Collection lausannoise

Camille Perrier Depeursinge / Nathalie Dongois /
Andrew M. Garbarski / Carlo Lombardini / Alain Macaluso
(éditeurs)

Cimes et Châtiments

Mélanges en l'honneur du Professeur Laurent Moreillon

Stämpfli Editions

Continuité de la preuve (numérique)

De la scène de crime au tribunal

DAVID-OLIVIER JAQUET-CHIFFELLE
Professeur en science forensique et identification numérique,
Faculté de droit, des sciences criminelles et d'administration publique,
Université de Lausanne

Table des matières

Bibliographie

DAVID-OLIVIER JAQUET-CHIFFELLE/EOGHAN CASEY, A Formalized Model of the Trace, Forensic Science International 2021/327 (cité : trace) ; DAVID-OLIVIER JAQUET-CHIFFELLE/EOGHAN CASEY/JONATHAN BOURQUENOUD, Tamperproof timestamped provenance ledger using blockchain technology, Forensic Science International : Digital Investigation 2020/33 (cité : tamperproof) ; PIERRE MARGOT, La trace comme vecteur fondamental de la police scientifique, Revue internationale de criminologie et de police technique et scientifique 2011, p. 72 ss ; JEAN-CLAUDE MARTIN ET AL., Investigation de scène de crime : fixation de l'état des lieux et traitement des traces d'objets, Lausanne 2014 ; MARK POLLITT ET AL., A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence, OSAC Technical Series 0002R1 2018 ; OLIVIER RIBAUX, Police scientifique : Le renseignement par la trace, Lausanne 2014.

I. Introduction et enjeux

L'élément de preuve est censé apporter un éclairage fiable, pertinent et objectif sur un évènement d'intérêt : un délit, une catastrophe naturelle, voire un simple incident. Il est séparé temporellement de l'évènement considéré et résulte d'une succession de processus et de nombreuses activités complémentaires. Comment s'assurer dès lors de son authenticité, c'est-à-dire qu'il se rapporte effectivement à l'évènement en question ? Comment garantir son intégrité, c'est-à-dire que l'information qu'il véhicule n'a pas été (trop) altérée et décrit suffisamment fidèlement l'évènement d'origine ? En d'autres termes, comment maintenir la continuité de la preuve, de sa détection jusqu'à son éventuelle présentation au tribunal ?

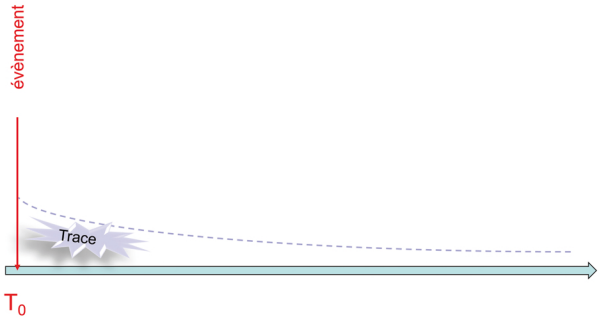
II. Évènement, trace et scène d'investigation

Tout commence par l'évènement d'intérêt lui-même. Comme tout évènement, il impacte son environnement. Il y apporte des modifications qui peuvent persister, évoluer, se déplacer, s'atténuer – parfois même s'amplifier – au-delà de l'évènement lui-même. Ces modifications servent à définir la trace de cet évènement, objet fondamental d'étude en science forensique (voir Figure 1). Lorsque l'évènement est terminé, sa trace peut subsister, évoluer selon une dynamique interne qui lui est propre, mais aussi être perturbée par d'autres évènements extrinsèques ultérieurs. La trace permet d'appréhender l'évènement originel *a posteriori* et *indirectement*, et de tenter de répondre aux questions que se posent l'enquêteur, l'expert forensicien, le procureur, les avocats, le juge ou les jurés.

La comparaison de traces en analyse criminelle permet de relier des évènements sans lien direct apparent, de mieux comprendre certains phénomènes et d'identifier des séries criminelles[1].

[1] RIBAUX.

Figure 1 : La trace (dynamique) d'un évènement



EDMOND LOCARD fournit une description empirique de la trace *: « La vérité est que nul ne peut agir avec l'intensité que suppose l'action criminelle sans laisser des marques multiples de son passage. Je voudrais faire toucher du doigt l'extrême variété de ces traces, non qu'il puisse s'agir d'écrire ici un traité de l'expertise criminelle, mais dans le but de montrer la souplesse et le polymorphisme de la méthode. Les indices dont je veux montrer ici l'emploi sont de deux ordres : tantôt le malfaiteur a laissé sur les lieux les marques de son passage, tantôt, par une action inverse, il a emporté sur son corps ou sur ses vêtements les indices de son séjour ou de son geste. Laissées ou reçues, ces traces sont de sortes extrêmement diverses. »* PIERRE MARGOT propose une définition pratique de la trace en science forensique [2]: *« Marque, signal ou objet, la trace est un signe apparent (pas toujours visible à l'œil nu), le vestige d'une présence ou d'une action à l'endroit de cette dernière. »*. Dans un article récent[3], EOGHAN CASEY et moi-même généralisons et formalisons le concept de trace à tout évènement – pas nécessairement une action. Nous développons une définition scientifique et mathématique de la trace d'un évènement en science forensique, en termes de modifications consécutives à cet évènement, perceptibles ultérieurement à un certain niveau de précision. Notre définition de la trace se veut universelle et s'applique aussi bien au monde analogique, qu'au numérique.

L'élément de preuve présenté au tribunal, issu de la trace, est le résultat d'une succession de processus et d'activités complémentaires, liés intrinsèquement les uns aux autres. Les processus forensiques fondamentaux sont l'authentification, l'identification, la classification, la reconstruction et l'évaluation. Les activités forensiques comprennent la détection, la préservation, l'observation, la documentation, l'analyse, l'intégration et l'interprétation des traces et de l'information qu'elles véhiculent. Ces processus et activités sont imbriqués. Ils

2 MARGOT.
3 JAQUET-CHIFFELLE/CASEY, trace.

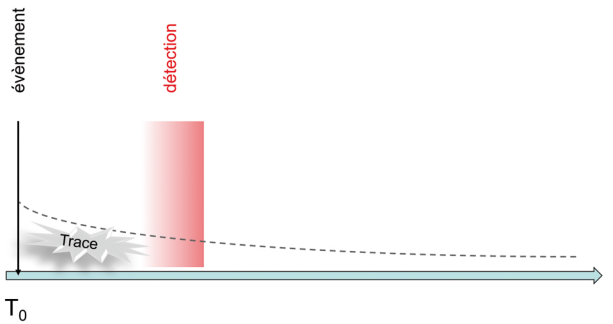
sont structurés et détaillés dans un rapport OSAC[4]. Ceux qui ont un impact sur la continuité de la preuve seront développés plus loin.

La notion de scène de crime est définie pour un évènement, qu'il soit un crime à proprement parler ou non. La scène de crime, si elle existe, est délimitée par la zone dans laquelle l'évènement s'est produit. La scène d'investigation – en général plus large – englobe la région considérée comme pertinente pour observer les nombreuses facettes de la trace liée à cet évènement. La région retenue peut varier au cours d'une enquête en fonction des éléments déjà trouvés et des hypothèses qui en découlent. Souvent, dans un premier temps, la scène d'investigation se limite à la scène de crime et à ses environs[5].

III. Détection

Les premiers intervenants sur une scène de crime[6] ont la responsabilité de détecter (voir Figure 2) – parfois révéler – les éléments de la trace qu'ils estiment authentiques et potentiellement pertinents (authenticité). Lorsque cela est possible, il s'agira de les prélever et les préserver tout en minimisant leur altération (intégrité). Certains de ces éléments conduiront peut-être à un élément de preuve.

Figure 2 : Détection de certaines facettes de la trace



Les chaînes d'authenticité et d'intégrité de la preuve commencent lors de la détection des facettes de la trace ; ensemble, ces deux chaînes permettent d'assurer la continuité de la preuve tout au long des étapes qui jalonnent le

4 POLLITT ET AL.
5 JAQUET-CHIFFELLE/CASEY, trace.
6 MARTIN ET AL.

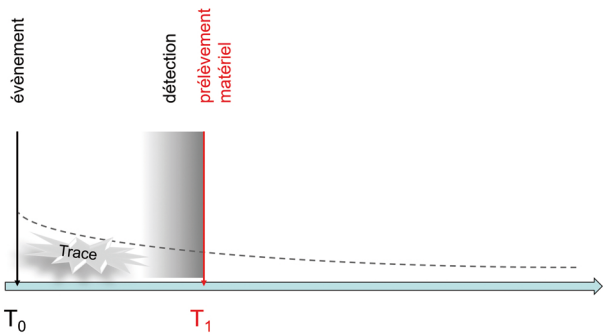
traitement des facettes observées de la trace, ainsi que des indices et éléments de preuve qui en découlent.

D'un point de vue pratique, seules certaines facettes de la trace sont détectées, révélées, observées, dans la mesure du possible préservées, avant d'être analysées. Les limitations sont multiples, inhérentes aux instruments de détection et d'analyse, aux contraintes temporelles, aux ressources limitées et aux biais cognitifs des intervenants[7].

IV. Prélèvement et préservation

Lorsque cela est possible, le prélèvement et la préservation des éléments matériels de la trace potentiellement pertinents (voir Figure 3) sont primordiaux pour la suite des processus et activités forensiques.

Figure 3 : Prélèvement d'éléments matériels



Pour garantir la chaîne d'authenticité, le forensicien prélève les éléments matériels de la trace qu'il considère pertinents, voire leurs supports, et les sécurise par des scellés lorsque cela fait sens. Par la suite, lorsqu'ils reçoivent un élément à analyser, les experts vérifient systématiquement la validité des scellés avant de les ouvrir, puis reconstituent de nouveaux scellés une fois leur travail terminé.

Pour renforcer la chaîne d'intégrité, le spécialiste protège au mieux ses prélèvements contre d'éventuelles perturbations ultérieures par des évènements extrinsèques ; il tente également de minimiser l'impact de la dynamique interne de la trace, c'est-à-dire de son évolution intrinsèque, par exemple en figeant

7 JAQUET-CHIFFELLE/CASEY, trace.

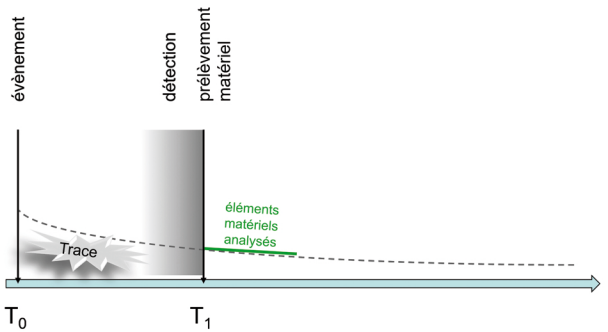
une observation de l'élément matériel en question sur une photographie ou en refroidissant une mémoire d'ordinateur.

Les éléments matériels ainsi préservés peuvent ensuite être observés, documentés et analysés.

V. Observations et analyses dans le monde physique

Lorsqu'un investigateur reçoit un élément matériel à observer et analyser (voir Figure 4), il s'assure de son authenticité en vérifiant par exemple la validité des scellés.

Figure 4 : Analyse d'éléments matériels



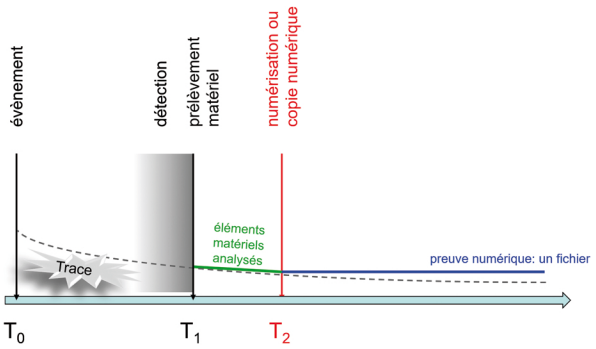
Pour maintenir l'intégrité, il préférera une analyse non destructive du composant de la trace qu'il a reçu. En effet, une analyse destructive est non reproductible et brise la chaîne d'intégrité, particulièrement si tout le matériel à disposition est altéré. Lorsqu'une telle analyse est indispensable, une documentation détaillée compense en partie la perte d'intégrité : enregistrement photographique ou vidéo de l'élément avant son analyse et parfois de l'analyse elle-même, buts de l'analyse, description des méthodes utilisées et de la succession des opérations effectuées pendant l'analyse, identification des intervenants, du contexte, du lieu, du moment. Une documentation détaillée renforce également la confiance en l'authenticité des résultats de l'analyse.

Certains résultats d'analyse peuvent être numériques : résultats d'une analyse chimique écrits dans un fichier ou résultats d'une analyse ADN. Les objets numériques sont a priori facilement modifiables, falsifiables, ou même interchangeables. Comment dès lors garantir le maintien de la qualité des chaînes d'authenticité et d'intégrité ? Comment maintenir la continuité de la preuve numérique ?

VI. Numérisation

Un élément de preuve numérique (voir Figure 5) découle soit de la numérisation d'un élément de preuve analogique (photographie numérique de traces papillaires, résultats numériques d'une analyse dans le monde physique) ou de son environnement (photographie numérique ou modélisation tridimensionnelle d'une scène de crime), soit de la copie d'une facette de la trace qui est numérique par nature (information sur le disque dur d'un ordinateur, contenu sur le web ou le Darkweb, enregistrements dans les journaux d'un serveur).

Figure 5 : Elément de preuve numérique



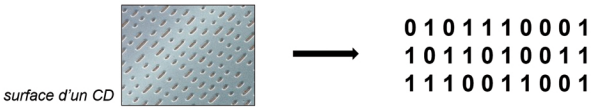
Un élément de preuve numérique n'est autre qu'un fichier informatique particulier.

Pour garantir la chaîne d'authenticité, le forensicien s'assure que l'élément de preuve analogique ou la facette numérique de la trace qu'il transforme – par numérisation ou par copie forensique – en élément de preuve numérique est authentique. Pour un élément de preuve matériel, il vérifie la validité de la chaîne actuelle d'authenticité, par exemple via les éventuels scellés. S'il reçoit directement les résultats numériques d'une l'analyse, il doit vérifier que ces résultats proviennent effectivement de l'analyse de l'élément de preuve analogique en question.

Dans le cas d'une copie numérique, pour assurer l'intégrité de l'élément de preuve numérique engendré, l'expert forensique copie *fidèlement* la facette numérique de la trace en question. La qualité de la preuve numérique engendrée dépend de plusieurs facteurs : est-ce que le forensicien a accès au support physique pour la facette de la trace considérée ? Ou doit-il au contraire se contenter d'observations indirectes, par exemple via des requêtes actives sur un serveur ?

La confiance en l'intégrité de l'élément de preuve numérique est renforcée si le processus de virtualisation qui l'engendre est reproductible. Typiquement, si le forensicien a accès au support physique, par exemple suite à la perquisition et à la séquestration d'un ordinateur ou du téléphone portable d'un suspect, la trace numérique physique est virtualisée pour être copiée (voir Figure 6) :

Figure 6 : Virtualisation d'une trace numérique physique



La virtualisation se fait par lecture et copie binaire du support physique. Afin de s'assurer que le support n'est pas modifié durant le processus, le spécialiste utilise un *write blocker*, une interface qui protège contre toute écriture sur le support physique et n'autorise que son accès en lecture. Une telle configuration permet d'envisager la reproductibilité du processus. Si le support n'a pas été altéré par le processus de copie forensique, on qualifie la copie de *parfaite*. Si l'information sur le support avant la copie est strictement la même que celle contenue dans la copie, on dit que la copie est *pure*. On parle d'*intégrité forte* lorsque la copie est à la fois pure et parfaite.

Dans la pratique, pour comparer l'information sur le support avant et après le processus de copie, ainsi que celle dans l'élément de preuve numérique engendré (la copie forensique du support), le spécialiste utilise une fonction de hachage cryptographique qui crée des empreintes numériques du support et de la copie forensique. Une empreinte numérique est très discriminante : le même objet numérique a toujours la même empreinte et la probabilité que deux objets différents aient la même empreinte, de façon fortuite, est infinitésimale. On considère que la copie est *parfaite* si l'empreinte du support est la même avant et après le processus de copie, et qu'elle est *pure* si l'empreinte du support avant la copie est la même que celle de l'élément de preuve numérique engendré (i.e., de la copie forensique).

Lorsque l'investigateur n'a pas accès au support physique (site web, serveur distant) ou que la lecture du support physique ne peut pas être répétée (écoute passive et directe des câbles intercontinentaux, DPI – *deep packet inspection*), l'observation ne peut être reproduite. Lors de l'investigation d'un site web, l'observation est active et indirecte. Elle se fait au travers de requêtes sur Internet. L'information observée est parfois même créée au moment de la requête, donc initiée par l'observation elle-même. Si une même requête est répétée, il

n'y a aucune garantie que l'information observée soit identique. En effet, l'information observée peut être influencée par – ou dépendre de – l'outil d'observation, la géolocalisation (apparente) de cet outil et le moment où ladite observation a lieu. Dans ce cas, l'information – donc son empreinte numérique – issue de l'observation de la source peut changer à chaque requête ; les notions de copie parfaite ou de copie pure perdent leur sens : l'intégrité forte n'est plus possible.

Comme l'observation n'est plus nécessairement reproductible, il faut l'appréhender comme une analyse destructive d'une facette de la trace. Une documentation précise s'impose pour ancrer la chaîne d'authenticité.

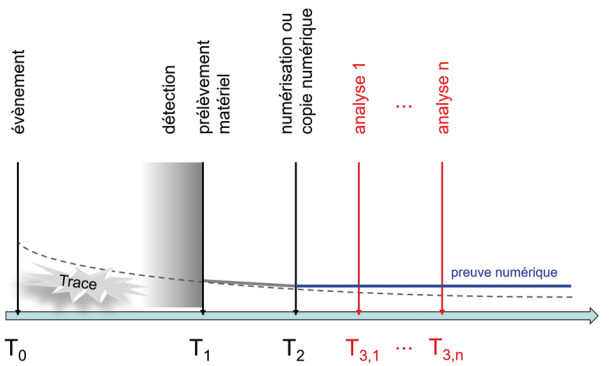
Finalement, comment rester confiant dans le fait que le fichier généré – élément de preuve numérique – correspond effectivement à l'élément de preuve authentique dont il est issu et qu'il n'a pas été modifié ultérieurement par inadvertance ou intentionnellement ?

Des mesures technico-organisationnelles s'imposent.

VII. Mesures pour maintenir la chaîne d'authenticité

Des mesures technico-organisationnelles sont mises en place pour maintenir la chaîne d'authenticité de l'élément de preuve numérique.

Figure 7 : Analyses futures



Lors de la création de l'élément de preuve numérique, un certificat numérique d'authenticité contenant les informations numérisées d'un éventuel scellé de la source (support qui a été copié, élément de preuve qui a été numérisé), la date et l'heure de création du fichier ainsi que l'empreinte numérique du fichier est

créé et signé numériquement par l'entité garante. De nouveaux scellés protégeant le support contenant la preuve numérique sont mis en place. Toute personne ayant accès au fichier est identifiée et un journal retrace l'historique des accès au fichier lors des analyses successives (voir Figure 7).

L'élément de preuve numérique ne doit plus être modifié. L'empreinte numérique du fichier sert à vérifier son intégrité. Les mesures technico-organisationnelles mise en place pour maintenir la chaîne d'authenticité ne sont toutefois pas suffisantes pour garantir l'intégrité de l'élément de preuve numérique.

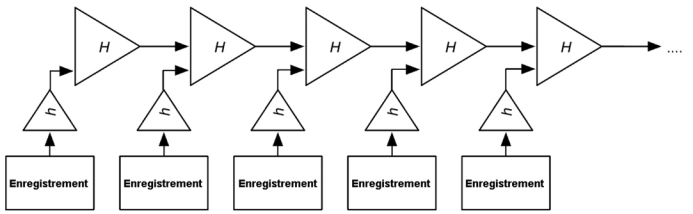
VIII. Mesures pour maintenir la chaîne d'intégrité

A. Mesures techniques

A priori, durant l'enquête, l'empreinte numérique d'un fichier permet uniquement de vérifier que ce fichier n'a pas été modifié ultérieurement *par inadvertance*. Elle ne protège pas contre une modification *intentionnelle* de ce fichier. Pour détecter toute modification ultérieure du fichier – intentionnelle ou non –, il faut rendre son empreinte numérique non modifiable. Signer cette empreinte ne suffit malheureusement pas. En effet, rien n'empêche le signataire de recalculer puis signer la nouvelle empreinte d'un fichier altéré. Un système d'horodatage fiable est indispensable pour se prémunir de modifications intentionnelles : l'empreinte doit être horodatée dès qu'elle a été créée. Elle est ainsi fixée temporellement et permet de garantir le contenu exact de ce fichier *à cet instant*.

Un prototype de système d'horodatage adapté au travail des investigateurs a été développé à l'ESC. La conception scientifique est détaillée dans un article scientifique[8].

Figure 8 : Chaînage des enregistrements



8 JAQUET-CHIFFELLE/CASEY/BOURQUENOUD, tamperproof.

Un système d'horodatage est un registre permanent d'informations ordonnées temporellement. Une fois dans le registre, une information ne peut plus être effacée, déplacée ou modifiée. Le registre est lisible publiquement : chacun peut analyser son contenu. Les enregistrements successifs sont chaînés de façon irréversible (voir Figure 8).

On peut envisager deux types de registre ordonné d'informations : un registre centralisé, géré par un tiers de confiance, ou un registre décentralisé, de type *blockchain* publique, dans lequel la confiance est distribuée. Le prototype développé à l'ESC utilise une *blockchain* publique.

Afin d'être en mesure de détecter toute modification ultérieure du fichier, plusieurs alternatives sont possibles, mais une seule est recommandée. Enregistrer directement l'intégralité du fichier dans un tel registre d'informations horodatées n'est pas envisageable pour des données d'enquêtes qui d'une part peuvent requérir des téraoctets de mémoire et, d'autre part, sont sensibles et confidentielles. En effet, chacun pourrait voir le contenu du fichier en question puisque le registre est accessible publiquement en lecture. Pour pallier à cela, il est possible d'envoyer uniquement l'empreinte numérique du fichier au système d'horodatage. Toutefois, cette option n'est pas non plus satisfaisante. Elle permettrait à un suspect de tester si certains de ses fichiers ont attiré l'attention des enquêteurs, en vérifiant si leurs empreintes ont été ou non horodatées. Une parade consiste à soumettre plutôt une empreinte numérique salée du fichier : l'empreinte est non plus calculée directement sur le fichier, mais sur une concaténation du fichier et d'un sel (une suite aléatoire de bits qui ne peut pas être devinée). Le sel est conservé avec le fichier. Pour vérifier l'horodatage, il suffit de connaître le fichier et le sel utilisé, de recalculer l'empreinte numérique salée et de vérifier l'appartenance de cette dernière dans le registre ordonné d'informations horodatées.

B. Mesures organisationnelles

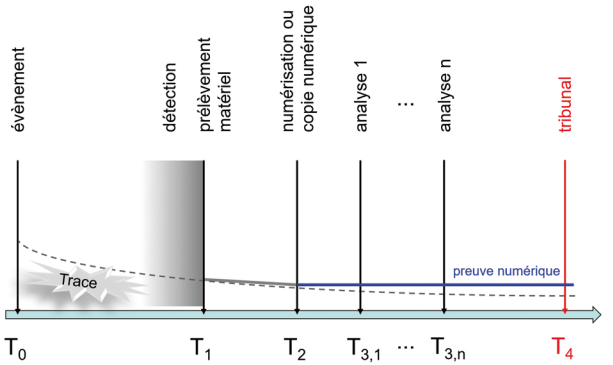
Les mesures techniques (empreintes numériques, système d'horodatage à disposition), seules, ne permettent pas de garantir la continuité de la preuve. Des directives organisationnelles précisant quelle information soumettre au système d'horodatage et quand l'enregistrer, ainsi que l'authentification des personnes accédant aux éléments de preuve numériques doivent être décidées dans le but de renforcer les mesures techniques. Ensemble, les mesures techniques et organisationnelles permettent de détecter toute modification ultérieure – intentionnelle ou non – des informations numériques importantes. Pour que cela fonctionne, il faut que l'investigateur horodate l'empreinte salée de tout fichier qu'il considère pertinent.

IX. La preuve (numérique) au tribunal : conclusion

De manière générale, une preuve judiciaire n'est pas une preuve au sens mathématique. Le terme *preuve* se révèle mal choisi et peut prêter à confusion. On devrait plutôt parler d'un élément dont on est *suffisamment* sûr qu'il est lié à l'évènement d'intérêt et dont on est *suffisamment* convaincu que l'information qu'il véhicule offre une description *suffisamment* fidèle de certains aspects de cet évènement.

Lorsque l'élément de preuve numérique arrive enfin au tribunal (voir Figure 9), toutes les personnes concernées (i.e., l'expert forensicien, le procureur, les avocats, le juge ou les jurés) peuvent vérifier le niveau de confiance à accorder à la continuité de cette preuve en évaluant la qualité des chaînes d'authenticité et d'intégrité.

Figure 9 : La preuve numérique au tribunal



La confiance absolue n'est ni réaliste, ni réalisable. Comme pour toute « preuve » judiciaire, une incertitude résiduelle est inévitable. Pour que l'élément de preuve numérique soit recevable, il est toutefois nécessaire que le niveau de confiance qui lui est associé soit suffisamment élevé. Le seuil de confiance à atteindre dépend des enjeux du procès et du poids de cet élément de preuve numérique dans les raisonnements que feront le juge ou les jurés au cours du processus global d'évaluation des faits conduisant à la décision judiciaire.

Collection lausannoise

Cimes et Châtiments

Mélanges en l'honneur du Professeur Laurent Moreillon

Édité par

Camille Perrier Depeursinge
Nathalie Dongois
Andrew M. Garbarski
Carlo Lombardini
Alain Macaluso

Stämpfli Editions

Information bibliographique de la Deutsche Nationalbibliothek
La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse http://dnb.d-nb.de.

Print ISBN 978-3-7272-2982-4

Dans notre librairie en ligne www.staempflishop.com,
la version suivante est également disponible :

E-Book ISBN 978-3-7272-6177-0