

Registry hive basics part 5: Lists

Recap

This is most likely the last of the Registry hive basics post. If you missed any of the previous ones, here they are:

- [Overview](http://binaryforay.blogspot.com/2015/01/registry-hive-basics.html) [http://binaryforay.blogspot.com/2015/01/registry-hive-basics.html]
- [NK records](http://binaryforay.blogspot.com/2015/01/registry-hive-basics-part-2-nk-records.html) [http://binaryforay.blogspot.com/2015/01/registry-hive-basics-part-2-nk-records.html]
- [VK records](http://binaryforay.blogspot.com/2015/01/registry-hive-basics-part-3-vk-records.html) [http://binaryforay.blogspot.com/2015/01/registry-hive-basics-part-3-vk-records.html]
- [SK records](http://binaryforay.blogspot.com/2015/02/registry-hive-basics-part-4-sk-records.html) [http://binaryforay.blogspot.com/2015/02/registry-hive-basics-part-4-sk-records.html]

It is recommended to read through those posts in order before reading this one.

Before getting into the various list structures, lets take a step back to look at the overall structure of the Registry.

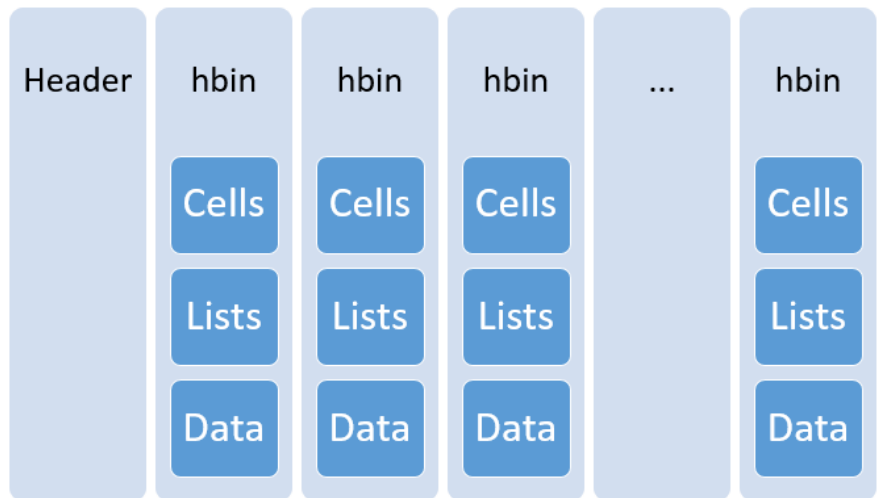
A hive is made up of a header followed by multiple hbin records. Inside each hbin record are cell records, list records, and data records.

Cell records would include NK, VK, and SK records.

List records would be things like li, ri, and db records (more on this later).

Data records are used to store things like a value's data.

This structure can be summarized as follows.



[http://4.bp.blogspot.com/-5gRR6fTZfA/VdTbM-pf1bl/AAAAAAAAA0s/Hgw1OHCb2_U/s1600/overview.png]

While the hbin records shown above look to be the same size, there is no requirement that they be the same. hbin records only have to be a multiple of 4096 bytes.

It helps to think of the hbins as containers for various record types. ***There is NO relationship between records based on their positions inside hbin records.*** The glue that holds the Registry together are the different types of list records which this post will cover in detail.

The general rules for parsing a hive can be summarized as follows:

1. Open file
2. Read header
 1. Get RootCellOffset
 2. Get length
3. Locate hbin
 1. Determine length of hbin
4. Find records in hbin
 1. Cells
 2. Lists
 3. Data
5. "Do stuff" with records
6. GOTO 3 until Length (Step 2.2) is reached
7. Close file

The starting point would be the NK record at RootCellOffset (Step 2.1). See [here](http://binaryforay.blogspot.com/2015/01/registry-hive-basics.html) [http://binaryforay.blogspot.com/2015/01/registry-hive-basics.html] for details on how to find the RootCellOffset. From here you can start walking the tree of keys and their related values and security records.

Lets take a look at a root cell as a frame of reference we can use for the

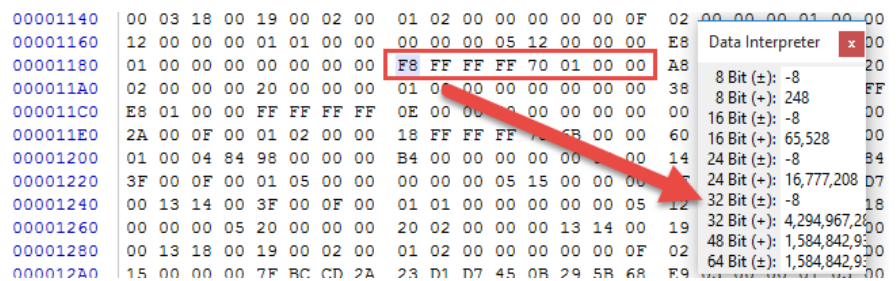
Technical details for 'S-1-5-21-718126207-1171771683-1750804747-1001_Classes'

NK record	Values	Subkeys	SK record	Full details as text	Hive details																																																																																																																																																																																																																																																									
General information																																																																																																																																																																																																																																																														
Size (Offset 0x00)		0x88 (136)																																																																																																																																																																																																																																																												
Relative offset		0x20 (32)																																																																																																																																																																																																																																																												
Absolute offset		0x1020 (4128)																																																																																																																																																																																																																																																												
Signature (Offset 0x04)		nk																																																																																																																																																																																																																																																												
Last write timestamp (Offset 0x08)		8/1/2013 7:21:56 PM +00:00																																																																																																																																																																																																																																																												
Is free		<input type="checkbox"/>																																																																																																																																																																																																																																																												
Flags (Offset 0x06)		0x0000002C																																																																																																																																																																																																																																																												
Flags present		HiveEntryRootKey, NoDelete, CompressedName																																																																																																																																																																																																																																																												
Name information																																																																																																																																																																																																																																																														
Name (Offset 0x50)		S-1-5-21-718126207-1171771683-1750804747-100...																																																																																																																																																																																																																																																												
Name length (Offset 0x4C)		0x35 (53)																																																																																																																																																																																																																																																												
Maximum name length (Offset 0x38)		0x5E (94)																																																																																																																																																																																																																																																												
Parent cell information																																																																																																																																																																																																																																																														
Parent cell index (Offset 0x14)		None (This is the root node)																																																																																																																																																																																																																																																												
Value information																																																																																																																																																																																																																																																														
Value count (Offset 0x28)		0x1 (1)																																																																																																																																																																																																																																																												
Value list cell index (Offset 0x2C)		0x188 (392)																																																																																																																																																																																																																																																												
Maximum value name length (Offset 0x40)		0x0 (0)																																																																																																																																																																																																																																																												
Maximum value data length (Offset 0x44)		0x2 (2)																																																																																																																																																																																																																																																												
Subkey information																																																																																																																																																																																																																																																														
Subkey count stable (Offset 0x18)		0x100 (256)																																																																																																																																																																																																																																																												
Subkey list stable cell index (Offset 0x20)		0x4B7020 (4943904)																																																																																																																																																																																																																																																												
Subkey count volatile (Offset 0x1C)		0x0 (0)																																																																																																																																																																																																																																																												
Subkey list volatile cell index (Offset 0x24)		0x0 (0)																																																																																																																																																																																																																																																												
Class information																																																																																																																																																																																																																																																														
Class length (Offset 0x4E)		0x0 (0)																																																																																																																																																																																																																																																												
Maximum class length (Offset 0x3C)		0x0 (0)																																																																																																																																																																																																																																																												
Class cell index (Offset 0x34)		0x0 (0)																																																																																																																																																																																																																																																												
Security key information																																																																																																																																																																																																																																																														
Security cell index (Offset 0x30)		0xA8 (168)																																																																																																																																																																																																																																																												
Other information																																																																																																																																																																																																																																																														
Debug (Offset 0x3B)		0x0 (0)																																																																																																																																																																																																																																																												
Virtual control flags (Offset 0x3A)		0x0 (0)																																																																																																																																																																																																																																																												
WorkVar (Offset 0x4B)		0x0 (0)																																																																																																																																																																																																																																																												
User flags (Offset 0x3A)		0x0 (0)																																																																																																																																																																																																																																																												
Padding (optional)		00-00-00																																																																																																																																																																																																																																																												
All indexes are relative. Add 0x1000 to find the same data in a hex editor																																																																																																																																																																																																																																																														
Double click 'Parent cell index' to load technical details for this key's parent																																																																																																																																																																																																																																																														
<table border="1"> <thead> <tr> <th></th> <th>00</th><th>01</th><th>02</th><th>03</th> <th>04</th><th>05</th><th>06</th><th>07</th> <th>08</th><th>09</th><th>0A</th><th>0B</th> <th>0C</th><th>0D</th><th>0E</th><th>0F</th> <th>10</th><th>11</th><th>12</th><th>13</th> </tr> </thead> <tbody> <tr> <td>00000000</td> <td>78</td><td>FF</td><td>FF</td><td>FF</td> <td>6E</td><td>6B</td><td>2C</td><td>00</td> <td>3A</td><td>B4</td><td>F9</td><td>62</td> <td>EC</td><td>8E</td><td>CE</td><td>01</td> <td>02</td><td>00</td><td>00</td><td>00</td> </tr> <tr> <td>00000014</td> <td>08</td><td>08</td><td>00</td><td>00</td> <td>00</td><td>01</td><td>00</td><td>00</td> <td>00</td><td>00</td><td>00</td><td>00</td> <td>20</td><td>70</td><td>48</td><td>00</td> <td>FF</td><td>FF</td><td>FF</td><td>FF</td> </tr> <tr> <td>00000028</td> <td>01</td><td>00</td><td>00</td><td>00</td> <td>88</td><td>01</td><td>00</td><td>00</td> <td>A8</td><td>00</td><td>00</td><td>00</td> <td>FF</td><td>FF</td><td>FF</td><td>FF</td> <td>5E</td><td>00</td><td>00</td><td>00</td> </tr> <tr> <td>0000003C</td> <td>00</td><td>00</td><td>00</td><td>00</td> <td>00</td><td>00</td><td>00</td><td>00</td> <td>00</td><td>00</td><td>00</td><td>00</td> <td>00</td><td>00</td><td>00</td><td>00</td> <td>35</td><td>00</td><td>00</td><td>00</td> </tr> <tr> <td>00000050</td> <td>53</td><td>2D</td><td>31</td><td>2D</td> <td>35</td><td>2D</td><td>32</td><td>31</td> <td>2D</td><td>37</td><td>31</td><td>38</td> <td>31</td><td>32</td><td>36</td><td>32</td> <td>30</td><td>37</td><td>2D</td><td>31</td> </tr> <tr> <td>00000064</td> <td>31</td><td>37</td><td>31</td><td>37</td> <td>37</td><td>31</td><td>36</td><td>38</td> <td>33</td><td>2D</td><td>31</td><td>37</td> <td>35</td><td>30</td><td>38</td><td>30</td> <td>34</td><td>37</td><td>34</td><td>37</td> </tr> <tr> <td>00000078</td> <td>2D</td><td>31</td><td>30</td><td>30</td> <td>31</td><td>5F</td><td>43</td><td>6C</td> <td>61</td><td>73</td><td>73</td><td>65</td> <td>73</td><td>00</td><td>00</td><td>00</td> <td></td><td></td><td></td><td></td> </tr> </tbody> </table> <table border="1"> <tbody> <tr> <td>x</td><td>y</td><td>y</td><td>y</td><td>h</td><td>k</td><td>.</td><td>.</td><td>'</td><td>ü</td><td>b</td><td>.</td><td>i</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td> </tr> <tr> <td>p</td><td>K</td><td>.</td><td>y</td><td>y</td><td>y</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td> </tr> <tr> <td>S</td><td>-</td><td>1</td><td>-</td><td>5</td><td>-</td><td>21</td><td>-</td><td>7181</td><td>26</td><td>20</td><td>7</td><td>-</td><td>1</td><td>7177</td><td>16</td><td>83</td><td>-</td><td>17</td><td>50</td> </tr> <tr> <td>-</td><td>1001</td><td>_</td><td>C</td><td>L</td><td>a</td><td>s</td><td>s</td><td>e</td><td>s</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td> </tr> </tbody> </table>							00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	00000000	78	FF	FF	FF	6E	6B	2C	00	3A	B4	F9	62	EC	8E	CE	01	02	00	00	00	00000014	08	08	00	00	00	01	00	00	00	00	00	00	20	70	48	00	FF	FF	FF	FF	00000028	01	00	00	00	88	01	00	00	A8	00	00	00	FF	FF	FF	FF	5E	00	00	00	0000003C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	35	00	00	00	00000050	53	2D	31	2D	35	2D	32	31	2D	37	31	38	31	32	36	32	30	37	2D	31	00000064	31	37	31	37	37	31	36	38	33	2D	31	37	35	30	38	30	34	37	34	37	00000078	2D	31	30	30	31	5F	43	6C	61	73	73	65	73	00	00	00					x	y	y	y	h	k	.	.	'	ü	b	.	i	p	K	.	y	y	y	S	-	1	-	5	-	21	-	7181	26	20	7	-	1	7177	16	83	-	17	50	-	1001	_	C	L	a	s	s	e	s
	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13																																																																																																																																																																																																																																										
00000000	78	FF	FF	FF	6E	6B	2C	00	3A	B4	F9	62	EC	8E	CE	01	02	00	00	00																																																																																																																																																																																																																																										
00000014	08	08	00	00	00	01	00	00	00	00	00	00	20	70	48	00	FF	FF	FF	FF																																																																																																																																																																																																																																										
00000028	01	00	00	00	88	01	00	00	A8	00	00	00	FF	FF	FF	FF	5E	00	00	00																																																																																																																																																																																																																																										
0000003C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	35	00	00	00																																																																																																																																																																																																																																										
00000050	53	2D	31	2D	35	2D	32	31	2D	37	31	38	31	32	36	32	30	37	2D	31																																																																																																																																																																																																																																										
00000064	31	37	31	37	37	31	36	38	33	2D	31	37	35	30	38	30	34	37	34	37																																																																																																																																																																																																																																										
00000078	2D	31	30	30	31	5F	43	6C	61	73	73	65	73	00	00	00																																																																																																																																																																																																																																														
x	y	y	y	h	k	.	.	'	ü	b	.	i																																																																																																																																																																																																																																										
p	K	.	y	y	y																																																																																																																																																																																																																																											
S	-	1	-	5	-	21	-	7181	26	20	7	-	1	7177	16	83	-	17	50																																																																																																																																																																																																																																											
-	1001	_	C	L	a	s	s	e	s																																																																																																																																																																																																																																											
Bytes selected: 0 Offset: NA ?																																																																																																																																																																																																																																																														

At the bottom of image we can see the raw hex that makes up the root cell.

The first list we encounter is the Value list cell index at offset 0x2C. In the above example, the value list cell index is 0x188, or 392 in decimal. This is the RELATIVE offset for where a list lives that contains the offsets to the values for this key. Since value count is equal to 1, we would need to go to offset 0x188 and read 1 offset. This offset will again be a relative offset to a VK record.

If we go to 0x1188, we see the following:



[http://1.bp.blogspot.com/-YlqOm015np4/VdTgxgRPigI/AAAAAAAAA1Q/T_VTTQ9AFcY/s1600/ListSize.png]

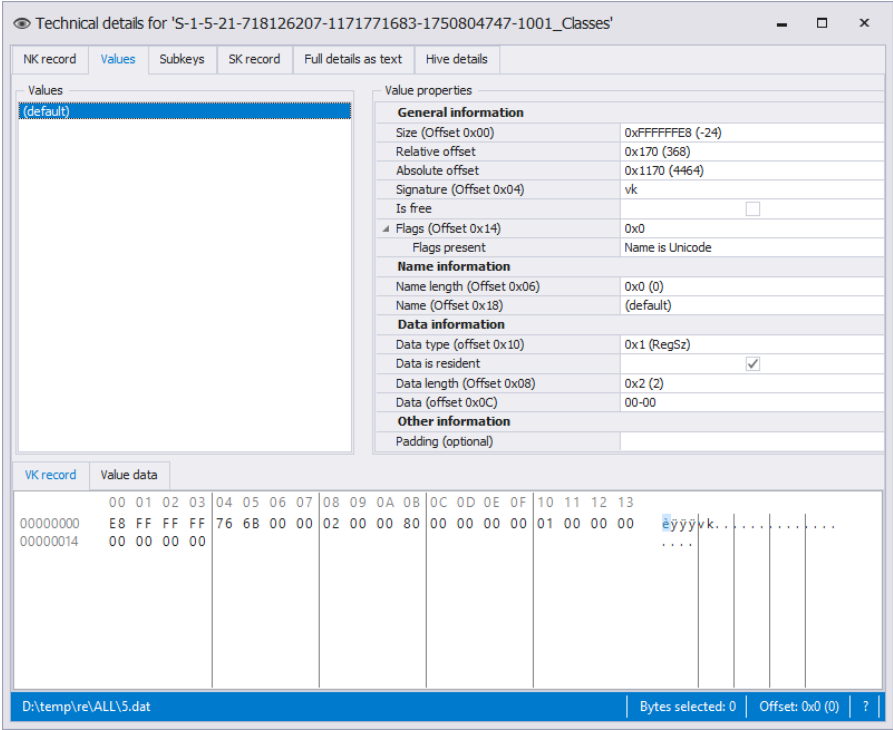
The first 4 bytes are the size. This is a signed 32 bit integer. We can see that the size of the list is -8 bytes long. As we have seen before in other places, the negative size simply means the list is in use. The bytes in the rectangle make up the list we are interested in.

Once we know the size, we can move forward to the start of the offsets. In this case we are left with a single, signed 32 bit integer, 0x0170, which is equivalent to 368 in decimal.

It is not always the case that the list pointing to values will contain the same number of offsets as the total number of values in an NK record. It may very well be there are more offsets or other "stuff" after our list of offsets to VK records. This extra data would be considered slack. In short, once you have the start of a list, you should read X number of 32 bit numbers where X is the number of values related to the NK cell you started from (1 in our case).

Now that we have the offset to where the VK record lives, we can now get the bytes that make up the VK record.

Below we can see what the value at relative offset 368 (0x170) looks like.



[<http://2.bp.blogspot.com/-B3PXpFbdC6U/VdTfzQPjHzI/AAAAAAAAA1E/ZpooC9VQVRA/s1600/rootval.png>]

In most cases, values will not use lists, but there are some cases where we will need to deal with lists when processing VK records (the big data case).

Getting to subkeys

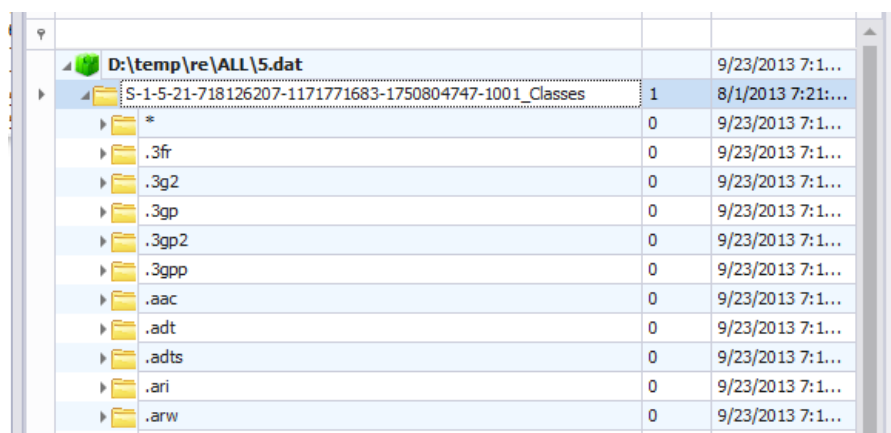
The next list we run into is the Subkey list stable cell index found at offset 0x20. In our example above, it lives at relative offset 0x4B7020 (4943904 in decimal).

If we add 0x1000 to 0x4B7020 and go to that offset, we see the following monster:

0x00000000	68 62 69 6E 00 70 4B 00	00 10 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	hbin.gif
0x00000001	28 76 FF FF 6C 66 00 01	90 01 00 2A 00 00 00 00	A8 04 00 00 2E 33 66 72	18 08 00 2E 33 67 32	00000000
0x00000002	98 05 00 00 2E 33 67 70	F0 05 00 00 2E 33 67 70	88 06 00 00 2E 33 67 70	00 06 00 00 2E 61 61 63	01 .3gp5 .3gp .3gp .aac
0x00000003	38 07 00 00 2E 61 64 74	F0 07 00 00 2E 61 64 74	48 08 00 00 2E 61 72 69	A0 08 00 00 2E 61 72 77	8 .adst5 .adstH .ari .arw
0x00000004	F8 08 00 00 2E 61 76 69	00 09 00 00 2E 62 61 79	38 0A 00 00 2E 62 6D 70	90 0A 00 00 2E 63 61 70	a .avria .bay8 .bmp .cap
0x00000005	E8 0A 00 00 2E 63 72 32	40 0B 00 00 2E 63 72 32	98 0B 00 00 2E 64 63 66	00 0B 00 00 2E 64 63 72	a .crt28 .crw" .dief .dot
0x00000006	C8 0C 00 00 2E 64 63 73	20 0D 00 00 2E 64 69 62	78 0D 00 00 2E 64 69 76	00 0D 00 00 2E 64 66 66	E .dca .dix .div6 .dmg
0x00000007	28 0E 00 00 2E 64 72 66	80 0E 00 00 2E 65 69 70	D8 0E 00 00 2E 65 72 66	30 0F 00 00 2E 66 66 66	(.dzt6 .eip0 .erf0 .fff
0x00000008	F0 0B 00 00 2E 67 69 64	48 0C 00 00 2E 68 64 70	88 0C 00 00 2E 68 74 6D	18 0C 00 00 2E 68 74 6D	0 .qstH .hdp" .hnh .hnc
0x00000009	C0 11 00 00 2E 69 69 71	18 12 00 00 2E 6A 66 69	70 12 00 00 2E 6A 70 65	C8 12 00 00 2E 6A 70 65	A .liq .frip .jpe5 .jpe
0x0000000A	80 13 00 00 2E 6A 70 67	38 14 00 00 2E 6A 78 72	90 14 00 00 2E 6B 32 35	E8 14 00 00 2E 6B 64 63	6 .jpg0 .jxr .k25a .kdc
0x0000000B	40 15 00 00 2E 6D 32 74	98 15 00 00 2E 6D 32 74	20 16 00 00 2E 6D 33 75	78 16 00 00 2E 6D 34 61	8 .m2t" .m2t .mbox .mfa
0x0000000C	00 17 00 00 2E 6D 34 76	E0 17 00 00 2E 6D 65 66	38 18 00 00 2E 6D 6D 76	00 18 00 00 2E 6D 6F 64	D .mva .mef5 .mxi" .mod
0x0000000D	E8 18 00 00 2E 6D 6F 73	40 19 00 00 2E 6D 6F 76	98 19 00 00 2E 6D 70 32	F0 19 00 00 2E 6D 70 33	a .mov8 .mov" .mp20 .mp3
0x0000000E	A8 1A 00 00 2E 6D 70 34	B8 1B 00 00 2E 6D 70 34	10 1C 00 00 2E 6D 70 61	68 1C 00 00 2E 6D 70 65	8 .mp4 .mp4 .mpah .mpe
0x0000000F	C0 1C 00 00 2E 6D 70 65	18 1D 00 00 2E 6D 70 67	70 1D 00 00 2E 6D 70 67	C8 1D 00 00 2E 6D 70 67	A .mpe .mpsp .mpo2 .mpv
0x00000010	20 1E 00 00 2E 6D 72 66	78 1E 00 00 2E 6D 72 77	D0 1E 00 00 2E 6D 74 73	F0 15 00 00 2E 6E 65 66	6 .mtx .mrub .mta5 .netf
0x00000011	48 16 00 00 2E 6E 72 67	A0 16 00 00 2E 6F 63 73	08 23 00 00 2E 6F 64 66	60 23 00 00 2E 6F 72 61	H .nzw .ocm # .cdf# .orf
0x00000012	B8 23 00 00 2E 6F 78 70	10 24 00 00 2E 70 64 66	98 23 00 00 2E 70 65 66	80 23 00 00 2E 70 6E 67	8 .omp # .pdfX .pdf" .png
0x00000013	78 24 00 00 2E 70 74 78	00 24 00 00 2E 70 78 65	28 27 00 00 2E 72 33 64	80 27 00 00 2E 72 61 66	A .psa .psa .psu" .rsc" .raf
0x00000014	D8 27 00 00 2E 72 61 77	30 28 00 00 2E 72 77 32	88 28 00 00 2E 72 77 6C	80 28 00 00 2E 72 77 7A	0" .raw0 .rw2" .rvia(.rwz
0x00000015	38 29 00 00 2E 73 68 74	00 29 00 00 2E 73 68 79	68 2A 00 00 2E 73 72 32	C0 2A 00 00 2E 73 72 66	8) .shd8) .skyt" .ar2a" .suf
0x00000016	18 2B 00 00 2E 73 72 77	70 2B 00 00 2E 74 68 6D	C8 2B 00 00 2E 74 69 66	20 2C 00 00 2E 74 69 66	* .swpa .tmb5 .tif .tif
0x00000017	78 2C 00 00 2E 74 6F 64	00 2C 00 00 2E 74 73 00	28 2D 00 00 2E 74 74 73	80 2D 00 00 2E 77 61 76	X" .todb .ts (- .tst5" .wav
0x00000018	D8 2D 00 00 2E 77 64 70	30 2E 00 00 2E 77 65 62	20 2E 00 00 2E 77 6D 00	78 2E 00 00 2E 77 6D 61	0- .vdp0 .web .vm x .wma
0x00000019	00 20 00 00 2E 77 6D 76	00 21 00 00 2E 77 70 6C	38 22 00 00 2E 78 33 66	90 22 00 00 2E 78 68 74	B .wmva .wpl8" .xif" .xht
0x0000001A	E8 2E 00 00 2E 78 68 74	80 2F 00 00 2E 78 6D 70	80 34 00 00 2E 78 70 73	D8 34 00 00 2E 78 76 69	A .xex/ .xmp4 .xmp5 .xvi
0x0000001B	00 35 00 00 2E 7A 70 6C	88 35 00 00 61 63 63 75	28 36 00 00 61 63 74 69	00 36 00 00 61 6C 6C 66	05 .xpl5 .accu(ActiB" AllF
0x0000001C	70 8E 0A 00 41 70 70 58	80 8D 0A 00 41 70 70 6C	60 8E 49 00 41 70 70 55	80 8A 49 00 41 70 70 58	8 .App" AppliH ApplU ApplU
0x0000001D	38 4C 49 00 41 70 70 55	A0 4E 49 00 41 70 70 55	E0 4A 47 00 41 70 70 58	8C 4C 41 00 41 70 70 58	00 ApplH ApplH ApplH ApplH
0x0000001E	E8 47 03 00 41 70 70 58	10 4E 13 00 41 70 70 58	60 8E 1F 00 41 70 70 58	38 3C 00 41 70 70 58	48 ApplX .ApplX" ApplX < ApplX
0x0000001F	A0 84 01 00 41 70 70 58	60 FF 13 00 41 70 70 58	68 7D 15 00 41 70 70 58	90 38 0E 00 41 70 70 58	# ApplX' ApplX) ApplX 8 ApplX
0x00000020	A8 7C 0E 00 41 70 70 58	38 7E 46 00 41 70 70 58	90 86 14 00 41 70 70 58	E7 15 00 41 70 70 58	1 ApplXf ApplXf ApplXf ApplXf
0x00000021	00 83 3A 09 41 70 70 58	C0 7B 09 41 70 70 58	E0 84 48 00 41 70 70 58	68 82 43 00 41 70 70 58	B8i ApplH ApplH ApplH ApplH
0x00000022	60 55 02 00 41 70 70 58	68 EB 38 00 41 70 70 58	F0 D1 15 00 41 70 70 58	A0 C0 15 00 41 70 70 58	'U ApplXh ApplXh ApplX 4 ApplX
0x00000023	18 A6 0C 00 41 70 70 58	E8 DA 46 00 41 70 70 58	48 17 03 00 41 70 70 58	88 0E 42 00 41 70 70 58	1 ApplXf ApplX ApplX B ApplX
0x00000024	20 56 4A 00 41 70 70 58	F8 42 14 00 41 70 70 58	A8 13 3B 00 41 70 70 58	90 64 05 00 41 70 70 58	'U ApplX ApplX" ApplX DE ApplX
0x00000025	50 87 3F 00 41 70 70 58	20 A5 44 00 41 70 70 58	00 2C 0B 00 41 70 70 58	18 B2 00 41 70 70 58	P4? ApplX WD ApplX .ApplX" ApplX
0x00000026	38 6A 24 00 41 70 70 58	20 B0 4A 00 41 70 70 58	A8 82 22 00 41 70 70 58	80 94 3C 00 41 70 70 58	818 ApplX "J ApplX" ApplXc ApplX
0x00000027	28 E2 14 00 41 70 70 58	A8 E8 00 00 41 70 70 58	10 17 3D 00 41 70 70 58	80 58 39 00 41 70 70 58	(4 ApplX" ApplX ApplX9 ApplX
0x00000028	C0 7B 38 00 41 70 70 58	D8 86 12 00 41 70 70 58	58 8D 3E 00 41 70 70 58	C8 45 14 00 41 70 70 58	Alf ApplX9 ApplX" > ApplXf ApplX
0x00000029	30 07 16 00 41 70 70 58	20 14 38 00 41 70 70 58	00 B0 15 00 41 70 70 58	D8 83 39 00 41 70 70 58	0 ApplX : ApplX : ApplX9 ApplX
0x0000002A	40 4C 4B 00 41 70 70 58	E0 E4 09 00 41 70 70 58	A8 9D 40 00 41 70 70 58	08 BE 0C 00 41 70 70 58	8LK ApplXa ApplX 8 ApplX 4 ApplX
0x0000002B	80 50 4B 00 61 75 64 69	A0 51 4B 00 61 75 64 69	90 52 4B 00 62 69 6E 67	68 53 4B 00 62 69 6E 67	*HE audt QF audt RF bingH8 bing
0x0000002C	48 54 4B 00 62 69 6E 67	38 55 4B 00 62 69 6E 67	00 56 4B 00 62 69 6E 67	C8 56 4B 00 62 69 6E 67	HTK bing80K bing VK bingH8V bing
0x0000002D	A0 57 4B 00 62 69 6E 67	78 58 4B 00 62 69 6E 67	50 59 4B 00 62 69 6E 67	68 D1 0A 00 63 61 6C 6C	WK bingX8K bingH8V bingH8 call
0x0000002E	E0 5A 0A 00 63 61 6C 6C	50 5E 0A 00 63 62 61 79	A8 E2 0A 00 65 62 61 79	A8 E2 0A 00 65 74 65	40 .CCTF9 Dire(2R eba9" Exce
0x0000002F	88 5A 4B 00 66 69 6C 6D	88 5E 0E 00 46 69 72 65	E0 82 0E 00 46 69 72 65	88 5B 4B 00 66 74 70 00	a2K rila" Fire4" Fire JK fsp
0x00000030	10 B6 0E 00 68 74 74 70	D8 89 0E 00 68 74 74 70	A0 8D 0E 00 49 6E 74 65	20 60 4B 00 68 69 6E 64	q http0" htp 4 Inte "K kind
0x00000031	D8 60 4B 00 6C 65 6E 6F	C0 61 4B 00 6C 65 6E 6F	D0 99 37 00 6C 6E 6B 66	00 BE 0E 00 4C 6F 63 61	0"K leno48 leno48" lnkf 4 Loos
0x00000032	F8 18 19 00 6D 61 69 6C	80 62 6B 00 6D 65 73 73	A0 63 4B 00 6D 65 73 73	80 64 4B 00 6D 65 73 73	a .mail"t mesa cff mesa80F mesa
0x00000033	68 65 4B 00 6D 65 73 73	20 64 49 00 6D 65 73 73	08 61 49 00 6D 69 63 72	E8 61 49 00 6D 69 63 72	hK mesa " mesa al micr4 micr
0x00000034	80 19 19 00 6D 69 6E 67	C8 62 49 00 6D 73 2D 6D	90 63 49 00 6D 73 63 68	58 64 49 00 6F 63 73 6D	* HIME8i m-a-a c1 mach8d1 ocam
0x00000035	68 7B 4B 00 6F 6E 65 6E	20 7C 4B 00 70 72 6F 66	10 7E 4B 00 70 72 6F 66	00 7E 4B 00 70 72 6F 66	hK mesa (K prof JK prof JK prof
0x00000036	F0 7E 4B 00 70 72 6F 66	50 66 4B 00 70 72 6F 66	10 67 4B 00 70 72 6F 66	00 68 4B 00 70 72 6F 66	A-K prof8F prof8F prof HK prof
0x00000037	E8 68 4B 00 70 72 6F 66	D8 69 4B 00 70 72 6F 66	C0 6A 4B 00 70 72 6F 66	F0 28 19 00 53 68 79 44	88K prof8K prof8K prof8K (SkyD
0x00000038	40 2A 19 00 53 68 79 44	A8 6B 4B 00 53 68 79 44	08 6E 4B 00 53 68 79 44	00 2C 19 00 53 68 79 44	8" SkyD k8 SkyD n8 SkyD .skyp
0x00000039	88 6F 4B 00 53 68 79 44	18 6B 4B 00 53 68 79 44	58 6F 19 00 53 6F 64 74	D8 83 4B 00 53 79 6E 63	"0K SkyD k8 m-a F- SkyD8 Sync
0x0000003A	58 86 4B 00 53 79 6E 63	F0 87 4B 00 54 79 70 65	B0 88 4B 00 76 69 64 65	80 8A 47 00 77 69 6E 64	XVX Sync8K tel X1 Type"K wide
0x0000003B	A0 89 4B 00 76 69 64 65	B0 31 19 00 56 69 72 74	90 8A 4B 00 77 61 6C 6C	38 8A 47 00 77 69 6E 64	8K wide"1 Varr 8K val1888 wind
0x0000003C	00 9D 00 00 77 69 6E 64	D0 21 38 00 77 69 6E 64	00 21 38 00 77 69 6E 64	00 21 38 00 77 69 6E 64	P K wind8K wind8K wind8K wind
0x0000003D	00 9C 4B 00 77 69 6E 64	C8 8D 4B 00 77 69 6E 64	38 3A 19 00 77 69 6E 64	F0 8E 4B 00 77 69 6E 64	8K wind8K wind8K wind8K wind
0x0000003E	48 9D 4B 00 77 69 6E 64	78 91 4B 00 77 69 6E 64	A8 92 4B 00 77 69 6E 64	D8 93 4B 00 77 69 6E 64	H K wind8K wind"K wind8K wind
0x0000003F	00 95 4B 00 77 69 6E 64	30 96 4B 00 77 69 6E 64	60 97 4B 00 77 69 6E 64	50 98 4B 00 77 69 6E 64	"K wind8K wind"K wind8K wloa
0x00000040	00 98 4B 00 77 69 6E 64	38 9B 4B 00 77 69 6E 64	60 9B 4B 00 77 69 6E 64	80 9C 4B 00 77 69 6E 64	w8 wind8K wloa8K wloa8K wloa
0x00000041	00 99 4B 00 77 69 6E 64	38 9B 4B 00 77 69 6E 64	60 9B 4B 00 77 69 6E 64	80 9C 4B 00 77 69 6E 64	"K zini .K zini .K zini
0x00000042	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000043	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000044	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000045	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000046	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000047	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000048	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000049	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004A	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004B	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004C	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004D	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004E	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x0000004F	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000051	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000052	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0x00000053	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00		

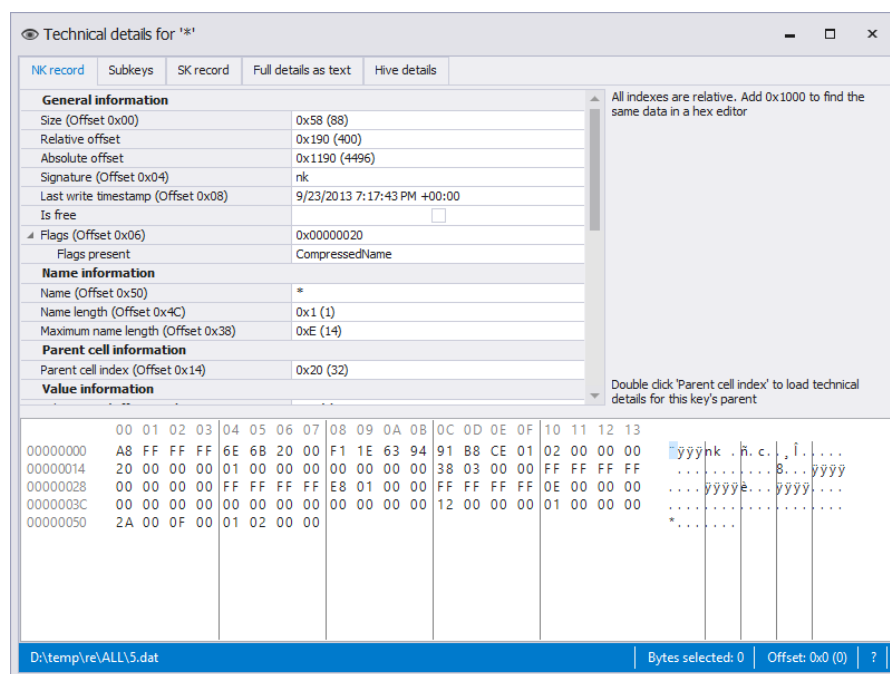
Now that we have a few offsets to some subkeys, we can look at them.

The hive we are working with, when loaded into Registry Explorer, looks like this:



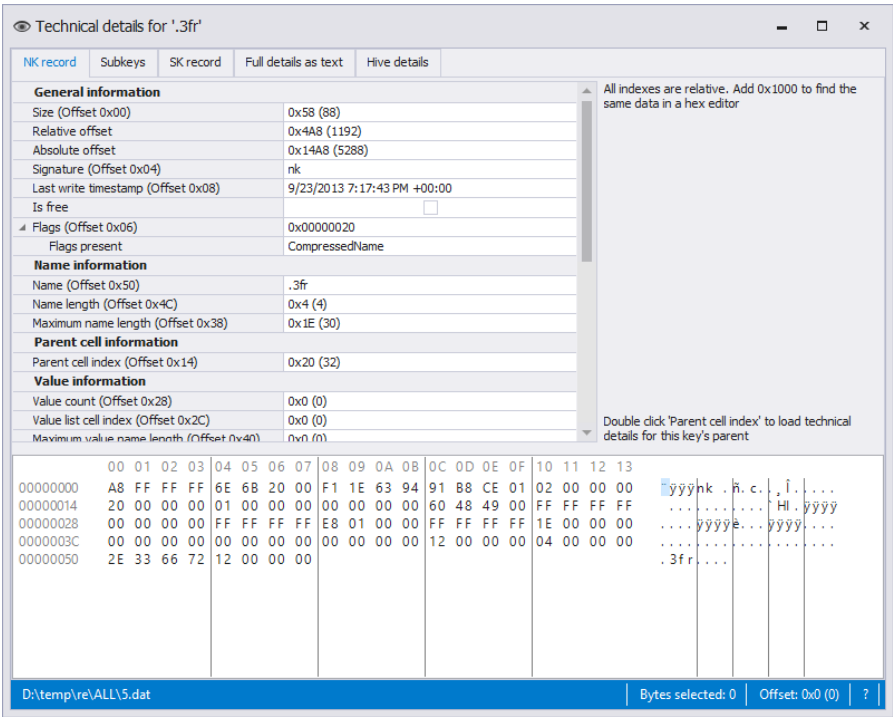
[\[http://2.bp.blogspot.com/-C3ZscPVLKs4/VdToXkv-uul/AAAAAAAAA10/jbuD4ISc6Ws/s1600/Review.png\]](http://2.bp.blogspot.com/-C3ZscPVLKs4/VdToXkv-uul/AAAAAAAAA10/jbuD4ISc6Ws/s1600/Review.png)

Now lets look at the NK record that is found at relative offset 0x0190 (400 decimal):



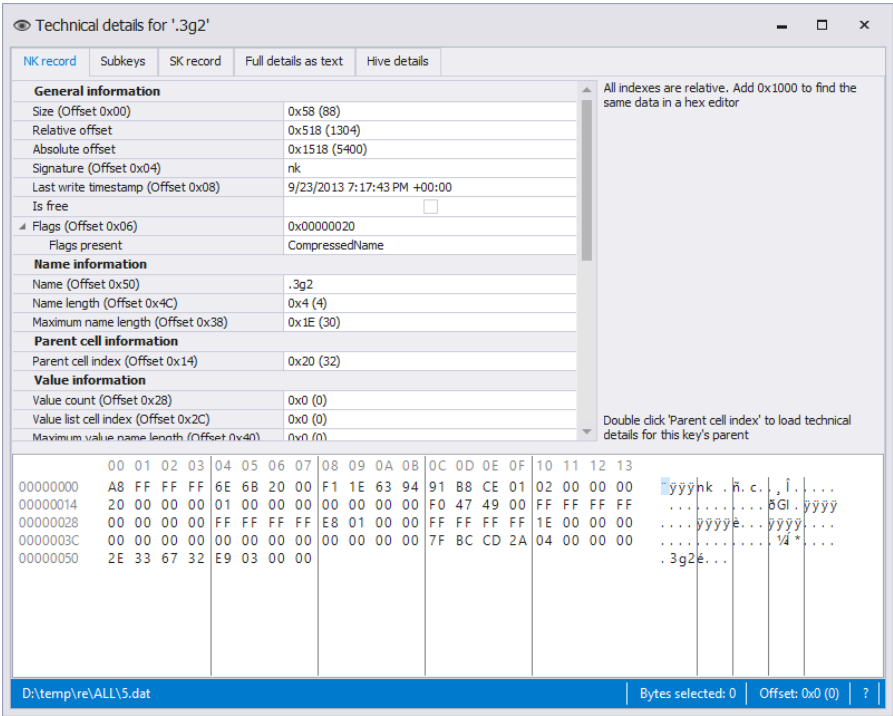
[\[http://4.bp.blogspot.com/-H7swrZ1wfmA/VdTokX1KtKI/AAAAAAAAA18/AsO3f7Y7LG4/s1600/firstsub.png\]](http://4.bp.blogspot.com/-H7swrZ1wfmA/VdTokX1KtKI/AAAAAAAAA18/AsO3f7Y7LG4/s1600/firstsub.png)

Next, the NK record at relative offset 0x04A8 (1192 decimal):



[http://3.bp.blogspot.com/-46cHAKocO04/VdTqJSRTVI/AAAAAAAAA2M/Yot7seL_D9k/s1600/os2.png]

And finally, the NK record at relative offset 0x0518 (1304 decimal):



[<http://3.bp.blogspot.com/-TgZ1jrHzaVM/VdTW8zngOI/AAAAAAAAA2U/PiRUArMyMB0/s1600/os3.png>]

This of course would be repeated a total of 256 times to get access to all the subkeys.

Lists

The previous section explained how lists are generally used in the Registry. As we discuss the different kinds of lists below we will not explain things again where the same pattern is used. In other words, If and lh lists work as we saw above (go to offset, read more offsets, go to those offsets, etc), so we won't unpack that again in the If and lh section.

There are 5 types of lists in Registry hives. The signatures for these lists are:

- If
- lh
- li
- ri
- db

If and lh lists

If and lh lists are very similar in structure. The basic structure looks like this:

- Offset 0x00: Size (4 bytes)
- Offset 0x04: Signature: (2 bytes)
- Offset 0x06: Number of entries (2 bytes)
- Offset 0x08: Offset record
 - Relative offset (4 bytes)
 - Hash (4 bytes)
- ...

where ... is a continuation of the offset structure, typically "Number of entries" long

The difference between the If and lh lists is the format of the Hash.

In If lists, the hash is the first 4 characters of the key name.

In lh lists, the hash is numerical and is simply an unsigned 32 bit integer.

The numerical hash basically works as follows:

1. First set hash value to zero
2. Then, working from left to right through the letters of the SubKey name, for each one, multiply Hash by 37 and then add the ASCII value of that letter

There are a few caveats tho. For full information on how this works, see section 4.29 [here](http://amnesia.gtisc.gatech.edu/~moyix/suzibandit.ltd.uk/MSc/Registry%20Structure%20-%20Main%20V4.pdf) [http://amnesia.gtisc.gatech.edu/~moyix/suzibandit.ltd.uk/MSc/Registry%20Structure%20-%20Main%20V4.pdf] .

That's pretty much it for this kind of list, but here is what an lh list looks

[illegible]

li and ri lists

- Offset 0x00: Size (4 bytes)
- Offset 0x04: Signature: (2 bytes)
- Offset 0x06: Number of entries (2 bytes)
- Offset 0x08: Offset record
 - Relative offset (4 bytes)
- ...

Here is an example of an li list.

00100100	65	62	64	60	66	61	63	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
----------	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Here is an example of an ri list.

```

00000000: 2E 00 64 00 65 00 76 00 69 00 63 00 65 00 64 00  dev 3430 .deviced
00000010: F0 FF FF FF 72 69 02 00 20 70 71 00 20 F0 72 00  esc % 0x726910f0
00000020: 02 00 00 00 08 49 6B 00 00 00 00 00 00 00 00 00  00000008496B0000

```

[\[http://2.bp.blogspot.com/-awvRmV_VLNQ/VdTx6XxCpDI/AAAAAAAAA24/EsvHHD_KDMs/s1600/ri.png\]](http://2.bp.blogspot.com/-awvRmV_VLNQ/VdTx6XxCpDI/AAAAAAAAA24/EsvHHD_KDMs/s1600/ri.png)

For the ri list, the size is -16 bytes. At offset 0x04 is the signature. At offset 0x06 is the number of entries, 2.

Starting at offset 0x8, we see the 2 offsets:

0x717020

0x72F020

ri lists are different in that their offsets do not directly point to NK records, but rather, ri lists point to other lists!

Recall from earlier that Registry hives have a version.

li records are only found in version 1.3 hives. For v1.3 hives, ri lists point to li lists. In v1.5 hives, ri lists always point to lh records.

If we take relative offset 0x717020 from above and look at what it points to, we see this:

```

00718020 80 D0 FF FF 6C 68 FA 01 60 49 6B 00 C6 D7 F1 25 B0 4A 6B 00 1F DD F1 25 00 4C 6B 00 20 DD F1 25 00 4C 6B 00 20 DD F1 25 00 4C 6B 00 20 DD F1 25 00 4C 6B 00 20 DD F1 25
00718040 50 4D 6B 00 21 DD F1 25 A0 4E 6B 00 23 DD F1 25 C8 8F 6B 00 BC 9D CD 11 18 91 6B 00 BD 9D CD 11 18 91 6B 00 BD 9D CD 11 18 91 6B 00 BD 9D CD 11 18 91 6B 00 BD 9D CD 11
00718060 78 92 6B 00 BE 9D CD 11 D8 93 6B 00 BF 9D CD 11 38 95 6B 00 C0 9D CD 11 98 96 6B 00 4F A9 70 B5 80 98 6B 00 A4 13 F7 3D 78 99 6B 00 A5 13 F7 3D F0 9A 6B 00 80 D9 F7 3D 68 9C 6B 00 5D 9F F8 3D 68 9C 6B 00 5D 9F F8 3D
00718080 E0 9D 6B 00 7E 3A 04 3E 58 9F 6B 00 81 3A 04 3E F0 50 6B 00 85 3A 04 3E 68 52 6B 00 F0 A7 04 3E 68 52 6B 00 F0 A7 04 3E 68 52 6B 00 F0 A7 04 3E 68 52 6B 00 F0 A7 04 3E
007180C0 E0 53 6B 00 F8 A7 04 3E 58 55 6B 00 F9 A7 04 3E D0 56 6B 00 0D A8 04 3E 48 58 6B 00 84 A8 04 3E 48 58 6B 00 84 A8 04 3E 48 58 6B 00 84 A8 04 3E 48 58 6B 00 84 A8 04 3E
007180E0 C0 59 6B 00 DB 8D 1E 6B 50 5B 6B 00 DF 8D 1E 6B E0 5C 6B 00 8F A8 04 3E 58 5E 6B 00 42 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD
00718100 C8 5F 6B 00 43 15 13 DD 38 61 6B 00 48 15 13 DD A8 62 6B 00 6A 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD
00718120 90 65 6B 00 7A 15 13 DD 00 67 6B 00 46 25 14 DD 70 68 6B 00 CE 61 BB 03 E8 69 6B 00 CF 61 BB 03 E8 69 6B 00 CF 61 BB 03 E8 69 6B 00 CF 61 BB 03 E8 69 6B 00 CF 61 BB 03
00718140 60 6B 6B 00 23 67 BB 03 D8 6C 6B 00 24 67 BB 03 50 6E 6B 00 25 67 BB 03 20 A0 6B 00 26 67 BB 03 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD
00718160 60 A1 6B 00 35 95 6B 12 D8 A2 6B 00 74 27 1E 95 48 A4 6B 00 BE 27 1E 95 B8 A5 6B 00 BF 27 1E 95 B8 A5 6B 00 BF 27 1E 95 B8 A5 6B 00 BF 27 1E 95 B8 A5 6B 00 BF 27 1E 95
00718180 28 A7 6B 00 C1 27 1E 95 98 A8 6B 00 C2 27 1E 95 08 AA 6B 00 C3 27 1E 95 78 AB 6B 00 13 57 1F CF 68 AC 6B 00 2E 57 1F CF 60 B1 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0
007181A0 E8 AC 6B 00 2E 57 1F CF 58 AE 6B 00 4E 57 1F CF 20 B0 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0 60 B1 6B 00 60 2F FC E0
007181C0 D0 B2 6B 00 47 A2 D8 73 40 B4 6B 00 68 A2 D8 73 B0 B5 6B 00 69 A2 D8 73 20 B7 6B 00 6A A2 D8 73 20 B7 6B 00 6A A2 D8 73 20 B7 6B 00 6A A2 D8 73 20 B7 6B 00 6A A2 D8 73
007181E0 90 B6 6B 00 A0 B2 D8 73 00 BA 6B 00 B2 55 DD 73 70 BB 6B 00 C8 55 DD 73 E0 BC 6B 00 37 56 DD 73 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD 18 64 6B 00 6B 15 13 DD
00718200 50 BE 6B 00 5A 56 DD 73 20 C0 6B 00 62 56 DD 73 50 C1 6B 00 8F 56 DD 73 C0 C2 6B 00 90 56 DD 73 C0 C2 6B 00 90 56 DD 73 C0 C2 6B 00 90 56 DD 73 C0 C2 6B 00 90 56 DD 73
00718220 30 C4 6B 00 16 6B DD 73 A0 C5 6B 00 75 E2 D9 AD 18 C7 6B 00 E3 AC B1 F6 A0 C8 6B 00 F9 CC B1 F6 A0 C8 6B 00 F9 CC B1 F6 A0 C8 6B 00 F9 CC B1 F6 A0 C8 6B 00 F9 CC B1 F6
00718240 28 CA 6B 00 DA DF C8 C6 B0 CB 6B 00 89 71 81 47 38 CD 6B 00 86 1D E2 AC B8 CE 6B 00 A4 9C AF E7 (E8 08E8*E8 kq GSIX t 4-,ik hu"q
00718260 80 D0 6B 00 85 AF C6 B7 F0 D1 6B 00 66 C2 DD 87 78 D3 6B 00 7A 89 91 52 E8 D4 6B 00 89 89 91 52 E8 D4 6B 00 89 89 91 52 E8 D4 6B 00 89 89 91 52 E8 D4 6B 00 89 89 91 52
00718280 58 D6 6B 00 57 03 66 59 E0 D7 6B 00 11 E6 93 C6 50 D9 6B 00 15 E6 93 C6 C0 DA 6B 00 16 E6 93 C6 X0X W f14vXk a"AF0K a"EA0K a"Z
007182A0 30 DC 6B 00 1E E6 93 C6 A0 DD 6B 00 77 F8 93 C6 10 DF 6B 00 C4 FC 93 C6 B0 E0 6B 00 92 06 94 C6 00K a"Z Yk w0"Z Bk Au"Zak ' "Z

```

[\[http://3.bp.blogspot.com/-sZJ5YLgOyVs/VdT0So_7sjl/AAAAAAAAA3M/f75ECr4xtYA/s1600/ripointer.png\]](http://3.bp.blogspot.com/-sZJ5YLgOyVs/VdT0So_7sjl/AAAAAAAAA3M/f75ECr4xtYA/s1600/ripointer.png)

Can you tell what version hive this particular list came from based on the kind of list 0x717020 points to?

Once you resolve the offsets in the ri list to the lists each ri offset points to, you can now process each list to get to the related NK records.

Are we having fun yet?

db list

The final list we will discuss is the db list, also known as the big data case. A db list is used in a VK record and is used when a VK record's value data is very large (greater than 16344 bytes). db lists are only found in hives with version greater than 1.3.

The db list structure is even simpler than the other lists we have seen.

- Offset 0x00: Size (4 bytes)
- Offset 0x04: Signature: (2 bytes)
- Offset 0x06: Number of offsets (2 bytes)
- Offset 0x08: Offset to offsets

Here is an example of a db list.

[\[http://2.bp.blogspot.com/-h4ErxmDjQwo/VdT6LYPdgcI/AAAAAAAAA3g/8allYFhyak/s1600/db.png\]](http://2.bp.blogspot.com/-h4ErxmDjQwo/VdT6LYPdgcI/AAAAAAAAA3g/8allYFhyak/s1600/db.png)

In this case, starting at offset 0x08, the relative offset to offsets is 0x078F30. If we add 0x1000 to this and look at it, we see this:

[\[http://2.bp.blogspot.com/-poZArP4A4SA/VdT7r71G-pl/AAAAAAAAA3s/1feY4-kQZIk/s1600/off2Off.png\]](http://2.bp.blogspot.com/-poZArP4A4SA/VdT7r71G-pl/AAAAAAAAA3s/1feY4-kQZIk/s1600/off2Off.png)

binary foray A blog about ...

search

make up the size

Registry Explorer plugin ...

XWFIM version 1.5 availa...

bstrings 0.9.8.0 released

bstrings 0.9.7.0 re... 2

Registry hive basics part ...

A few updates

AmcacheParser: Reduci...

bstrings 0.9.5.0 released

bstrings 0.9.0.0 released

Introducing bstrings, a B...

These offsets contain the data for a VK record.

With these offsets in hand, we can now read each in turn and concatenate the bytes found at each offset together to assemble our complete VK value data.


Each offset will point to a data record which is size (32 bit signed int) followed by the data we are interested in.

The beginning of the data (length is -16352) at relative offset 0x07B020 looks like this:

[\[http://3.bp.blogspot.com/-YBg64W0rz5M/VdT8tEUCRxI/AAAAAAAAA34/KfLkCv0MMKw/s1600/dboff1.png\]](http://3.bp.blogspot.com/-YBg64W0rz5M/VdT8tEUCRxI/AAAAAAAAA34/KfLkCv0MMKw/s1600/dboff1.png)


<http://binaryforay.blogspot.tw/2015/08/registry-hive-basics-part-5-lists.html>

12/15




ShellBags Explore... 6


The end of XWFRT?




Registry Explorer ... 1




ShellBags Explorer 0.5.4... 1




Introducing Regist... 6




Exploring the Registry at ... 1




ShellBags Explore... 1




XWFIM and XWFRT v1.0 ... 1




Registry hive basics part ... 1



Registry hive basi... 3

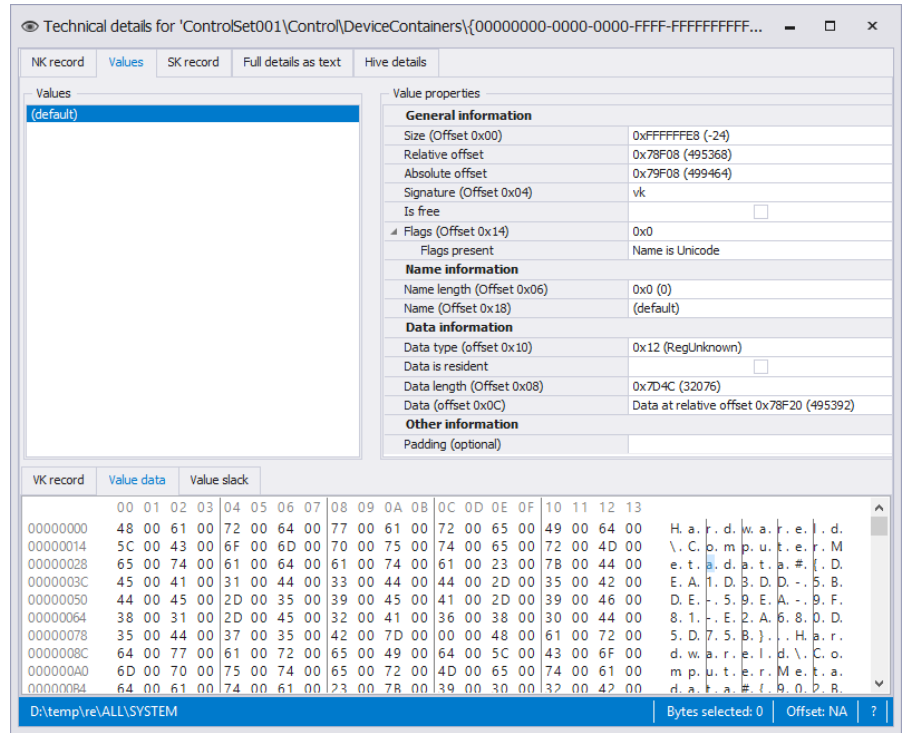
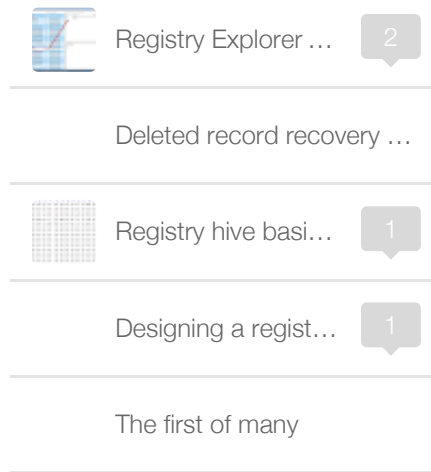


ShellBags Explorer 0.5.1... 1



Registry hive basi... 2

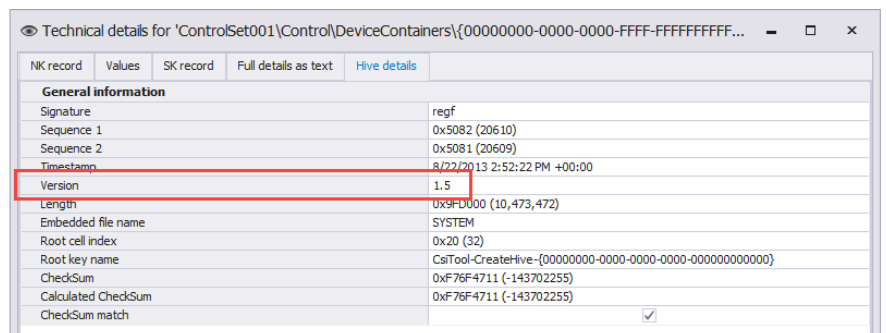
13/15



[\[http://4.bp.blogspot.com/-VeOOSAEDwU/VdXc7gT_QGI/AAAAAAAAA4c/nshO1PK0d_I/s1600/bigvk.png\]](http://4.bp.blogspot.com/-VeOOSAEDwU/VdXc7gT_QGI/AAAAAAAAA4c/nshO1PK0d_I/s1600/bigvk.png)

Note that both of our data records have size 16,352. If we take away the 4 bytes for the size, that leaves us 16,348. Since we have 2 of them, that makes 32,696 total bytes. Like every other VK record, we do not necessarily need all that data. Once the data is reassembled, you have to then honor the VK record's data length property (offset 0x08). In our example, the data length is 0x7D4C, or 32,076 in decimal, bytes. That leaves a difference of 620 bytes, which is a combination of value slack and padding.

Earlier we said that db records are only found in hives with version greater than 1.3. Looking at the hive properties where the above value is, we can see that the version number is 1.5.



[\[http://2.bp.blogspot.com/-2GRzICIHjsw/VdXdLN8DLI/AAAAAAAAA4k/M7I3f7_5gDo/s1600/vers.png\]](http://2.bp.blogspot.com/-2GRzICIHjsw/VdXdLN8DLI/AAAAAAAAA4k/M7I3f7_5gDo/s1600/vers.png)

That's about it for lists and the Registry basics series. I hope you found

it interesting. If there are any other topics you would like to see discussed, please hit me up in the usual places and let me know.

Posted 20th August by ERZ

Labels: [Registry](#), [Registry Explorer](#)



Add a comment

Enter your comment...

Comment as: ggyy (Google) ▾

Publish

Preview

☐ **Notify me**

Sign out