Nuix Immaterial Items, the Grey Area

20. June 2014, by Irène Wilson

Introduction

Nuix documentation (v5.2.1_0 p. 53-54) describes the immaterial items as follows:

> 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.).

Further information is added later (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

There are several interesting points in this description. Let's dissect it and shine light on some hidden details.

Finding Immaterial Items

While immaterial items can easily be hidden in a case or even totally disappear through the "Hide immaterial items (text rolled up to parent)" option, finding them is less intuitive. Here is the query that returns only immaterial items:

NOT flag:audited

Immaterial Items in Practice

Running this query is the first step to understand what immaterial items really are. You might have notice that Nuix description gives you a rather vague definition of what immaterial items are and only lists some examples. I can't give you a clearer definition either; none exists. However, what I would recommend, to the thorough investigators that you are, is to take time to discover them in practice.

First, run the query above. Then, change the results view to the Statistics > Files to see which file types are flagged as immaterial. Already at this stage you might see your assumptions about immaterial definition waver. Now, just for fun, combine the query above with "has-image:1". Did you use to exclude immaterial images from your OCR candidates without a second thought? Oops... The image below is larger than 2MB and is actually considered

immaterial.

Figure 1: Immaterial image of more than 2MB

Now let's enter the 4th dimension. Are you ready to discover the true power of immaterial items? So run the query above combined with "contains-text:1". Well, yes, immaterial items can actually contain text. Although you could have expected it, as the description of the "Hide immaterial items (text rolled up to parent)" option especially mentions text (even though it doesn't mention images).

If you read the Nuix description of immaterial items again, you might now wonder how relative and finely nuanced the expression "do not necessarily have intrinsic value in legal context" is...
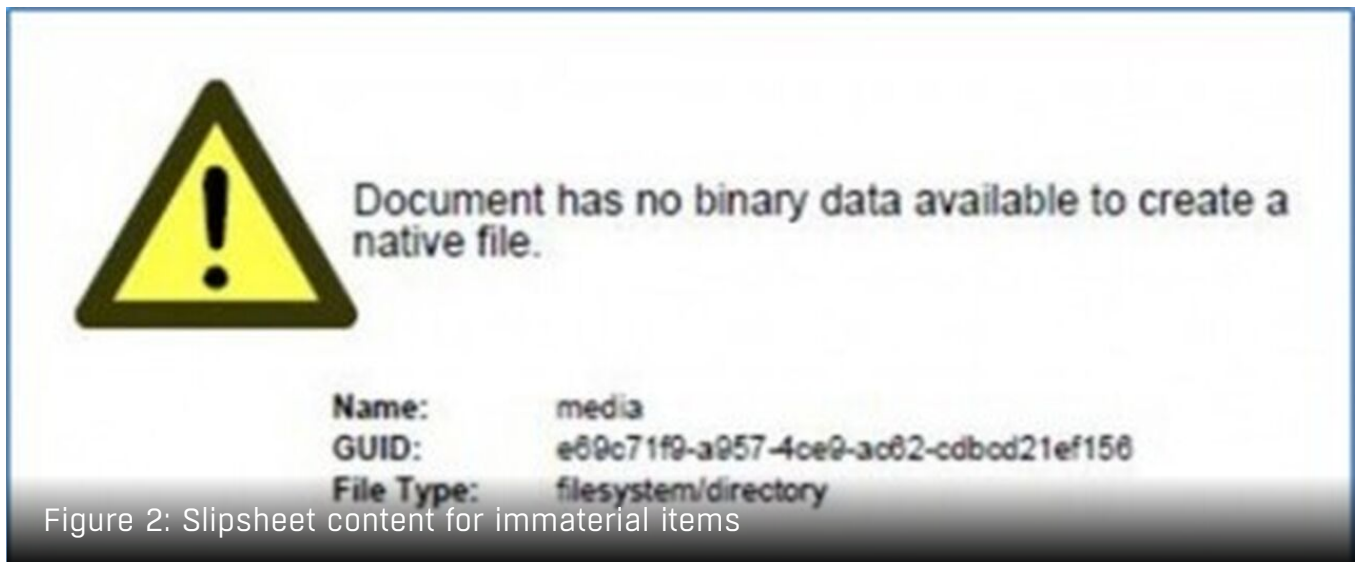
Immaterial Items Consistency

Even though the immaterial item definition remains out of reach, you now have a better idea of what it can actually include. Another interesting fact that needs to be mentioned is the inconsistency of immaterial items through Nuix evolution. Items flagged as immaterial have

proven to be different from one Nuix version to the other, and this change is not always documented with much details.

Legal Export and Immaterial Items

If this article has convinced you to look twice at your immaterial items, I have good news for you: unlike what is mentioned in the Nuix quotation above, immaterial items can be exported through legal exports. If when doing a legal export you select the option "Export items: Selected Items only", all your selected items will be exported, no matter whether they are material or not. The native file of items without a real content (folders or containers) will be replaced by a slipsheet while the other items will be exported correctly. The OCR export also works on most immaterial images.

Figure 2: Slipsheet content for immaterial items

Conclusion

Nothing is ever as it seems and immaterial items can hide treasures. As usual, best effort is the key. Whether you consider them or not is up to you, just be sure to make an informed decision. Using the best tools on the market won't make you an expert; only having an in-depth knowledge of your tools will.

Irène Wilson

Irene Wilson specializes in Digital Forensics and eDiscovery, with many years of experience in a wide range

of industries across Europe. Her qualifications include the illustrious Master titles for Nuix Workstation and Nuix Discover.