 à 23:16:29	Copie de 20076517123273.pdf dans les trois variantes.
05/01/2009 21:44	Création/export des fichiers de clés EFS PFX.

05/01/2009 22:00	Mise à jour des métadonnées de plusieurs dossiers.
------------------	--

Ces dates décrivent la fabrication du corpus de test. Elles ne décrivent pas une chaîne d'attaque.

8. Interprétation forensique

- Le média est un volume NTFS autonome et non un disque système Windows complet.
- Les mêmes documents sont présents sous trois formes : non compressée, compressée NTFS et chiffrée EFS.
- Les clés PFX à la racine sont cohérentes avec un exercice EFS.
- Aucun IOC de malware, aucune persistance, aucun compte utilisateur et aucun événement réseau ne peuvent être établis.
- Les enregistrements orphelins sans nom ne doivent pas être automatiquement qualifiés de fichiers supprimés malveillants ; ils peuvent correspondre à des attributs NTFS ou à des extensions de données.

Réponse finale apprenant - L'hypothèse « poste Windows compromis » n'est pas confirmée. L'image permet une analyse de structure NTFS, de compression et de chiffrement EFS, mais pas une investigation complète de compromission.

9. Livrables attendus - modèle rempli

9.1 Résumé exécutif

L'image E01 a été vérifiée puis exportée en média logique. Le système de fichiers identifié est NTFS. L'analyse de la MFT montre un corpus de test composé de fichiers identiques stockés dans des répertoires RAW, Compressed et Encrypted, ainsi que de clés EFS au format PFX. Aucun artefact ne permet de conclure à une compromission du système.

9.2 Tableau de preuves

Type	Horodatage	Chemin	Indicateur	Raison
Dossier	2008-12-31 22:44:17	/RAW	MFT 27	Stockage non compressé
Dossier	2008-12-31 22:44:33	/Compressed	MFT 28	Comparaison compression NTFS
Dossier	2008-12-31 22:44:43	/Encrypted	MFT 29	Comparaison chiffrement EFS
Certificat	2009-01-05 21:44:06	/EFS-key-no-password.pfx	MFT 43	Clé EFS de test
Texte	2009-01-05	/EFS-key-info.txt	MFT 46	Documentation associée aux clés

9.3 Colonnes CSV recommandées

record_id,status,type,timestamp_type,timestamp,path,size,sha256,reason,analyst_note

10. Conclusion et recommandations

- Renommer le lab en « Analyse forensique d'un volume NTFS : fichiers RAW, compressés et chiffrés ».
- Retirer les questions sur les utilisateurs, les applications installées, les autoruns et le réseau pour ce corpus.
- Ajouter une seconde image Windows complète si l'objectif pédagogique reste la détection d'une compromission.
- Conserver les commandes fls, icat, istat, fsstat et mactime, qui sont parfaitement adaptées à ce jeu de données.
- Exiger une séparation claire entre observation, interprétation et hypothèse dans le rapport apprenant.

Annexe A - Commandes consolidées

```
mkdir -p ~/cyberlab/data /mnt/ewf
cp 'L01-ntfs1-gen2(2).E01' ~/cyberlab/data/ntfs1-gen2.E01
sha256sum ~/cyberlab/data/ntfs1-gen2.E01
ewfinfo ~/cyberlab/data/ntfs1-gen2.E01
ewfverify ~/cyberlab/data/ntfs1-gen2.E01
ewfmount ~/cyberlab/data/ntfs1-gen2.E01 /mnt/ewf
fsstat /mnt/ewf/ewf1
fls -r -p /mnt/ewf/ewf1
fls -r -d -p /mnt/ewf/ewf1
istat /mnt/ewf/ewf1 43
icat /mnt/ewf/ewf1 46 > ~/cyberlab/data/EFS-key-info.txt
fls -r -m /mnt/ewf/ewf1 > ~/cyberlab/data/bodyfile.txt
mactime -b ~/cyberlab/data/bodyfile.txt -d > ~/cyberlab/data/timeline.csv
```

Annexe B - Grille de correction

Critère	Points	Attendu
Intégrité de la preuve	10	Empreinte calculée et distinction E01/média logique.
Montage en lecture seule	10	Volume /data:ro et ewfmount correct.
Identification NTFS	15	Secteurs, clusters, MFT et taille correctement interprétés.
Inventaire	20	RAW, Compressed, Encrypted, PFX et fichiers documentés.
Timeline	20	Bodyfile, mactime CSV et événements clés.
Interprétation	15	Absence de conclusion abusive sur une compromission.
Rapport	10	Observations, preuves, limites et recommandations.