

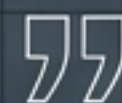


Collecte et conservation des preuves numériques

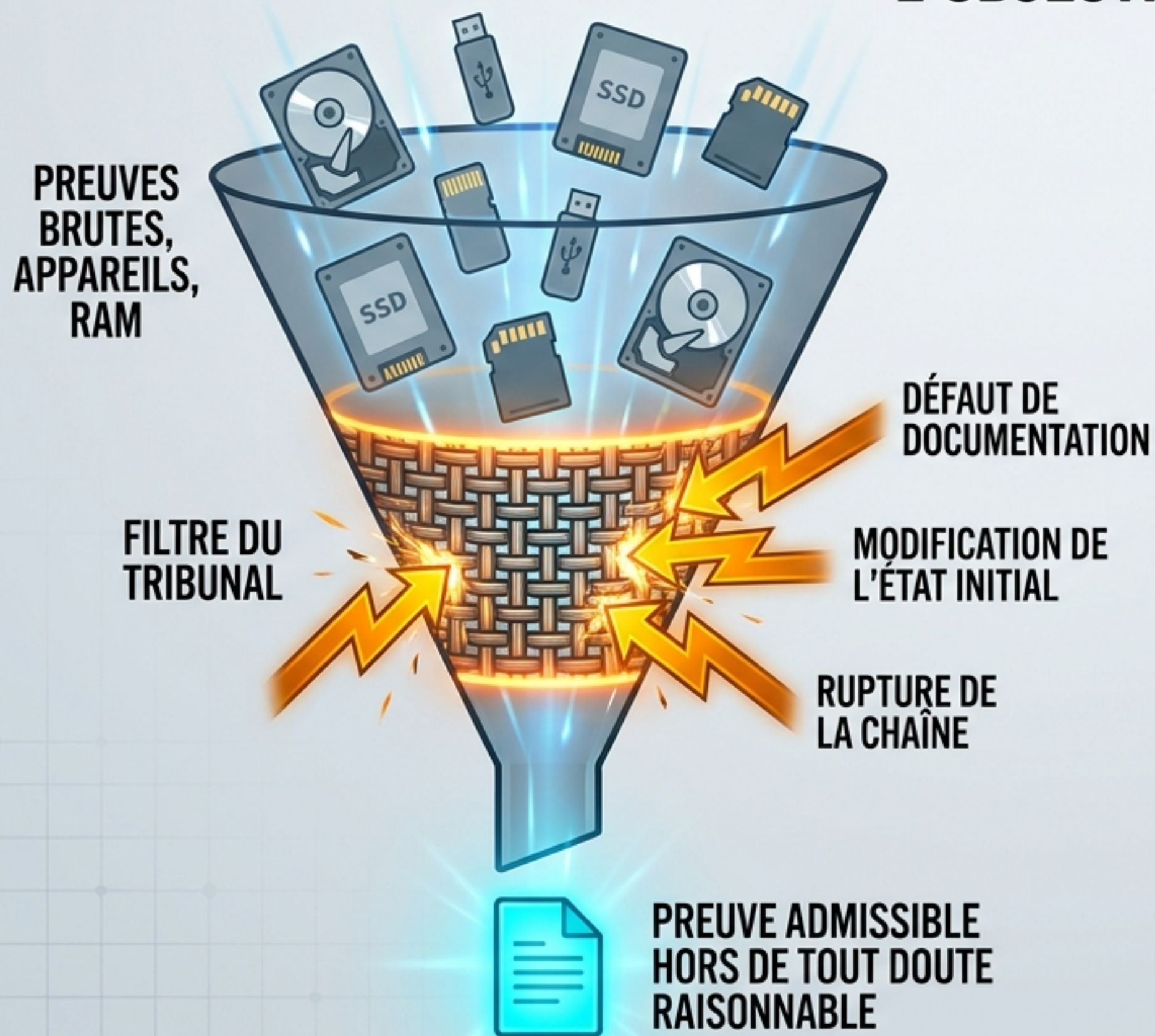
Le manuel tactique de survie juridique et technique pour les premiers intervenants.



« *Des affirmations extraordinaires exigent des preuves extraordinaires.* »



— Carl Sagan



L'OBJECTIF ULTIME N'EST PAS LA DÉCOUVERTE, MAIS LA NON-CONTAMINATION.

Une erreur de collecte compromet l'ensemble du travail sur le plan juridique.



Toute modification non documentée est une contamination introduite par l'enquêteur, pas par le criminel.

L'incapacité à répondre aux contestations de la défense entraîne le rejet absolu des preuves.

Sécuriser la scène : L'établissement du périmètre

1. Identifier



Repérer tout appareil doté d'une capacité de stockage (Ordinateurs, mobiles, caméras, serveurs, routeurs, équipements IoT).

2. Isoler



Délimiter la zone. Empêcher l'accès aux personnes non autorisées et empêcher le suspect d'effacer ses traces.

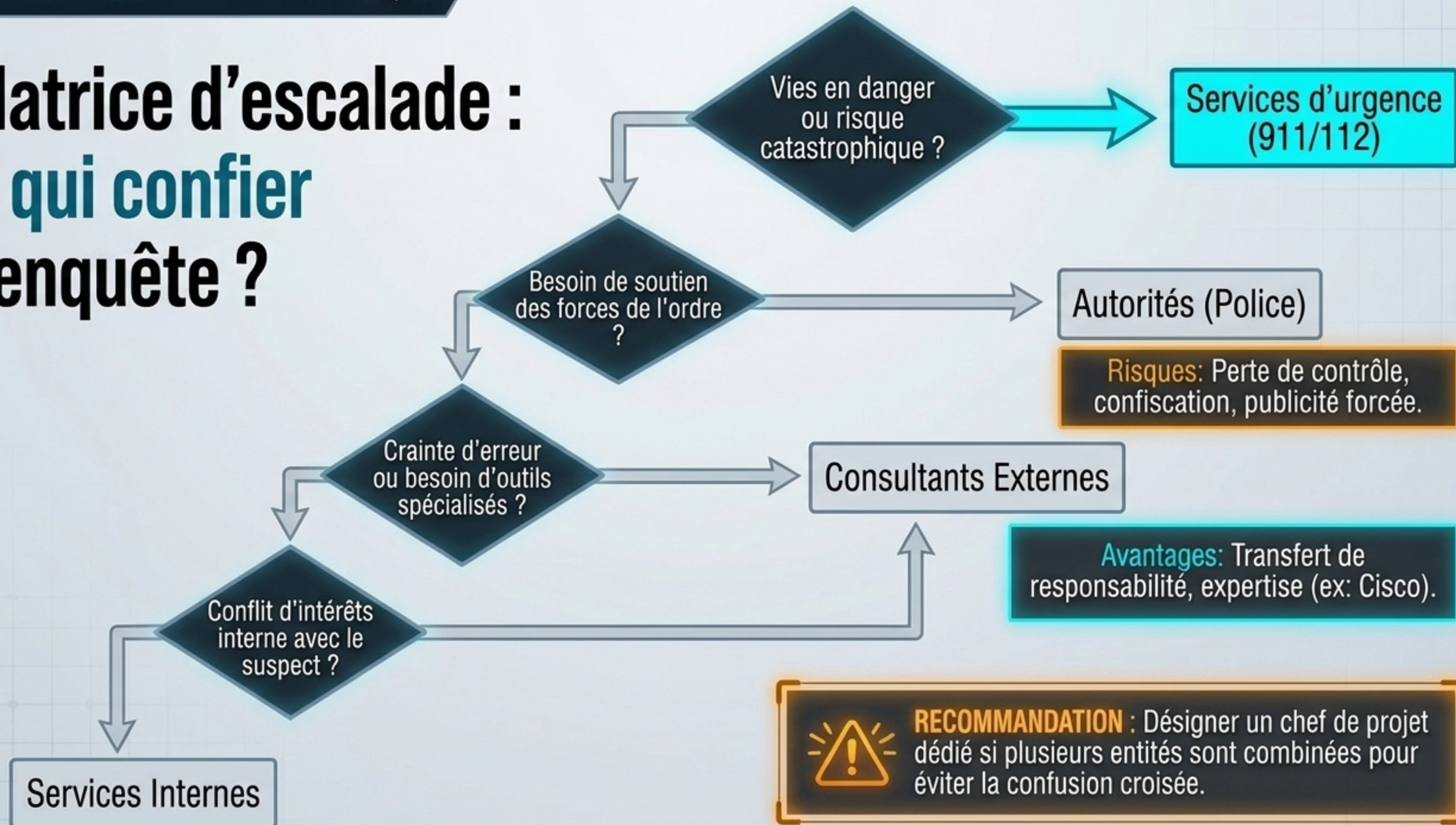
3. Documenter



Figurer l'environnement avant toute investigation. Si le transport est impossible, copier l'état actuel sur place.

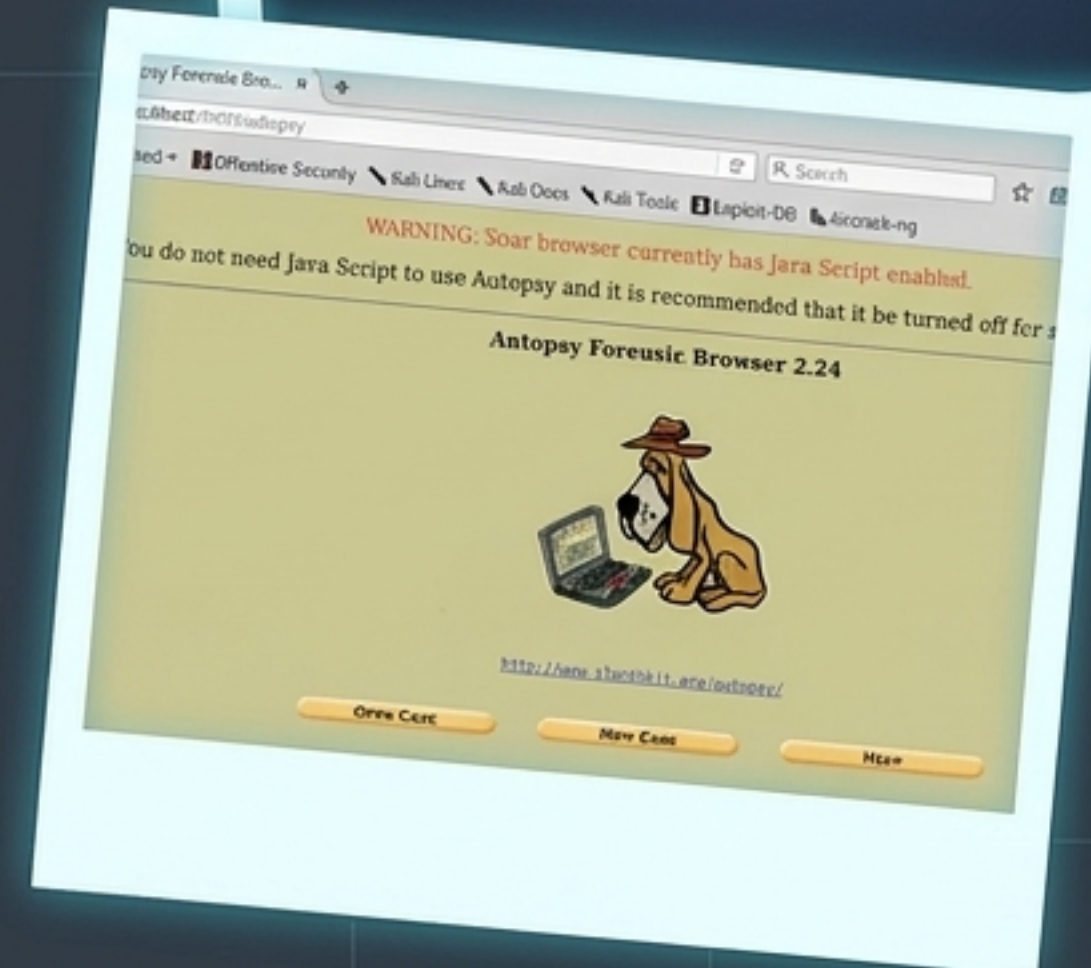
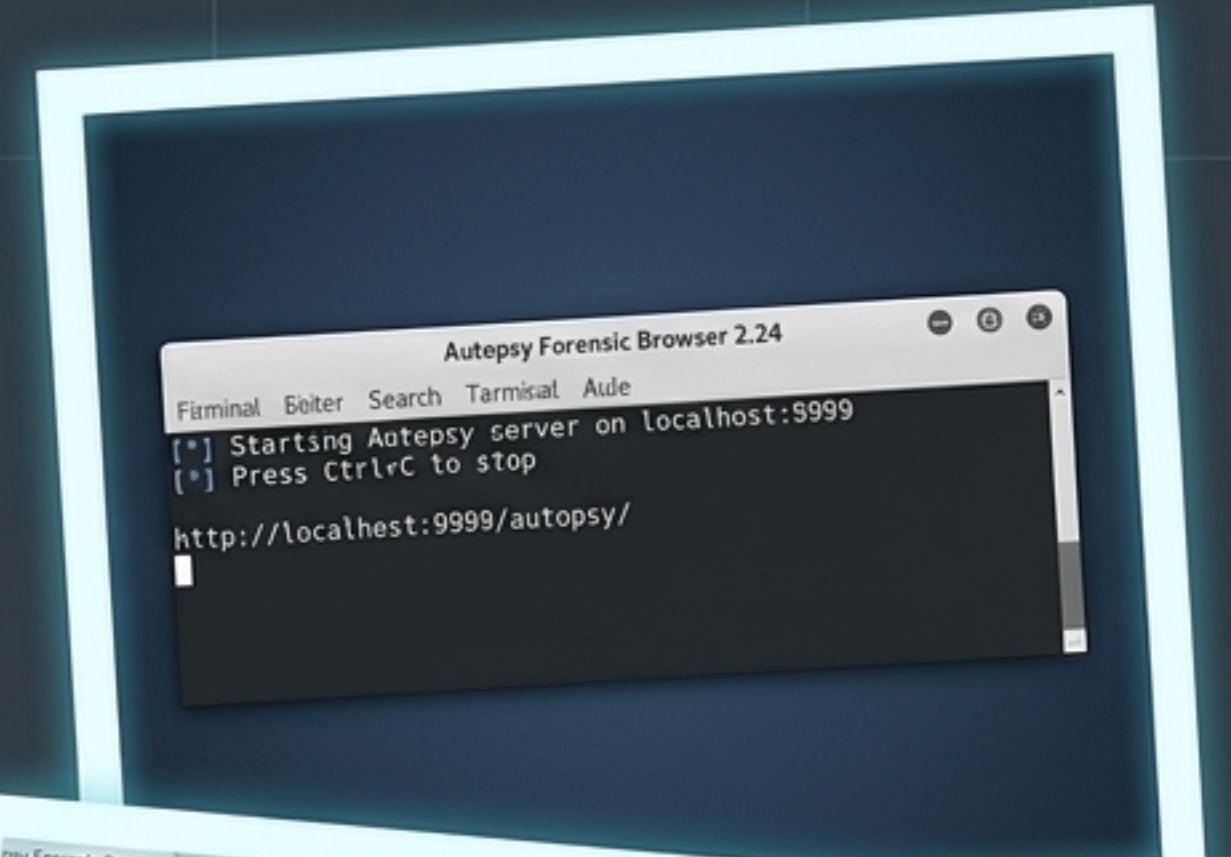
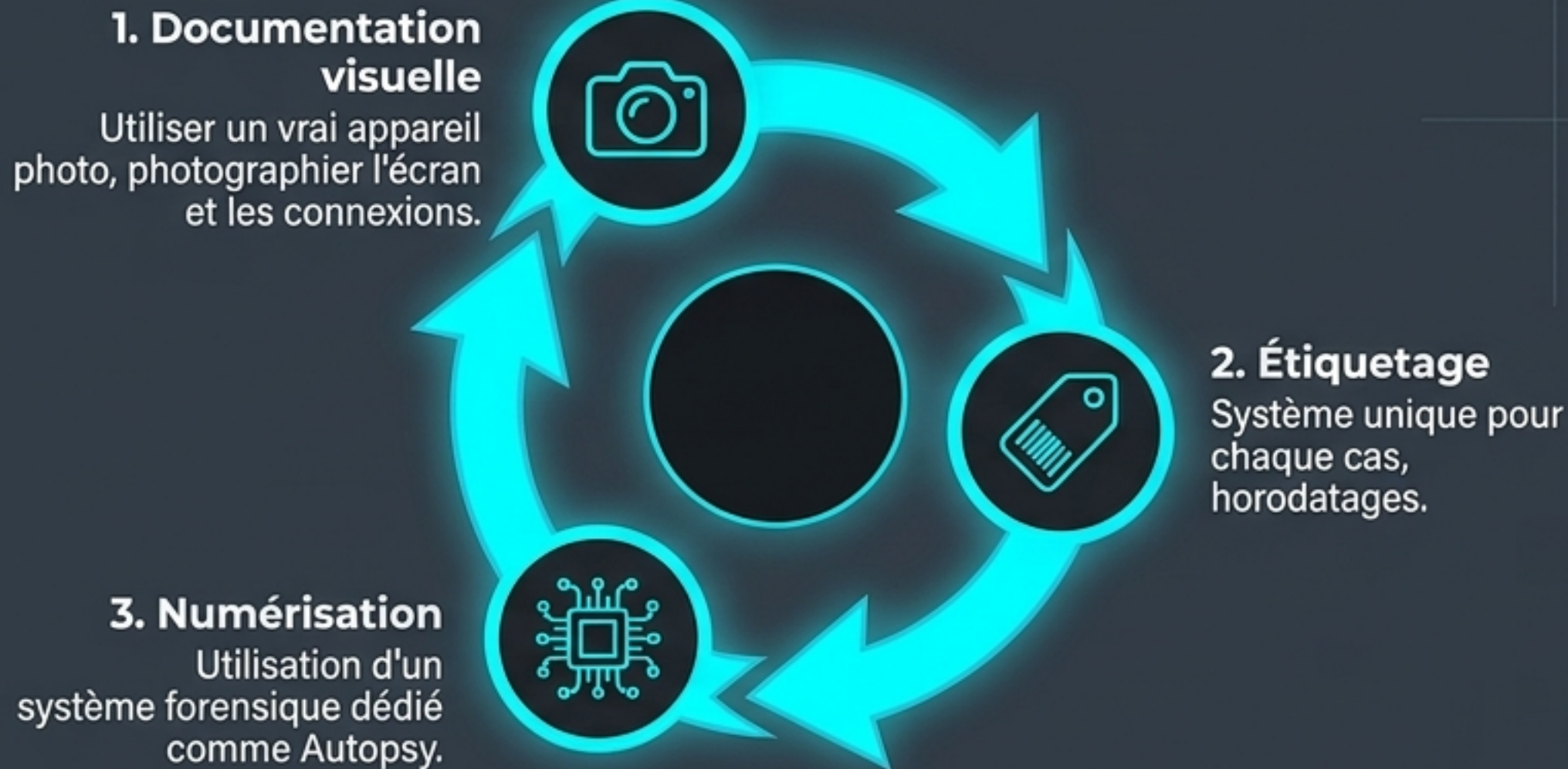
SÉCURITÉ PHYSIQUE D'ABORD : Éliminer tout facteur de risque (individus, menaces) dans la zone avant de toucher aux appareils numériques.

Matrice d'escalade : À qui confier l'enquête ?



La chaîne de possession : De la saisie à la disposition

« Documentation chronologique et traçabilité écrite retraçant la saisie, la garde, le contrôle, le transfert, l'analyse et la disposition des preuves. »



Autorisations légales et sécurisation du transport



Approbation du propriétaire
Validation de la cession des droits légaux à l'employeur



Mandat
Autorisation judiciaire obligatoire selon les lois locales



Formulaires (NDA)
Protection des secrets commerciaux et configurations réseau

Alimentation
Maintien de l'appareil allumé



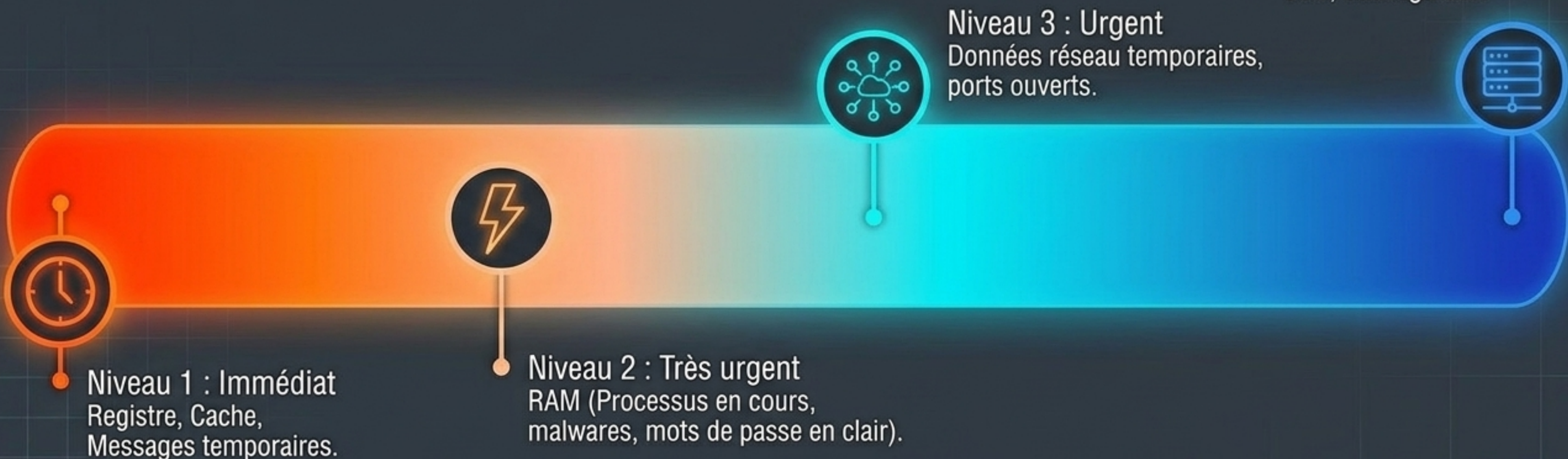
Cage de Faraday
Blocage des effacements à distance



RISQUE : Chiffrement du disque au repos déclenché par la déconnexion réseau.

Le spectre de la volatilité : L'urgence d'acquisition

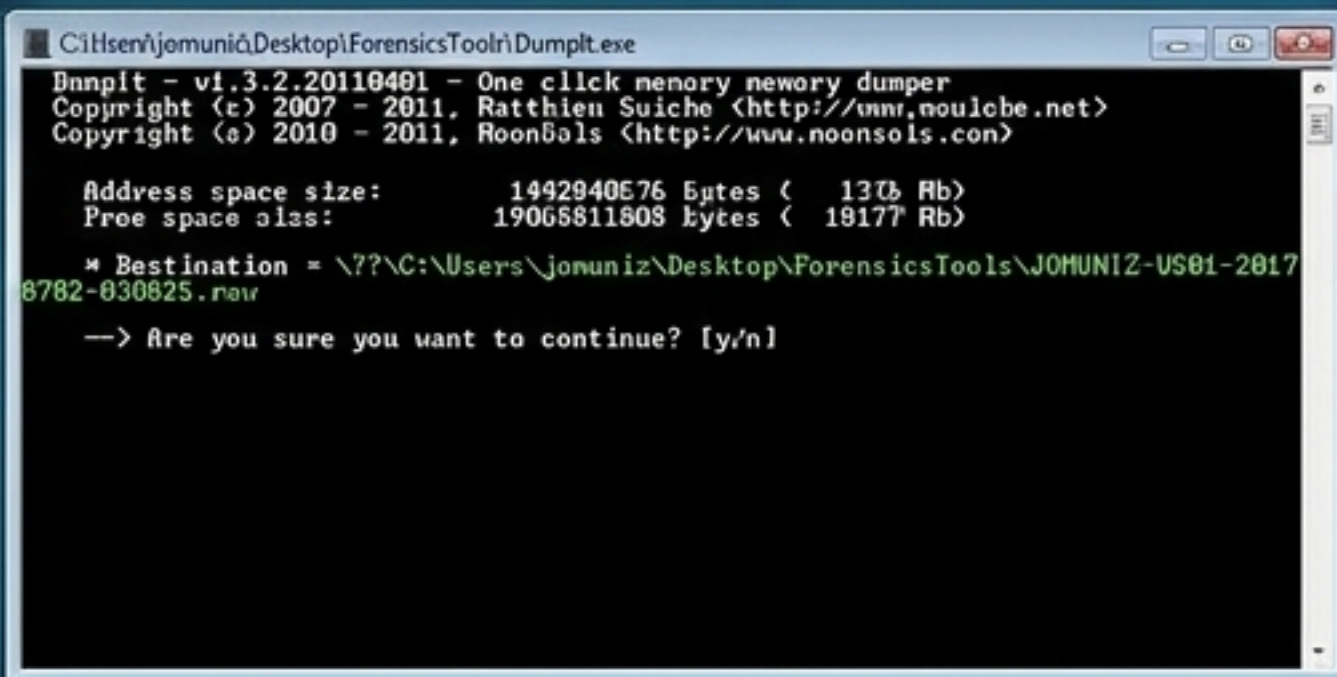
Les données volatiles disparaissent lors de la mise hors tension.
Certains malwares ne sont jamais écrits sur le disque.



Figurer la mémoire vive : DumpIt vs LiME

DumpIt (Systèmes Windows)

- Méthode : Simple fichier exécutable lancé depuis une clé USB.
- Résultat : Capture absolue dans un fichier .raw.



```
C:\Hsen\Jomuniz\Desktop\ForensicsTools\DumpIt.exe
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Ratthien Suicho <http://www.noulche.net>
Copyright (c) 2010 - 2011, RoonSals <http://www.noonsois.com>

Address space size:      1442940576 Bytes ( 1376 Mb)
Free space size:        19065811808 Bytes ( 18177 Mb)

* Destination = \\??C:\Users\jomuniz\Desktop\ForensicsTools\JOMUNIZ-US01-2017-8782-830825.raw
-> Are you sure you want to continue? [y/n]
```

VS

LiME (Systèmes Linux)

- Méthode : Compilation (make) et création d'un module noyau (.ko).
- Dépannage : Utiliser 'rmmod lime' si le module est déjà chargé.

```
root@kali:~/Downloads/LiME-master/src# ls
disk.c      lime.h      lime.o      Makefile    Module.symvers
disk.o      lime.mod.c  main.c      Makefile.sample  tcp.c
lime-4.3.0-kali-amd64.ko  lime.mod.o  main.o      modules.order  tcp.o
root@kali:~/Downloads/LiME-master/src# sudo insmod lime-4.3.0-kali-amd64.ko "
path=/root/RANDump.lime format=raw"
root@kali:~/Downloads/LiME-master/src#
```

L'analyse de la mémoire avec Volatility

PROFILAGE

`volatility -f <dump.raw> imageinfo`
Estime l'architecture et le système d'exploitation.

VÉRIFICATION

`... --profile=<profil> kdbgscan`
Valide l'adresse kdbg pour éviter les faux positifs.

EXTRACTION TACTIQUE

`pslist / pscan` : Révéler les processus cachés
`hashdump` : Extraire les hachages de mots de passe
`connections` : Identifier les ports ouverts
`cmdscan` : Historique des commandes

Offset(U)	Name	Exis	PID	FPID	Thds	Hnds	Sess	Voë
Mo-4 Start								
0x77f5fa00024519c0	System		4	0	121	623	-----	
0x77f5fa00024519c0	2017-01-12 22:01:07 UTC+0000							
0x77f5fa00024519c0	2017-01-12 22:01:07 UTC+0000		268	4	2	32	-----	
0x77f5fa00024519c0	2017-01-12 22:01:07 UTC+0000		273	268	0			0
0x77f5fa00024519c0	2017-01-12 23:01:09 UTC+0000	2017-01-12 22:01:09 UTC+0000	476	392	10	994		0
0x77f5fa00024519c0	2017-01-12 23:01:09 UTC+0000		504	268	0			1
0x77f5fa00024519c0	2017-01-12 22:01:09 UTC+0000	2017-01-12 22:01:09 UTC+0000	512	392	3	81		0
0x77f5fa00024519c0	2017-01-12 22:01:09 UTC+0000		520	504	8	370		1
0x77f5fa00024519c0	2017-01-12 23:01:09 UTC+0000		560	504	3	115		1
0x77f5fa00024519c0	2017-01-12 23:01:09 UTC+0000		604	512	10	296		0

Matrice d'acquisition : **Formats et outils Linux**

RAW (.dd / .raw)	EnCase (.E01)	AFF (.aff1)
Copie absolue de bout en bout. Ignore les erreurs, aucune métadonnée intégrée. Acceptation universelle.	Format propriétaire. Tactique juridique : Force l'avocat adverse à acheter une licence logicielle coûteuse.	Norme ouverte. Métadonnées arbitraires, compression ajustable et vérification d'erreurs.

La Boîte à Outils Native (Linux)

dd : L'outil de base. Ex: `dd if=/dev/sdb of=/media/diskcopy.dd`

dcfldd : Version DoD. Ajoute le hachage à la volée et la barre de progression.

ddrescue : Le sauveur. Contourne les secteurs endommagés là où 'dd' échoue.

Interfaces de connexion et montage



INTERNES



SATA

Standard moderne

ATA/IDE



Héritage/Obsoleète

SCSI / Fibre Channel *

Serveurs d'entreprise

USB



Variations de vitesse

Thunderbolt ⚡

Jusqu'à 7 périphériques

FireWire / eSATA



Processus de montage sécurisé (Linux)

```
fdisk -l  
# Identifier le disque  
  
sudo mkdir /mnt/USB1  
# Créer le point de montage  
  
sudo mount /dev/sdb1 /mnt/USB1  
# Monter pour l'image
```

⚠ NOTE TACTIQUE : L'adaptateur matériel (ex: MicroSD vers USB) est l'outil le plus critique du kit d'intervention pour les appareils mobiles.

Matrice de diagnostic RAID en contexte **forensique**

RAID 0	Vitesse pure. Aucune redondance. Répartition complexe.
RAID 1	Miroir. Simple à dupliquer, mais coûteux en stockage.
RAID 5 / 6	Parité distribuée. Complexe, nécessite de reconstruire la carte de répartition via la parité.
RAID 10 / 15	Combinaisons (0+1 / 1+5). Haute difficulté.

Défis de l'enquêteur

Risque de contrôleurs
propriétaires limitant la
lecture.

Si la configuration BIOS est
perdue, la reconstitution
manuelle (taille des blocs,
période physique) justifie
l'appel à des experts.

L'exception SSD : Quand l'appareil **détruit la preuve**

- **Mappage aléatoire** : Répartition non linéaire des données.
- **Équilibrage d'usure** : Déplacement continu des données risquant la corruption.
- **La commande TRIM** : Purge autonome et définitive des secteurs libres. Récupération impossible.

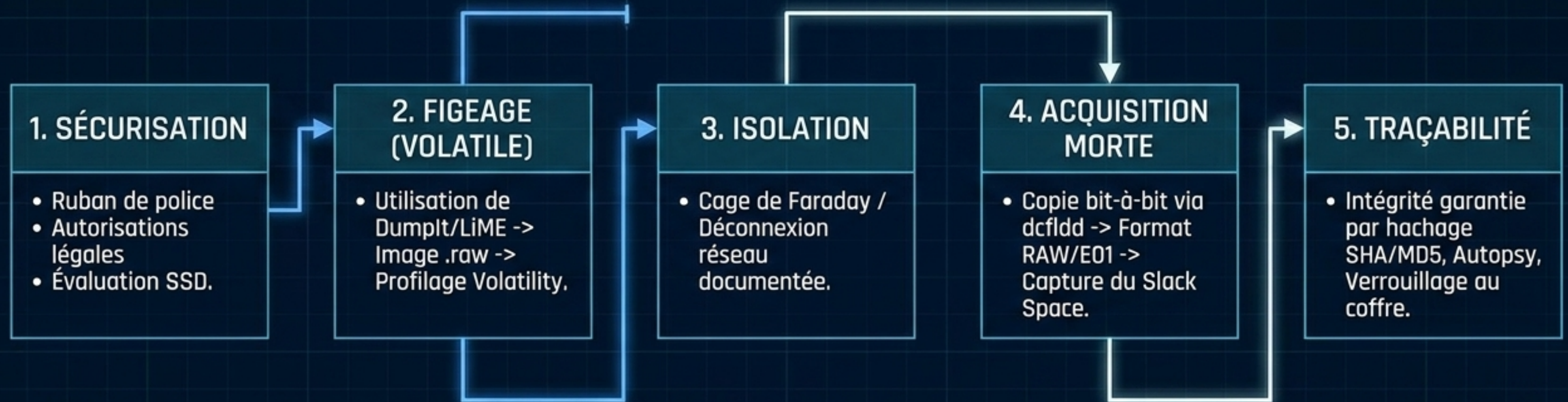


LA RUPTURE DE PROCÉDURE

Règle classique : « Ne jamais débrancher un système ».

Exception SSD : Si une suppression (TRIM) est en cours, **IL FAUT couper l'alimentation immédiatement** pour stopper l'hémorragie des données.

Le schéma directeur de l'acquisition numérique



Le dossier d'instruction numérique est scellé.
La preuve est prête pour le tribunal.