# Analyse Forensique • Projet

Benjamin MOREAU • Master 2 Cybersécurité • 2025-02-14

**Le présent rapport retrace les activités liées à l'étude des méthodes et outils de garantie de l'intégrité des données au cours du temps dans le cadre d'un projet d'Analyse Forensique.**

N'ayant pas d'expérience dans le domaine, et le sujet nécessitant d'être plus détaillé que les notions abordées en Cours Magistral, j'ai fait des recherches sur ce thème, pour explorer notamment les tenants et aboutissants fonctionnels. Ces recherches sont consignées dans le présent rapport, en long préambule à une mise en œuvre pratique qui sera présentée en séance.

🕰️ Un pictogramme « montre » matérialise les éléments de synthèse pour relier spécifiquement la préservation des données à un aspect temporel .

---

Les enjeux principaux de la discipline d'Analyse Forensique sont de garantir l'intégrité, l'authenticité, et la recevabilité des preuves sur le plan légal. À cet effet, le technicien chargé d'explorer le contenu d'un système doit prendre toutes les précautions nécessaires pour préserver l'intégrité des preuves, de la même manière qu'il prendrait des mesures sur une scène de crime.

La discipline repose sur trois grands axes :

- **La recopie fidèle.** C'est le premier processus à mettre en œuvre dans le cadre de la discipline, qui consiste à limiter au maximum les actions sur la machine à analyser, à en figer les données sur une ou plusieurs copies bit à bit de ses disques durs.
  Le technicien travaillera uniquement sur ces copies sans altérer le support original. Il pourra analyser leur contenu à l'aide d'un « write blocker », un dispositif matériel ou logiciel qui empêche toute écriture sur le support.

- **Le hashage**. C'est une technique qui utilise un algorithme mathématique pour générer une signature unique, ou empreinte numérique, d'un ensemble de données, comme un fichier ou l'image d'un disque dur.
  En calculant l'empreinte numérique (hash) d'un fichier avec un algorithme de hashage réputé robuste, on obtient une chaîne courte de caractères alphanumériques courte correspondant à une signature mathématique du contenu de ce fichier. Si celui-ci vient à être modifié, ne serait-ce que d'un bit, le même algorithme produira un hash très différent.
  La comparaison de l'empreinte des données originales avec celle des données utilisées pour l'analyse forensique permet de garantir, lorsque les empreintes sont identiques, que les données sur lesquelles on se base pour expliquer les faits sont intactes.

- **La chaîne de conservation** (également appelée chaîne de garde, *chain of custody*) **;** en matière juridique et scientifique, c'est un processus de traçabilité qui permet de suivre et contrôler un échantillon de preuve pour en maintenir la recevabilité. Les principaux éléments habituels inclus dans une chaîne de conservation sont
  - **L'identification** de la preuve ou de l'échantillon (nature, date et lieu d'acquisition)

- **Les personnes impliquées** qui ont manipulé ou eu accès à la preuve où l'échantillon
- **Les dates et heures** exactes de leurs manipulations, stockages, transferts
- **Les lieux** des opérations de ce type
- **Le but** de ces opérations

Nous allons, au cours de ce document, développer ces axes, et examiner comment garantir l'intégrité, l'authenticité et l'admissibilité des preuves, afin de renforcer la crédibilité des conclusions d'une enquête comportant des preuves numériques.

S'agissant, à présent, de l'aspect temporel des choses :

Quels sont les défis liés à la préservation des données dans le temps ?

Quelles méthodes permettent de garantir l'intégrité des données face aux menaces temporelles ?

Je propose, d'explorer le sujet en s'appuyant d'abord sur des généralités liées à l'Analyse Forensique et à la préservation des données ; ensuite des techniques et outils pour la discipline. Enfin, je présenterai en séance un développement que j'ai réalisé en Powershell pour mettre en œuvre un TimeStamping auprès d'une autorité de TSA, FreeTSA.org.

## Enjeux et défis de la préservation des données numériques dans le temps

1. Problématiques générales de conservation des preuves numériques
2. Risques liés à l'altération et à la perte des données
3. Contraintes juridiques et réglementaires
4. Norme ISO 27037

## Méthodes et outils garantissant l'intégrité des données au fil du temps

1. Recopie fidèle d'un disque de serveur
2. Techniques cryptographiques : hashage, signatures numériques
3. Mécanismes de stockage sécurisé : WORM, archivage légal
4. L'horodatage numérique et les autorités de confiance
5. L'apport des blockchains et autres technologies émergentes

## Mise en pratique

1. Démarche projet

2. **DEXTER • D**ispositif **EX**périmental de **T**imestamping **E**lectronique **R**éprouvable

## Enjeux et défis de la préservation des données numériques dans le temps

Si le principe de la conservation des données sur les supports numériques n'a pas évolué fondamentalement depuis les cartes perforées des métiers à tisser d'il y a 100 ans, ils sont devenus omniprésents dans notre quotidien, aussi bien sur un plan professionnel que personnel.

Avec une intégration aussi profonde dans la Société, il est normal que les problématiques liées au numérique s'invitent elles aussi dans les conflits juridiques, des délits, des crimes. Les données numériques, immatérielles par nature, doivent faire l'objet de précautions particulières pour que les indices, les preuves matérielles aient une crédibilité équivalente aux éléments matériels.

### 1. Problématiques générales de conservation des preuves numériques

La nature même des données numériques et des supports qui les contiennent rend complexe le « figeage » des informations. Voici quelques facettes du défi à relever

**Volatilité et fragilité :** les preuves numériques sont extrêmement sensibles aux modifications involontaires (accès à un fichier, mise à jour automatique, corruption de données) et peuvent être perdues facilement (panne, suppression accidentelle, chute du support, cyberattaques…).

**Altération et falsification :** Les supports sont conçus pour modifier les données à l'envi, et la plupart du temps, sans laisser de trace particulière. Il est donc crucial d'établir des mécanismes permettant de prouver que les preuves n'ont pas été altérées (hashage, signature, horodatage).

**Obsolescence technologique :** Les formats de fichiers, les supports, et les logiciels utilisés pour lire les données deviennent obsolètes. Une preuve numérique conservée sur un ancien support pourrait être inutilisable si elle n'est pas migrée régulièrement vers des technologies plus récentes. Des choix stratégiques doivent être faits (serveurs sécurisés, stockage WORM, archivage légal) en tenant compte de la durée de vie des supports.

**Cadre juridique :** Diverses législations (RGPD, …) imposent des règles sur la conservation des données personnels en général, qui peuvent s'appliquer à la conservation des preuves numériques. Il conviendra de respecter le cadre législatif pour ne pas compromettre leur admissibilité en justice. Certaines preuves contiennent des informations sensibles ou personnelles. Un équilibre est à trouver entre protection de ces données et disponibilité des preuves pour les autorités compétentes.

### 2. Risques liés à l'altération et à la perte des données

Les risques sont nombreux qui sont susceptibles de compromettre la fiabilité des preuves numériques dans le cadre d'une enquête forensique :

**Altération accidentelle des données** : Erreur humaines (l'ouverture d'un fichier peut modifier ses métadonnées comme la date d'accès) • Mises à jours automatiques du système • Erreurs de manipulations

**Modification malveillante des preuves :** Altération intentionnelle (modification de logs, insertion de données, …) • Effacement ou corruption de données • Manipulation des horodatages

**Perte de données due à des pannes matérielles :** Un support de stockage peut tomber en panne • se dégrader naturellement au fil du temps • ou subir un accident environnemental (inondation, …)

**Cyberattaques et menaces externes :** Présence d'un ransomware, malware • Intrusion et piratage • Attaques sur la chaîne de conservation, si la chaîne de garde des preuves n'est pas bien sécurisée.

**Obsolescence technologique :** disponibilité des logiciels pour ouvrir un format de fichier après plusieurs années • Technologie de support obsolète • Évolution des algorithmes cryptographiques : un hachage considéré sécurisé aujourd'hui peut ne plus l'être demain, compromettant l'authenticité des preuves conservées.

## 3. Contraintes juridiques et réglementaires

Elles varient suivant le pays et contexte de l'enquête. Les preuves doivent-être **intègres, authentiques et traçables** pour être recevables en justice. La chaîne de conservation (Chain of custody) doit être documentée pour garantir qu'aucune altération n'a eu lieu.

En France, la réglementation à prendre en compte pour garantir la fiabilité et la recevabilité des preuves numériques en cas de litige ou d'enquête judiciaire se trouve notamment

- Dans le **Code de procédure pénale** qui encadre la collecte et l'exploitation des preuves numériques
- Dans la **LCEN** (Loi pour la Confiance dans l'Économie Numérique) qui implique des obligations de conservation des données pour les hébergeurs et fournisseurs d'accès (1 an date, heure, durée, adresse IP attribuées • 3 ans pour la conservation des documents contractuels).
- Dans le **RGPD** qui protège les données personnelles dans les pays européens, et impose des restrictions sur leur traitement et leur conservation au strict nécessaire.
- Auprès de la **CNIL** qui fournit des guides sur la sécurité des données personnelles vis-à-vis du RGPD, des référentiels sur la gestion des logs, des recommandations pour l'horodatage afin de garantir l'authenticité et la valeur probante des enregistrements numériques.
- Auprès de l'**ANSSI** qui édite des bonnes pratiques pour garantir l'intégrité et la sécurité des données (RGS), un guide d'hygiène informatique pour prévenir l'altération des données, des recommandations sur l'archivage électronique sur le long terme.

## 4. Norme ISO 27037

Une norme ISO, NF EN ISO/IEC 27037 existe qui donne des **Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuve numériques.**

La norme a été diffusée en 2012 (2017 pour sa traduction française). J'ai pu la consulter grâce au CEA. Elle ne peut néanmoins être reproduite dans ce rapport. Elle fournit des lignes directrices pour les activités spécifiques au traitement de preuves numériques éventuelles.

Cette norme est un guide de bonnes pratiques, mais il ne s'agit pas pour autant d'une loi. En France, c'est le **code de procédure pénale** qui encadre la recevabilité de la preuve, **y compris numérique**. Celle-ci doit être **Licite** (obtenue légalement), **Loyale** (pas obtenue par ruse excessive, sauf exceptions), et **Fiable** (on doit pouvoir prouver son authenticité, son intégrité et sa traçabilité).

L'**article 1366** du code civil stipule que ***« L'écrit électronique a la même force probante que l'écrit sur support papier »***… à condition que l'on puisse identifier l'auteur et garantir son intégrité.

La norme ISO/IEC 27037 n'a pas de caractère obligatoire, mais elle est régulièrement utilisée comme référence technique, et son application rend des éléments de preuves numériques mieux défendables devant un juge.

S'agissant du sujet exploré ma synthèse du document est la suivante :

Les paragraphes **5.4.5** et **7.1.4** abordent des **généralités théoriques et pratiques sur la préservation des données numériques**. Ils mentionnent l'usage de la signature électronique et la biométrie.

Le paragraphe **6.1** décrit la **Chaîne de Contrôle**, son importance et les éléments qu'elle doit comporter, notamment

- **L'identifiant unique** des preuves
- **Les personnes ayant accédé** à ces preuves, le lieu et l'heure
- **Les personnes ayant vérifié les transactions d'entrée  sortie** des preuves des installations de préservation, et l'horodatage
- **La raison pour lesquelles les preuves ont été vérifiées**, sous quelle autorité
- **Toute modification inévitable** qui aurait pu survenir ces preuves.

**L'annexe A** de la norme résume les compétences du DEFR (Digital Evidence First Responder • Département Expertise Forensique et Réponse dans la version Norme Française) – Le premier intervenant en contact avec les preuves numériques, sur les différentes activités relatives à la discipline. Elle met en évidence notamment le besoin de veille technologique et d'actualisation continue des connaissances.

1️⃣ Identification des preuves numériques,
2️⃣ Collecte des preuves numériques,
3️⃣ Acquisition des preuves numériques,
4️⃣ **Préservation des preuves numériques.**

Un point fort du document est son **chapitre 7 « Exemple d'identification, de collecte, d'acquisition et de préservation »** qui illustre les compromis à faire face à différentes situations rencontrées sur le terrain (systèmes de grande taille, volumes de données considérables, systèmes sous tension ou hors tension, volatilité des données, chiffrement, altérations inévitables, …) et qui inscrit les activités de la discipline dans une réalité pragmatique.

Il en découle que le discernement du DEFR est capital pour identifier les sous-ensembles de données à collecter pour réaliser une enquête pertinente, et que son professionnalisme est crucial pour que les preuves soient recevables.

⏱️ **Le processus de préservation de données commence dès la collecte. Il est capital que le DEFR documente et justifie** chacune des décisions qu'il aura prises et chacun des protocoles qu'il aura appliqué pour identifier, collecter, manipuler, et conserver les preuves numériques, et ce d'autant que les cas d'altération inévitables sont nombreux, et qu'une enquête est susceptible de s'inscrire dans un temps long.

Nous allons à présent faire un panorama non exhaustif d'outils ou de concepts qu'un DEFR pourrait être amené à utiliser dans le cadre de ces activités.

## Méthodes et outils garantissant l'intégrité des données au fil du temps

### 1. Recopie fidèle d'un disque de serveur et vérification de son intégrité.

C'est la première étape du processus, qui consiste à réaliser une copie exacte du disque de la machine à analyser sans altérer les données d'origine. Il faut veiller à faire une reproduction intégrale du contenu du disque ; y compris les fichiers effacés et les espaces non alloués.

**Utilisation d'un write blocker :**

Ce type de dispositif matériel permet d'empêcher toute modification du disque original pendant la copie.

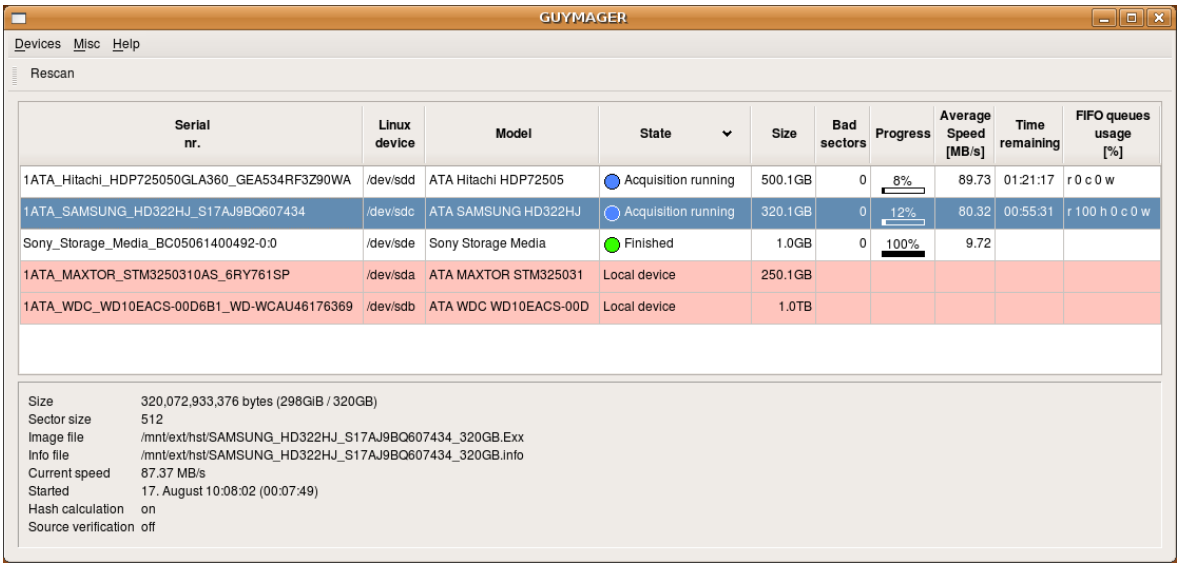

*SiliconForensics • Kit de duplication « Comprehensible Write Block Kit » ($2,349.00)*

**Logiciels :** des outils comme

🐧 la commande **dd** sous linux

🐧 l'utilitaire open source **dcfldd**, basé sur dd, qui va effectuer des copies bit à bit, des hachages MD5, SHA1, des verifications d'images, des effacement sécurisés, apporter de la gestion d'erreurs, des barres de progression, effectuer des duplications multiples.

🐧 l'outil graphique **Guymager**, avec un moteur multithread, qui permet de calculer des haches pour vérifier l'intégrité des images qu'il réalise.




*Sourceforge • Guymager*

- L'outil payant **FTK Imager** proposé par l'éditeur Exterro (~$5,000.00. *Pricing* variable)
- L'outil payant **Encase Forensic** proposé par l'éditeur Opentext (~$1,000.00 / an)

## Formats de stockage :

Les formats courants pour l'enregistrement de l'image d'un disque sous forme d'un fichier sont le E01 (EnCase Evidence File) ou RAW (fichier brut sans compression ni métadonnées supplémentaires).

## Principe d'authentification de la copie :

- On calcule l'empreinte cryptographique (hash) du disque original.
- On effectue la copie bit à bit.
- On recalcule l'empreinte cryptographique de la copie.
- Si les deux empreintes sont **identiques**, la copie est fidèle à l'original.

## 2. Techniques cryptographiques : hashage, signatures numériques

La cryptographie est une discipline mathématique qui joue un rôle fondamental en sécurité informatique. Pour notre sujet, garantir l'intégrité des données numériques au fil du temps, le hashage et les signatures sont particulièrement utiles.

## Le hashage :

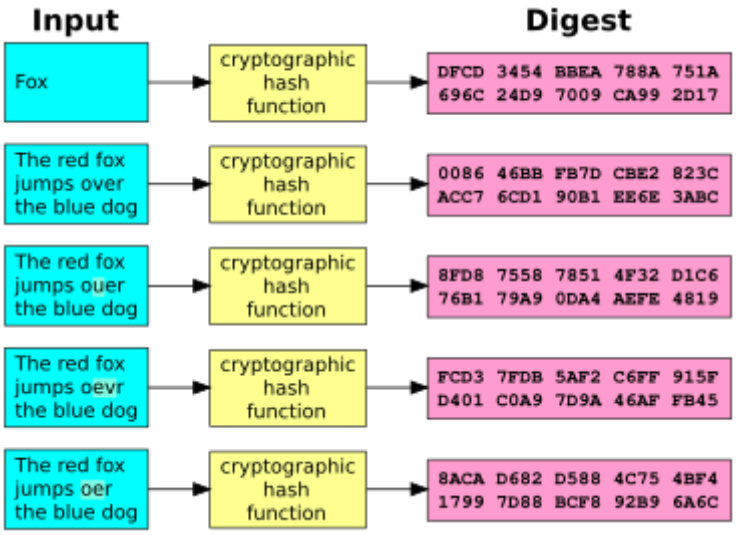
C'est une technique qui consiste à transformer une donnée de taille variable (un fichier, un email, une archive .ZIP, l'image d'un disque dur, …) en une empreinte unique de longueur fixe, que l'on appelle le hash. Toute modification, même infime, de la donnée d'origine entraine un changement significatif du hash.

Les fonctions de hachages telles SHA-256 ou SHA-3 doivent respecter trois propriétés essentielles :

• **L'unidirectionnalité** : il doit être impossible de retrouver les données d'origine à partir de l'empreinte,

• **La résistance aux collisions** : il doit être extrêmement difficile de trouver deux ensembles de données produisant la même empreinte,

• **La rapidité et l'efficacité :** le temps de calcul de l'empreinte doit être rapide, même pour les fichiers volumineux comme nos images de disques.




*Jorge Stolfi • Wikimedia Commons • Cryptographic Hash Function*

Le hashage permet de garantir que les preuves numériques **n'ont pas été altérées entre leur acquisition et leur analyse**, en générant les empreintes des images disques originaux, et de leurs duplications. La technique de hashage peut bien sûr s'appliquer sur un sous-ensemble de données, comme des fichiers de logs.

À tout instant, les images peuvent être comparées en calculant le hash de l'une et de l'autre, qui doivent aboutir au même résultat.

Un enjeu juridique majeur réside dans la **robustesse de l'algorithme de hashage utilisé** pour établir l'empreinte. Certains algorithmes, comme MD5, ont fait l'objet de démonstrations de vulnérabilités aux collisions. Une défense juridique avisée pourrait réfuter des preuves dont l'empreinte a été réalisée avec ce type d'algorithme, en arguant du fait que l'intégrité n'est pas garantie. Par ailleurs, **la découverte ultérieure de vulnérabilités est susceptible de remettre en cause, dans le temps, la recevabilité d'une preuve.**

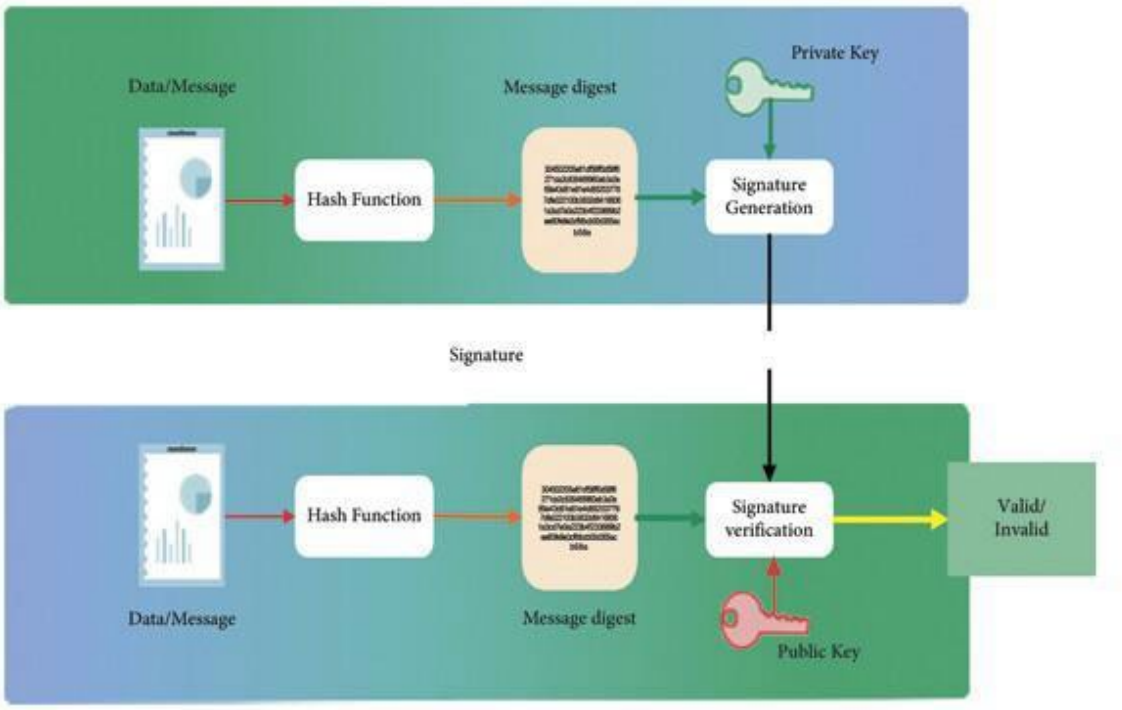
## La signature numérique :

En complément du hashage, qui permet de garantir l'intégrité des données, la signature numérique assure leur authenticité et leur non-répudiation. Les méthodes de signatures reposent sur la cryptographie asymétrique et utilisent une paire de clés.

- 🔑 **Clé privée** utilisée pour signer une donnée.
- 🔑 **Clé publique** utilisée pour vérifier l'authenticité de la signature.

Parmi les principaux algorithmes de signature, on retrouve RSA, DSA, ECDSA et ED25519. Étant donné la lenteur intrinsèque d'un algorithme asymétrique robuste, la signature s'applique plutôt au hash de la donnée à signer, plutôt qu'à la donnée elle-même, ce qui permet de signer plus rapidement un fichier volumineux comme une image disque.

Le mécanisme de signature va permettre d'authentifier l'auteur d'une preuve numérique et en participant à la fiabilité de la chaîne de conservation, va contribuer à la crédibilité du dossier juridique constitué par l'enquête.




*University of Ghana • Shankar, Ai-Farhani, Samrori • Process of digital signature*

🕐 La signature numérique reposant sur une infrastructure de gestion des clés (PKI), il faut néanmoins s'assurer, pour la problématique qui nous concerne, de **la pérennité de celle-ci dans le temps**. Si la PKI devenait indisponible, la vérification fiable des certificats de signature ne pourrait plus être garantie, compromettant ainsi la pérennité des preuves numériques.

## 3. Mécanismes de stockage sécurisé : WORM, archivage légal

La préservation des éléments de l'enquête ne repose pas uniquement sur les mécanismes cryptographiques, mais aussi sur des conditions de stockage adaptées. Il est nécessaire d'utiliser des supports de stockage sécurisés qui garantissent que les informations ne puissent pas être altérées, supprimées ou modifiées après leur enregistrement initial. Parmi ces solutions, les technologies WORM et l'archivage légal jouent un rôle central.

### Technologie WORM (Write Once, Read Many) :

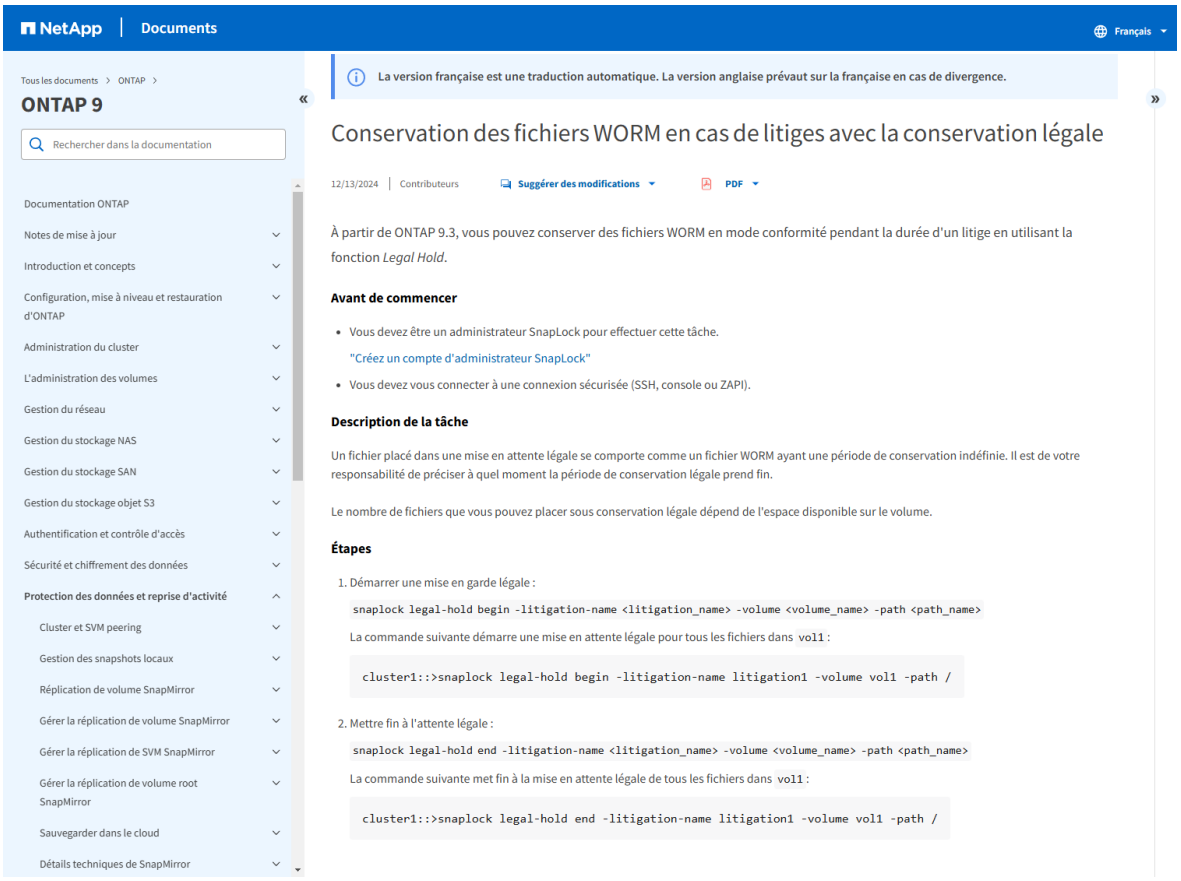
Le principe de ces technologies est de proposer un enregistrement initial, avec des données qui se veulent définitives, empêchant toute modification ou suppression ultérieure. Une fois écrites sur un support WORM, les données ne peuvent être que lues, garantissant ainsi leur intégrité dans le temps.

Les supports WORM sont couramment utilisés dans l'**archivage de documents comptables et financiers** (obligations de conservations légales), le **stockage de journaux d'événements et logs de sécurité** (pour l'analyse forensique), les **preuves numériques dans le cadre judiciaire** (qui nécessitent une garantie d'intégrité totale).

Ils incluent les disques optiques (CD-R, DVD(R, Blu-Ray WORM), des bandes magnétiques WORM.


*Supports WORM*

Des solutions logicielles existent également, qui implémentent des protections logiques « WORM » sur des systèmes de stockage classique (ex : NetApp SnapLock, certifié aux états-unis, mais pas qui ne l'est pas aux yeux de la Loi Française) .




*https://docs.netapp.com • Instructions sur la mise en œuvre de snaplock sur ONTAP 9*

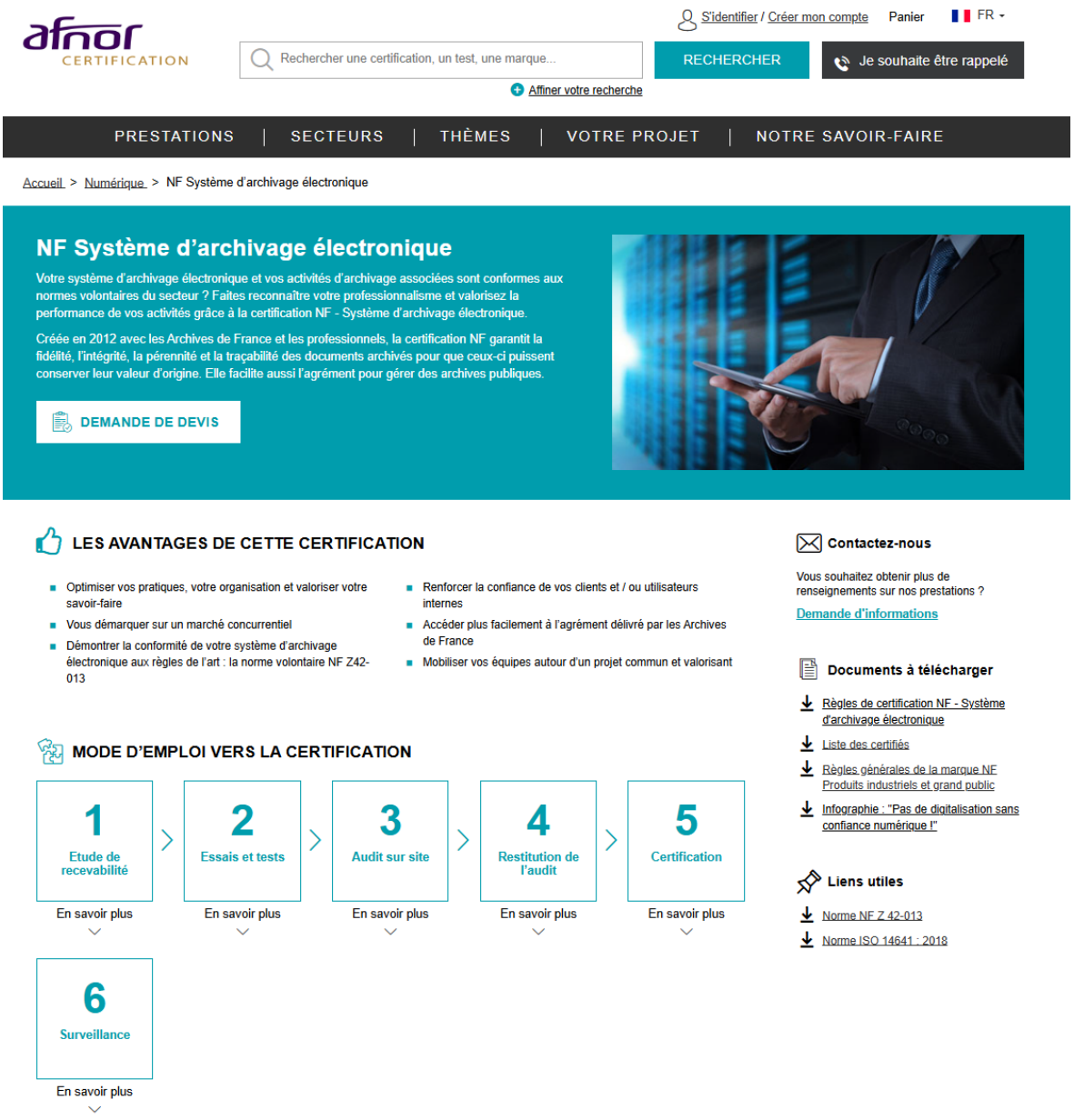
## L'archivage légal et le cadre réglementaire :

L'archivage légal vise à assurer la conservation des données dans des conditions permettant leur exploitation juridique et leur opposabilité en cas de litige. La reconnaissance de la validité d'un moyen par les autorités devient un point crucial à prendre en compte pour la recevabilité des preuves dans un pays donné qui aura ses propres exigences en matière de sécurité, et potentiellement ses propres processus de certification.

Plus qu'un simple stockage, Un Système d'Archivage Électronique (SAE) doit répondre aux exigences d'Intégrité, d'Authenticité, de Traçabilité et de Pérennité.

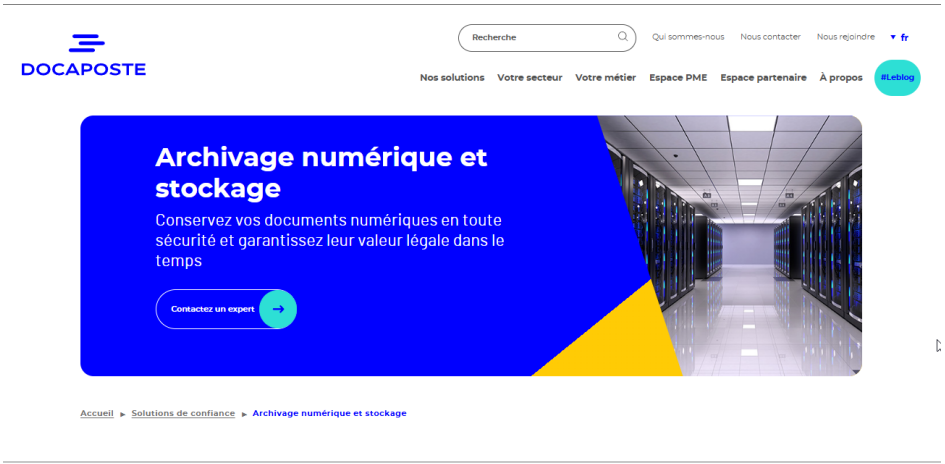
En France, la norme **NF Z42-013** définit les exigences de conformité d'un SAE. Au niveau international, la norme **ISO 14641-1** établit des bonnes pratiques pour l'archivage sécurisé.

Pour la conservation des preuves lors d'enquêtes *forensics*, il est possible de se tourner vers des solutions de **coffre-forts numériques** ou de **systèmes de stockage certifiés**. En France, la conformité des systèmes de stockage est attestée par la certification **NF 461** délivrée par l'AFNOR.




*certification.afnor.org • Certification AFNOR NF 461 : Systèmes d'archivages numériques*

Parmi les prestataires certifiés NF461, DOCAPOSTE • ARKHINEO, filiale du groupe Laposte, revient comme une solution qui semble présenter les garanties réglementaires recherchées pour l'activité forensique.




La législation permet de s'affranchir du papier et d'utiliser des documents nativement numériques et recevables juridiquement. Les documents électroniques sont par ailleurs soumis aux mêmes durées de conservation que les documents papier.

Le véritable enjeu est de permettre **une conservation garantissant leur intégrité, pendant toute la durée des obligations.**

**Docaposte assure la conservation intègre et à long terme des données numériques, quel que soit votre secteur d'activité, public ou privé. Toutes les entreprises sont concernées par l'archivage électronique, socle de conservation des processus 100% numériques.**

### Qu'est-ce que l'archivage électronique ?

**L'archivage électronique garantit la préservation à long terme des documents** et l'accès aux archives. **Il pérennise la valeur légale des informations archivées**, en garantissant la durabilité, **l'authenticité** et la **sécurité des documents**. Le stockage numérique est considéré comme un élément essentiel en termes de sécurité légale, fiscale et financière pour les entreprises.

Complémentaires aux offres de gestion électronique de documents (GED) et au service de coffre-fort numérique, nos services d'archivage électronique (SAE) vont bien au-delà d'un simple stockage et préservent l'opposabilité de vos fonds d'archives sur le long terme.

*[…]*

## Les certifications de Docaposte autour de l'archivage numérique

### Archivage à valeur probatoire certifié NF 461*

Docaposte dispose de la certification NF 461« Système d'archivage électronique ». Les SAE permettent de garantir l'intégrité des documents dans le temps et donc de conserver leur valeur probante.

- Contrôle et validation au moment du dépôt : conversion en formats lisibles dans le temps pour garantir la pérennité de l'archive
- Construction de l'archive : horodatage, attribution d'un Identifiant Unique d'Archive (IUA), calcul de l'empreinte
- Scellement de l'archive et Journalisation pour assurer la traçabilité de tous les évènements
- Conservation intègre
- Traçabilité des actions réalisées sur les documents dans les journaux de cycle de vie.

### Numérisation fidèle certifiée NF 544**

Docaposte dispose de la certification NF 544 « Prestations de numérisation fidèle de documents sur support papier ». Les chaines de traitement certifiées sont situées sur ses sites de Paris, Ballainvilliers et Louviers. La numérisation induit une traçabilité sur toute la chaine assurant la fidélité formelle de la copie numérique.

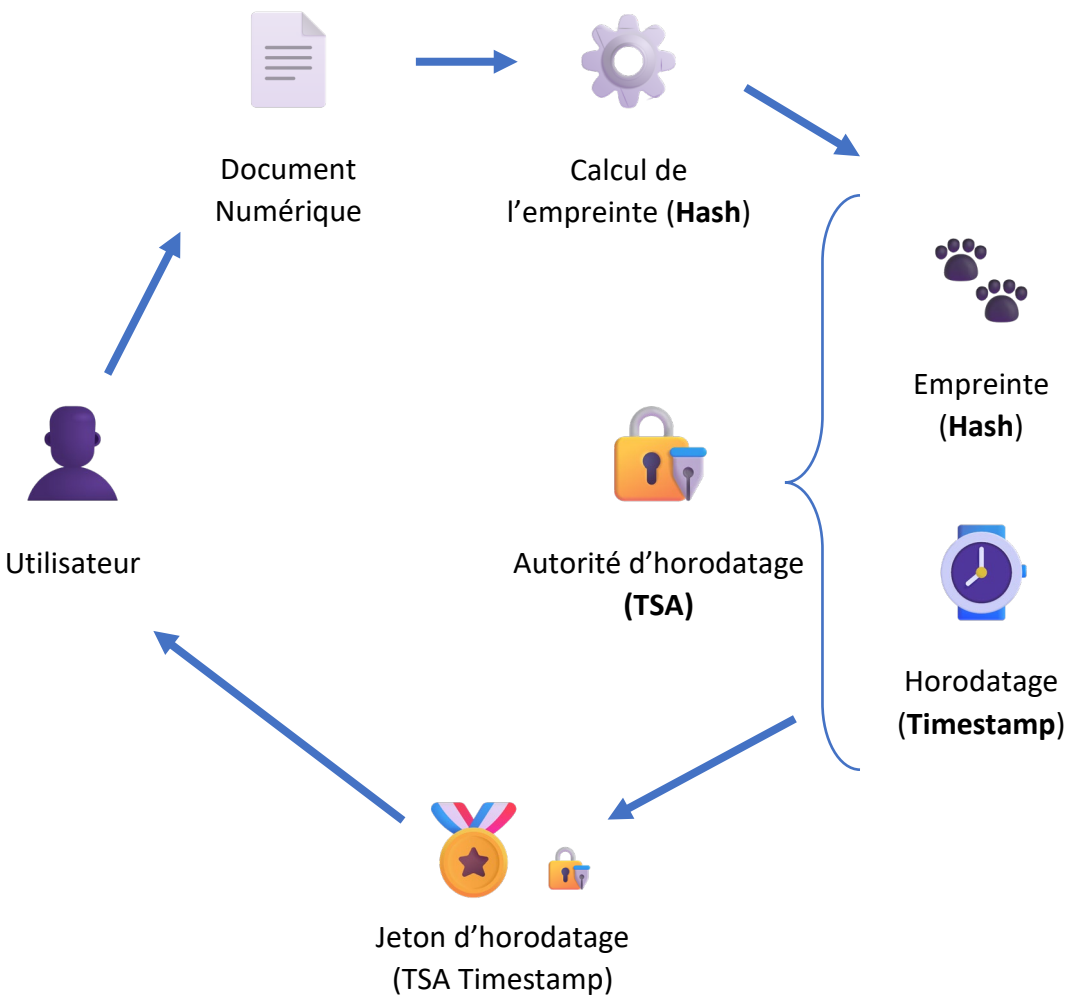
- Convention de numérisation
- Acquisition documentaire : préparation et numérisation
- Contrôles d'exhaustivité, cohérence, de résolution, etc.
- Création de la copie numérique
- Enrichissement des métadonnées
- Fourniture d'attestations de numérisation

*docaposte.com • Solutions d'archivage Numérique*

## 4. L'horodatage numérique et les autorités de confiance

L'horodatage numérique est un mécanisme essentiel pour garantir l'intégrité et l'authenticité au fil du temps. On associe une date et une heure précises à un fichier ou une transaction pour constituer une preuve de son existence à un instant donné.

Le processus repose sur des autorités d'horodatage (Timestamping Authority, TSA) qui délivrent un jeton d'horodatage certifiant l'antériorité et l'intégrité d'un document, en combinant une empreinte numérique (hash) et une signature électronique horodatée (timestamp) pour générer un sceau temporal infalsifiable. C'est ce mécanisme qui sera illustré lors de la mise en œuvre pratique.




*Processus d'horodatage numérique*

Cette méthode est utilisée dans des domaines variés (contrats électroniques, archivage légal, blockchain et forensique numérique), et permet de prouver qu'un fichier n'a pas été modifié après une certaine date. Pour être opposable juridiquement, l'horodatage doit être réalisé par un tiers de confiance reconnu, garantissant la valeur probante des documents horodatés. En France, l'ANSSI est l'autorité compétente qui qualifie ces prestataires (**AR24**, **Certinomis**, **Docusign**, **Yousign,** …), conformément au règlement européen eIDAS.

## 5. L'apport des blockchains et autres technologies émergentes

Le principe des blockchains apporte une réponse différente à l'intégrité des données en adoptant une approche originale. Leur nature décentralisée et immuable offre un autre moyen de garantir la traçabilité et l'authenticité des informations sur le long terme. Chaque transaction ou enregistrement ajouté à une blockchain est cryptographiquement sécurisé, horodaté, et distribué à travers un réseau de nez, rendant toute modification quasi impossible sans concensus global.

Des plateformes comme **Originstamp, Bitcoin Timestamping ou Thereum Smart Contracts** permettent de sceller le hash d'un document dans une blockchain, en fournissant une preuve d'antériorité vérifiable publiquement.

La nature décentralisée de la technologie utilisée permet de s'affranchir d'un tiers de confiance et assurent une disponibilité mondiale.

D'autres technologies seraient susceptibles de répondre à certains aspects de la garantie de la conservation des données à travers le temps :

**Le stockage distribué** : Permet de stocker des fichiers de manière résiliente et redondante sur un réseau pair-à-pair (IPFS, Filecoin, Arweave)

**Preuve à divulgation nulle de connaissance** (ZKP, Zero-Knowledge Proofs), qui permet de prouver la validité de l'information sans pour autant divulguer l'information elle-même. ZKP garantit l'anonymat des transactions en cryptomonnaie.

## Mise en œuvre pratique

### 1. Démarche Projet

Nous l'avons découvert dans les chapitres précédents, le sujet traité, *étude des méthodes et outils de garantie de l'intégrité des données au cours du temps* est assez vaste, et se prête finalement assez peu à la mise en œuvre de la démonstration d'un outil libre en particulier qui assurerait les fonctionnalités de bout en bout de la Chaîne de Conservation.

J'avais songé au départ faire une démonstration comparative d'un timestamping en ligne auprès d'une autorité TSA « classique » d'une part, et une autre s'appuyant sur la blockchain. Mais j'ai rencontré des problématiques de délai dans les réponses de timestamping ne favorisant pas une démonstration en direct.

J'ai cherché ensuite des services « clé en main » susceptibles d'illustrer le principe de la Chaîne de Conservation, mais par nature, les services ayant « pignon sur rue » sont généralement certifiés, donc payants. En effet, les compétences, les ressources humaines et matérielles ont un coût important qui est refacturé à l'utilisateur.

Je me suis donc orienté vers une solution plus « artisanale » et j'ai développé un script en powershell pour illustrer, le temps d'une présentation, les mécanismes intervenants dans un horodatage effectué auprès d'une autorité de Timestamping.

Le script est disponible à cette adresse : **https://github.com/FadeOutAgain/Dexter**

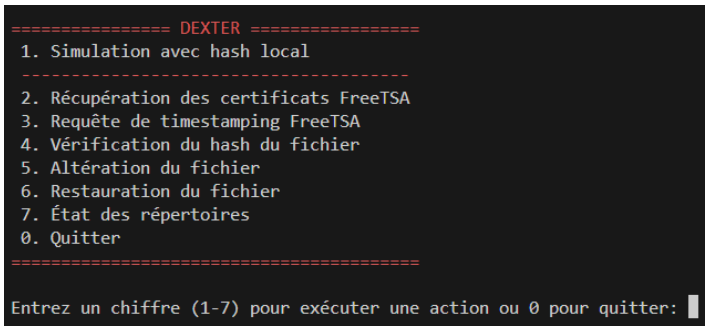
### 2. DEXTER • **D**ispositif **EX**périmental de **T**imestamping **E**lectronique **R**éprouvable

**Prérequis :**

- Powershell (Testé avec la version 7.5.0)
- OpenSSL (Testé avec la version 1.1.1h du 22 Septembre 2022)
- Accès à FreeTSA.org (https://freetsa.org/index_en.php)

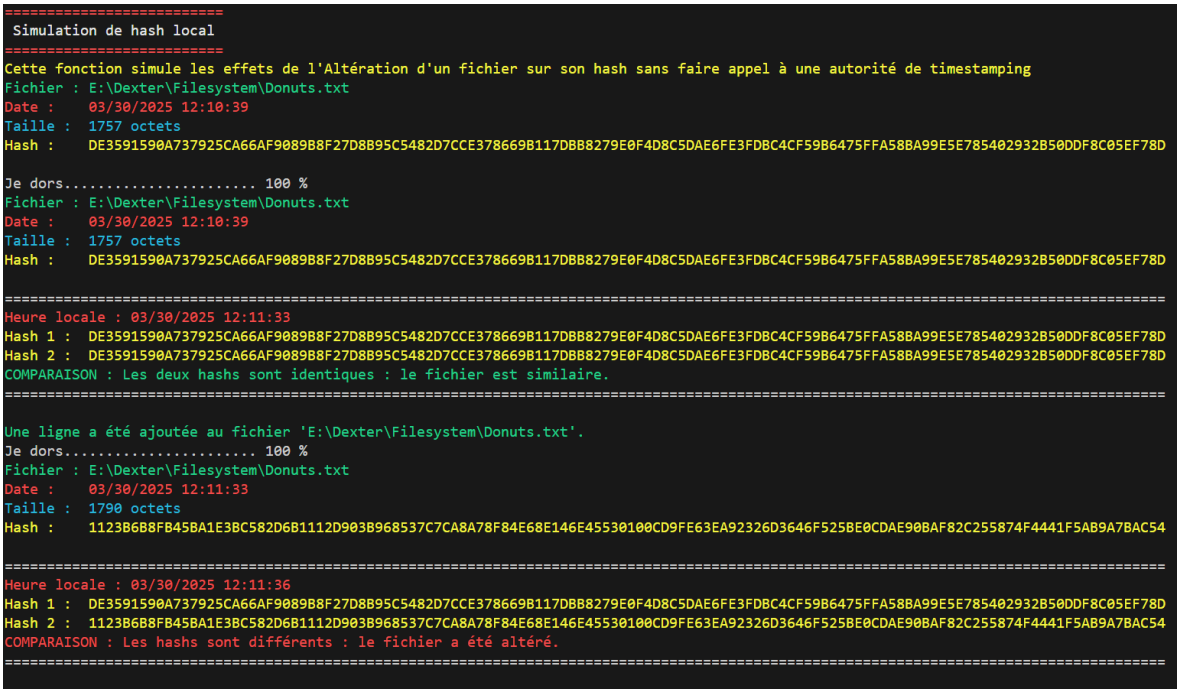
**Fonctionnalités :**

Celles-ci sont déclinées dans un menu à entrées multiples qui suivent les étapes de la démonstration.



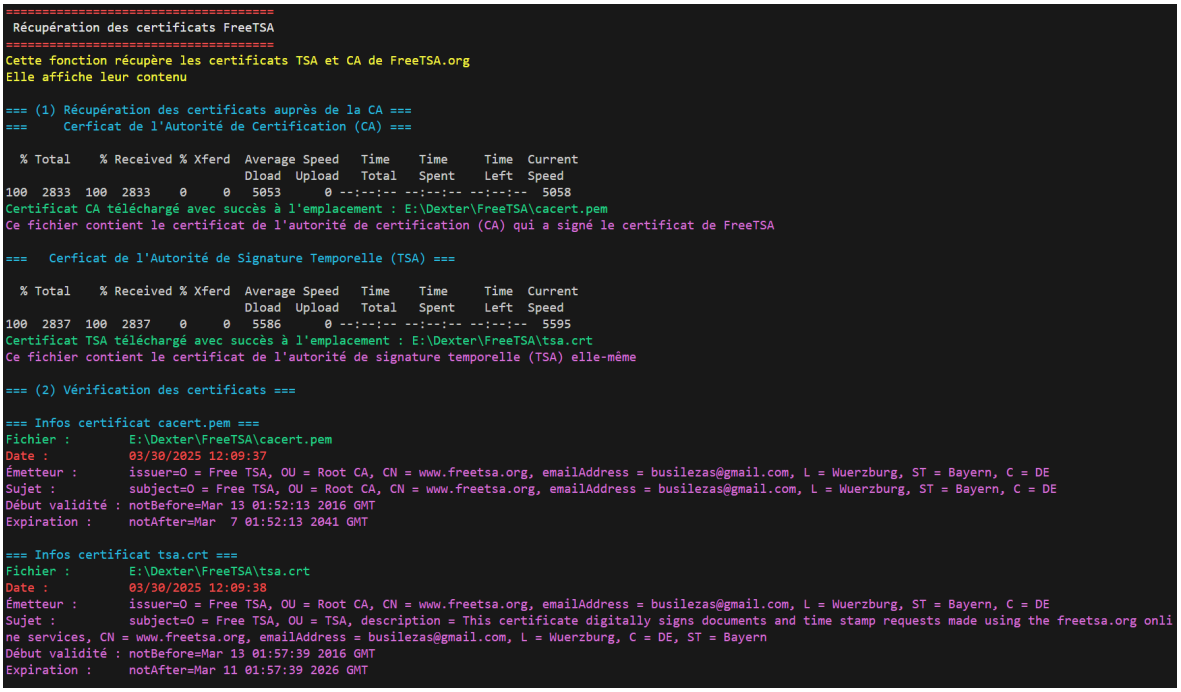

*DEXTER – Menu principal*

Entrée 1 > Simule les effets de l'Altération d'un fichier sur son hash sans faire appel à une autorité de timestamping



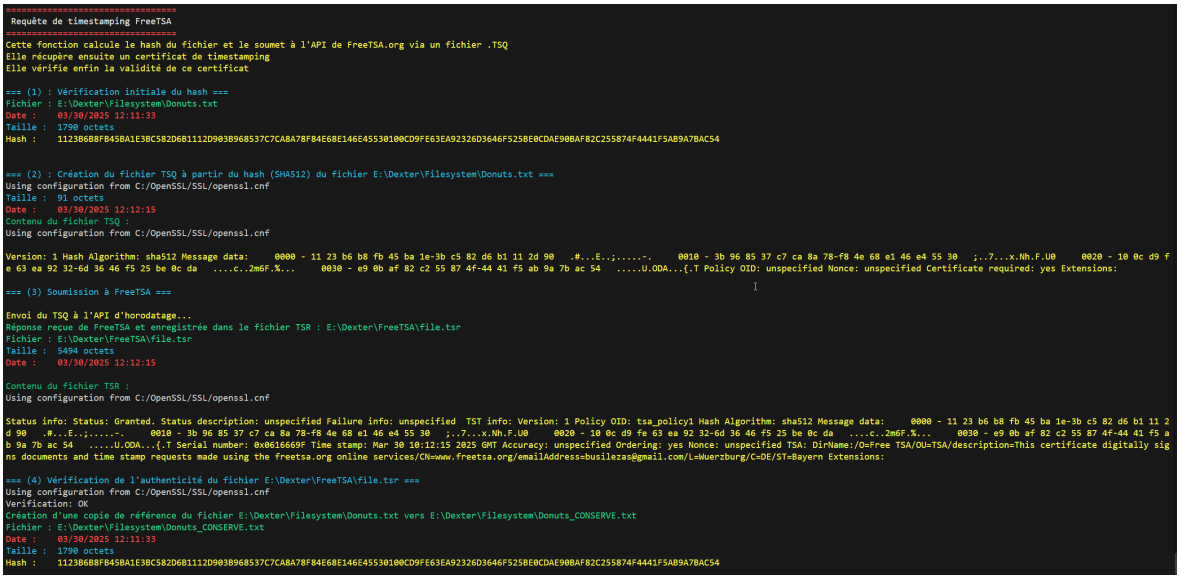

1. *Simulation avec hash local*

Entrée 2 > Récupère les certificats TSA et CA de FreeTSA.org et affiche leur contenu



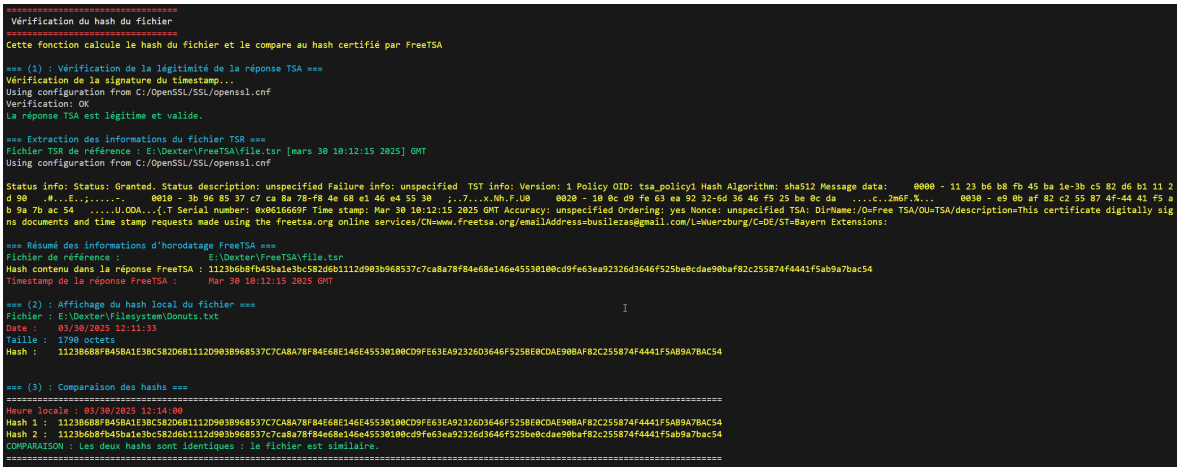

2. *Récupération des certificats FreeTSA*

Entrée 3 > Calcule le hash du fichier de référence et le soumet à l'API de FreeTSA.org via un fichier .TSQ, récupere le certificat de timestamping .TSR, et en vérifie la validité. Le fichier de référence est « mis de côté » pour restauration ultérieure.



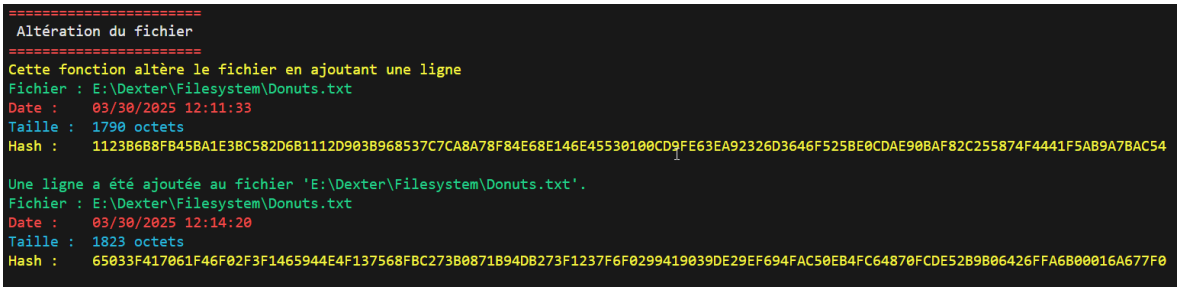

*3. Requête de timestamping FreeTSA*

Entrée 4 > Calcule le hash du fichier de référence et le compare au hash certifié par FreeTSA, après s'être assuré que celui-ci était valide




*4. Vérification du hash du fichier*

Entrée 5 > Altère le fichier de référence en ajoutant une ligne




*5. Altération du fichier*

Entrée 6 > Restaure le fichier de référence (sauvegardé au moment de la soumission à FreeTSA)

```
==========================
 Restauration du fichier
==========================
Cette fonction restaure le fichier dans sa version d'origine
Fichier : E:\Dexter\Filesystem\Donuts.txt
Date :    03/30/2025 12:14:20
Taille :  1823 octets
Hash :    65033F417061F46F02F3F1465944E4F137568FBC273B0871B94DB273F1237F6F0299419039DE29EF694FAC50EB4FC64870FCDE52B9B06426FFA6B00016A677F0

Cette fonction restauration du fichier E:\Dexter\Filesystem\Donuts_CONSERVE.txt vers E:\Dexter\Filesystem\Donuts.txt
Fichier : E:\Dexter\Filesystem\Donuts.txt
Date :    03/30/2025 12:11:33
Taille :  1790 octets
Hash :    1123B6B8FB45BA1E3BC582D6B1112D903B968537C7CA8A78F84E68E146E45530100CD9FE63EA92326D3646F525BE0CDAE90BAF82C255874F4441F5AB9A7BAC54
```

*6. Restauration du fichier*

Entrée 7 > Affiche le contenu du fichier de référence et des répertoires de travail.

```
======================
 État des répertoires
======================
Cette fonction affiche le contenu du fichier de réference et des répertoires de travail

Fichier : E:\Dexter\Filesystem\Donuts.txt
Date :    03/30/2025 12:11:33
Taille :  1790 octets
Hash :    1123B6B8FB45BA1E3BC582D6B1112D903B968537C7CA8A78F84E68E146E45530100CD9FE63EA92326D3646F525BE0CDAE90BAF82C255874F4441F5AB9A7BAC54

Dans la série télévisée « Dexter », le personnage principal, Dexter Morgan, a une relation particulière avec les donuts :

• Un outil social :
Dexter utilise les donuts comme un moyen de s'intégrer socialement et de maintenir son apparence de personne normale.
Il apporte régulièrement des boîtes de donuts à ses collègues du département de police de Miami Metro.
Cette habitude lui permet de créer des liens et de gagner la confiance de ses collègues
Ces éléments sont essentiels pour dissimuler sa véritable nature de tueur en série.

• Une partie de sa routine :
Les donuts font partie intégrante de la routine quotidienne de Dexter au travail.
Ils sont devenus une sorte de marque de fabrique pour lui.

• Les origines des Donut :
Dans la série « Dexter : Original sin », il est expliqué que Dexter a commencé par apporter un plateau de légume.
Suite à la réaction négative de ses collègues, il a opté pour les Donut, qui on eu un succès retentissant.

Les donuts représentent un élément important de la personnalité de Dexter.
Ils symbolisant sa tentative de se conformer aux normes sociales tout en cachant son côté sombre.
Et puis... ça nous change des cookies !
----------------------------------------------------------------------------------------------------------------------------Suppression d'un donut dans la boîte
Suppression d'un donut dans la boîte
Suppression d'un donut dans la boîte
Ajout d'un donut dans la boîte
Suppression d'un donut dans la boîte
Suppression d'un donut dans la boîte
Ajout d'un donut dans la boîte
Ajout d'un donut dans la boîte
Ajout d'un donut dans la boîte
Ajout d'un donut dans la boîte
Suppression d'un donut dans la boîte
Ajout d'un donut dans la boîte
=== Détails des fichiers dans le répertoire 'E:\Dexter\Filesystem': ===

Nom du fichier      Taille (o) Dernière modification Date de création
--------------      ---------- -------------------- ----------------
Donuts_CONSERVE.txt       1790 2025-03-30 12:11:33   2025-03-29 13:03:50
Donuts_ORIGINE.txt        1358 2025-03-30 08:34:54   2025-03-30 08:34:59
Donuts.txt                1790 2025-03-30 12:11:33   2025-03-30 08:37:03

=== Détails des fichiers dans le répertoire 'E:\Dexter\FreeTSA': ===

Nom du fichier Taille (o) Dernière modification Date de création
-------------- ---------- -------------------- ----------------
cacert.pem           2833 2025-03-30 12:09:37   2025-03-23 10:24:15
file.tsq               91 2025-03-30 12:12:15   2025-03-29 10:48:36
file.tsr             5494 2025-03-30 12:12:15   2025-03-29 10:45:20
tsa.crt              2837 2025-03-30 12:09:38   2025-03-23 10:24:15
```

*7. État des répertoires*

**Limitations**

Elles sont nombreuses !

- DEXTER ne prend en charge qu'un fichier de référence (Donuts.txt) pour effecter ses opérations (hachages, altérations, soumission, comparaison)
- DEXTER ne fait pas référence à une base de temps de référence autre que celle de l'autorité de Timestamping. Il ne prend pas en charge les Timezones.
- DEXTER n'applique pas les nécessaires précautions de lecture seule sur un filesystem à mettre en oeuvre dans le cas de l'analyse forensique.
- DEXTER ne prend pas en compte les modifications des métadonnées d'un fichier. Le hash reste le même si on modifie les propriétés du fichier dans le système d'exploitation.
- DEXTER fonctionnerait néanmoins sur une image de volume dont le hash serait altéré si une métadonnée de fichier ou du système de fichier venait à être modifiée.
- DEXTER n'inclut pas de journalisation de ses actions
- DEXTER ne crée pas de bases de données de timestamping pour "raccrocher" un timestamp à un fichier.

**Paramétrage**

- Le script Dexter.PS1 comporte une série de variables autoporteuses modifiables par l'utilisateur avant exécution.
- Les éléments à configurer impérativement sont
    - Le répertoire d'installation du script.
    - Le chemin vers OpenSSL

## 3. Perspectives

DEXTER n'a été réalisé que pour illustrer le mécanisme de comparaisons de hash. D'abord localement, puis en faisant appel à une Autorité de Timestamping (TSA) libre, freeTSA.org.

Pour devenir un outil crédible, les aspects suivants seraient à développer :

- **Utilisation d'une base de temps de référence pour un horodatage des actions locales indépendant de l'heure du système :**
  J'ai essayé d'implémenter des appels à l'API worldtimeapi.org, mais les réponses n'étaient pas consistantes. L'implémentation d'appels au service NTP pool.ntp.org, m'a paru un peu complexe par rapport à mon besoin.
  Après réflexion, j'ai finalement jugé l'heure locale suffisante pour l'illustration souhaitée.

- **Gestion des fichiers de référence, d'images de volumes ou de répertoires :**
  Le développement de ces fonctionnalités aurait nécessité de nombreuses heures sans apporter de grande nouveauté au mécanisme de timestamping.
  J'ai choisi de ne pas m'avancer dans cette voie, n'ayant pas l'objectif de développer un utilitaire complet de Timestamping

- **Base de données de timestamps et journalisation :**

Cet aspect aurait été intéressant à développer même dans le cadre d'un "proof of concept".
Un sequestre de logs et de timestamps associés à des fichiers permettrait de clarifier les actions "fonctionnelles" d'horodatage.
Il aurait balisé le chemin vers la création d'une main courante électronique.

- **Certification du code, et des mécanismes utilisés :**
  En développant soi-même du code pour explorer les mécanismes cryptographiques du timestamping, j'ai été confronté à la qualité de mon propre code (retour d'un contrôle OK alors qu'il ne l'est pas, ...). J'ai également fait face à la garantie des éléments tiers sur lesquels j'ai cherché à m'appuyer. La discipline reposant sur des chaînes de confiance, chaque maillon de la chaîne doit pouvoir être authentifié et certifié conforme à l'État de l'Art des technologies mises en oeuvre. Les entités "sérieuses" proposant des services certifiés (base de temps, timestamping, stockage de fichiers, ...) monnayent lesdits services. Les compétences, les moyens humains et matériels requis pour mettre en place et maintenir ces systèmes certifié ANSSI ou EiDAS induisent inévitablement des coûts pour l'utilisateur. Les services ouverts, gratuits et de qualité ne sont pas légion. FreeTSA.org fait figure d'exception, sans toutefois être reconnu officiellement. Il n'a donc aucune valeur légale. J'ai néanmoins pu explorer une partie des mécanismes mis en oeuvre dans la RFC 3161 sur le protocole d'horodatage basé sur des PKI.