Creating Hash Sets manually

by Sharren Redmond

These are the files we and values we want to create a hash set for:

FILE NAME	HASH VALUE	SIZE	DATE	TIME	TIME ZONE
ADR001.JPG	6399D93EC5AEA0B5301CC0BC012F3E73	216775	03/03/2000	14:35	PST
ADR001P.JPG	1B51EF8587265A099059EBABE999594F	7644	03/03/2000	14:35	PST
ADR002.JPG	DAFFAF4DD6A7A16C235D56832FCADF59	188032	03/03/2000	14:37	PST
ADR002P.JPG	9D60B7C66AAA39B0A2D0C5076CAF5F30	8200	03/03/2000	14:37	PST
ADR003.JPG	4789914D2CEDBBB2823A4B2CF7D3868B	174023	03/03/2000	14:38	PST
ADR003P.JPG	366AAE4A0B253D244D3457FC821DDB4D	8214	03/03/2000	14:39	PST

You have to create a .hke and .hsh file (same filename). The hsh file requires all the information above, the hke file literally reads the .hsh file and creates the set, which results in a .hash file being created.

<u>The .hsh file</u>

The .hsh file starts like this, with all headings separated by commas:

```
"file_id","hashset_id","file_name","directory","hash","file_size","date_modified","time_modified","time_zone","comments","date_accessed","time_accessed"
```

file id = individual number for each hash set, i.e. for those above I used 1 – 6
hashset_id = number for actual set, i.e. for those above I used 1. If you want the hke file to create 3 different hash sets from a single .hsh file then you'd use say '1' for the six values above and call them 'kp hashes', then use '2' for another lot of values and call them something different.
Filename = self explanatory. <u>Place data in quotation marks *i.e. "xxx"*</u>
Directory = I guess this is the directory where the files are stored (I don't put anything here)
Hash = the full hash value. <u>Place data in quotation marks *i.e. "xxx"*</u>
File size = self explanatory
Date modified = I use the date shown in the details above
Time modified = I use the time shown in details above
Time zone = PST, GMT etc
Comments = e.g. 'child porn hash' or 'hacker tools' etc. <u>Place data in quotation marks *i.e. "xxx"*</u>
Date accessed = I don't put anything here
Time accessed = I don't put anything here

If you choose not to input data for one of the headings, don't leave a space just place a comma and continue with the next data, i.e.

"time_modified","time_zone","comments"
14:35,,"child porn"
↑

no details for 'time zone'

So, the .hsh file for the above data should look like this:

```
"file_id","hashset_id","file_name","directory","hash","file_size","date_modified","time_modified","tim
e_zone","comments","date_accessed","time_accessed"

1,1,"ADR001.JPG",,"6399D93EC5AEA0B5301CC0BC012F3E73",216775,03/03/2000,14:35:00,PST,"
KNOWN CHILD PORN",,
2,1,"ADR001P.JPG",,"1B51EF8587265A099059EBABE999594F",7644,03/03/2000,14:35:00,PST,"K
NOWN CHILD PORN",,
3,1,"ADR002.JPG",,"DAFFAF4DD6A7A16C235D56832FCADF59",188032,03/03/2000,14:37:00,PST
,"KNOWN CHILD PORN",,
4,1,"ADR002P.JPG",,"9D60B7C66AAA39B0A2D0C5076CAF5F30",8200,03/03/2000,14:37:00,PST,"
KNOWN CHILD PORN",,
5,1,"ADR003.JPG",,"4789914D2CEDBBB2823A4B2CF7D3868B",174023,03/03/2000,14:38:00,PST,"
KNOWN CHILD PORN",,
6,1,"ADR003P.JPG",,"366AAE4A0B253D244D3457FC821DDB4D",8214,03/03/2000,14:39:00,PST,"
KNOWN CHILD PORN",,
```

The .hke file

The .hke file starts like this, with all headings separated by commas:

```
"hashset_id","name","vendor","package","version","authenicated_flag","notable_flag","initials","num_o
f_files","description","date_loaded"
```

hashset id = same as above (they must match)

name = the number and name you want the hash set to go by. All hash sets relating to child pornography on Brian Deerings hash set message board begin with ZZ. This is because Encase looks at the hash sets in alphabetical order so all the ZZ files are grouped together, *e.g. 'ZZ001 suspected KP'*

vendor = if the hash set is of say the Excel program, then vendor would be 'Microsoft'

package = I never fill these in – no idea what they are for

version = If it's a hash set for a program, version may be 'Windows'

authenticated flag = I always put a **1** here

notable flag = has a **1** if its notable and a **0** if its known

initials = can put your initials here, Brian Deerings have NDIC

number of files = there is always a **0** here

Description = *i.e. 'ZZ001 suspected child porn'*

Date loaded = todays date

So, the .hke file for the above data should look like this:

```
"hashset_id","name","vendor","package","version","authenicated_flag","notable_flag","initials","num_o
f_files","description","date_loaded"

1,"ZZ known Child Porn",,,,1,1,,0,"Known Child Porn",
```

If I had loaded 3 different hash sets into the .hsh file, i.e. hashset_id 1, 2 and 3. Then the hke file needs to also have a line of data for hash set id 2 and 3, and unique names for the sets.

Loading into Encase

Click Tools/Hash Sets
Choose – 'Import hashkeeper sets'
Point to the hke file (make sure the .hsh file is in the same directory path)
Encase should read the .hke and ask if you want to rebuild the new library with the new sets. Choose Rebuild.
You may not see the new hash set straight away. You may have to close the hash sets box and reopen it to refresh.
You should now see a set called 'ZZ Known child porn' – or whatever you called it.
You'll also note that a .hash file has been created in the directory path that looks something like this:

```
HASH
ÿ □□□

ZZ known Child Porn                                                                    Qï…‡&Z
        _Yë«é™YO  6j®J
%=$M4Wü,ÛM  G‰'M,í»_,:K,÷Ó†‹  c™Ù>Å® µ0À_/□s  _`·Æjª9°¢_Ål□_0
Úÿ¯MÖ§¡l#]Vƒ/ÊßY
```

I have absolutely no idea what this is but I'm sure it means something to Encase.

You can then get rid of the hke file and just retain the .hsh and .hash.