

**Réf :** PROC-PTS-002

**Usage :** Investigation de terrain / Saisie de supports (Disque dur, Clé USB, Smartphone)

**Objectif :** Garantir l'intégrité et l'admissibilité de la preuve devant un tribunal.

---

## [ DOCUMENT : GUIDE DE SAISIE DE SCELLÉ NUMÉRIQUE ]

### ÉTAPE 01 : LA SÉCURISATION PHYSIQUE

- **Le Bloqueur d'écriture (Write Blocker) :** C'est la règle d'or. Jamais, au grand jamais, on ne branche un support saisi directement sur son PC de labo. On utilise un pont matériel (ex: Tableau) qui empêche l'OS d'écrire le moindre bit sur le support (comme la date de dernier accès).
- **Mode Avion / Cage de Faraday :** Pour les smartphones, on coupe immédiatement les réseaux. On veut éviter une commande de "Remote Wipe" (effacement à distance) par le suspect.

### ÉTAPE 02 : LA CRÉATION DE L'IMAGE DISQUE (IMAGING)

*On ne travaille jamais sur l'original. On crée un "clône bit-à-bit".*

- **Format :** On privilégie le format **E01** (EnCase) ou **RAW (dd)**.
- **Outils :** FTK Imager ou Guymager.
- **Action :** On copie chaque secteur, même l'espace vide (Unallocated Space) qui peut contenir des fichiers effacés.

### ÉTAPE 03 : LE CALCUL DE L'EMPREINTE (HASHING)

*C'est le moment où on signe l'acte de naissance de la preuve.*

- **Protocole :** On génère une empreinte **SHA-256** (plus robuste que le MD5).
- **Double vérification :** On calcule le Hash du support original ET le Hash de la copie. Ils doivent être rigoureusement identiques.
- **Certification :** On note ce code immédiatement. Il prouve que la preuve n'a pas été modifiée depuis la seconde où elle a été saisie.

**Réf :** PROC-PTS-002

**Usage :** Investigation de terrain / Saisie de supports (Disque dur, Clé USB, Smartphone)

**Objectif :** Garantir l'intégrité et l'admissibilité de la preuve devant un tribunal.

---

## ÉTAPE 04 : LE PROCÈS-VERBAL DE CONSTATATION (PV)

*Une preuve sans papier n'existe pas en droit français. Le PV doit mentionner :*

- **L'inventaire :** Marque, modèle, numéro de série du support.
- **L'état :** Description physique (rayures, état des ports).
- **La traçabilité :** Heure de saisie, identité de l'agent, outils logiciels utilisés et leur version.
- **Le Hash :** Inscrit noir sur blanc pour "geler" l'état du scellé.

## ÉTAPE 05 : LA CHAÎNE DE CUSTODIE (CHAIN OF CUSTODY)

- **Logistique :** Chaque mouvement du scellé doit être tracé. "Sorti du coffre le 24/02 à 09h00 par l'Expert X, réintégré à 17h00".
- **Sécurité :** Utilisation de sacs de transport scellés avec signature sur la languette.

*Tu peux trouver la preuve du siècle, si tu n'as pas utilisé de bloqueur d'écriture ou si ton Hash est absent du PV, l'avocat de la défense va t'atomiser à l'audience. En PTS, on ne joue pas les cowboys, on joue les horlogers. La rigueur, c'est l'arme fatale.*

[ SYSTEM\_LOG : PROTOCOLE\_CERTIFIE\_PAR\_LA\_SENTINELLE ]

[ MOTO : WARRIOR SOUL // SHADOW HUNTER // HOPE BUILDER ]