Technisches Wissen

Immaterial Items in Nuix: Eine Grauzone

20. Juni 2014, von Irène Wilson

Einleitung

Die Nuix Dokumentation (v5.2.1_0 p. 53-54) beschreibt immaterial items wie folgt:

> 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.).

Diese Beschreibung enthält einige interessante Aspekte, die wir in diesem Artikel genauer unter die Lupe nehmen werden.

Finding Immaterial Items

Während immaterial items in einem Nuix Case durch die Option Immaterial items: Hide sehr einfach versteckt werden können oder durch die Processing Option Hide immaterial items (text rolled up to parent) sogar komplett verschwinden, ist das Auffinden ebendieser Elemente weniger intuitiv. Trotzdem gibt es einen eifachen Weg um diese Elemente zu finden. Mit folgender Abfrage werden ausschliesslich immaterial items retourniert:

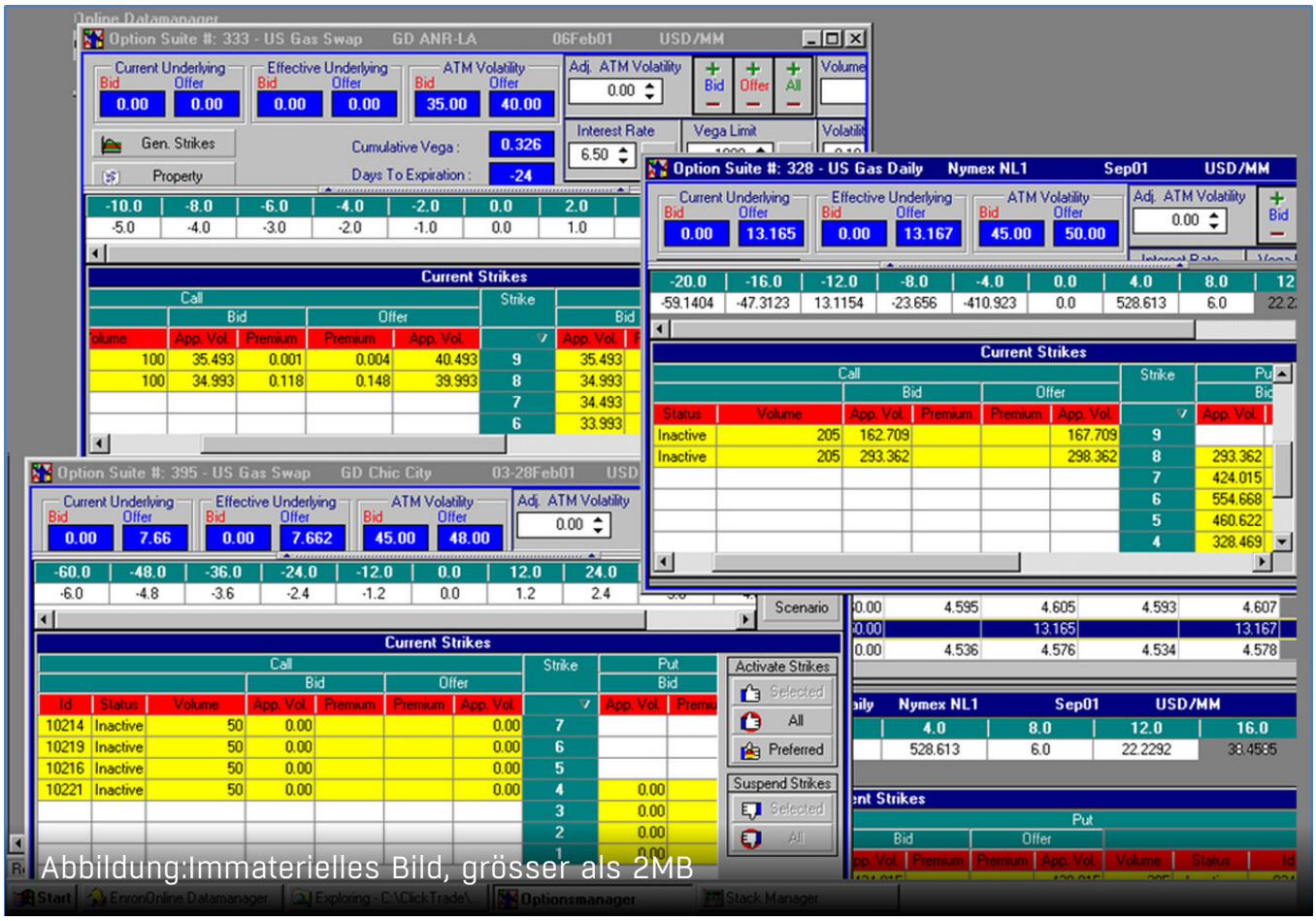
NOT flag:audited

Immaterial items in der Praxis

Das Ausführen obiger Abfrage ist der erste Schritt zum Verstehen, was immaterial items wirklich sind. Wie Sie bemerkt haben, ist ihre Definition in der offiziellen Nuix-Anleitung vage und enthält lediglich einige wenige Beispiele. Eine klare Definition existiert leider nicht. Es ist deshalb von Vorteil, immaterial items selber einmal auszuprobieren.

Als erster Schritt sollte die oben genannte Abfrage ausgeführt werden. Wechseln Sie anschliessend die Ansicht zu Statistics › Files um zu sehen, welche Filetypen als immaterial markiert wurden. Kombinieren Sie jetzt die vorherige Abfrage mit has-image:1

Haben Sie immaterielle Bilder bisher ohne genauer hinzusehen als OCR (Optical Character Recognition) Kandidaten ausgeschlossen? Ups! Das unten gezeigte Bild betrachtet Nuix als immaterial item! Es ist grösser als 2MB, könnte aber sehr wohl wichtige Informationen enthalten.



Gehen wir noch einen Schritt weiter, so wird ersichtlich wie viele Informationen eigentlich in immaterial items enthalten sein können. Führen Sie die vorherige Abfrage erneut mit contains-text:1 aus. So, immaterial items können also durchaus Text enthalten. Dies war eigentlich, durch die Existenz der Option Hide immaterial items (text rolled up to parent) zu erwarten, allerdings, offensichtlich ist es keineswegs.

Wenn Sie nun die Beschreibung der immaterial items von Nuix nochmals lesen, wird sehr deutlich, wie ungenau die Aussage „do not necessarily have intrinsic value in legal context“ wirklich ist...

Konsistenz von immaterial items

Obwohl keine Definition von immaterial items existiert – und dieser Artikel auch keine liefern kann – geben wir hier einen Einblick, was der Begriff alles einschliessen kann.
Ein weiterer wichtiger Aspekt ist die Inkonsistenz, mit welcher die verschiedenen Nuix-Versionen in der Vergangenheit immaterial items klassifiziert haben. Immaterial items in neueren Versionen sind nicht mehr gleich klassifiziert wie in früheren. Zudem sind diese Änderungen manchmal gar nicht und oft nur spärlich dokumentiert.

Legal Export und immaterial items

Falls Sie dieser Blogartikel neugierig macht, immaterial items genauer zu untersuchen, so gibt es gute Neuigkeiten: Im Gegensatz zur Nuix-Dokumentation können immaterial items sehr wohl über legal exports exportiert werden. Dies ist möglich, wenn bei einem legal export die Option Export items: Selected Items only ausgewählt wird. So werden alle selektierten Objekte exportiert, egal ob diese unter die Kategorie immaterial fallen oder nicht. Native Dateien von Objekten, welche keinen Inhalt haben (z.B. Ordner oder Container) werden durch einen Platzhalter ersetzt. Andere Objekte werden korrekt exportiert. Auch der OCR-Export funktioniert bei den meisten immateriellen Bildern.

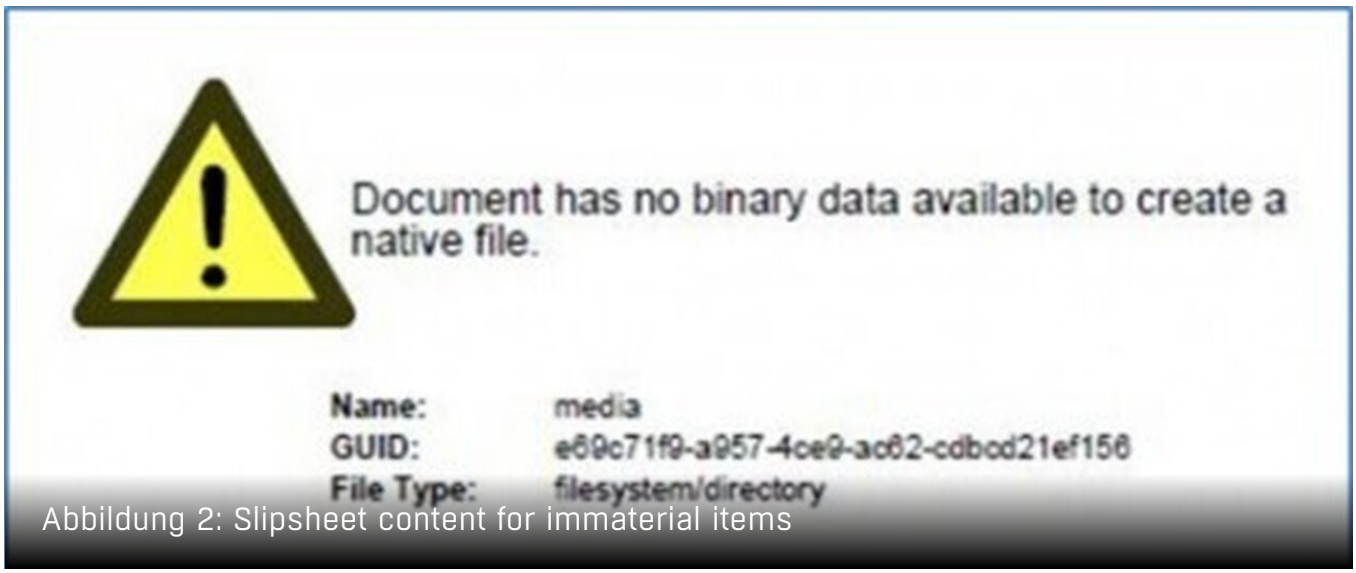


Abbildung 2: Slipsheet content for immaterial items

Fazit

Wie hier verdeutlicht, können immaterial items sehr wohl material sein und wichtige Informationen enthalten. Falls Sie in Ihre Untersuchungen immaterial items mit einbeziehen, begründen Sie diese Entscheidung ausführlich. Marktführende Forensik-Tools wie Nuix vereinfachen unsere Arbeit, aber das Verständnis und das Wissen, was diese Tools genau tun, ist entscheidend.

Irène Wilson

Irene Wilson ist auf digitale Forensik und eDiscovery spezialisiert und hat im Laufe ihrer langjährigen Erfahrung für Kunden aus einer Vielzahl von Branchen in ganz Europa gearbeitet. Zu ihren Qualifikationen

gehören die renommierten Master-Titel für Nuix Workstation und Nuix Discover.