NORME INTERNATIONALE

ISO/IEC 27037

Première édition
2012-10-15

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

Numéro de référence
ISO/IEC 27037:2012(F)

© ISO/IEC 2012



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2012, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vi**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **2**

4 Abréviations **4**

5 Vue d'ensemble **6**
5.1 Contexte de collecte des preuves numériques 6
5.2 Principes de preuves numériques 6
5.3 Exigences concernant le traitement des preuves numériques 6
5.3.1 Généralités 6
5.3.2 Vérifiabilité 7
5.3.3 Répétabilité 7
5.3.4 Reproductibilité 7
5.3.5 Justification 7
5.4 Processus de traitement des preuves numériques 8
5.4.1 Vue d'ensemble 8
5.4.2 Identification 8
5.4.3 Collecte 9
5.4.4 Acquisition 9
5.4.5 Préservation 10

6 Éléments clés de l'identification, de la collecte, de l'acquisition et de la préservation des preuves numériques **11**
6.1 Chaîne de contrôle 11
6.2 Précautions à prendre sur le site de l'incident 11
6.2.1 Généralités 11
6.2.2 Personnel 12
6.2.3 Preuves numériques éventuelles 12
6.3 Rôles et responsabilités 13
6.4 Compétence 13
6.5 Faire preuve d'une diligence raisonnable 14
6.6 Documentation 14
6.7 Réunion d'information 15
6.7.1 Généralités 15
6.7.2 Spécificité des preuves numériques 15
6.7.3 Spécificité du personnel 16
6.7.4 Incidents en temps réel 16
6.7.5 Autres informations 16
6.8 Priorisation de la collecte et de l'acquisition 17
6.9 Préservation des preuves numériques éventuelles 18
6.9.1 Vue d'ensemble 18
6.9.2 Préservation des preuves numériques éventuelles 18
6.9.3 Emballage des appareils numériques et des preuves numériques éventuelles 18
6.9.4 Transport des preuves numériques éventuelles 20

7 Exemples d'identification, de collecte, d'acquisition et de préservation **20**
7.1 Ordinateurs, périphériques et supports de stockage numérique 20
7.1.1 Identification 20
7.1.2 Collecte 23
7.1.3 Acquisition 27
7.1.4 Préservation 31
7.2 Appareils en réseau 32
7.2.1 Identification 32

© ISO/IEC 2012 – Tous droits réservés

7.2.2 Collecte, acquisition et préservation 34
7.3 Collecte, acquisition et préservation de systèmes CCTV 36
Annexe A (informative) **Description du savoir-faire et compétences élémentaires du DEFR** **39**
Annexe B (informative) **Exigences relatives à la documentation minimale pour le transfert de preuves** **41**
Bibliographie **42**

 © ISO/IEC 2012 – Tous droits réservés

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/IEC 27037 a été élaborée par le comité technique ISO/TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

© ISO/IEC 2012 – Tous droits réservés

Introduction

La présente Norme internationale fournit des lignes directrices pour les activités spécifiques au traitement de preuves numériques éventuelles; ces processus sont les suivants: l'identification, la collecte, l'acquisition et la préservation de preuves numériques éventuelles. Ces processus sont requis lors d'une investigation destinée à préserver l'intégrité des preuves numériques, une méthodologie acceptable pour obtenir les preuves numériques qui contribuera à sa recevabilité en cas de poursuites judiciaires et disciplinaires ainsi que dans d'autres cas requis. La présente Norme internationale fournit également des lignes directrices générales pour la collecte de preuves non numériques susceptibles de s'avérer utiles lors de la phase d'analyse des preuves numériques éventuelles.

La présente Norme internationale a pour objet de fournir des préconisations aux personnes chargées de l'identification, de la collecte, de l'acquisition et de la préservation des preuves numériques éventuelles. Ces personnes incluent les premiers intervenants en contact avec les preuves numériques (DEFR), les spécialistes des preuves numériques (DES), les spécialistes en réponse aux incidents et les responsables des laboratoires forensiques. La présente Norme internationale garantit que les personnes responsables traitent les preuves numériques éventuelles de façon acceptable partout dans le monde, avec pour objectif de faciliter l'investigation impliquant des appareils numériques et des preuves numériques de façon systématique et impartiale tout en préservant leur intégrité et leur authenticité.

La présente Norme internationale vise également à informer les décideurs qui ont besoin de déterminer la fiabilité des preuves numériques qui leur sont présentées. Elle s'applique aux organismes devant protéger, analyser et présenter des preuves numériques éventuelles. Elle est pertinente dans le contexte des organismes en charge de l'établissement de politiques, qui créent et évaluent des modes opératoires en rapport avec les preuves numériques, souvent dans le cadre d'un ensemble plus vaste de preuves.

Les preuves numériques éventuelles auxquelles il est fait référence dans la présente Norme internationale peuvent provenir de différents types d'appareils numériques, de réseaux, de bases de données, etc. Elles désignent des données se trouvant déjà au format numérique. La présente Norme internationale n'a pas pour objectif de couvrir la conversion de données analogiques au format numérique.

En raison de la fragilité des preuves numériques, il est nécessaire d'appliquer une méthodologie acceptable pour garantir l'intégralité et l'authenticité des preuves numériques éventuelles. La présente Norme internationale n'exige pas l'utilisation d'outils ou de méthodes spécifiques. Des composants clés qui fournissent une crédibilité au cours de l'investigation constituent la méthodologie appliquée au cours du processus et les personnes qualifiées pour exécuter les tâches sont spécifiées dans la méthodologie. La présente Norme internationale ne traite pas de la méthodologie concernant les procédures judiciaires, les procédures disciplinaires et les autres actions associées concernant le traitement des preuves numériques éventuelles se trouvant en dehors du domaine d'application de l'identification, de la collecte, de l'acquisition et de la préservation.

L'application de la présente Norme internationale requiert le respect des lois, règles et réglementations nationales. Il convient qu'elle ne remplace pas les exigences légales spécifiques d'une quelconque juridiction. Au lieu de cela, elle peut servir de ligne directrice pratique pour tout DEFR ou DES dans le cadre d'investigations impliquant des preuves numériques éventuelles. Elle ne s'étend pas à l'analyse des preuves numériques et ne remplace pas les exigences spécifiques à la juridiction concernant des sujets comme la recevabilité, la valeur probatoire, la pertinence et d'autres limites soumises au contrôle judiciaire concernant l'utilisation de preuves numériques éventuelles devant les cours de justice. La présente Norme internationale peut faciliter l'échange de preuves numériques éventuelles entres les juridictions. Afin de préserver l'intégrité des preuves numériques, les utilisateurs de la présente Norme internationale doivent adapter et amender les modes opératoires décrits dans la présente Norme internationale conformément aux exigences légales spécifiques de la juridiction concernant les preuves.

Bien que la présente Norme internationale n'inclue pas la préparation forensique, la préparation forensique adéquate peut en grande partie prendre en charge l'identification, la collecte, l'acquisition et le processus de préservation des preuves numériques. La préparation forensique désigne le fait d'atteindre un niveau approprié de capacité par un organisme lui permettant d'identifier, de collecter, d'acquérir, de préserver, de protéger et d'analyser des preuves numériques. Si les processus et activités

 © ISO/IEC 2012 – Tous droits réservés

décrits dans la présente Norme internationale sont essentiellement des mesures réactives utilisées pour investiguer sur un incident après sa survenue, la préparation forensique est un processus proactif visant à essayer de planifier de tels événements.

La présente Norme internationale complète l'ISO/IEC 27001 et l'ISO/IEC 27002, et, notamment, les exigences de contrôle portant sur l'acquisition des preuves numériques éventuelles en fournissant des préconisations complémentaires concernant la mise en œuvre. En outre, la présente Norme internationale s'appliquera dans des contextes indépendants de l'ISO/IEC 27001 et l'ISO/IEC 27002. Il convient de lire la présente Norme internationale en parallèle avec d'autres normes relatives aux preuves numériques et à l'investigation concernant des incidents de sécurité de l'information.

© ISO/IEC 2012 – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

1 Domaine d'application

La présente Norme internationale fournit des lignes directrices pour les activités spécifiques au traitement des preuves numériques que sont l'identification, la collecte, l'acquisition et la préservation des preuves numériques susceptibles de présenter une valeur probatoire. La présente Norme internationale fournit des préconisations aux personnes concernant des situations courantes rencontrées au cours du processus de traitement des preuves numériques, apporte une aide aux organismes en ce qui concerne leurs procédures disciplinaires et vise à faciliter l'échange de preuves numériques éventuelles entre les juridictions.

La présente Norme internationale fournit des préconisations concernant les appareils et/ou fonctions suivants utilisés dans diverses circonstances:

— supports de stockage numérique utilisés dans les ordinateurs standard comme les disques durs, disquettes, disques optiques et magnéto-optiques, supports d'informations dotés de fonctions similaires;

— téléphones mobiles, assistants numériques personnels, appareils électroniques personnels, cartes mémoires;

— systèmes de navigation mobiles;

— appareils photo et caméras vidéo numériques (comprenant la télévision en circuit fermé (CCTV));

— ordinateurs standard dotés de connexions réseau;

— réseaux basés sur TCP/IP et d'autres protocoles numériques; et

— appareils dotés de fonctions similaires à celles citées ci-dessus.

NOTE 1 La liste des appareils ci-dessus est une liste indicative et non exhaustive.

NOTE 2 Ces circonstances incluent les appareils ci-dessus se présentant sous diverses formes. Par exemple, un système automobile peut inclure un système de navigation mobile, un système de stockage des données et un système sensoriel.

2 Références normatives

Les documents ci-après sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/TR 15801, *Images électroniques — Stockage électronique d'informations — Recommandations pour les informations de valeur et leur fiabilité*

ISO/IEC 17020, *Évaluation de la conformité — Exigences pour le fonctionnement de différents types d'organismes procédant à l'inspection*

ISO/IEC 17025:2005, *Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais*

© ISO 2012 – Tous droits réservés

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 27000, l'ISO/IEC 17020, l'ISO/IEC 17025 et l'ISO/TR 15801, ainsi que les suivants s'appliquent.

3.1
acquisition
processus de création d'une copie de données d'un ensemble défini

Note 1 à l'article: Le résultat d'une acquisition est une copie des preuves numériques éventuelles.

3.2
espace dédié
zone d'un support numérique, comprenant la mémoire principale, utilisée pour le stockage des données, comprenant les métadonnées

3.3
collecte
processus consistant à rassembler des éléments physiques contenant des preuves numériques éventuelles

3.4
appareil numérique
équipement électronique utilisé pour traiter ou stocker des données numériques

3.5
preuves numériques
informations ou données, stockées ou transmises sous forme binaire susceptibles d'être invoquées comme preuves

3.6
copie de preuves numériques
copie de preuves numériques réalisées pour préserver la fiabilité des preuves incluant à la fois les preuves numériques et les moyens de vérification où la méthode de vérification des preuves peut être soit intégrée, soit indépendante des outils utilisés pour la vérification

3.7
premier intervenant en contact avec les preuves numériques
DEFR
personne autorisée, formée et qualifiée pour agir en premier lieu sur la scène d'un incident afin de réaliser la collecte et l'acquisition des preuves numériques et étant responsable du traitement de ces preuves

Note 1 à l'article: L'autorité, la formation et la qualification sont des exigences prévues nécessaires pour produire des preuves numériques fiables, mais des cas particuliers peuvent avoir pour conséquence qu'une personne ne satisfait pas à l'ensemble de ces trois exigences. En pareil cas, il convient de considérer la législation locale, la politique de l'organisme et les cas particuliers.

3.8
spécialiste en preuves numériques
DES
personne en mesure d'exécuter les tâches d'un DEFR et disposant de connaissances, de savoir-faire et de capacités spécialisés lui permettant de traiter un large éventail de problèmes techniques

Note 1 à l'article: Un DES peut disposer de compétences spécifiques complémentaires, par exemple, acquisition de réseaux, acquisition de RAM, connaissances en logiciels de système d'exploitation ou en ordinateurs centraux.

© ISO/IEC 2012 – Tous droits réservés

3.9
support de stockage numérique
appareil sur lequel il est possible d'enregistrer des données numériques

[SOURCE: Adapté de l'ISO/IEC 10027:1990]

3.10
installation de préservation des preuves
environnement sécurisé ou lieu où les preuves collectées ou acquises sont stockées

Note 1 à l'article: Il convient de ne pas exposer une installation de préservation des preuves aux champs magnétiques, à la poussière, à des vibrations, à l'humidité ou à tout autre élément environnemental (comme une température ou une humidité extrêmes) qui pourraient endommager les preuves numériques éventuelles dans l'installation.

3.11
valeur de hachage
chaîne de bits issue d'une fonction de hachage

[SOURCE: ISO/IEC 10118-1:2000]

3.12
identification
processus impliquant la recherche, la reconnaissance et la documentation des preuves numériques éventuelles

3.13
création d'image
processus de création d'une copie bit à bit de supports de stockage numérique

Note 1 à l'article: La copie bit à bit est également appelée copie physique.

EXEMPLE Lorsqu'il crée une image d'un disque dur, le DEFR copie également les données qui ont été supprimées.

3.14
périphérique
appareil relié à un appareil numérique afin d'étendre sa fonctionnalité

3.15
préservation
processus destiné à préserver et protéger l'intégrité et/ou l'état initial des preuves numériques éventuelles

3.16
fiabilité
propriété relative à un comportement et des résultats prévus et cohérents

[SOURCE: ISO/IEC 27000:2009]

3.17
répétabilité
propriété d'un processus visant à obtenir les mêmes résultats d'essai sur le même environnement d'essai (même ordinateur, disque dur, mode de fonctionnement, etc.)

3.18
reproductibilité
propriété d'un processus visant à obtenir les mêmes résultats d'essai sur un environnement d'essai différent (ordinateur, disque dur, opérateur différents, etc.)

© ISO/IEC 2012 – Tous droits réservés

3.19
altération de preuves
acte consistant à appliquer ou autoriser une/des modification(s) à des preuves numériques éventuelles, qui diminue leur valeur probatoire

3.20
heure système
heure générée par l'horloge du système et utilisée par le système d'exploitation, et non heure calculée par le système d'exploitation

3.21
sabotage
acte consistant à appliquer ou autoriser une/des modification(s) à des preuves numériques (c'est-à-dire altération délibérée ou volontaire de preuves)

3.22
horodatage
paramètre de variante temporelle qui indique un point dans le temps par rapport à une référence temporelle commune

[SOURCE: ISO/IEC 11770-1:1996]

3.23
espace non alloué
zone d'un support numérique, comprenant la mémoire principale, qui n'a pas été alloué par le système d'exploitation, et qui est disponible pour le stockage des données, comprenant les métadonnées

3.24
validation
confirmation, par la fourniture de preuves objectives, que les exigences relatives à une utilisation prévue ou une application prévue ont été satisfaites

[SOURCE: ISO/IEC 27004:2009]

3.25
fonction de vérification
fonction utilisée pour vérifier que deux ensembles de données sont identiques

Note 1 à l'article: Il convient que deux ensembles de données non identiques ne se traduisent pas par une concordance identique à partir d'une fonction de vérification.

Note 2 à l'article: Les fonctions de vérification sont, en général, mises en œuvre à l'aide de fonctions de hachage comme MD5, SHA1, etc., mais d'autres méthodes peuvent être utilisées.

3.26
données volatiles
données sujettes au changement et facilement modifiables

Note 1 à l'article: Un changement peut être la mise hors tension ou le franchissement d'un champ magnétique. Les données volatiles incluent également des données qui changent lorsque l'état du système change. Les exemples comprennent des données stockées dans la RAM et des adresses IP dynamiques.

4 Abréviations

AVI Entrelacement audio/vidéo (Audio Video Interleave)

CCTV Télévision en circuit fermé (Closed Circuit Television)

CD Disque compact (Compact Disc)

© ISO/IEC 2012 – Tous droits réservés