

# Windows NT Registry File (REGF) format specification

*Analysis of the NT Registry File format*

By Joachim Metz <joachim.metz@gmail.com>

## Summary

A Windows NT Registry File is used by Microsoft Windows NT (or later) to store a part of the Windows Registry. This specification is based on earlier work on the format and was complimented by reverse engineering.

This document is intended as a working document for the Windows NT Registry File (REGF) format specification. Which should allow existing Open Source forensic tooling to be able to process this file type.

## Document information

**Author(s):** Joachim Metz <joachim.metz@gmail.com>

**Abstract:** This document contains information about the Windows NT Registry File format.

**Classification:** Public

**Keywords:** Windows Registry File, REGF

## License

Copyright (c) 2009-2013 Joachim Metz <joachim.metz@gmail.com>. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

## Version

Version	Author	Date	Comments
0.0.1	J.B. Metz	July 2009	Initial version.
0.0.2	J.B. Metz	October 2009	Additional information.
0.0.3	J.B. Metz	January 2010	Small changes
0.0.4	J.B. Metz	June 2010	Additional information regarding data blocks.
0.0.5	J.B. Metz	October 2010	Small changes
0.0.6	J.B. Metz	March 2012	Added information about key and value names.
0.0.7	J.B. Metz	April 2012	Update regarding hash algorithm.
0.0.8	J.B. Metz	May 2012	Updates for Windows 8 Consumer Preview.
0.0.9	J.B. Metz	August 2012	Small changes.
0.0.10	J.B. Metz	September 2012	Small changes.
0.0.11	J.B. Metz	February 2013	Small changes.
0.0.12	J.B. Metz	April 2013	Additional information regarding value data.
0.0.13	J.B. Metz	April 2013	More information on corruption scenarios.

# Table of Contents

1. Overview.....	1
1.1. Test version.....	2
1.2. Overview.....	2
2. File header.....	3
2.1. Dirty vector.....	4
3. Hive bin.....	4
3.1. Hive bin header.....	4
3.2. Hive bin cell.....	5
4. Hive bin cell values.....	5
4.1. Named key.....	6
4.1.1. Flags.....	7
4.2. Security key.....	8
4.3. Sub key list.....	8
4.3.1. “lf” and “lh” sub key element.....	9
4.3.2. “li” sub key element.....	9
4.3.3. “ri” sub key element.....	9
4.4. Value key.....	9
4.4.1. Data types.....	10
4.4.2. Flags.....	11
4.5. Values list.....	11
4.6. Value data.....	12
4.6.1. Data block key.....	12
4.6.2. Data block segment list.....	12
4.6.3. Data block segment data.....	13
5. Hash algorithms.....	13
5.1. LH sub key hash algorithm.....	13
6. Corruption scenarios.....	13
6.1. Value data size exceeds hive bin cell value size.....	13
6.2. Value key size too small.....	13
6.3. Integer value data too large.....	13
6.4. String value data too small.....	14
6.5. String value data too large.....	14
7. Notes.....	15
7.1. Transaction log.....	15
Appendix A. References.....	17
Appendix B. GNU Free Documentation License.....	17

# 1. Overview

A Windows NT Registry File (REGF) is used by Microsoft Windows NT (or later) to store a part of the Windows Registry. These parts are referred to as hives. The Registry uses the following hives:

Hive name	Description
HKEY_CLASSES_ROOT	<b>TODO</b> Used by Windows NT 4 and later Refers to the class key in HKEY_LOCAL_MACHINE
HKEY_CURRENT_USER	Information regarding the current active user Used by Windows NT 4 and later Refers to the active user key in HKEY_USERS
HKEY_CURRENT_CONFIG	<b>TODO</b> Used by Windows NT 4 and later Refers to the active control set in HKEY_LOCAL_MACHINE\CONTROL\
HKEY_USERS	Information about all active users Used by Windows NT 4 and later
HKEY_LOCAL_MACHINE	Local settings Used by Windows NT 4 and later

There are REGF with different names for parts of the Registry, some are:

Filename	Windows	Description
default	NT4 and later	<b>TODO</b>
NTUSER.DAT	NT4 and later	User specific part of the registry Location: %UserProfile%\ Registry key: HKEY_CURRENT_USER
NTUSER.MAN	NT4 and later	Mandatory user specific part of the registry Location: %UserProfile%\
SAM	NT4 and later	Security Account Manager (SAM) part of the registry Location: %SystemRoot%\System32\Config\
SOFTWARE	NT4 and later	Software specific part of the registry Location: %SystemRoot%\System32\Config\ Registry key: HKEY_LOCAL_MACHINE\Software
SYSTEM	NT4 and later	System specific part of the registry Location: %SystemRoot%\System32\Config\ Registry key: HKEY_LOCAL_MACHINE\System
userdiff	NT4 and later	Location: %SystemRoot%\System32\Config\
UsrClass.dat	2000 and later	File associations and COM registry entries Location: %UserProfile%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
UsrClass.dat	Vista and later	File associations and COM registry entries %UserProfile%\Local Settings\Application

Filename	Windows	Description
		Data\Microsoft\Windows\Usrclass.dat

## 1.1. Test version

The following version of programs were used to test the information within this document:

- Windows NT 4
- Windows 2000
- Windows XP (SP2, SP3)
- Windows 2003
- Windows Vista
- Windows 2008
- Windows 7
- Windows 8

## 1.2. Overview

A REGF consist of the following distinguishable elements:

- file header
- hive bins
- trailing empty blocks

Characteristics	Description
Byte order	little-endian
Date and time values	Filetime in UTC
Character string	ASCII strings are stored in extended ASCII with a codepage. Unicode strings are stored in UTF-16 little-endian without the byte order mark (BOM).

According to [MSDN]:

- a key name has a limit of 255 characters
- a value name has a limit of 16383 characters (for Windows 2000 this is limit is 260 ASCII or 16383 Unicode characters)
- a Registry tree can be 512 levels deep

Both key and values names are case insensitive. The \ character is used as the key separator. Note that the \ character can be used in value names. The / character is used in both key and value names. Some examples of which are:

Key:	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\NetBT\Parameters\
Value:	Size/Small/Medium/Large

Key:	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal
Value:	\Device\Video0

Key:	
------	--

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\xmlprov\Parameters\SchemaGroups\User\http://www.microsoft.com/provisioning/eaptlsuserpropertiesv1\
Value: SchemaFile
```

Note it seems that duplicate key and value names are possible.

## 2. File header

The file header is stored in a 4096 byte header block. However transaction log files can have a header block of 1024 bytes.

The file header is 512 bytes of size and consists of:

offset	size	value	description
0	4	“regf”	The signature
4	4		Primary sequence number Matches the secondary sequence number if the hive was properly synchronized
8	4		Secondary sequence number Matches the primary sequence number if the hive was properly synchronized
12	8		Last modification date and time in UTC Filetime
20	4		Major version
24	4		Minor version
28	4		File type 0x0000 => normal 0x0001 => transaction log
32	4		Unknown (format) 0x0001
36	4		The root key offset Primary sequence number Matches the secondary sequence number if the hive was properly synchronized
40	4		Hive bins data size
44	4		Unknown 0x0001
48	64		Unknown Sometimes contains the last part of the filename in UTF-16 LE most of the time with an end-of-string character, but not always. Unused bytes are 0.
112	396		Unknown Can contain remnant data Padding used for the checksum?

offset	size	value	description
508	4		Checksum XOR-32 of the previous 508 bytes

```
file offset = ( hive bin number x hive block size ) + header block size
             = ( hive bin number x 4096 ) + 4096
             = ( hive bin number + 1 ) x 4096
```

Version (Major.Minor)	Description
1.3	used in NTUSER.DAT, SAM
1.5	used in .sav REGF, SYSTEM

Note: if sequence numbers don't match the hive has partial data, apply .LOG on top of PRIMARY

## 2.1. Dirty vector

For a transaction log the first block contains the dirty vector. The dirty vector is variable of size and consists of:

offset	size	value	description
512	4		In transaction log: the dirty vector signature "DIRT"
516	...		In transaction log: bitmap of dirty hive bin pages 1 => indicates a dirty hive bin page
...	....		Padding to 4096

## 3. Hive bin

The hive bin consists of:

- the hive bin header
- the hive bin cells

### 3.1. Hive bin header

The hive bin header is 32 bytes of size and consists of:

offset	size	value	description
0	4	"hbin"	The signature
4	4		The offset of the hive bin Value in bytes and relative from the start of the hive bin data
8	4		Size of the hive bin Value in bytes

offset	size	value	description
12	4		Reserved 0 most of the time, can contain remnant data
16	4		Reserved 0 most of the time, can contain remnant data
20	8		Timestamp 0 most of the time, can contain remnant data Only the root (first) hive bin seems to contain a valid filetime
28	4		Spare Value similar to the size Number of bytes

### 3.2. Hive bin cell

The hive bin cell is variable of size and consists of:

offset	size	value	description
0	4		Cell size The value contains the 4 bytes of the size itself. The value is negative if the cell is allocated or positive if the cell is unallocated. The size is 8 byte aligned
4	...		Cell data

If a hive bin cell becomes unallocated and is adjacent to another unallocated cell, they are merged by having the first cell's size extended.

## 4. Hive bin cell values

A hive bin cell values contain different types of data. Some of the types of data are identifier by a 2 byte signature value.

Value	Description
“lf” “lh” “li” “ri”	Sub keys list
“nk”	Named key
“sk”	Security key
“vk”	Value key
“db”	Data block key

## 4.1. Named key

The named key is variable of size and consists of:

offset	size	value	description
0	2	“nk”	Signature
2	2		Flags See section: 4.1.1 Flags
4	8		Last (key) written date and time Filetime
12	4		Unknown Empty value
16	4		Parent key offset The offset value is in bytes and relative from the start of the hive bin data
20	4		number of sub keys
24	4		number of volatile sub keys
28	4		Sub keys list offset The offset value is in bytes and relative from the start of the hive bin data Refers to a sub keys list or contains -1 (0xffffffff) if empty. See section: 4.3 Sub key list
32	4		Volatile sub keys list offset The offset value is in bytes and relative from the start of the hive bin data Refers to a sub keys list or contains -1 (0xffffffff) if empty. See section: 4.3 Sub key list
36	4		number of values
40	4		Values list offset The offset value is in bytes and relative from the start of the hive bin data Refers to a values list or -1 (0xffffffff) if empty. See section: 4.5 Values list
44	4		Security key offset The offset value is in bytes and relative from the start of the hive bin data Refers to a security key or -1 (0xffffffff) if empty. See section: 4.2 Security key
48	4		Class name offset The offset value is in bytes and relative from the start of the hive bin data

offset	size	value	description
			Refers to a class name or -1 (0xffffffff) if empty.
52	4		Largest sub key name size
56	4		Largest sub key class name size
60	4		Largest value name size
64	4		Largest value data size
68	4		Unknown Some run-time caching index or hash?
72	2		Key name size
74	2		Class name size
76	...		Key name string ASCII or Unicode string not terminated by an end-of-string character Maximum of 255 characters
...	...		Padding due to 8 byte alignment of cell size Sometimes contains remnant data

#### 4.1.1. Flags

Value	Identifier	Description
0x0001		Is volatile key
0x0002		Is mount point (of another registry hive)
0x0004		Is root key (of current registry hive)
0x0008		Cannot be deleted
0x0010		Is symbolic link key
0x0020		Name is an ASCII string Otherwise the name is an Unicode (UTF-16 little-endian) string
0x0040		Is predefined handle
0x0080		Unknown
0x1000		Unknown
0x4000		Unknown

#### TODO

Value	Meaning
REG_STANDARD_FORMAT	
1	

The key or hive is saved in standard format. The standard format is the only format supported by Windows 2000.

REG\_LATEST\_FORMAT  
2

The key or hive is saved in the latest format. The latest format is supported starting with Windows XP. After the key or hive is saved in this format, it cannot be loaded on an earlier system.

REG\_NO\_COMPRESSION  
4

The key or hive is saved with no compression. This option accommodates faster save operations.

## 4.2. Security key

The security key is variable of size and consists of:

offset	size	value	description
0	2	"sk"	Signature
2	2		Unknown
4	4		Previous security key offset The offset value is in bytes and relative from the start of the hive bin data
8	4		Next security key offset The offset value is in bytes and relative from the start of the hive bin data
12	4		Reference count
16	...		NT security descriptor

## 4.3. Sub key list

The sub key list is variable of size and consists of:

offset	size	value	description
0	2	"lf", "lh", "li", "ri"	Signature
2	2		Number of elements
4	...		Sub key list elements
			Padding due to 8 byte alignment of cell size Sometimes contains remnant data

### 4.3.1. “lf” and “lh” sub key element

For “lf” and “lh” sub key lists the sub key list element is 8 bytes of size and consists of:

offset	size	value	description
0	4		Named key offset The offset value is in bytes and relative from the start of the hive bin data <b>What about data offset 0 and 0xffffffff?</b>
4	4		Hash value A different hash function is used for different sub key list types

**LF => Leaf ?**

**LH => Hashed leaf ?**

### 4.3.2. “li” sub key element

For “li” sub key lists the sub key list element is 4 bytes of size and consists of:

offset	size	value	description
0	4		Named key offset The offset value is in bytes and relative from the start of the hive bin data. <b>What about data offset 0 and 0xffffffff?</b>

**LI => Leaf item ?**

### 4.3.3. “ri” sub key element

For “ri” sub key lists the sub key list element is 4 bytes of size and consists of:

offset	size	value	description
0	4		Sub key list offset The offset value is in bytes and relative from the start of the hive bin data <b>What about data offset 0 and 0xffffffff?</b>

**RI => Reference item ?**

## 4.4. Value key

The value key is variable of size and consists of:

offset	size	value	description
0	2	“vk”	Signature
2	2		Value name size If the value name size is 0 the value name is “(default)”

offset	size	value	description
4	4		Data size See note below
8	4		Data offset The offset value is in bytes and relative from the start of the hive bin data. <b>What about data offset 0 and 0xffffffff?</b>
12	4		Data type See section: 4.4.1 Data types
16	2		Flags See section: 4.4.2 Flags
18	2		<b>Unknown (padding)</b> <b>Can contain remnant data</b>
20	...		Value name ASCII or Unicode string not terminated by an end-of-string character Maximum of 260 ASCII characters or 16383 Unicode characters
...	...		Padding due to 8 byte alignment of cell size Sometimes contains remnant data

A data size of 0 represents that the value is not set (or NULL).

If the MSB 0x80000000 of the data size is set the data offset actually contains the data value.

- A data size of 4 uses all 4 bytes of the data offset
- A data size of 2 uses the last 2 bytes of the data offset (on a little-endian system)
- A data size of 1 uses the last byte (on a little-endian system)
- A data size of 0 represents that the value is not set (or NULL).

**The behavior on a big-endian system is unknown.**

#### 4.4.1. Data types

Value	Identifier	Description
0x00000000	REG_NONE	Undefined type
0x00000001	REG_SZ	String [MSDN] states that this is either in ASCII or Unicode with an end-of-string character Although the string seems to be always stored as UTF-16 little-endian and sometimes the end-of-string character is not included. Also see: 6 Corruption scenarios
0x00000002	REG_EXPAND_SZ	String that contains expandable (environment) variables like %PATH% Either in ASCII or Unicode with an end-of-string character
0x00000003	REG_BINARY	Binary data

Value	Identifier	Description
0x00000004	REG_DWORD REG_DWORD _LITTLE_ENDIAN	32-bit integer (double word) little-endian
0x00000005	REG_DWORD _BIG_ENDIAN	Integer 32-bit signed little-endian (double word)
0x00000006	REG_LINK	String that contains a symbolic link Either in ASCII or Unicode with an end-of-string character
0x00000007	REG_MULTI_SZ	Array of strings Either in ASCII or Unicode with an end-of-string character
0x00000008	REG_RESOURCE_LIST	Resource list
0x00000009	REG_FULL_RESOURCE_DESCRIPTOR	Full resource descriptor
0x0000000a	REG_RESOURCE_REQUIREMENTS_LIST	Resource requirements list
0x0000000b	REG_QWORD REG_QWORD _LITTLE_ENDIAN	Integer 64-bit signed little-endian (quad word)

#### 4.4.2. Flags

Value	Identifier	Description
0x0001		Name is an ASCII string Otherwise the name is an Unicode (UTF-16 little-endian) string

#### 4.5. Values list

The value list is variable of size and consists of:

offset	size	value	description
0	...		Value key list entries
...	...		Padding due to 8 byte alignment of cell size Sometimes contains remnant data

A value list entry is 4 bytes of size and consists of:

offset	size	value	description
0	4		Value key offset The offset value is in bytes and relative from the start of the hive bin data.

offset	size	value	description
			What about data offset 0 and 0xffffffff?

## 4.6. Value data

The value data is stored directly in a hive bin cell.

According to [MSDN] the value data has a maximum size of the available memory in the latest format (1.5) and 1 MiB in the standard format (1.3). In the latest format (1.5) values larger than 16344 bytes are stored in multiple segments. Data about these segments is stored in the data block key. These large values are also referred to as long values.

[MSDN] Long values (more than 2,048 bytes) should be stored as files with the file names stored in the registry. This helps the registry perform efficiently.

### 4.6.1. Data block key

The data block key is 12 bytes of size and consists of:

offset	size	value	description
0	2	“db”	Signature
2	2		number of segments
4	4		Data block (segment) list offset The offset value is in bytes and relative from the start of the hive bin data. What about data offset 0 and 0xffffffff?
8	4		Padding due to 8 byte alignment of cell size Sometimes contains remnant data

### 4.6.2. Data block segment list

The data block segment list is variable of size and consists of:

offset	size	value	description
0	...		Data block segment list entries
...	...		Padding due to 8 byte alignment of cell size Sometimes contains remnant data

A data block list entry is 4 bytes of size and consists of:

offset	size	value	description
0	4		Data block segment data offset The offset value is in bytes and relative from the start of the hive bin data. What about data offset 0 and 0xffffffff?

### 4.6.3. Data block segment data

The data block segment data is stored directly in a hive bin cell.

## 5. Hash algorithms

### 5.1. LH sub key hash algorithm

Note that the hash operations are modulus 32-bit and the string is traversed per character. E.g. for an UTF-16 little-endian string the character is 2 bytes of size.

```
uint32_t hash_value = 0

for( string_index = 0;
    string_index < string_length;
    string_index++ )
{
    hash_value *= 37;
    hash_value += uppercase( string[ string_index ] );
}
```

Note that uppercase must be able to handle Unicode.

It's unknown how extended UTF-16 (4-byte) characters are handled.

## 6. Corruption scenarios

### 6.1. Value data size exceeds hive bin cell value size

In this scenario the value data size exceeds the hive bin cell value size it currently is assumed that the cell value size is the one to be used. Seeing it operates on a lower level then the value data size.

Is the next hive bin cell value unallocated?

### 6.2. Value key size too small

In this scenario the values list references the offset of a value key of which the actual hive bin cell value size is too small to be the size of the value key. Also the data in the bin cell value does not match a value key. Was the hive bin cell value unallocated?

### 6.3. Integer value data too large

In this scenario the value is e.g. of type REG\_DWORD\_LITTLE\_ENDIAN and the value data consist of more than 4 bytes. It is assumed the same applies to REG\_DWORD\_BIG\_ENDIAN and REG\_QWORD\_LITTLE\_ENDIAN.

```
Value key data:
00000000: 76 6b 06 00 08 00 00 00 50 54 cf 01 04 00 00 00 vk..... PT.....
00000010: 01 00 6f 00 6c 50 61 72 61 6d 00 00 ..o.lPar am..

signature           : vk
value name size     : 6
data size           : 0x00000008 (8)
```

```

data offset          : 0x01cf5450
data type           : 4 (REG_DWORD_LITTLE_ENDIAN) Integer 32-bit
signed little-endian
flags               : 0x0001
                   Value name is an ASCII string

unknown1           : 0x006f (111)
value name         : lParam
value name hash    : 0x4343bfdd
padding:
00000000: 00 00                                ..

value data:
00000000: 00 00 00 00 00 00 00 00 30 00 00 00  ..... 0...

value data padding:
00000000: 30 00 00 00                                0...

```

The Windows Registry-editor indicates this as an invalid value and presents it as binary data.

## 6.4. String value data too small

In this scenario the value is of type REG-SZ. The value data contains an UTF-16 little-endian string but the value data size is 1 too small. The size of the hive bin cell value is larger than the value data.

In this scenario the additional byte was a 0-byte and can be safely ignored.

Note that this can also apply to values stored in the data offset.

```

signature           : vk
value name size    : 11
data size          : 0x80000003 (3)
data offset       : 0x00000031
data type          : 1 (REG_SZ) String
flags              : 0x0001
                   Value name is an ASCII string

unknown1           : 0x0000 (0)
value name         : bEnableFlag
value name hash    : 0x6f09ddef
padding:
00000000: 00 00 00 00 00                                .....

```

## 6.5. String value data too large

In this scenario the value is e.g. of type REG\_SZ and the value data consist of more bytes than the size of the string. It is assumed the same applies to REG\_EXPAND\_SZ.

```

Value key data:
00000000: 76 6b 0b 00 0b 02 00 00 b8 7b 35 00 01 00 00 00 vk..... {5.....
00000010: 01 00 00 00 57 50 50 46 69 6c 65 4e 61 6d 65 00 ....WPPF fileName.
00000020: 00 00 00 00                                ....

signature           : vk
value name size    : 11

```

```

data size           : 0x0000020b (523)
data offset        : 0x00357bb8
data type          : 1 (REG_SZ) String
flags              : 0x0001
                   Value name is an ASCII string

unknown1          : 0x0000 (0)
value name        : WPPFileName
value name hash   : 0x4588b1a4
padding:
00000000: 00 00 00 00 00 .....

value data:
00000000: 4d 00 65 00 64 00 69 00 61 00 53 00 74 00 61 00 M.e.d.i. a.S.t.a.
00000010: 63 00 6b 00 00 00 00 00 d0 3e 9f 01 30 46 9f 01 c.k..... .>..0F..
00000020: f0 f4 06 00 ff ff ff ff c8 f7 06 00 20 e9 90 7c ..... ..|
...

```

The Windows Registry-editor indicates this as a valid value and presents the string “MediaStack”.

## 7. Notes

```

SPARE value in XP SYSTEM regf
unknown spare           : 0x00000000 (0)
unknown spare           : 0x00002000 (8192)
unknown spare           : 0x0011a000 (1155072)
unknown spare           : 0x0011c000 (1163264)
unknown spare           : 0x00120000 (1179648)
unknown spare           : 0x00122000 (1187840)
unknown spare           : 0x00123000 (1191936)
unknown spare           : 0x00125000 (1200128)
unknown spare           : 0x00126000 (1204224)
unknown spare           : 0x00127000 (1208320)
unknown spare           : 0x0012a000 (1220608)
unknown spare           : 0x0012d000 (1232896)
unknown spare           : 0x0012e000 (1236992)
unknown spare           : 0x00131000 (1249280)
unknown spare           : 0x00143000 (1323008)
unknown spare           : 0x00145000 (1331200)
unknown spare           : 0x00148000 (1343488)
unknown spare           : 0x00152000 (1384448)
unknown spare           : 0x00184000 (1589248)
unknown spare           : 0x00185000 (1593344)
unknown spare           : 0x00186000 (1597440)
unknown spare           : 0x00187000 (1601536)
unknown spare           : 0x00188000 (1605632)
unknown spare           : 0x00189000 (1609728)
unknown spare           : 0x0018a000 (1613824)
unknown spare           : 0x001bf000 (1830912)
unknown spare           : 0x001c7000 (1863680)
unknown spare           : 0x00218000 (2195456)
unknown spare           : 0x00224000 (2244608)

```

### 7.1. Transaction log

Hive bins size is set but the file has not sufficient size to store the hive bins.



## Appendix A. References

[PROBERT03]

Title: Windows Kernel Internals - NT Registry Implementation  
Author(s): David B. Probert  
Date: August 29, 2003  
URL: <http://www.i.u-tokyo.ac.jp/edu/training/ss/lecture/new-documents/Lectures/09-Registry/Registry.pdf>

[NORRIS09]

Title: The Internal Structure of the Windows Registry  
Author(s): Peter Norris  
Date: February 2009  
UTL: <http://amnesia.gtisc.gatech.edu/~moyix/suzibandit.ltd.uk/MSc/>

[MORGAN09]

Title: The Windows NT\* Registry File Format  
Version: 0.4  
Author(s): Timothy D. Morgan  
Date: June 9, 2009  
URL: <http://www.sentinelchicken.com/data/TheWindowsNTRegistryFileFormat.pdf>

[WINREG]

Title: WinReg.txt  
Author(s): B.D.

[MSDN]

Title: Registry  
URL: <http://msdn.microsoft.com>  
URL: [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724872\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724872(v=vs.85).aspx)

## Appendix B. GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.  
<<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## **1. APPLICABILITY AND DEFINITIONS**

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or

PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## **2. VERBATIM COPYING**

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## **3. COPYING IN QUANTITY**

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you

distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

#### **4. MODIFICATIONS**

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## **5. COMBINING DOCUMENTS**

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

## **6. COLLECTIONS OF DOCUMENTS**

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## **7. AGGREGATION WITH INDEPENDENT WORKS**

A compilation of the Document or its derivatives with other separate and independent documents or

works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## **8. TRANSLATION**

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## **9. TERMINATION**

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

## **10. FUTURE REVISIONS OF THIS LICENSE**

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option

of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

## **11. RELICENSING**

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.