LOCK AND CODE

COMPUTER FORENSIC EXAMINER

QUICK REFERENCE GUIDE

REVISION 13

- UNAUTHORISED REPRODUCTION PROHIBITED -

IACIS

The International Association of Computer Investigative Specialists

- UNAUTHORISED REPRODUCTION PROHIBITED -

Common conventions used throughout this booklet:

Colored blocks	Blocks of bytes that reoccur throughout this booklet are bound by a colored box. Some common blocks of bytes occur on multiple pages and will always appear in the same color for increased readability.
[O1] / [L1]	Hard brackets indicate a variable. "O" is shorthand for offset and "L" is shorthand for "length". Variables are highlighted in yellow for increased visibility.
Offset A / B	Where offsets are listed as part A and part B it is necessary to add the values of A and B to determine the absolute offset. Any variables eg. [O1] should be resolved first. Where multiple values or variables appear in the Part A field, they should be totaled prior to adding the Part B value.
Attribute charts	NTFS attributes exist within a $MFT "FILE" Record. When using the attribute charts the user should note the offset at the start of the given attribute and treat all offsets displayed on the chart as relative to the start of the given attribute.
Index Nodes	Index Nodes exist either within an Index Root Attribute 0x90 or within an Index "INDX" record (referenced by an Index Allocation Attribute 0xA0). Offsets on the Index Node chart should be treated as relative to the start of the Index Node.

Suggestions for additional booklet content should be sent to:

quickref@lockandcode.com

QUICK REFERENCE GUIDE - Table of Contents

UNAUTHORISED REPRODUCTION PROHIBITED

Topic	Reference	Page
NTFS	Volume Boot Sector	4
	Metafiles	5
	"$MFT" "FILE" Record	6
	Attribute Types	7
	Standard Information Attribute 0x10 (Resident)	8
	File Name Attribute 0x30 (Resident)	9
	Data Attribute 0x80 (Resident)	10
	Data Attribute 0x80 (Non-Resident)	11
	Index Root Attribute 0x90 (Resident)	12
	Index Allocation Attribute 0xA0 (Non-Resident)	13
	Index "INDX" Record	14
	Index Node Breakdown (MFT Example)	15
FAT	Fat 12/16 Boot Sector	16
	Fat 32 Boot Sector	17
	Short File Name Directory Entry	18
	Long File Name Directory Entry	19
Windows Registry	Hive Locations on Windows 7	20
Internet Explorer 8	INDEX.DAT File Locations on Windows 7	21
ASCII Chart	Ranging: 0 to 63	22
	Ranging: 64 to 127	23
	Ranging: 128 to 191	24
	Ranging: 192 to 255	25
First Responder	IACIS Electronic Evidence Seizure Triage Flowchart	26

NTFS - Volume Boot Sector

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	3 bytes	JMP Instructions
0x03	3	8 bytes	OEM ID (ASCII) eg. "NTFS"
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 byte	Sectors per cluster
0x0E	14	2 bytes	Reserved sectors
0x10	16	1 byte	Number of file allocation tables
0x11	17	2 bytes	Max directory entries
0x13	19	2 bytes	Total sectors
0x15	21	1 byte	Media descriptor
0x16	22	2 bytes	Sectors per file allocation table
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sectors
0x20	32	4 bytes	Total sectors
0x24	36	4 bytes	Unused
0x28	40	8 bytes	Total Sectors on the volume
0x30	48	8 bytes	LCN[1] for the $MFT's starting extent
0x38	56	8 bytes	LCN[1] for the $MFTMirr's starting extent
0x40	64	1 byte	Clusters Per $MFT Record
0x41	65	3 bytes	Unused
0x44	68	1 byte	Clusters Per Index Buffer
0x45	69	3 bytes	Unused
0x48	72	8 bytes	Volume Serial Number
0x50	80	4 bytes	Unused

1 Logical Cluster Number

2 If the signed value (x) is positive then it represents the clusters per MFT record. If it is negative, the size of the file record in bytes is 2 raised to the absolute value of x.

Note: Greyed text denotes fields that are unused by NTFS

BIOS Parameter Block (BPB)

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Metafiles (NTFS v3.0+)

File Record	Filename	Description
0	$MFT	Master File Table (MFT)
1	$MFTMirr	MFT Mirror – backup of first 4 MFT Records
2	$LogFile	Volume recovery information
3	$Volume	Volume information Volume Label, Serial Number & Version
4	$AttrDef	Definition file for all supported attributes
5	. (dot)	Root directory of the volume
6	$Bitmap	A bit representation of allocated and unallocated clusters
7	$Boot	Boot record for the volume
8	$BadClus	List of bad clusters on the volume
9	$Secure	Security descriptors for all files on volume
10	$UpCase	Table of uppercase characters used for conversion
11	$Extend	Directory for $Boot, $Bitmap, $Secure and $UpCase
12-15		RESERVED
16-23		UNUSED
Any	$ObjId	Storage location for Unique Object IDs for each file
Any	$Quota	Storage location for disk space quota information
Any	$Reparse	Storage location for reparse point information
Any	$UsnJrnl	NTFS Update Sequence Number (USN)

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - $MFT "FILE" Record

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Signature [46 49 4C 45] ie. "FILE"
	0x04	4	2 bytes	Offset to Fixup Array [O1]
	0x06	6	2 bytes	Number of entries in the Fixup array [L1]
	0x08	8	8 bytes	Update Sequence Number (USN)
0x00+	0x10	16	2 bytes	Incremental sequence count
	0x12	18	2 bytes	Link count
	0x14	20	2 bytes	Offset to start of the attributes [O2]
	0x16	22	2 bytes	Flags[1]
	0x18	24	4 bytes	Logical size of the $MFT record [L3]
	0x1C	28	4 bytes	Physical size of the $MFT record
	0x20	32	8 bytes	File reference to the base record
	0x28	40	2 bytes	Next available attribute identifier
	0x2A	42	2 bytes	Fixup values and attributes
	0x2C	44	4 bytes	$MFT File Record Number (NTFS 3.1+)
[O1]+	0x00	0	[L1] * 2	Fixup Array
[O2]+	0x00	0	[L3] – [O2]	Attributes

1 Of bits ranging from 0 to 15, bit 0 set denotes "allocated" status and bit 1 set denotes a "directory".
Note: The last two bytes of each sector in a $MFT "FILE" Record need to be replaced with the corresponding two bytes in the fixup array.

Fixup Header

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Attribute Types

Type	Name	Location	Min Size	Max Size
0x10	$STANDARD_INFORMATION	Resident	0x30	0x48
0x20	$ATTRIBUTE_LIST	Non-Resident	-	-
0x30	$FILE_NAME	Resident	0x44	0x242
0x40	$OBJECT_ID	Resident	-	0x100
0x50	$SECURITY_DESCRIPTOR	Non-Resident	-	-
0x60	$VOLUME_NAME	Resident	0x02	0x100
0x70	$VOLUME_INFORMATION	Resident	0x0C	0x0C
0x80	$DATA	Either	-	-
0x90	$INDEX_ROOT	Resident	-	-
0xA0	$INDEX_ALLOCATION	Non-Resident	-	-
0xB0	$BITMAP	Non-Resident	-	-
0xC0	$REPARSE_POINT	Non-Resident	-	0x4000
0xD0	$EA_INFORMATION	Resident	0x08	0x08
0xE0	$EA	Either	-	0x10000
0xF0	$PROPERTY_SET	Either		
0x100	$LOGGED_UTILITY_STREAM	Non-Resident	-	0x10000

Note: The above attribute types and their associated residency and size properties are as documented of NTFS v3.1 and can be used as a guide. However, all values are variable and therefore the correct properties should be read directly from the $AttrDef (Attribute Definition) file of the target file system.

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Standard Information Attribute 0x10 (Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 bytes	Resident / Non-Resident Flag [1]
	0x09	9	1 bytes	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Length of attribute content [L2]
	0x14	20	2 bytes	Offset to attribute content [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	8 bytes	Creation Date and Time
	0x08	8	8 bytes	Last Modified Date and Time
	0x10	16	8 bytes	$MFT Modified Date and Time
	0x18	24	8 bytes	Last Accessed Date and Time
	0x20	32	4 bytes	Flags
	0x24	36	4 bytes	Maximum number of versions
	0x28	40	4 bytes	Version number
	0x2C	44	4 bytes	Class ID
	0x30	48	4 bytes	Owner ID
	0x34	52	4 bytes	Security ID
	0x38	56	4 bytes	Quota Charged
	0x40	64	8 bytes	Update Sequence Number ("USN")

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 are currently unused.

Attribute Header
Resident Header
Attribute Body

UNAUTHORISED REPRODUCTION PROHIBITED.

NTFS - File Name Attribute 0x30 (Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 bytes	Resident / Non-Resident Flag [1]
	0x09	9	1 bytes	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Length of attribute content [L2]
	0x14	20	2 bytes	Offset to attribute content [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	6 bytes	$MFT Record number of the parent dir
	0x06	6	2 bytes	Sequence number of the parent dir
	0x08	8	8 bytes	Creation Date and Time
	0x10	16	8 bytes	Last Modified Date and Time
	0x18	24	8 bytes	$MFT Modified Date and Time
	0x20	32	8 bytes	Last Accessed Date and Time
	0x28	40	8 bytes	Allocated size of the index
	0x30	48	8 bytes	Actual size of the index
	0x38	56	4 bytes	Flags
	0x3C	60	4 bytes	Reparse value
	0x40	64	1 byte	Filename length in characters [L3]
	0x41	65	1 byte	Filename namespace
	0x42	66	[L3] * 2	Filename

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident.
Bits 1 through 7 are currently unused.

Attribute Header
Resident Header
Attribute Body

UNAUTHORISED REPRODUCTION PROHIBITED

NTFS - Data Attribute 0x80 (Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 bytes	Resident / Non-Resident Flag [1]
	0x09	9	1 bytes	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Length of attribute content [L2]
	0x14	20	2 bytes	Offset to attribute content [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	[L2]	Resident Data

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 are currently unused.

Attribute Header
Resident Header
Attribute Body

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Data Attribute 0x80 (Non-Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 bytes	Resident / Non-Resident Flag [1]
	0x09	9	1 bytes	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	8 bytes	Starting VCN of the runlist
	0x18	24	8 bytes	Ending VCN of the runlist
	0x20	32	2 bytes	Offset to the runlist [O2]
	0x22	34	2 bytes	Compression unit [2]
	0x24	36	4 bytes	Padding
	0x28	40	8 bytes	Allocated size of the content in bytes
	0x30	48	8 bytes	Actual size of the content in bytes
	0x38	56	8 bytes	Initialized size of the content in bytes
	0x40	64	8 bytes	Compressed size of the content in bytes
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	Var	Runlist of clusters containing the non-resident data

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 are currently unused.
2 A value other than zero denotes compression is present.

Attribute Header
Non-Resident Header
Present only in stream compressed
Attribute Body

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Index Root 0x90 (Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 byte	Resident / Non-Resident Flag [1]
	0x09	9	1 byte	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Length of attribute content [L2]
	0x14	20	2 bytes	Offset to attribute content [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	4 bytes	Type of attribute stored in the index
	0x04	4	4 bytes	Collation sorting rule
	0x08	8	4 bytes	Size of each index record in bytes
	0x0C	12	1 byte	Size of each index record in clusters
	0x0D	13	3 bytes	Padding
[O2]+ 0x10+	0x00	0	4 bytes	Relative Offset to Index Node [O3]
	0x04	4	4 bytes	Index Node length [L3]
	0x08	8	4 bytes	Index Node allocation length
	0x0C	12	4 bytes	Flags
[O2]+ 0x10+ [O3]+	0x00	0	[L3]	Index Root Node (See Note Breakdown page 5)

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 are currently unused.

Attribute Header
Resident Header
Index Node Header
Index Node Body

UNAUTHORISED REPRODUCTION PROHIBITED.

NTFS - Index Allocation 0xA0 (Non-Resident)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Attribute Type
	0x04	4	4 bytes	Length of attribute
	0x08	8	1 bytes	Resident / Non-Resident Flag [1]
	0x09	9	1 bytes	Length of stream name in characters [L1]
	0x0A	10	2 bytes	Offset to the stream name [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	8 bytes	Starting VCN of the runlist
	0x18	24	8 bytes	Ending VCN of the runlist
	0x20	32	2 bytes	Offset to the runlist [O2]
	0x22	34	2 bytes	Compression unit [2]
	0x24	36	4 bytes	Padding
	0x28	40	8 bytes	Allocated size of the content in bytes
	0x30	48	8 bytes	Actual size of the content in bytes
	0x38	56	8 bytes	Initialized size of the content in bytes
	0x40	64	8 bytes	Compressed size of the content in bytes
[O1]+	0x00	0	[L1] * 2	Stream Name (Unicode Characters)
[O2]+	0x00	0	Var.	Runlist of clusters containing the non-resident data (ie. INDX records)

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 are currently unused.
2 A value other than zero denotes compression is present.

Attribute Header
Non-Resident Header
Present only if stream compressed
Attribute Body

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Index "INDX" Record

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	4 bytes	Signature [49 4E 44 58] ie. "INDX"
	0x04	4	2 bytes	Offset to Fixup array [O1]
	0x06	6	2 bytes	Number of entries in the Fixup array [L1]
	0x08	8	8 bytes	Update Sequence Number (USN)
0x00+	0x10	16	8 bytes	VCN Index Allocation
0x18+	0x00	0	4 bytes	Relative offset to the Index Node [O2]
	0x04	4	4 bytes	Index Node length [L2]
	0x08	8	4 bytes	Index Node allocation length
	0x0C	12	4 bytes	Flags
[O1]+	0x00	0	[L1] * 2	Fixup Array
0x18+ [O2]+	0x00	0	[L2]	Index Node (See Index Node Breakdown, page 15)

Note: The last two bytes of each sector in an Index "INDX" Record must be replaced with the corresponding two bytes in the fixup array.

Record Header
Index Node Header
Index Node Body

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS Index Node Breakdown ($I30 example)

Offset Part A	Offset Part B Hex	Offset Part B Dec	Length	Field Name and Definition
0x00+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length [O1]
	0x0A	10	2 bytes	Index data length [L1]
	0x0C	12	2 bytes	Flags [1]
0x00+	0x10	16	[L1]	Index Entry Data [2] (ie. Filename Attribute Body)
[O1]+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length [O2]
	0x0A	10	2 bytes	Index data length [L2]
	0x0C	12	2 bytes	Flags [1]
[O1]+	0x10	16	[L2]	Index Entry Data [2] (ie. Filename Attribute Body)
[O1]+ [O2]+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length [O3]
	0x0A	10	2 bytes	Index data length [L3]
	0x0C	12	2 bytes	Flags [1]
[O1]+ [O2]+	0x10	16	[L3]	Index Entry Data (ie. Filename Attribute Body)
[O1]+ [O2]+ [O3]+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length
	0x0A	10	2 bytes	Index data length
	0x0C	12	2 bytes	Flags [1]

This Node example contains 3 index entries. A node may contain zero or more index entries.

1 Of bits ranging from 0 to 15, bit 0 set denotes the existence of a child node and bit 1 set denotes this as the last entry in the node.

2 If a child node exists, this region will also contain the child node identifier.

Index Entry Header
Header Body
Header/Terminator

UNAUTHORISED REPRODUCTION PROHIBITED

FAT12/FAT16 - Boot Sector

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	3 bytes	JMP Instructions
0x03	3	8 bytes	OEM ID (ASCII) eg. "MSWIN4.1"
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 byte	Sectors per cluster
0x0E	14	2 bytes	Reserved sectors
0x10	16	1 byte	Number of file allocation tables
0x11	17	2 bytes	Root directory entries
0x13	19	2 bytes	Total sectors
0x15	21	1 byte	Media descriptor
0x16	22	2 bytes	Sectors per file allocation table
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sectors
0x20	32	4 bytes	Total sectors
0x24	36	1 byte	Bios Drive Number
0x25	37	1 byte	Reserved
0x26	38	1 byte	Extended boot signature
0x27	39	4 bytes	Volume serial number
0x2B	43	11 bytes	Volume label (ASCII)
0x36	54	8 bytes	File system type (ASCII)

BIOS Parameter Block (BPB)

- UNAUTHORISED REPRODUCTION PROHIBITED -

FAT32 - Boot Sector

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	3 bytes	JMP Instructions
0x03	3	8 bytes	OEM ID (ASCII) eg. "MSWIN4.1"
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 byte	Sectors per cluster
0x0E	14	2 bytes	Reserved sectors
0x10	16	1 bytes	Number of file allocation tables
0x11	17	2 bytes	Root directory entries
0x13	19	2 bytes	Total sectors
0x15	21	1 bytes	Media descriptor
0x16	22	2 bytes	Sectors per file allocation table
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sectors
0x20	32	4 bytes	Total sectors
0x24	36	4 bytes	Sectors per file allocation table
0x28	40	2 bytes	Extended flags
0x2A	42	2 bytes	FAT version
0x2C	44	4 bytes	Root directory starting cluster number
0x30	48	2 bytes	File system information sector
0x32	50	2 bytes	Backup boot sector, sector number
0x34	52	12 bytes	Reserved
0x40	64	1 bytes	Bios Drive Number
0x41	65	1 bytes	Reserved
0x42	66	1 bytes	Extended boot signature
0x43	67	4 bytes	Volume serial number
0x47	71	11 bytes	Volume label (ASCII)
0x52	82	8 bytes	File system type (ASCII)

BIOS Parameter Block (BPB) — FAT32 Extension of BPB

UNAUTHORISED REPRODUCTION PROHIBITED

FAT - Short File Name Directory Entry

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	8 bytes	File/folder name (ASCII)
0x08	8	3 bytes	File/folder extension (ASCII)
0x0B	11	1 byte	File/folder attributes (See bit assignments below)
0x0C	12	1 byte	Reserved for Windows NT
0x0D	13	1 byte	Creation Time (10ths of seconds)
0x0E	14	2 bytes	Creation Time
0x10	16	2 bytes	Creation Date
0x12	18	2 bytes	Last Accessed Date
0x14	20	2 bytes	Starting cluster number (high word)
0x16	22	2 bytes	Modification Time
0x18	24	2 bytes	Modification Date
0x1A	26	2 bytes	Starting cluster, cluster number (low word)
0x1C	28	4 bytes	File size

File/Folder Attributes	
Bit	Description
0	Read Only
1	Hidden
2	System
3	Volume Label
4	Directory
5	Archive

Date Breakdown	
Bit	Description
0-4	Day
5-8	Month
9-15	Year (+1980)

Time Breakdown	
Bit	Description
0-4	Seconds x2
5-10	Minutes
11-15	Hour

- UNAUTHORISED REPRODUCTION PROHIBITED -

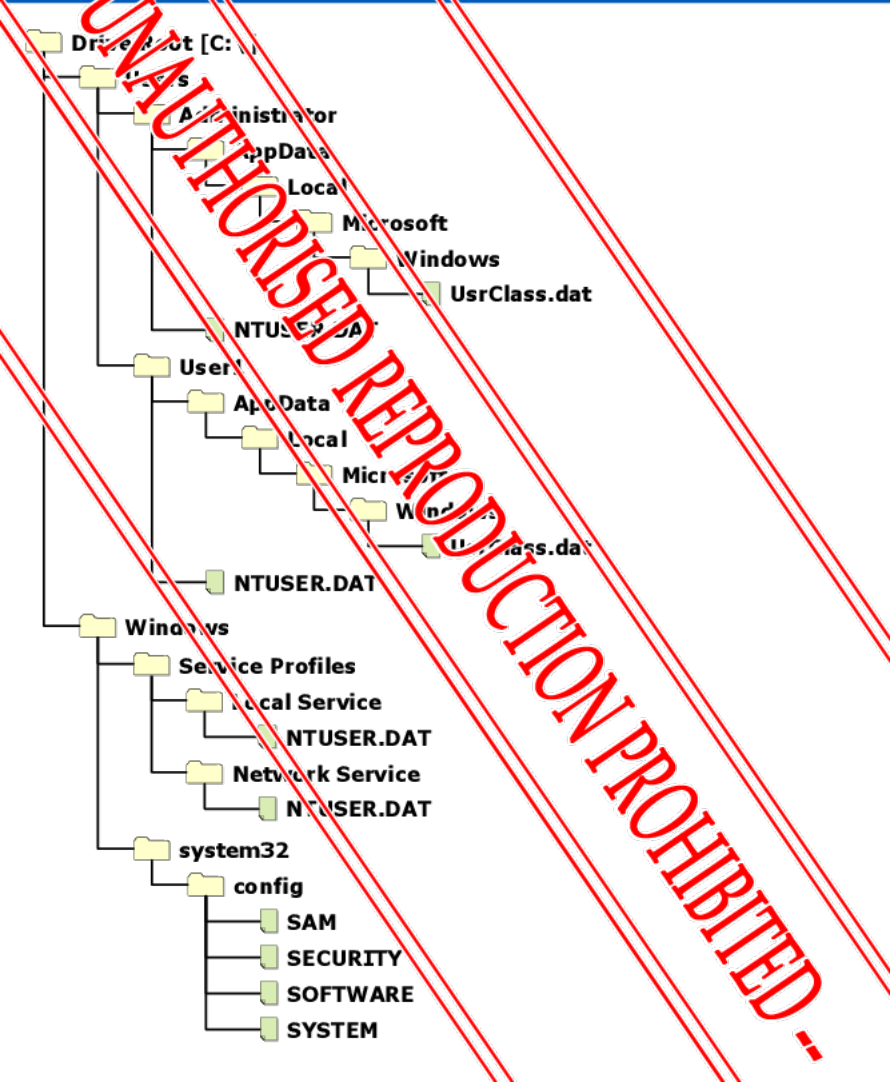
FAT - Long File Name Directory Entry

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	1 bytes	LFN Signature (See bit assignments below)
0x01	1	10 bytes	LFN text, characters 0 through 4 (Unicode)
0x0B	11	1 bytes	File/folder attributes
0x0C	12	1 bytes	Reserved for Windows NT
0x0D	13	1 bytes	Short file name checksum value
0x0E	14	12 bytes	LFN text, characters 5 through 10 (Unicode)
0x1A	26	2 bytes	Unused
0x1C	28	4 bytes	LFN text, characters 11 through 12 (Unicode)

LFN Signature	
Bit	Description
0-5	Sequence Number
6	Denotes last LFN entry
7	Denotes deleted LFN

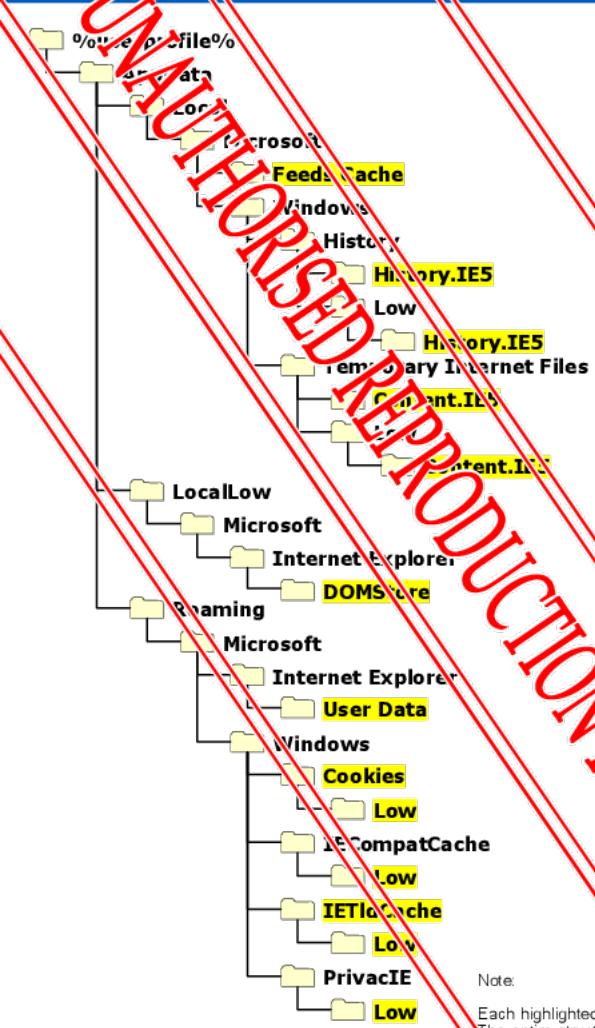
- UNAUTHORISED REPRODUCTION PROHIBITED -

WINDOWS REGISTRY - Hive Locations on Windows 7



- UNAUTHORISED REPRODUCTION PROHIBITED -

IE3 - INDEX.DAT File Locations on Windows 7



Note:

Each highlighted folder contains an INDEX.DAT file. The entire structure above is repeated for each user profile on the system.

UNAUTHORISED REPRODUCTION PROHIBITED

ASCII CHART - 0 to 63

DEC	OCT	HEX	BINARY	SYMBOL	DEC	OCT	HEX	BINARY	SYMBOL
0	000	00	00000000	NUL	32	040	20	00100000	Space
1	001	01	00000001	SOH	33	041	21	00100001	!
2	002	02	00000010	STX	34	042	22	00100010	"
3	003	03	00000011	ETX	35	043	23	00100011	#
4	004	04	00000100	EOT	36	044	24	00100100	$
5	005	05	00000101	ENQ	37	045	25	00100101	%
6	006	06	00000110	ACK	38	046	26	00100110	&
7	007	07	00000111	BEL	39	047	27	00100111	'
8	010	08	00001000	BS	40	050	28	00101000	(
9	011	09	00001001	TAB	41	051	29	00101001	)
10	012	0A	00001010	LF	42	052	2A	00101010	*
11	013	0B	00001011	VT	43	053	2B	00101011	+
12	014	0C	00001100	FF	44	054	2C	00101100	,
13	015	0D	00001101	CR	45	055	2D	00101101	-
14	016	0E	00001110	SO	46	056	2E	00101110	.
15	017	0F	00001111	SI	47	057	2F	00101111	/
16	020	10	00010000	DLE	48	060	30	00110000	0
17	021	11	00010001	DC1	49	061	31	00110001	1
18	022	12	00010010	DC2	50	062	32	00110010	2
19	023	13	00010011	DC3	51	063	33	00110011	3
20	024	14	00010100	DC4	52	064	34	00110100	4
21	025	15	00010101	NAK	53	065	35	00110101	5
22	026	16	00010110	SYN	54	066	36	00110110	6
23	027	17	00010111	ETB	55	067	37	00110111	7
24	030	18	00011000	CAN	56	070	38	00111000	8
25	031	19	00011001	EM	57	071	39	00111001	9
26	032	1A	00011010	SUB	58	072	3A	00111010	:
27	033	1B	00011011	ESC	59	073	3B	00111011	;
28	034	1C	00011100	FS	60	074	3C	00111100	<
29	035	1D	00011101	GS	61	075	3D	00111101	=
30	036	1E	00011110	RS	62	076	3E	00111110	>
31	037	1F	00011111	US	63	077	3F	00111111	?

- UNAUTHORISED REPRODUCTION PROHIBITED -

ASCII CHART - 64 to 127

DEC	OCT	HEX	BINARY	SYMBOL
64	100	40	01000000	@
65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_

DEC	OCT	HEX	BINARY	SYMBOL
96	140	60	01100000	`
97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y
122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	DEL

-UNAUTHORISED REPRODUCTION PROHIBITED-

ASCII CHART - 128 to 191

DEC	OCT	HEX	BINARY	SYMBOL
128	200	80	10000000	€
129	201	81	10000001	
130	202	82	10000010	‚
131	203	83	10000011	ƒ
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž
159	237	9F	10011111	Ÿ

DEC	OCT	HEX	BINARY	SYMBOL
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	-
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	•
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾
191	277	BF	10111111	¿

UNAUTHORISED REPRODUCTION PROHIBITED

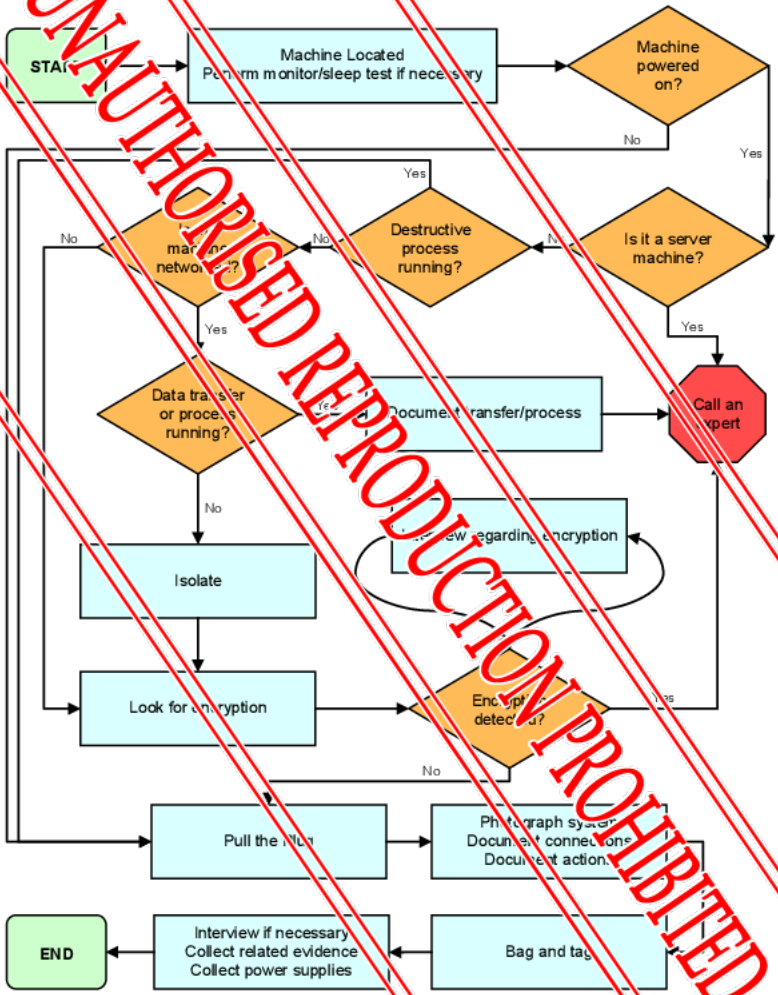
ASCII CHART 192 to 255

DEC	OCT	HEX	BINARY	SYMBOL
192	300	C0	11000000	¶
193	301	C1	11000001	•
194	302	C2	11000010	¸
195	303	C3	11000011	¹
196	304	C4	11000100	¬
197	305	C5	11000101	»
198	306	C6	11000110	¼
199	307	C7	11000111	½
200	310	C8	11001000	¿
201	311	C9	11001001	À
202	312	CA	11001010	Á
203	313	CB	11001011	Â
204	314	CC	11001100	Ã
205	315	CD	11001101	Ä
206	316	CE	11001110	Å
207	317	CF	11001111	Æ
208	320	D0	11010000	Ð
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ
223	337	DF	11011111	ß

DEC	OCT	HEX	BINARY	SYMBOL
224	340	E0	11100000	à
225	341	E1	11100001	á
226	342	E2	11100010	â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í
238	356	EE	11101110	î
239	357	EF	11101111	ï
240	360	F0	11110000	ð
241	361	F1	11110001	ñ
242	362	F2	11110010	ò
243	363	F3	11110011	ó
244	364	F4	11110100	ô
245	365	F5	11110101	õ
246	366	F6	11110110	ö
247	367	F7	11110111	÷
248	370	F8	11111000	ø
249	371	F9	11111001	ù
250	372	FA	11111010	ú
251	373	FB	11111011	û
252	374	FC	11111100	ü
253	375	FD	11111101	ý
254	376	FE	11111110	þ
255	377	FF	11111111	ÿ

- UNAUTHORISED REPRODUCTION PROHIBITED -

FIRSTRESPONDER - Evidence Seizure Triage Flowchart



UNAUTHORISED REPRODUCTION PROHIBITED!

Copyright © 2011 International Association of Computer Investigative Specialists (IACIS)
Included in this booklet with the permission of IACIS.