Horodatage des fichiers

JT Cnejita – 23 septembre 2014

Horodatage des fichiers

- Théoriquement, il faut l'huissier ou sa version électronique (le coffre-fort électronique, la signature électronique) pour avoir une heure certaine, mais... il y a peut-être d'autres alternatives
- Les ordinateurs sont souvent synchronisés avec une horloge internet
- Les opérations laissent des traces dans quantité de réceptacles (cf Evidence Processor Encase, RVS de Xways, métadonnées)
- Dans quels cas peut-on les exploiter pour produire de la preuve ?

- A quoi correspond la date restituée par un outil?
- Le système qui a stocké la date était-il altérable?
- L'altération laisse-t-elle des traces?
- Les croisements de dates sont-ils redondants?

Cas de figure rencontrés

- Heure d'hiver ou heure d'été ou heure UTC?
- Un journal d'événements intact
- Des métadonnées rares

Un mail extrait d'outlook

- Il y a une pièce jointe
- Les dates système sont à la date de l'extraction du mail puis de la PJ
- Les dates internes (en-tête mail et métadonnées Word) sont cohérentes avec l'histoire
- Mais...
  - Dates internes Outlook falsifiables (export eml avec ToutMail, modif puis reimport msg avec toumail)
  - Dates internes Word créables facilement depuis un ordinateur qui n'est pas sous mon contrôle
- Le mail n'est pas probant

Les métadonnées

- Une collection de tableaux Excel d'époque
  - Les fichiers
  - Les métadonnées
- Dans ce cas, les métadonnées étaient consistantes avec l'histoire racontée
  - Dates de créations, modification internes au fichiers cohérentes avec les dates annoncées
  - Version d'Excel en cours à l'époque
  - Historique des interventions sur le fichier
  - Version de Windows en cours à l'époque
- Je ne connais pas d'outils capable d'éditer les métadonnées des docs Office (je ne sais pas non plus comment
- Les éléments sont crédibles parce qu'une scène de ce type est difficile à reproduire

Le journal d'événements

- L'ordinateur qui a servi à fabrique le fichier à dater « fichierADater.ai » et son export « fichierADater.jpg »
- Le fichier porte les dates cohérentes avec l'histoire
- Les fichiers temporaires, thumbnail, lnk
- Sauf que ... Je sais reproduire la même scène en modifiant l'horloge par le bios
- Lecture du journal d'événement – pas de traces de désordre dans la séquence, pas de traces de modification de l'heure
- Logs antivirus – pas de traces de désordres mais simple fichier texte
- Recherche internet ne montre pas d'outils capable de modifier un journal d'événements
- Eléments validés grâce à une triple vérification
  - Système de fichier, lnk, base de registre ... permettent de dire qu'un fichier de titre « fichierADater.ai » a été créé et modifié à la date dite (disons 2010)
  - Le journal d'événement ne montre pas d'altération de l'horloge (ni séquence desordonnée, ni événement de changement d'heure)
  - Le thumbnail permet de montrer que l'image contenue dans fichierADater.ai n'a pas été changée
- Ultime vérification
  - Pour identifier les traces laissées par une modif de date, test d'une modification de date sur une machine virtuelle utilisant l'image disque – validation sur la machine d'origine – utilisation de l'image pour remettre le disque en état après la manip

Mails dans Google

- Un constat d'huissier montre des mails présents dans Google et relève les dates associées. Est-ce suffisant?
- Non
  - Des tests montrent que si des messages sont remontées dans un compte gmail via imap, ils apparaissent dans Gmail avec la date contenu dans les en-têtes du message
  - Les en-têtes de message sont facile à trafiquer
- Qu'aurait-il fallu de plus?
  - Lors que le message est remonté dans Google via imap, il perd ses en-têtes. Il aurait fallu que l'huissier afficher les en-têtes du message (fonction « afficher l'original du message » dans Gmail)

Routage de mails

- Un message est vu deux fois :
  - Le message reçu,
  - La retransmission du message
- Entre les deux instances, il y a 1 seconde d'écart affichée
  - Message reçu à 11h22mn02s
  - Message retransmis : affiché comme reçu à 11h22mn03s
- Est-ce que la date est intègre?
- Analyse
  - Dans ce cas précis, l'analyse des en-têtes montre que le message a été reçu à 11h22mn02s950ms
  - Il est possible que le système qui prend la date pour la retransmission fasse un arrondi et que celui qui affiche la date ne le fasse pas.
  - Les en-têtes montrent aussi que dans le routage, 'il y a eu une passerelle X400->SMTP
  - Le scénario de l'écart d'arrondi est jugée crédible et l'écart d'1 seconde n'est pas suffisant pour écarter le message.

Discussion

- Autres exemples?
- Des hypothèses encore à l'épreuve
  - Altération des métadonnées Office
  - Altération d'un journal d'événement) sont-elles solides
  - Arrondi dans les routages X400→SMTP
  - Reprise de la date des en-têtes lors de la remontée SMTP
- Travaux à suivre
  - Elina Nikoazm – Jean-Louis Courteaud