

Benjamin MOREAU
Analyse Forensique - Projet

Étude des méthodes et outils de garantie de l'intégrité des données au cours du temps





Norme NF EN ISO/IEC 27037

- **Lignes directrices pour**

- **1** l'identification,
- **2** la collecte
- **3** l'acquisition
- **4** **préservation de preuve numériques.**



Norme NF EN ISO/IEC 27037

2 Chaîne de contrôle (§ 6.1)



Norme NF EN ISO/CEI 27037 • §6.1 – Chaîne de Contrôle

Norme NF EN ISO/IEC 27037

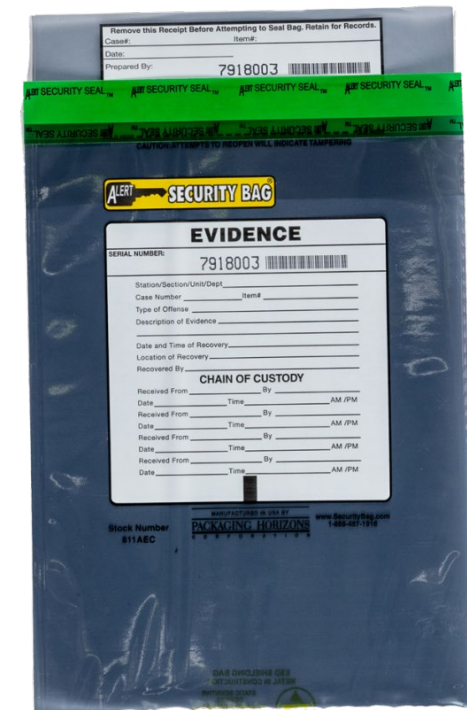
Guides pratiques et précautions globales : collecte & préservation (§7)

 **Preuves non numériques & consignes de terrain**
Documentations, mots de passe, #séries ...

 **Conditionnement des matériels, des disques...**











www.mosequipment.com • BlockBox lab XL



Emballages antistatiques  ID

Norme NF EN ISO/IEC 27037

Guides pratiques et précautions globales : collecte & préservation (§7)

-  Identification, définition du périmètre collectable / à collecter
-  Système sous tension ou hors tension ?
-  Données volatiles • non volatiles
-  État de chiffrement des systèmes
-  Acquisition partielle ou complète ? Guide pour les compromis.
-  Acquisition de données sur place ou en laboratoire ?
-  Protocole de collecte, copies de travail,
-  Altérations évitables / inévitables...



Grande responsabilité du DEFR et de ses compétences.





Norme NF EN ISO/IEC 27037

4

Rôles du DEFR

Département d'Expertise Forensique et Réponse • **Digital Evidence First Responder**

Document de travail - Version 1.0

Annexe A
(Informative)

Norme NF EN ISO/IEC 27037

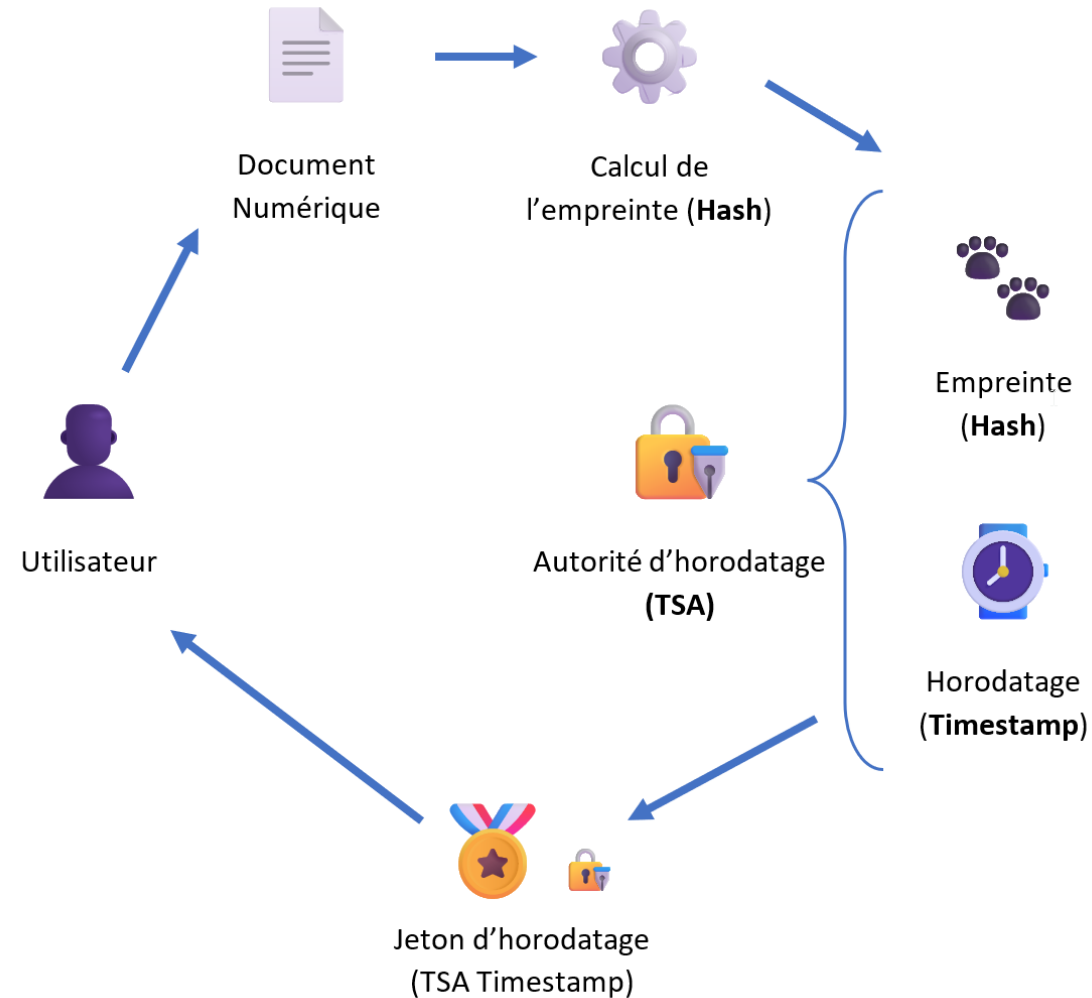
Description du contenu des rôles et compétences attendues du DEFR

Tableau A.1 - Description des rôles et compétences attendues

Rôle	Compétences attendues	Responsabilités	Compétences attendues	Responsabilités
1. Gestion de l'incident	1.1. Identification de l'incident	1.2. Notification de l'incident	1.3. Prise en charge de l'incident	1.4. Coordination de l'incident
2. Investigation	2.1. Recherche de preuves	2.2. Analyse de preuves	2.3. Interrogation des témoins	2.4. Rédaction de rapports
3. Réponse	3.1. Restauration des données	3.2. Nettoyage des systèmes	3.3. Mise à jour des systèmes	3.4. Surveillance des systèmes
4. Formation	4.1. Sensibilisation des utilisateurs	4.2. Formation des équipes	4.3. Mise à jour des procédures	4.4. Révision des procédures



Horodatage numérique avec TSA



Dispositif
EXperimental de
Timestamping
Electronique
Reprouvable



<https://github.com/FadeOutAgain/Dexter>

DEXTER





Limitations

- Fichier unique de référence
- Base de temps locale peu fiable, sans gestion des timezones
- Légitimité de FreeTSA ?
- Pas de lecture seule sur le filesystem
- Pas de prises en compte des métadonnées du fichier (même hash)
- Pas de journalisation des actions
- Pas de base de données des timestamping effectués

Merci !

