Connaissance technique

« Immaterial Items » dans Nuix, la zone d'ombre

20. juin 2014, by Irène Wilson

Introduction

La documentation de Nuix (v5.2.1_0 p. 53-54) décrit les « immaterial items » comme suit:

> Immaterial items are those items that are extracted for forensic completeness, but do not necessarily have intrinsic value in a legal context. Additionally, these items will NOT be exported as part of a legal export and are not included in the total size calculation for audited licenses. These items include, folders (file system, email, etc.), embedded inline graphics (email signatures, text items in PDF files, embedded objects without text, the zip container itself (not the contents), and mailbox files (PST, OST, NSF, MBOX, etc.).

De plus amples détails sont ajoutés plus loin (p.71):

> Immaterial items are those items that are extracted for forensic completeness, but do not necessarily have intrinsic value in a legal context. Additionally, these items are not exported as part of a legal export and are not included in the total size calculation for audited licenses. Immaterial items include: Folders (file system, email, etc.) embedded inline graphics (email signatures, embedded items in PDF files) embedded objects without text the zip container itself (not the contents) mailbox files like PST, OST, NSF, MBOX, EDB, STM, etc

Il y a plusieurs aspects intéressants dans cette description. Passons-la à présent à la loupe et mettons en lumière quelques détails méconnus.

A la Recherche des « Immaterial Items »

Les « immaterial items » sont faciles à cacher et peuvent même complètement disparaître au travers de l'option « Hide immaterial items (text rolled up to parent) ». Les trouver est toutefois bien moins intuitif. Voici la recherche qui retourne uniquement les « immaterial items »:

NOT flag:audited

« Immaterial Items » en Pratique

Lancer cette recherche est le premier pas vers la compréhension de ce que sont réellement les « immaterial items ». Vous avez peut-être remarqué que la description que Nuix fait de ces objets est bien vague et consiste plutôt en une liste d'exemples. Je ne peux malheureusement pas vous donner de définition plus claire; il n'en existe pas. Cependant, ce que je recommande aux investigateurs chevronnés que vous êtes, c'est de prendre le temps de les découvrir dans la pratique.

Tout d'abord, lancez la recherche ci-dessus. Ensuite, changez la vue des résultats pour Statistics › Files afin de découvrir quels types de fichiers sont étiquetés comme immatériels. Déjà à ce stade, vos certitudes en matière d'objets immatériels vacillent. Maintenant, juste

pour le plaisir, combinez la recherche ci-dessus avec « has-image:1 ». Aviez-vous pour habitude d'exclude d'office les images immatérielles de vos candidats pour la reconnaissance optique de caractères (OCR) sans même une seconde pensée? Oups… L'image ci-dessous fait plus de 2MB et est en fait considérée par Nuix comme immatérielle.

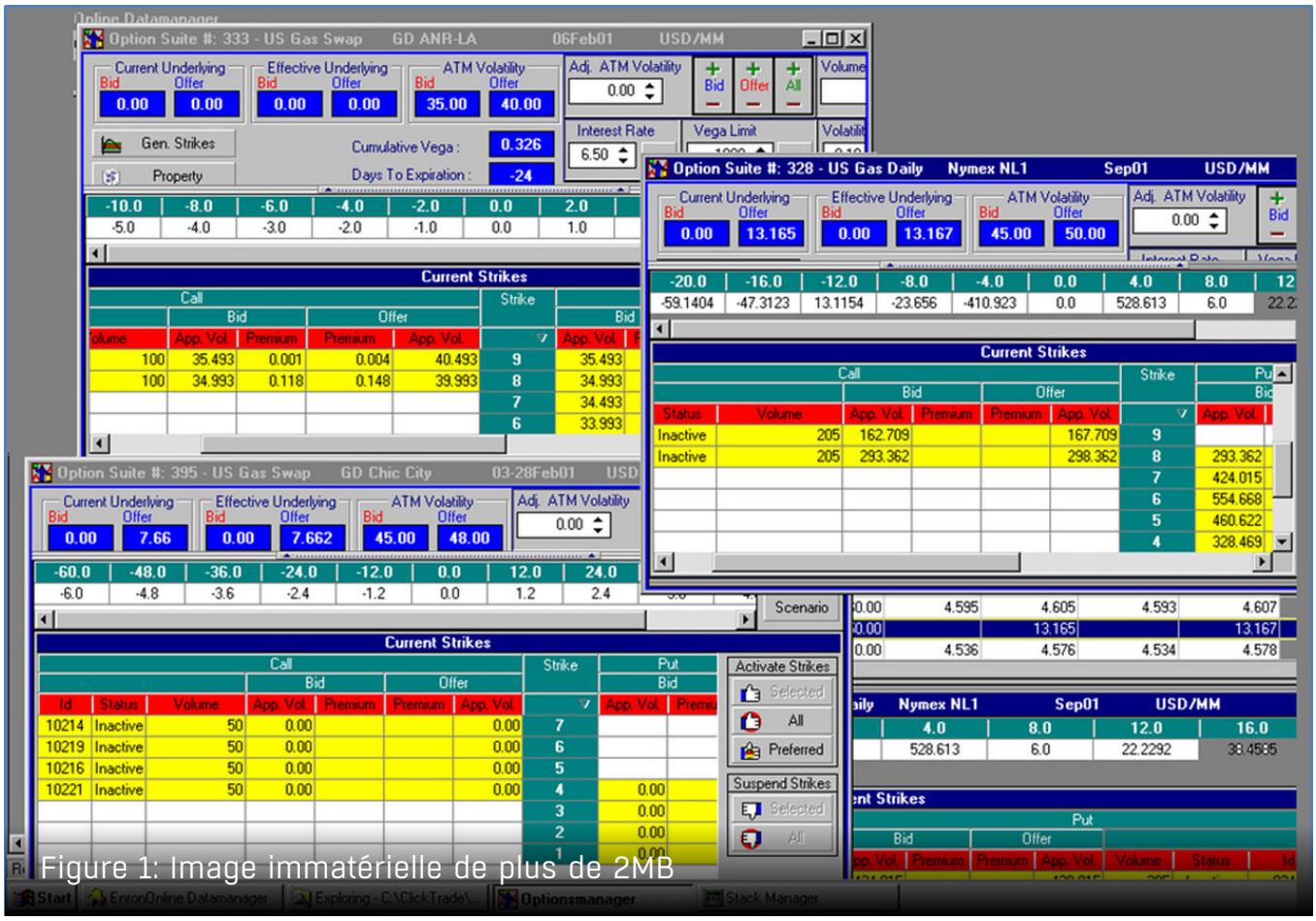

Figure 1: Image immatérielle de plus de 2MB

Maintenant entrons tout droit dans la 4ème dimension… Etes-vous prêts à découvrir la vraie force des « immaterial items »? Alors lancer la recherche pour les trouver, combinée avec « contains-text:1 ». Et oui, les objets immatériels peuvent en fait contenir du texte. Vous pouviez toutefois vous y attendre, puisque la description de l'option « Hide immaterial items (text rolled up to parent) » mentionne spécifiquement du texte (bien qu'elle ne mentionne pas d'images).

Si vous relisez la description que fait Nuix de ses « immaterial items », vous pouvez à présent admirer toute la relativité et la finesse de l'expression « do not necessarily have intrinsic value in legal context »…

De la Cohérence des « Immaterial Items »

Bien que la définition des « immaterial items » demeure hors de portée, vous avez maintenant une meilleure compréhension de ce qu'ils peuvent inclure. Un autre fait d'intérêt qui mérite assurément d'être mentionné ici est l'incohérence des objets immatériels au travers de l'évolution de Nuix. Les objets étiquetés comme étant immatériels se sont avérés différents selon la version de Nuix utilisée. La documentation de ces changements n'est malheureusement pas toujours très détaillée.

Du Marriage des Notions de « Legal Export » et « Immaterial Items »

Si cet article vous a convaincu de regarder à deux fois à vos objets immatériels, j'ai une bonne nouvelle pour vous: contrairement à ce que stipule la citation de Nuix citée plus haut, les « immaterial items » peuvent être exportés au travers de « legal exports ». Si vous sélectionnez l'option « Export items: Selected Items only » lors de votre export, tous les objets sélectionnés seront exportés, peu importe qu'ils soient matériels ou non. Le fichier natif des objets sans réel contenu (dossiers ou conteneurs) sera remplacé par une « slipsheet » alors que les autres objets seront exportés correctement. La reconnaissance optique de caractères (OCR) fonctionne également sur la plupart des images immatérielles.

Figure 2: Contenu d'une « slipsheet » pour des objets immatériels

Conclusion

Ne vous fiez pas aux apparences: les « immaterial items » peuvent cacher des trésors. Comme d'habitude, la proportionalité est la clé. Que vous preniez en compte ces objets ou

non est entièrement à votre libre appréciation, assurez-vous juste de prendre une décision éclairée. Utiliser les meilleurs outils présents sur le marché ne fera pas de vous un expert; seule une connaissance en profondeur de vos outils vous rapprochera de ce but.

Irène Wilson

Irène Wilson est spécialisée dans l'investigation informatique et dans l'eDiscovery. Au cours de ses nombreuses années d'expérience, elle a travaillé pour des clients de nombreux secteurs différents dans toute l'Europe. Parmi ses nombreuses qualifications, figurent les prestigieux titres de master pour Nuix Workstation et Nuix Discover.

Swiss FTS | https://swiss-fts.com/fr | +41 43 266 78 50 | info@swiss-fts.com

https://swiss-fts.com/fr/blog/dans-nuix-la-zone-dombre