**Hinweise**

* Alles in den Values steht im Little Endian Format

**Meine Idee fürs Vorgehen**

* Auf jeden Fall muss die **Hierarchie** in den Shellbags mit Subkeys und Subsubkeys berücksichtigt werden 🡪 es muss also ersichtlich sein, welcher Unterordner Teil eines übergeordneten Ordners ist
* Eventuell auch den Pfad in den ShellBags mit hinschreiben?? + Anzahl der Children (Subkeys)
* Analyse der Values (Doppelklick auf die Zahlen unter BagMRU bzw. den Subkey) 🡪 zuerst Untersuchung des Class type Indicators an Offset 0x02 🡪 dieser bestimmt die Art des Shell Items 🡪 vllt auch den Namen des Shell Items hinschreiben, also Root Folder, Volume, File Entry
* Welche Infos sollten danach ausgewertet werden und im Tool auftauchen:

1. Root Folder Shell Items

* Nach dem Indicator den Sort Index betrachten 🡪 spezifiziert das Root Folder Shell Item 🡪 Ordnername mit hinschreiben
* Zum Schluss die GUID korrekt auflösen (siehe Grundlagen)

2. Volume Shell Items

* Hier haben wir bisher keine anderen Infos außer den Indicator
* Dokumentation von Joachim Metz Shelltypes!!! + Hinweis Belegarbeit
* Vermutlich sind Netzlaufwerke auch Volume Shell Items mit dem Indicator von 2F und dem Laufwerksbuchstaben an Offset 0x03 🡪 hier könnte man also nochmal spezifizieren

3. File Entry Shell Items

* Class Type Indicator analysieren : 31 für Ordner, 32 für ZIP-komprimierte Ordner
* Dann den Rest dazu auswerten: Modification Date and Time, Primary Name
* Hinweise zum Extension Block:
* Suche nach der Signatur BEEF0004 🡪 damit findet man den Anfang und kann die Infos auswerten
* Hinweise zum langen Namen von File Entry Shell Items:
* Kurzer Name ist immer an einem festen Offset 🡪 Form „zeit“
* Langer (kompletter) Name ist nicht immer am selben Offset 🡪 Form „z.e.i.t.“🡪 wie finden? 🡪 vllt Suche des kurzen Namens am festen Offset 🡪 = der Namensanfang des Ordners 🡪 diesen dann im weiteren Verlauf suchen
* Extension Blocks 🡪 variabler Offset 🡪 Suche nach BEEF0004

**Fazit:** eigentlich haben wir alle Informationen, außer die Volume Shell Items sind noch uneindeutig bzw. Netzlaufwerke und externe Speichermedien (ggf. lassen wir die weg, weil sich das nicht testen lässt in virtual box???)

Da die Struktur in den ShellBags der Verzeichnisstruktur entspricht, sollten wir die genau so auswerten