LOCK AND CODE

COMPUTER FORENSIC EXAMINER

QUICK REFERENCE GUIDE

REVISION 2.0

- UNAUTHORISED REPRODUCTION PROHIBITED -

IACIS
The International Association of Computer Investigative Specialists

Available on the App Store

Copyright © 2011-2014
Lock and Code Pty Ltd

- UNAUTHORISED REPRODUCTION PROHIBITED -

Common conventions and assumptions used throughout this booklet:

Audience: This booklet is for practitioners in the field of computer forensics. It is for quick reference purposes and is not designed to teach a topic from scratch.

Colored blocks: Blocks of bytes that reoccur throughout this booklet are bound by a colored box and will always appear in the same color for increased readability.

Units: Unless explicitly stated, all lengths/offsets are measured in bytes.

Byte order: Unless explicitly stated, all values are in Little Endian byte order.

Timestamps: Unless explicitly stated, all timestamps are in UTC time.

Hex strings: Signatures expressed in [00 01 02 03 04 05 06 07 08] notation should be interpreted as an array of individual bytes. Endianness is not a factor as it applies only to multi-byte data types.

Double lines: Double lines between charts/rows indicate that values of low importance have been omitted. Special attention should be paid to the offset value immediately following a double line.

[O1] / [L1]: A single letter and number inside brackets indicate a variable. "O" is shorthand for offset and "L" 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: Unless explicitly stated, all offsets within NTFS attribute charts are relative to the start of the 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 charts should be treated as relative to the start of the Index Node.

QUICK REFERENCE GUIDE - Index

Author: Darren Freestone
Lock and Code Pty Ltd

Contributing author: Terry Olson
Nebraska State Patrol Technical Crimes/ICAC Lab

Questions / feedback / suggestions / tailored bulk orders:
quickref@lockandcode.com

Topic	Pages
Partitioning Schemes [MBR / GPT]	4 – 7
New Technology File System (NTFS)	8 – 19
File Allocation Table File System (FAT)	20 – 22
Extended File Allocation Table File System (exFAT)	23 – 25
Hierarchical File System Plus (HFS+)	26 – 27
Extended File System 2, 3 & 4 (EXT2/3/4)	28 – 31
Windows Registry	32 – 35
Internet Explorer	36 – 38
Windows Artifacts	39 – 43
Dates & Times	44
File Signatures	45
ASCII Chart	46 – 49
IACIS Electronic Evidence Seizure Triage Flowchart	50

Computer Forensic Examiner Quick Reference Guide 2.2 ISBN: 978-0-98,309[illegible]-2-8
ABN: 64 581 5[illegible]
Copyright © 2011-2014 Lock and Code Pty Ltd (unless otherwise specified)
Licensed to IACIS® for reproduction and distribution
All rights reserved
Printed in the USA

- UNAUTHORISED REPRODUCTION PROHIBITED -

PARTITIONING SCHEMES – Master Boot Record (MBR)

Offset		Length	Field Name and Definition
Hex	Dec		
MBR LBA Sector 0			
0x00	0	440 bytes	Boot code
0x1B8	440	4 bytes	Disk signature [1]
0x1BC	444	2 bytes	Undocumented, usually zero
0x1BE	446	16 bytes	Partition entry 1
0x1CE	462	16 bytes	Partition entry 2
0x1DE	478	16 bytes	Partition entry 3
0x1EE	494	16 bytes	Partition entry 4
0x1FE	510	2 bytes	Signature [55 AA]
Partition Entry			
0x00	0	1 bytes	Bootable flag [2]
0x01	1	3 bytes	Starting CHS address
0x04	4	1 bytes	Partition type
0x05	5	3 bytes	Ending CHS address
0x08	8	4 bytes	Starting LBA sector offset
0x0C	12	4 bytes	Partition sector count

1 Value set during disk initialisation in Windows and can be used to uniquely identify a disk.
Used by the Windows Registry: HKLM\System\MountedDevices.

2 A value of 0x80 indicates the partition is bootable.

3 The cylinders value is 10 bits long and split between bytes 1 and 2.

CHS Breakdown		
Byte	Bit	Description
0	0-7	Head
1	0-5	Sectors
1	6-7	Cylinders (high 2 bits) [3]
2	0-7	Cylinders (low 8 bits) [3]

- UNAUTHORISED REPRODUCTION PROHIBITED -

PARTITIONING SCHEMES - MBR Partition Types

MBR Partition Types by OS		
OS	Hex	Description
N/A	0x00	Empty
	0x05	Extended partition
	0x0F	Extended partition, LBA
	0xEE	EFI partition
	0x01	FAT12, CHS
	0x04	FAT16, <=32MB, CHS
	0x06	FAT16, <=2GB, CHS
	0x07	NTFS / exFAT
	0x0B	FAT32, CHS
	0x0C	FAT32, LBA
	0x0E	FAT16, LBA
	0x11	Hidden FAT12, CHS
	0x14	Hidden FAT16, <=32MB, CHS
	0x16	Hidden FAT16, <=2GB, CHS
	0x1B	Hidden FAT32, CHS
	0x1C	Hidden FAT32, LBA
	0x1E	Hidden FAT16, LBA
	0x81	Linux/Minix
	0x82	Linux swap / Solaris x86
	0x83	Linux (Ext2-4, Reiserfs, xiafs)
	0xA8	Mac OSX
	0xAB	Mac OSX boot
	0xFB	VMWare filesystem
	0xFC	VMWare swap

MBR Partition Types by Code	
Hex	Description
0x00	Empty
0x01	FAT12, CHS
0x04	FAT16, <=32MB, CHS
0x05	Extended partition
0x06	FAT16, <=2GB, CHS
0x07	NTFS / exFAT
0x0B	FAT32, CHS
0x0C	FAT32, LBA
0x0E	FAT16, LBA
0x0F	Extended partition, LBA
0x11	Hidden FAT12, CHS
0x14	Hidden FAT16, <=32MB, CHS
0x16	Hidden FAT16, <=2GB, CHS
0x1B	Hidden FAT32, CHS
0x1C	Hidden FAT32, LBA
0x1E	Hidden FAT16, LBA
0x81	Linux/Minix
0x82	Linux swap / Solaris x86
0x83	Linux (Ext2-4, Reiserfs, xiafs)
0xA8	Mac OSX
0xAB	Mac OSX boot
0xEE	EFI partition
0xFB	VMWare filesystem
0xFC	VMWare swap

- UNAUTHORIZED REPRODUCTION PROHIBITED -

Offset Hex	Offset Dec	Length	Field Name and Definition
GPT LBA Sector 1			
0x00	0	8 bytes	Signature ["EFI PART"] (ASCII)
0x08	8	4 bytes	Version
0x0C	12	4 bytes	GPT header length
0x10	16	4 bytes	GPT header CRC32 checksum
0x14	20	4 bytes	Reserved (zeroed)
0x18	24	8 bytes	GPT header LBA sector offset
0x20	32	8 bytes	Backup GPT header LBA sector offset
0x28	40	8 bytes	Reserved LBA sector count
0x30	48	8 bytes	Usable LBA sector count
0x38	56	16 bytes	Disk GUID [1]
0x48	72	8 bytes	Partition table LBA sector offset
0x50	80	4 bytes	Partition table entry count
0x54	84	4 bytes	Partition table entry length
0x58	88	4 bytes	Partition table CRC32 checksum
0x5C	92	420 bytes	Reserved (zeroed)
Partition Entry			
0x00	0	16 bytes	Partition type GUID
0x10	16	16 bytes	Unique partition GUID
0x20	32	8 bytes	Partition LBA starting sector
0x28	40	8 bytes	Partition LBA ending sector
0x30	48	8 bytes	Attribute flags
0x38	56	72 bytes	Partition name (UNICODE)

Note: The first sector (LBA 0) is reserved and contains a legacy Master Boot Record (MBR).

1 Globally Unique Identifiers (GUIDs) are 16 byte (128 bit) values typically displayed as 32 hexadecimal characters and enclosed in curly braces as follows:
{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

Attribute Flags	
Bit	Description
0	System partition
60	Read-only
62	Hidden
63	Do not automount

UNAUTHORISED REPRODUCTION PROHIBITED

GPT Partition Types by OS		
OS	Description	GUID
NA	Unused entry	00000000-0000-0000-0000-000000000000
	MBR partition scheme	024DEE41-33E7-11D3-9D69-0008C781F39F
	EFI system partition	C12A7328-F81F-11D2-BA4B-00A0C93EC93B
	BIOS boot partition	21686148-6449-6E6F-744E-656564454649
	Microsoft reserved partition	E3C9E316-0B5C-4DB8-817D-F92DF00215AE
	Basic data partition	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7
	LDM metadata partition	5808C8AA-7E8F-42E0-B1D2-E1E90434CFB3
	LDM data partition	AF9B60A0-1431-4F62-BC68-3311714A69AD
	Windows recovery env.	DE94BBA4-06D1-4D40-A16A-BFD50179D6AC
	IBM GPFS partition	37AFFC90-EF7D-4E96-91C3-2D7AE055B174
	Linux file system data	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7
	RAID partition	A19D880F-05FC-4D3B-A006-743F0F84911E
	Swap partition	0657FD6D-A4AB-43C4-84E5-0933C84B4F4F
	LVM partition	E6D6D379-F507-44C2-A23C-238F2A3DF928
	Reserved	8DA63339-0007-60C0-C436-083AC8230908
	HFS+ partition	48465300-0000-11AA-AA11-00306543ECAC
	Apple UFS partition	55465300-0000-11AA-AA11-00306543ECAC
	ZFS partition	6A898CC3-1DD2-11B2-99A6-080020736631
	Apple RAID partition	52414944-0000-11AA-AA11-00306543ECAC
	Apple RAID partition, offline	52414D14-5F48-11AA-AA11-00306543ECAC
	Apple boot partition	426F6F74-0000-11AA-AA11-00306543ECAC
	Apple label	4C616265-6C00-11AA-AA11-00306543ECAC
	Apple TV recovery partition	5265636F-7665-11AA-AA11-00306543ECAC
	Apple core storage partition	53746F72-6167-11AA-AA11-00306543ECAC

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Volume Boot Sector

Offset Hex	Offset Dec	Length	Field Name and Definition
0x00	0	3 bytes	JMP instructions
0x03	3	8 bytes	OEM ID eg. ["NTFS "] (ASCII)
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 byte	Sectors per cluster
0x0E	14	2 bytes	Reserved sector count
0x10	16	1 byte	File allocation table (FAT) count eg. 2
0x11	17	2 bytes	Root directory entries
0x13	19	2 bytes	Total sector count
0x15	21	1 byte	Media descriptor
0x16	22	2 bytes	File allocation table (FAT) sector count
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sector count
0x20	32	4 bytes	Total sector count
0x24	36	4 bytes	Unused
0x28	40	8 bytes	Total sector count
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 x 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 of 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, $BadClus, $Secure and $UpCase
12-15		RESERVED
16-23		UNUSED
Any	$ObjId	Storage location for unique object ID 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] "FILE" (ASCII)
	0x04	4	2 bytes	Fixup array offset [01]
	0x06	6	2 bytes	Fixup array entry count [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	Attribute starting offset [02]
	0x16	22	2 bytes	Flags[1]
	0x18	24	4 bytes	$MFT record logical size [L3]
	0x1C	28	4 bytes	$MFT record physical size
	0x20	32	8 bytes	File reference to the base record
	0x28	40	2 bytes	Next available attribute identifier
	0x2A	42	2 bytes	Fixup codes and attributes
	0x2C	44	4 bytes	$MFT "FILE" record number (NTFS 3.1+)
[01]+	0x00	0	[L1] * 2	Fixup array
[02]+	0x00	0	[L3] – [02]	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.

[1] Record Header

- UNAUTHORISED REPRODUCTION PROHIBITED -

NTFS - Attribute Types

Type	Attribute Name	Content 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 an summary as 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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [01]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Attribute content length [L2]
	0x14	20	2 bytes	Attribute content offset [02]
	0x16	22	2 bytes	Padding
[01]+	0x00	0	[L1] * 2	Stream name (UNICODE)
[02]+	0x00	0	8 bytes	Creation timestamp
	0x08	8	8 bytes	Last modified timestamp
	0x10	16	8 bytes	$MFT modified timestamp
	0x18	24	8 bytes	Last accessed timestamp
	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	8 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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [O1]
	0x0C	12	4 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Attribute content length [L2]
	0x14	20	2 bytes	Attribute content offset [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream name (UNICODE)
[O2]+	0x00	0	6 bytes	Parent directory $MFT record number
	0x06	6	2 bytes	Parent directory sequence number
	0x08	8	8 bytes	Creation timestamp
	0x10	16	8 bytes	Last modified timestamp
	0x18	24	8 bytes	$MFT modified timestamp
	0x20	32	8 bytes	Last accessed timestamp
	0x28	40	8 bytes	Index allocated length
	0x30	48	8 bytes	Index actual length
	0x38	56	4 bytes	Flags
	0x3C	60	4 bytes	Reparse value
	0x40	64	1 bytes	Filename unicode character length [L3]
	0x41	65	1 bytes	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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [O1]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Attribute content length [L2]
	0x14	20	2 bytes	Attribute content offset [O2]
	0x16	22	2 bytes	Padding
[O1]+	0x00	0	[L1] * 2	Stream name (UNICODE)
[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.

DATA INTERPRETER
Available on the App Store

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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [01]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	8 bytes	Runlist starting VCN
	0x18	24	8 bytes	Runlist ending VCN
	0x20	32	2 bytes	Runlist offset [02]
	0x22	34	2 bytes	Compression unit [2]
	0x24	36	4 bytes	Padding
	0x28	40	8 bytes	Attribute content allocated length
	0x30	48	8 bytes	Attribute content actual length
	0x38	56	8 bytes	Attribute content initialized length
	0x40	64	8 bytes	Attribute content compressed length
[01]+	0x00	0	[L1] *2	Stream name (UNICODE)
[02]+	0x00	0	Variable	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 if 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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [01]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	4 bytes	Attribute content length [L2]
	0x14	20	2 bytes	Attribute content offset [02]
	0x16	22	2 bytes	Padding
[01]+	0x00	0	[L1] *2	Stream name (UNICODE)
[02]+	0x00	0	4 bytes	Indexed attribute type
	0x04	4	4 bytes	Collation sorting rule
	0x08	8	4 bytes	Index record length
	0x0C	12	1 bytes	Index record cluster length
	0x0D	13	3 bytes	Padding
[02]+ 0x10+	0x00	0	4 bytes	Index node relative offset [03]
	0x04	4	4 bytes	Index node length [L3]
	0x08	8	4 bytes	Index node allocation length
	0x0C	12	4 bytes	Flags
[02]+ 0x10+ [03]+	0x00	0	[L3]	Index root node (See Node Breakdown, page 19)

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	Attribute length
	0x08	8	1 bytes	Resident / non-resident flag [1]
	0x09	9	1 bytes	Stream name unicode char length [L1]
	0x0A	10	2 bytes	Stream name offset [01]
	0x0C	12	2 bytes	Flags
	0x0E	14	2 bytes	Attribute identifier
0x00+	0x10	16	8 bytes	Runlist starting VCN
	0x18	24	8 bytes	Runlist ending VCN
	0x20	32	2 bytes	Runlist offset [02]
	0x22	34	2 bytes	Compression unit [2]
	0x24	36	4 bytes	Padding
	0x28	40	8 bytes	Attribute content allocated length
	0x30	48	8 bytes	Attribute content actual length
	0x38	56	8 bytes	Attribute content initialized length
	0x40	64	8 bytes	Attribute content compressed length
[01]+	0x00	0	[L1] *2	Stream name (UNICODE)
[02]+	0x00	0	Variable	Runlist of clusters containing the non-resident data (i.e. INDX records)

1 Of bits ranging from 0 to 7, bit 0 set to 1 denotes non-resident. Bits 1 through 7 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] "INDX" (ASCII)
	0x04	4	2 bytes	Fixup array offset [01]
	0x05	6	2 bytes	Fixup array entry count [L1]
	0x08	8	8 bytes	Update sequence number (USN)
0x00+	0x10	16	8 bytes	Index allocation VCN
0x18+	0x00	0	4 bytes	Index node relative offset [02]
	0x04	4	4 bytes	Index node length [L2]
	0x08	8	4 bytes	Index node allocation length
	0x0C	12	4 bytes	Flags
[01]+	0x00	0	[L1]	Fixup array
0x18+ [02]+	0x00	0	[L2]	Index Node (See Node breakdown, page 19)

Note: The last two bytes of each sector in an Index "INDX" Record are to 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 [01]
	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)
[01]+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length [02]
	0x0A	10	2 bytes	Index data length [L2]
	0x0C	12	2 bytes	Flags [1]
[01]+	0x10	16	[L2]	Index entry data [2] (ie. Filename attribute body)
[01]+ [02]+	0x00	0	8 bytes	$MFT reference number
	0x08	8	2 bytes	Index entry length [03]
	0x0A	10	2 bytes	Index data length [L3]
	0x0C	12	2 bytes	Flags [1]
[01]+ [02]+	0x10	16	[L3]	Index entry data [2] (ie. Filename attribute body)
[01]+ [02]+ [03]+	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]

Note: 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/Tail

- UNAUTHORISED REPRODUCTION PROHIBITED -

FAT12/FAT16 - Volume Boot Record (VBR)

Offset Hex	Offset	Length	Field Name and Definition
0x00	0	3 bytes	JMP instructions
0x03	3	8 bytes	OEM ID eg. ["MSWIN4.1"] (ASCII)
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 bytes	Sectors per cluster
0x0E	14	2 bytes	Reserved sector count
0x10	16	1 bytes	File allocation table (FAT) count eg. 2
0x11	17	2 bytes	Root directory entries
0x13	19	2 bytes	Total sector count
0x15	21	1 bytes	Media descriptor
0x16	22	2 bytes	File allocation table (FAT) sector count
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sector count
0x20	32	4 bytes	Total sector count
0x24	36	1 bytes	Bios drive number
0x25	37	1 bytes	Reserved
0x26	38	1 bytes	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 - Volume Boot Record (VBR)

Offset Hex	Offset Dec	Length	Field Name and Definition
0x00	0	3 bytes	JMP instructions
0x03	3	8 bytes	OEM ID eg. ["MSWIN4.1"] (ASCII)
0x0B	11	2 bytes	Bytes per sector
0x0D	13	1 byte	Sectors per cluster
0x0E	14	2 bytes	Reserved sector count
0x10	16	1 byte	File allocation table (FAT) count eg. 2
0x11	17	2 bytes	Root directory entries
0x13	19	2 bytes	Total sector count
0x15	21	1 byte	Media descriptor
0x16	22	2 bytes	File allocation table (FAT) sector count
0x18	24	2 bytes	Sectors per track
0x1A	26	2 bytes	Number of heads
0x1C	28	4 bytes	Hidden sector count
0x20	32	4 bytes	Total sector count
0x24	36	4 bytes	File allocation table (FAT) sector count
0x28	40	2 bytes	Extended flags
0x2A	42	2 bytes	FAT version
0x2C	44	4 bytes	Root directory starting cluster offset
0x30	48	2 bytes	File system information sector
0x32	50	2 bytes	Backup boot sector, sector offset
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 Expansion of BPB

UNAUTHORISED REPRODUCTION PROHIBITED

FAT - Short/Long File Name Directory Entries

Offset Hex	Offset Dec	Length	Field Name and Definition
			Short File Name Directory Entry
0x00	0	11 bytes	File/folder name and extension (ASCII) [1]
0x0B	11	1 byte	File/folder attributes (See "Entry Attributes" table below)
0x0C	12	1 byte	Reserved for Windows NT
0x0D	13	1 byte	Creation time (10ths of seconds)
0x0E	14	4 bytes	Creation timestamp (DOSTIME + DOSDATE) [2]
0x12	18	2 bytes	Last accessed date (no time) (DOSDATE)
0x14	20	2 bytes	Starting cluster, cluster offset (high word) [3]
0x16	22	4 bytes	Modification timestamp (DOSTIME + DOSDATE) [2]
0x1A	26	2 bytes	Starting cluster, cluster offset (low word)
0x1C	28	4 bytes	File size
			Long File Name Directory (LFN) Entry
0x00	0	1 bytes	LFN signature (See "LFN Signature" table below)
0x01	1	10 bytes	LFN text, characters 0 through 4 (UNICODE)
0x0B	11	1 bytes	File/folder attributes (See "Entry Attributes" table below)
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)

1 Of the 11 bytes, 8 bytes are reserved for the file name and 3 bytes for the file extension.

2 Of the 4 bytes, 2 bytes are reserved for the time and 2 bytes for the date. See breakdown below.

3 The starting cluster value is calculated by combining the high and low words.

LFN Signature	
Bit	**Description**
0-5	Sequence number
6	Last LFN entry
7	Deleted LFN

Entry Attributes	
Bit	**Description**
0	Read Only
1	Hidden
2	System
3	Volume label
4	Directory
5	Archive

Date and Time	
Bit	**Description**
0-4	Seconds x2
5-10	Minutes
11-15	Hours
16-20	Day
21-24	Month
25-31	Year (+1980)

- UNAUTHORISED REPRODUCTION PROHIBITED -

exFAT - Volume Boot Record (VBR)

Offset Hex	Offset Dec	Length	Field Name and Definition
0x00	0	3 bytes	JMP instructions
0x03	3	8 bytes	OEM ID eg. ["EXFAT "] (ASCII)
0x0B	11	25 bytes	Placeholder - BIOS Parameter Block (BPB)
0x24	36	28 bytes	Placeholder - FAT32 Expansion of BPB
0x40	64	8 bytes	Volume sector offset (from MBR)
0x48	72	8 bytes	Volume sector count
0x50	80	4 bytes	FAT sector offset (from VBR)
0x54	84	4 bytes	FAT sector count
0x58	88	4 bytes	Cluster bitmap sector offset (from VBR)
0x5C	92	4 bytes	Cluster bitmap cluster offset
0x60	96	4 bytes	Root directory cluster offset (from VBR)
0x64	100	4 bytes	Volume serial number
0x68	104	2 bytes	exFAT version (VV.mm)
0x6A	106	2 bytes	Volume flags[1]
0x6C	108	1 byte	Bytes per sector, as a power of 2
0x6D	109	1 byte	Sectors per cluster, as a power of 2
0x6E	110	1 byte	File allocation table (FAT) count eg. 2
0x6F	111	1 byte	Drive select, used by INT 13, typically 0x80
0x70	112	1 byte	Data area usage percentage, 0xff - not available
0x71	113	7 bytes	Reserved
0x78	120	390 bytes	Boot code
0x1FE	510	2 bytes	Signature [55 AA]

1 Of bits ranging from 0 to 15, bit 0's value indicates the active FAT (0 = first, 1 = second). Bit 1 set indicates a dirty volume. Bit 2 set indicates media failure. Bits 4 through 7 are currently unused.

BIOS Parameter Block (BPB) | FAT32 Expansion of BPB

UNAUTHORISED REPRODUCTION PROHIBITED

exFAT - Records 1/2

Offset Hex	Offset Dec	Length	Field Name and Definition
			File Attributes Record
0x00	0	1 bytes	Record type (0x85, 0x05 if unallocated) [1]
0x01	1	1 bytes	Number of 32 byte records in the entry
0x02	2	2 bytes	Checksum
0x04	4	2 bytes	File attributes [2]
0x06	6	2 bytes	Reserved
0x08	8	4 bytes	Created timestamp (DOSTIME + DOSDATE) [3]
0x0C	12	4 bytes	Last access timestamp (DOSTIME + DOSDATE) [3]
0x10	16	4 bytes	Last modified timestamp (DOSTIME + DOSDATE) [3]
0x14	20	1 bytes	Created 10ms value
0x15	21	1 bytes	Last modified 10ms value
0x16	22	1 bytes	Created timezone value
0x17	23	1 bytes	Last modified timezone value
0x18	24	1 bytes	Last accessed timezone value
0x19	25	7 bytes	Reserved
			Data Stream Record
0x00	0	1 bytes	Record type (0xC0, 0x40 if unallocated) [1]
0x01	1	1 bytes	Secondary flags [4]
0x02	2	1 bytes	Reserved
0x03	3	1 bytes	Name length
0x04	4	2 bytes	Name hash
0x06	6	2 bytes	Reserved
0x08	8	8 bytes	Valid data length
0x10	16	4 bytes	Reserved
0x14	20	4 bytes	Starting cluster offset
0x18	24	8 bytes	Length of file

1 Of bits ranging 0 to 7, bit 7 indicates the record is allocated.

2 exFAT attributes are identical to FAT attributes with the exception of bit 3. See FAT attributes.

3 exFAT dates and times are identical to FAT dates and times. 2 bytes for time followed by 2 bytes for date. See FAT dates and times.

4 Of bits ranging from 0 through 7, bit 0 set to 1 indicates "allocation possible".

- UNAUTHORISED REPRODUCTION PROHIBITED -

exFAT - Records 2/2

Offset Hex	Offset D	Length	Field Name and Definition
			File Name Extension Record
0x00	0	1 bytes	Record type (0xC1, 0x41 if unallocated) [1]
0x01	1	1 bytes	Secondary flags
0x02	2	30 bytes	File name (UNICODE)
			Volume Label Record
0x00	0	1 bytes	Record type (0x83, 0x03 if no volume label is set)
0x01	1	1 bytes	Volume label unicode character length (maximum 11)
0x02	2	22 bytes	Volume label (UNICODE)
0x18	24	8 bytes	Reserved
			Bitmap Record
0x00	0	1 bytes	Record type (0x81)
0x01	1	1 bytes	Bitmap flags (0=1st bitmap, 1=2nd bitmap)
0x02	2	18 bytes	Reserved
0x14	20	4 bytes	Starting cluster offset
0x18	24	8 bytes	Bitmap length
			Up-Case Table Record
0x00	0	1 bytes	Record type (0x82)
0x01	1	3 bytes	Reserved
0x04	4	4 bytes	Table checksum
0x08	8	12 bytes	Reserved
0x14	20	4 bytes	Starting cluster offset
0x18	24	8 bytes	Up-case table length
			GUID Record
0x00	0	1 bytes	Record type (0xA0)
0x01	1	1 bytes	Secondary count
0x02	2	2 bytes	Set checksum
0x04	4	2 bytes	Primary flags
0x06	6	16 bytes	Volume GUID
0x16	22	10 bytes	Reserved

1 Of bits ranging 0 to 7, bit 7 indicates the record is allocated.

- UNAUTHORISED REPRODUCTION PROHIBITED -

HFS+ - Volume Header

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	2 bytes	Signature [48 2B] "H+"
0x02	2	2 bytes	Version
0x04	4	4 bytes	Attribute flags
0x08	8	4 bytes	Last mounted version [48 46 53 4A] "HFSJ"
0x0C	12	4 bytes	Journal info block
0x10	16	4 bytes	Volume creation timestamp (MACTIME32) [1]
0x14	20	4 bytes	Volume last modified timestamp (MACTIME32)
0x18	24	4 bytes	Volume backup timestamp (MACTIME32)
0x1C	28	4 bytes	Volume checked timestamp (MACTIME32)
0x20	32	4 bytes	File count
0x24	36	4 bytes	Folder count
0x28	40	4 bytes	Allocation block size
0x2C	44	4 bytes	Allocation block total
0x30	48	4 bytes	Allocation block free
0x34	52	4 bytes	Next allocation
0x38	56	4 bytes	Resource clump size
0x3C	60	4 bytes	Data clump size
0x40	64	4 bytes	Next catalog node id
0x44	68	4 bytes	Write count
0x48	72	8 bytes	Encodings bitmap
0x50	80	32 bytes	Finder info
0x70	112	80 bytes	Fork data – Allocation file
0xC0	192	80 bytes	Fork data – Extents file
0x110	272	80 bytes	Fork data – Catalog file
0x160	352	80 bytes	Fork data – Attributes file
0x1B0	432	80 bytes	Fork data – Startup file

Note: Values within HFS and HFS+ file systems are stored in Big Endian byte order, unless otherwise stated.

1 From OSX 8.1 onwards, the volume creation timestamp stores the local time instead of UTC time.

- UNAUTHORISED REPRODUCTION PROHIBITED -

HFS+ - Catalog File/Folder Record

Offset Hex	Offset Dec	Length	Field Name and Definition
			Catalog File Record
0x00	0	2 bytes	Record type (0x02 for file record)
0x02	2	2 bytes	Flags
0x04	4	4 bytes	Reserved
0x08	8	4 bytes	File ID
0x0C	12	4 bytes	Created timestamp (MACTIME32)
0x10	16	4 bytes	Content modified timestamp (MACTIME32)
0x14	20	4 bytes	Attribute modified timestamp (MACTIME32)
0x18	24	4 bytes	Last accessed timestamp (MACTIME32)
0x1C	28	4 bytes	Backup timestamp (MACTIME32)
0x20	32	16 bytes	Permissions
0x30	48	16 bytes	File information
0x40	64	16 bytes	Extended file info
0x50	80	4 bytes	Text encoding
0x54	84	4 bytes	Reserved
			Catalog Folder Record
0x00	0	2 bytes	Record type (0x01 for folder record)
0x02	2	2 bytes	Flags
0x04	4	4 bytes	Valence
0x08	8	4 bytes	Folder ID
0x0C	12	4 bytes	Created timestamp (MACTIME32)
0x10	16	4 bytes	Content modified timestamp (MACTIME32)
0x14	20	4 bytes	Attribute modified timestamp (MACTIME32)
0x18	24	4 bytes	Last accessed timestamp (MACTIME32)
0x1C	28	4 bytes	Backup timestamp (MACTIME32)
0x20	32	16 bytes	Permissions
0x30	48	16 bytes	Folder information
0x40	64	16 bytes	Extended folder info
0x50	80	4 bytes	Text encoding
0x54	84	4 bytes	Reserved

- UNAUTHORISED REPRODUCTION PROHIBITED -

EXT2/3/4 - Super Block (Part 1/3)

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	4 bytes	Total inodes count
0x04	4	4 bytes	Total blocks count – low 32 bits [1]
0x08	8	4 bytes	Reserved blocks count – low 32 bits [1]
0x0C	12	4 bytes	Free blocks count – low 32 bits [1]
0x10	16	4 bytes	Free inodes count
0x14	20	4 bytes	First data block
0x18	24	4 bytes	Block size [2]
0x1C	28	4 bytes	Fragment size [2/3]
0x20	32	4 bytes	Blocks per group
0x24	36	4 bytes	Fragments per group [3]
0x28	40	4 bytes	Inodes per group
0x2C	44	4 bytes	Mount time (UNIXTIME32)
0x30	48	4 bytes	Write time stamp (UNIXTIME32)
0x34	52	2 bytes	Mount count
0x36	54	2 bytes	Maximal mount count
0x38	56	2 bytes	Magic signature [53 EF]
0x3A	58	2 bytes	File system state [4]
0x3C	60	2 bytes	Error detection behaviour [5]
0x3E	62	2 bytes	Minor revision level
0x40	64	4 bytes	Last check time stamp (UNIXTIME32)
0x44	68	4 bytes	Max time between checks
0x48	72	4 bytes	Operating system [6]
0x4C	76	4 bytes	Revision level [7]

1 In EXT2/3, a stand-alone 32 bit field. In EXT4, the low 32 bits of a 64 bit field.

2 Raise the base value of 1024 to this value to calculate the size. Ex: 1024^0 = 32, 1024^1 = 2048.

3 These fields are obsolete in EXT4.

4 State values include: 1 = unmounted cleanly, 2 = errors detected.

5 In the event of an error: 1 = continue, 2 = remount readonly, 3 = panic.

6 Operating system values include: 0 = Linux, 1 = Hurd, 2 = Masix, 3 = FreeBSD, 4 = Lites.

7 Revision level values include: 0 = original, 1 = version 2 with dynamic inode sizes.

EXT 2/4
EXT 3/4
EXT 4 Only

UNAUTHORISED REPRODUCTION PROHIBITED

EXT2/3/4 - Super Block (Part 2/3)

Offset		Length	Field Name and Definition
Hex	Dec		
0x50	80	2 bytes	Reserved blocks default UID [8]
0x52	82	2 bytes	Reserved blocks default GID [8]
0x54	84	4 bytes	First non-reserved inode
0x58	88	2 bytes	Size of inode structure
0x5A	90	2 bytes	Block group number of this superblock
0x5C	92	4 bytes	Compatible feature set [9]
0x60	96	4 bytes	Incompatible feature set [9]
0x64	100	4 bytes	Readonly-compatible feature set [9]
0x68	104	16 bytes	Volume UUID
0x78	120	16 bytes	Volume Name (ASCII)
0x88	136	64 bytes	Directory where last mounted
0xC8	200	4 bytes	Algorithm usage bitmap
0xCC	204	1 bytes	Pre-allocation blocks
0xCD	205	1 bytes	Pre-allocation directory blocks
0xCE	206	2 bytes	Reserved GDT blocks [10]
0xD0	208	16 bytes	Journal superblock UUID
0xE0	224	4 bytes	Journal file inode number
0xE4	228	4 bytes	Journal file device number
0xE8	232	4 bytes	Start of inode delete list
0xEC	236	16 bytes	HTREE hash seed
0xFC	252	1 bytes	Default hash version
0xFD	253	1 bytes	Journal backup type [11]
0xFE	254	2 bytes	Group descriptor size [11]
0x100	256	4 bytes	Mount options (default)
0x104	260	4 bytes	First metablock block group

8 A UID of 0 indicates the root user. A GID of 0 indicates root group.

9 Collection of bit flags which define the features of the file system. The complete list of feature flags is too large to include but is available at: www.lockandcode.com/resources/ext-feature-flags

10 Unused in EXT2 and classed as padding/alignment.

11 Unused in EXT3 and classed as padding/alignment.

EXT 2/4
EXT 3/4
EXT 4 Only

UNAUTHORISED REPRODUCTION PROHIBITED

EXT2/3/4 - Super Block (Part 3/3)

Offset		Length	Field Name and Definition
Hex	Dec		
0x108	264	4 bytes	File system creation timestamp (UNIXTIME32)
0x10C	268	68 bytes	Journal inode backup
0x150	336	4 bytes	Total blocks count – high 32 bits [8]
0x154	340	4 bytes	Reserved blocks count – high 32 bits [8]
0x158	344	4 bytes	Free blocks count – high 32 bits [8]
0x15C	348	2 bytes	Minimum inode data length
0x15E	350	2 bytes	New inode data reserved length
0x160	352	4 bytes	Miscellaneous flags ***
0x164	356	2 bytes	RAID stride
0x166	358	2 bytes	Multi-mount protection (MMP) update interval
0x168	360	8 bytes	Multi-mount protection (MMP) block
0x170	368	4 bytes	RAID stripe width
0x174	372	1 byte	Log groups per flex
0x175	373	1 bytes	Padding – Alignment
0x176	374	2 bytes	Padding – Alignment
0x178	376	8 bytes	Lifetime kilobytes written
0x180	384	4 bytes	Active snapshot inode number
0x184	388	4 bytes	Active snapshot sequential ID
0x188	392	8 bytes	Active snapshot reserved blocks
0x190	400	4 bytes	Snapshot list inode number
0x200	512	64 bytes	Mount options
0x240	576	4 bytes	Tracking inode for user quota
0x244	580	4 bytes	Tracking inode for group quota
0x248	584	4 bytes	File system blocks/clusters overhead
0x24C	588	436 bytes	Reserved

8 The high 32 bits of a 64 bit integer.

EXT 2/3/4
EXT 3/4
EXT 4 Only

UNAUTHORISED REPRODUCTION PROHIBITED

EXT2/3/4 - Inode

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	2 bytes	File mode eg. "drwxrwxrwx" [1]
0x02	2	2 bytes	Owner ID (UID) – low 16 bits
0x04	4	4 bytes	File size – lower 32 bits
0x08	8	4 bytes	Accessed timestamp (UNIXTIME32)
0x0C	12	4 bytes	Inode last changed timestamp (UNIXTIME32)
0x10	16	4 bytes	Last modified timestamp (UNIXTIME32)
0x14	20	4 bytes	Deletion timestamp (UNIXTIME32)
0x18	24	2 bytes	Group ID (GID) – low 16 bits
0x1A	26	2 bytes	Links count
0x1C	28	4 bytes	Blocks count – low 32 bits
0x20	32	4 bytes	File flags [1]
0x24	36	4 bytes	Version – low 32 bits
0x28	40	60 bytes	Pointers to blocks
0x64	100	4 bytes	NFS file version
0x68	104	4 bytes	File ACL – low 32 bits
0x6C	108	4 bytes	File size – high 32 bits
0x70	112	4 bytes	Fragment address (obsolete)
0x74	116	2 bytes	Blocks count – high 16 bits
0x76	118	2 bytes	File ACL – high 16 bits
0x78	120	2 bytes	Owner ID (UID) – high 16 bits
0x7A	122	2 bytes	Group ID (GID) – high 16 bits
0x7C	124	4 bytes	Reserved
0x80	128	2 bytes	Isize extra
0x82	130	2 bytes	Padding
0x84	132	4 bytes	Inode last changed timestamp extra
0x88	136	4 bytes	Last modified timestamp extra
0x8C	140	4 bytes	Accessed timestamp extra
0x90	144	4 bytes	File creation timestamp
0x94	148	4 bytes	File creation timestamp extra
0x98	152	4 bytes	Version – high 32 bits

EXT 2/3/4
EXT 3/4
EXT 4 Only

- UNAUTHORISED REPRODUCTION PROHIBITED -

1 Detailed breakdown of these values available at: www.lockandcode.com/resources/ext-inode-flags

WINDOWS REGISTRY - Hive Locations

Note:
In the below chart, the %WINDIR% variable represents the path to the Windows folder eg. "C:\Windows" and the %USERNAME% variable represents the name of the user's profile folder eg. "Administrator".

Windows 3.1, Windows 3.11	Windows 95, Windows 98, Windows ME	Windows NT	Windows 2000, Windows XP, Windows Server 2003	Windows Vista, Windows 7, Windows Server 2008	Windows 8, Windows Server 2012	Active Registry Hives and Paths	
■						REG.DAT	%WINDIR%
	■					SYSTEM.DAT	%WINDIR%
	■					USER.DAT	%WINDIR%
	■					USER.DAT	%WINDIR%\Profiles\%USERNAME% [1]
		■	■	■	■	SAM	%WINDIR%\system32\config
		■	■	■	■	SECURITY	%WINDIR%\system32\config
		■	■	■	■	SOFTWARE	%WINDIR%\system32\config
		■	■	■	■	SYSTEM	%WINDIR%\system32\config
		■				NTUSER.DAT	%WINDIR%\Profiles\%USERNAME%
			■			NTUSER.DAT	\Documents and Settings\%USERNAME%
				■	■	NTUSER.DAT	\Users\%USERNAME%
			■			UsrClass.dat	\Documents and Settings\%USERNAME%\Local Settings\Application Data\Microsoft\Windows
				■	■	UsrClass.dat	\Users\%USERNAME%\AppData\Local\Microsoft\Windows
				■	■	BCD	\Boot
					■	DRIVERS	%WINDIR%\System32\config
					■	AmCache.hve	%WINDIR%\AppCompat\Programs
						Backup Registry Hives and Paths	
	■					Rb00?.cab	%WINDIR%\SYSBCKUP
		■				*._ntuser.dat	%WINDIR%\Repair [3]
			■			[original names]	%WINDIR%\repair
				■		_REGISTRY_MACHINE_*	\System Volume Information_restore{GUID}\rp[nnn]
				■	■	[original names]	%WINDIR%\system32\config\RegBack

1 For multiuser installations of Windows 9x and Windows NT.

2 BCD may reside on the Recovery partition for Windows 7 & 8.

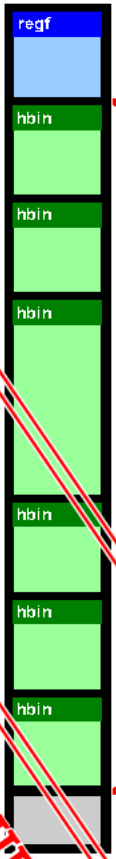
3 Windows NT backs up when/if the user runs `rdisk /s`

4 Windows Vista/7/8 utilise Volume Shadow Snapshot (VSS). Earlier revisions of hives can exist in VSS.

UNAUTHORISED REPRODUCTION PROHIBITED

WINDOWS REGISTRY - File Layout

Offset Hex	Offset Dec	Length	Field Name and Definition
			REGF Block
0x00	0	4 bytes	Signature [72 65 67 66] "regf"
0x04	4	4 bytes	1st sequence number [1]
0x08	8	4 bytes	2nd sequence number [1]
0x0C	12	8 bytes	Modified timestamp (FILETIME)
0x14	20	4 bytes	Registry major version
0x18	24	4 bytes	Registry minor version
0x1C	28	4 bytes	Registry hive type [2]
0x20	32	4 bytes	Undocumented
0x24	36	4 bytes	Root key offset [3]
0x28	40	4 bytes	HBIN region length
0x2C	44	4 bytes	Undocumented
0x30	48	460 bytes	Unused space
0x1FC	508	4 bytes	Checksum
			HBIN Block
0x00	0	4 bytes	Signature [68 62 69 6E] "hbin"
0x04	4	4 bytes	HBIN block offset [3]
0x08	8	4 bytes	HBIN block length [L1]
0x0C	12	4 bytes	Undocumented
0x10	16	4 bytes	Undocumented
0x14	20	8 bytes	HBIN timestamp (FILETIME) [4]
0x1C	28	4 bytes	Undocumented
0x20	32	[L1] - 32 bytes	Records area



* As illustrated, the HBIN region is comprised of multiple HBIN blocks. It commences at offset 0x1000 (4096). The byte length of each HBIN block is always a multiple of 0x1000 (4096). eg. 0x1000, 0x2000.

1 Sequence numbers are incremented over time. Matching values indicate synchronisation.

2 A value of 0x00000000 indicates a normal registry hive.

3 Offset is relative to the start of the HBIN region. i.e. offset 0x1000.

4 Only the first HBIN block of the HBIN region contains a timestamp.

- UNAUTHORISED REPRODUCTION PROHIBITED -

WINDOWS REGISTRY - Key Record

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	4 bytes	Record length [1]
0x04	4	2 bytes	Signature [6E 6B] "nk"
0x06	6	2 bytes	Flags (see flags table below)
0x08	8	8 bytes	Key last modified timestamp (FILETIME)
0x10	16	4 bytes	Virtualisation reference
0x14	20	4 bytes	Parent key record offset [2]
0x18	24	4 bytes	Subkey count
0x1C	28	4 bytes	Volitile subkey count
0x20	32	4 bytes	Subkey-list offset [2]
0x24	36	4 bytes	Volitile subkey reference
0x28	40	4 bytes	Value record count
0x2C	44	4 bytes	Value-list offset [2]
0x30	48	4 bytes	Security key offset [2]
0x34	52	4 bytes	Class name offset
0x38	56	4 bytes	Subkey name buffer length [3]
0x3C	60	4 bytes	Class name buffer length [3]
0x40	64	4 bytes	Value name buffer length [3]
0x44	68	4 bytes	Value data buffer length [3]
0x4C	76	2 bytes	Key name length [illegible]
0x4E	78	2 bytes	Class name length
0x50	80	[illegible] bytes	Key name (ASCII)

1 Signed integer whose absolute value is the length of the record. Positive values are unallocated and negative are allocated.

2 Offset is relative to the start of the HBIN region.

3 The length of the buffer required to store the corresponding value component's data. E.g. Value name buffer length equals the space required to store the longest value name contained within the key.

Flag values - Key		
Bit	Mask	Description
0	0x01	Key is volatile
1	0x02	Mount point
2	0x04	Root key
3	0x08	Key cannot be deleted
4	0x10	Symlink key
5	0x20	Key name is in ASCII
6	0x40	Predefined handle

-UNAUTHORISED REPRODUCTION PROHIBITED-

WINDOWS REGISTRY - Value Record

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	4 bytes	Record length
0x04	4	2 bytes	Signature [76 6B] "vk"
0x06	6	2 bytes	Value name length [L1]
0x08	8	4 bytes	Data length
0x0C	12	4 bytes	Data offset [2]
0x10	16	4 bytes	Data value type (see data type table)
0x14	20	2 bytes	Flags [3]
0x16	22	2 bytes	Padding
0x18	24	[L1] bytes	Value name

1 Signed integer whose absolute value is the length of the record. Positive values are unallocated and negative are allocated.

2 This value is typically the offset to the value data. However, when the data is extremely small ie. <= 4 bytes, the data itself is stored in this location instead of the offset to the data. Also, when the data is extremely large this value is an offset to a "big data" or "db" record which consists of an array of offsets to the actual value data. All offsets are relative to the start of the HBIN region.

3 Of bits 1 to 15, bit 0 set to 1 indicates an ASCII value name.

Data Types		
Value	Microsoft Constant Name	Description
0x00	REG_NONE	Undefined, handled as REG_BINARY
0x01	REG_SZ	UTF-16 little endian string
0x02	REG_EXPAND_SZ	REG_SZ supporting env. variables
0x03	REG_BINARY	Raw data displayed in hexadecimal
0x04	REG_DWORD	32-bit little endian integer
0x05	REG_DWORD_BIG_ENDIAN	32-bit big endian integer
0x06	REG_LINK	Symbolic link
0x07	REG_MULTI_SZ	Multiple REG_SZ separated by 00
0x0B	REG_QWORD	64-bit little endian integer

- UNAUTHORISED REPRODUCTION PROHIBITED -

INTERNET EXPLORER - Database Locations

Table 1

Operating System	Windows "Local Settings" location
2000 / XP	%userprofile%\Local Settings\
Vista / 7 / 8	%userprofile%\AppData\Local\Microsoft\Windows\

Table 2

IE Version	Subfolder	Filename
IE9 and under or IE10 upgrade [2]	.\History\History.IE5 [2] .\History\History.low\History.IE5 [1 2] .\Temporary Internet Files\Content.IE5 .\Temporary Internet Files\Low\Content.IE5 [1]	index.dat
IE10	.\WebCache	WebCacheV01.dat (Windows 7) WebCacheV24.dat (Windows 8)

Note: The location where Windows stores Local Settings (including browser artifacts) depends on the version of Windows. Determine this using Table 1.
The location and type of database files (index.dat or WebCacheV*.dat) depends on the version of Internet Explorer (IE). Determine this using Table 2.

1 When User Access Control (UAC) is active, "Low" folders are created.

2 Upgrading to IE10 from an earlier version will result in the index.dat database format being preserved.

3 The "History.IE5" folder will also contain subfolders each with their own "HEX.DAT" file. These relate to either daily or weekly history. The exact period is encoded into the subfolder name (e.g. "MSHist01yyyymmddyyyymmdd").

Windows Version	IE 5	IE 6	IE 7	IE 8	IE 9	IE 10 / 11
Windows 2000	✓	✓				
Windows XP		✓	✓	✓		
Windows VISTA			✓	✓	✓	
Windows 7				✓	✓	✓
Windows 8						✓

- UNAUTHORISED REPRODUCTION PROHIBITED -

INTERNET EXPLORER - INDEX.DAT Header

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	28 bytes	Signature ["Client UrlCache MMF Ver #.#"]
0x1C	28	4 bytes	Index.dat file size
0x20	32	4 bytes	First hash table offset [1]
0x24	36	4 bytes	Total block count [2]
0x28	40	4 bytes	Allocated block count [2]
0x2C	44	4 bytes	Padding
0x30	48	8 bytes	Cache size (quota) limit of container
0x38	56	8 bytes	Cache size of the container
0x40	64	8 bytes	Non-releasable cache size of the container
0x48	72	4 bytes	Cache directory count [3]
0x4C	76	4 bytes	Directory 0: File count
0x50	80	8 bytes	Directory 0: Directory name (ASCII)
0x58	88	4 bytes	Directory 1: File count
0x5C	92	8 bytes	Directory 1: Directory name (ASCII)
0x64	100	4 bytes	Directory 2: File count
0x68	104	8 bytes	Directory 2: Directory name (ASCII)
0x70	112	4 bytes	Directory 3: File count
0x74	116	8 bytes	Directory 3: Directory name (ASCII)
0x7C	124	4 bytes	Directory 4: File count
0x80	128	8 bytes	Directory 4: Directory name (ASCII)
0x88	136	4 bytes	Directory 5: File count
0x8C	140	8 bytes	Directory 5: Directory name (ASCII)
0x94	148	4 bytes	Directory 6: File count
0x98	152	8 bytes	Directory 6: Directory name (ASCII)
0xA0	160	4 bytes	Directory 7: File count
0xA4	164	8 bytes	Directory 7: Directory name (ASCII)

1 Hash tables exist within INDEX.DAT files to facilitate faster lookups of records. The hash tables can be used as an index to locate individual records within the INDEX.DAT file.

2 From offset 0x4000 (16384) onwards, the INDEX.DAT file is broken into 128 byte blocks. Blocks containing records are classed as allocated.

3 Describes how many directories are present for storing cache. A 4 byte file count and 8 byte directory name for each will follow. The table above illustrates a value of "8" for the directory count.

UNAUTHORISED REPRODUCTION PROHIBITED

INTERNET EXPLORER - URL Record

Offset Hex	Offset Dec	Length	Field Name and Definition
0x00	0	4 bytes	Signature [55 52 4C 20] "URL " [1]
0x04	4	4 bytes	Record block count (x 128 = record length)
0x08	8	8 bytes	Date 1 (FILETIME) [2]
0x10	16	8 bytes	Date 2 (FILETIME) [2]
0x18	24	8 bytes	Date 3 (DOSTIME) [2]
0x20	32	4 bytes	File Size
0x34	52	4 bytes	String 1 offset [01]
0x38	56	1 bytes	Cache directory ordinal index number [3]
0x39	57	3 bytes	Padding
0x3C	60	4 bytes	String 2 offset [02]
0x40	64	4 bytes	Cache entry flags
0x44	68	4 bytes	Data offset [03]
0x48	72	4 bytes	Data length [L3]
0x50	80	4 bytes	Date 4 (DOSTIME) [2]
0x54	84	4 bytes	Hit count
0x5C	92	4 bytes	Cookie "expired" timestamp (DOSTIME) [4]
[01]	-	Null term.	String 1 (ASCII)
[02]	-	Null term.	String 2 (ASCII)
[03]	-	[L3] bytes	Data - HTTP headers, etc.

1 Other record type signatures include "REDR", "LEAK" and "FILE".

2 The exact definition of this field varies depending on the type of INDEX.DAT file. See table below.

3 Will correspond with a directory name and file count in the INDEX.DAT header.

4 A valid date is only present in entry records of Cookie INDEX.DAT files.

	Cache	History Global	History Daily	History Weekly	Cookies
Date 1	Server Modified	Last Visited	Last Visited [5]	Last Visited [5]	Modified
Date 2	Last Checked	Last Visited	Last Visited	File Created	Last Accessed
Date 3	Expiry Date	Expiry Date	Expiry Date	Expiry Date	Expiry Date
Date 4	Last Accessed	Last Visited	Last Visited	File Created	Last Accessed
String 1	File URL	Visited:URL	[Date]:URL	:[DATE]:URL	Cookie:URL
String 2	Cached Filename	Title Bar	<unused>	<unused>	Cookie Filename

5 Dates and times are stored in local time. Where not explicitly stated, dates appear in UTC time.

-UNAUTHORISED REPRODUCTION PROHIBITED-

WINDOWS ARTIFACTS - File Locations

Windows 95, Windows 98, Windows ME
Windows NT
Windows 2000
Windows XP, Windows Server 2003
Windows Vista, Windows 7, Windows Server 2008
Windows 8, Windows Server 2012

Note:
In the below chart, the %WINDIR% variable represents the path to the Windows folder eg. "C:\Windows" and the %USERPROFILE% variable represents the path to the user's profile folder eg. "C:\Users\Administrator".

Filename	Paths
Event Logs	
*.evt	%WINDIR%\system32\config
*.evtx	%WINDIR%\system32\winevt\Logs
Jump Lists	
*.automaticDestinations-ms	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\AutomaticDestinations
*.customDestinations-ms	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\CustomDestinations
Prefetch	
*.pf	%WINDIR%\Prefetch
Recent Documents	
*.lnk	%WINDIR%\Recent
*.lnk	%USERPROFILE%\Recent
*.lnk	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
Recycle Bin	
INFO2	\Recycled
INFO	\RECYCLER\{GUID}
INFO2	\RECYCLER\{GUID}
$I[file-id].[ext] [2]	\$Recycle.Bin\{GUID}
ThumbCache	
thumbcache_[size].db [3]	%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

1 INFO and INFO2 files contain records for all recycle bin entries, whereas a $I file exists for each entry.

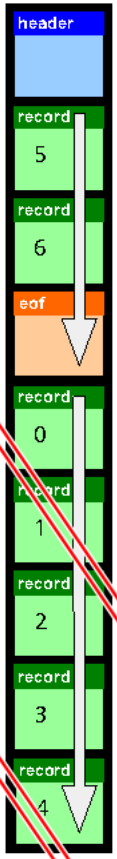
2 The [file-id] string is 6 characters in length and is comprised of characters within the range of A to Z and 0 to 9. It is generated to uniquely identify a file when transferred to the recycle bin.

3 The [size] is either "32", "96", "256" or "1024". For example, "thumbcache_1024.db".

- UNAUTHORISED REPRODUCTION PROHIBITED -

EVENT LOGS (EVT) - Header & EOF Records

Offset Hex	Offset Dec	Length	Field Name and Definition
			Header Record
0x00	0	4 bytes	Header record length [1]
0x04	4	4 bytes	Signature [4C 66 4C 65] "LfLe"
0x08	8	4 bytes	Major version
0x0C	12	4 bytes	Minor version
0x10	16	4 bytes	First record offset
0x14	20	4 bytes	EOF entry offset
0x18	24	4 bytes	Current record number
0x1C	28	4 bytes	Oldest record number
0x20	32	4 bytes	Maximum file length
0x24	36	4 bytes	Flags [2]
0x28	40	4 bytes	Retention
0x2C	44	4 bytes	Header record length [1]
			EOF Record
0x00	0	4 bytes	EOF record length [1]
0x04	4	4 bytes	Signature [11 11 11 11]
0x08	8	4 bytes	Signature [22 22 22 22]
0x0C	12	4 bytes	Signature [33 33 33 33]
0x10	16	4 bytes	Signature [44 44 44 44]
0x14	20	4 bytes	First record offset
0x18	24	4 bytes	EOF entry offset
0x1C	28	4 bytes	Current record number
0x20	32	4 bytes	Oldest record number
0x24	36	4 bytes	EOF record length [1]



Note: The .evt event log format is used in Windows XP and earlier. Windows Vista/7 uses the .evtx format.

1 The record starts and finishes with a four byte value which contains the length of the record.

2 Bit 0 indicates the event log file has not been properly closed (dirty). Bit 1 indicates the event log has wrapped (see illustration). Bit 2 indicates an error has occurred due to insufficient space. Bit 3 indicates the file system archive flag for the event log file is set.

UNAUTHORISED REPRODUCTION PROHIBITED

Navigation Lock

EVENT LOGS (EVT) - Event Record

Offset		Length	Field Name and Definition
Hex	Dec		
0x00	0	4 bytes	Event record length [1]
0x04	4	4 bytes	Signature [4C 66 4C 65] "LfLe"
0x08	8	4 bytes	Record number
0x0C	12	4 bytes	Event generated timestamp (UNIXTIME32)
0x10	16	4 bytes	Event written timestamp (UNIXTIME32)
0x14	20	4 bytes	Event ID
0x18	24	2 bytes	Event type [2]
0x1A	26	2 bytes	Event strings count [C1]
0x1C	28	2 bytes	Event category
0x1E	30	2 bytes	Reserved flags (reserved)
0x20	32	4 bytes	Closing record number (reserved)
0x24	36	4 bytes	Event strings array offset [01]
0x28	40	4 bytes	User SID length [L2]
0x2C	44	4 bytes	User SID offset [02]
0x30	48	4 bytes	Data length [L3]
0x34	52	4 bytes	Data offset [03]
0x38	56	Variable	Source string (UNICODE)
		Variable	Computer name string (UNICODE) [3]
[02]		[L2] bytes	User SID
[01]		[03] – [01] bytes	Event strings array (UNICODE) [4]
[03]		[L3] bytes	Data (ASCII or UNICODE)
		Variable	Padding
		4 bytes	Event record length [1]

1 The record starts and finishes with a four byte value which contains the size of the record.

2 Event types: 0x1 = Error, 0x2 = Warning, 0x04 = Information, 0x8 = Success Audit, 0x10 = Failure Audit.

3 The "Computer name string" immediately follows the "Source string" terminating after the 0000.

4 If [C1] is greater than 0 an "Event strings array" will exist at offset [01] and contain [C1] UNICODE strings.

- UNAUTHORISED REPRODUCTION PROHIBITED -

PREFETCH (PF) - Header and File Layout

Offset Hex	Offset Dec	Length	Field Name and Definition
0x00	0	4 bytes	Version / revision [1]
0x04	4	4 bytes	Signature [53 43 43 41] "SCCA"
0x08	8	4 bytes	Undocumented [2]
0x0C	12	4 bytes	File length
0x10	16	60 bytes	Program name
0x4C	76	4 bytes	Prefetch hash [3]
0x54	84	4 bytes	Page index table offset
0x58	88	4 bytes	Page index table record count
0x5C	92	4 bytes	Page list table offset
0x60	96	4 bytes	Page list table length
0x64	100	4 bytes	String table offset
0x68	104	4 bytes	String table length
0x6C	108	4 bytes	Volume section offset
0x70	112	4 bytes	Volume section count
0x74	116	4 bytes	Volume section length
0x80*	128	8 bytes	Timestamp (FILETIME) [4]
0x98*	152	4 bytes	Run Count

1 For Vista/7 this value is set to 0x17. For XP this value is set to 0x11.

2 For Vista/7 this value is set to 0x11. For XP this value is set to 0x00.

3 The hash value is calculated using a specific algorithm based on the full path of the application (eg. C:\Windows\Notepad.exe). The hash value also appears appended to the prefetch file name immediately preceding the .pf extension to ensure filename uniqueness eg. NOTEPAD.EXE-C5670914.pf.

4 The date and time of the last time the application was executed.

* These offsets represent the locations within a Windows Vista or Windows 7 prefetch file. Under Windows XP, the timestamp is located at offset 0x78 and the Run Count is located at offset 0x90.

header

page idx

page list

string

volume

- UNAUTHORISED REPRODUCTION PROHIBITED -

RECYCLE BIN - INFO2 Format and $I/$R Format

Offset Hex	Offset Dec	Length	Field Name and Definition
			INFO2 File Header
0x00	0	4 bytes	INFO2 version eg. [05 00 00 00]
0x04	4	4 bytes	Allocated records
0x08	8	4 bytes	Total records [1]
0x0C	12	4 bytes	Record length [2]
0x10	16	4 bytes	Total logical size of all files [1]
			INFO2 Record
0x00	0	260 bytes	Filename and path (ASCII) [3]
0x104	260	4 bytes	Record index
0x108	264	4 bytes	Drive number of recycled file
0x10C	268	8 bytes	Recycled timestamp (FILETIME)
0x114	276	4 bytes	Physical file size of recycled file [4]
0x118	280	520 bytes	Filename and path (UNICODE) [5]

Note: INFO2 recycled name convention: [Drive Letter][Record Number].[Extension]

1 These values may not be present or may contain "0" instead, depending on version.

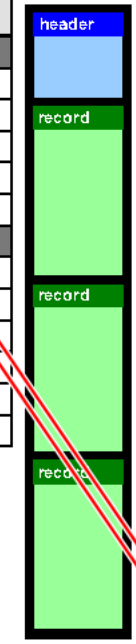
2 In order to correctly locate and parse INFO2 file records, the record length value is needed. File records begin at offset 0x14 and are "Record length" long in bytes.

3 Depending on the INFO2 version, operating system etc. the ASCII file path may contain RAM stack between the end of the filename and the end of the record.

4 The physical size of the recycled file is the number of clusters needed to store the file multiplied by the cluster size of the file system it resided on. Ie. "Size on disk".

5 The UNICODE file path is not present in earlier versions of the INFO2 format.

INFO2



Offset Hex	Offset Dec	Length	Field Name and Definition
			$I/$R File Header
0x00	0	8 bytes	Signature eg. [01 00 00 00 0[illegible] 00]
0x08	8	8 bytes	Logical file size of recycled file
0x10	16	8 bytes	Recycled timestamp (FILETIME)
0x18	24	520 bytes	Filename and path (UNICODE)

Note: $R recycled name convention: $R[6 Alphanumeric Characters].[Extension]

The $I/$R recycle bin format replaces the INFO2 format and is present in Windows Vista, Windows 7 and Windows Server 2008.

UNAUTHORISED REPRODUCTION PROHIBITED

DATES & TIMES

Name	Length	Properties
FILETIME	8 bytes [1]	Usage: NTFS, REG, IE, LNK, DBX, PST, WAB, PF Interval: 100 nanoseconds Range: 01 JAN 1601 00:00:00 [2] — 28 MAY 60056 05:36:10
SYSTEMTIME	16 bytes	Usage: REG Interval: 1 millisecond Range: 01 JAN 1601 00:00:00 [2] — 31 DEC 30827 23:59:59
MSDOS	4 bytes	Usage: FAT12/16/32, exFAT, IE, LNK, REG Interval: 2 seconds Range: 01 JAN 1980 00:00:00 [2] — 31 DEC 2107 23:59:58
HFS+	4 bytes	Usage: HFS+ File system, Apple products Interval: 1 second Range: 01 JAN 1904 00:00:00 [2] — 06 FEB 2040 06:28:15
UNIX32	4 bytes	Usage: EXT2/3, FS, Unix, Linux, EVT, Blackberry IPD Interval: 1 second Epoch: 01 JAN 1970 00:00:00 Range: 13 DEC 1901 20:45:52 — 19 JAN 2038 03:14:07
UNIX64	8 bytes	Usage: Unix, Linux Interval: 1 second Epoch: 01 JAN 1970 00:00:00 Range: ~293 billion years BC — ~293 billion years AD
WEBKIT	8 bytes [3]	Usage: Google Chrome, Safari Interval: 1 microsecond Epoch: 01 JAN 1601 00:00:00 Range: -292000 years from 1601 — 292000 years from 1601
PRTime	8 bytes [3]	Usage: Firefox Databases Interval: 1 microsecond Epoch: 01 JAN 1970 00:00:00 Range: -292000 years from 1970 — 292000 years from 1970

1 FILETIME can be found expressed as a pair of 32-bit integers ie. IE cookies.

2 The epoch date and time is the same as the minimum date and time.

3 WEBKIT and PRTime can be found expressed as a text string containing a 64-bit integer.

Note: The following abbreviations used above are defined as follows:
REG = Windows Registry, IE = Internet Explorer, LNK = Shortcut Files, PF = Prefetch Files
DBX = Outlook Express Email Archive, PST = Outlook Email Archive, WAB = Windows Address Book.

Note: The ranges above are calculated from the interval/epoch/bit-width. Upper or lower limits may apply.

-UNAUTHORISED REPRODUCTION PROHIBITED-

FILE SIGNATURES - Video, Graphics and Archive Formats

Video File Formats	
Adobe Flash Video [.flv]	Header: **46 4C 56 01** ASCII: FLV.
RIFF - Audio Video Interleave [.avi]	Header: **52 49 46 46 _ _ _ _ 41 56 49 20 4C 49 53 54** ASCII: RIFF....AVI LIST
Windows Media [.asf, .wma, .wmv]	Header: **30 26 B2 75 8E 66 CF 11 A6 D9 00 AA 00 62 CE 6C** ASCII: 0&²u.fÏ.¦Ù.ª.bÎl
MPEG-4 Video [.mp4]	Header: **00 00 00 18 66 74 79 70 33 67 70 35** ASCII: ftyp3gp5
MPEG Video [.mpeg, .mpg]	Header: **00 00 01 B_** Footer: **00 00 00 B7**
Ogg Vorbis [.oga, .ogg, .ogv, .ogx]	Header: **4F 67 67 53 00 02 00 00 00 00 00 00 00 00** ASCII: OggS.... ...
QuickTime Movie [.mov]	Header: **00 00 00 20 66 74 79 70 4D 34 41 20 00 00 00 00** ASCII: ....ftypM4A ..
Graphic File Formats	
Graphic Interchange Format [.gif]	Header: **47 49 46 38 37 61** or **47 49 46 38 39 61** ASCII: GIF87a or GIF89a
Portable Network Format [.png]	Header: **89 50 4E 47 0D 0A 1A 0A** ASCII: ‰PNG....
JPEG/JFIF [.jpg, .jpeg, .jfif]	Header: **FF D8 FF E0 _ _ 4A 46 49 46 00 00** Footer: **FF D9** ASCII: ÿØÿà..JFIF.
JPEG/EXIF [.jpg, .jpeg]	Header: **FF D8 FF E1 _ _ 45 78 69 66 00 00** Footer: **FF D9** ASCII: ÿØÿá..Exif..
Archive Formats	
7-Zip File [.7z]	Header: **37 7A BC AF 27 1C** ASCII: 7z¼¯'.
Microsoft Cabinet File [.cab]	Header: **4D 53 43 46** ASCII: MSCF
WinRar File [.rar]	Header: **52 61 72 21 1A 07 00** ASCII: Rar!..
Zip File [.zip]	Header: **50 4B 03 04** ASCII: PK..

- 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	DEC	OCT	HEX	BINARY	SYMBOL
64	100	40	01000000	@	96	140	60	01100000	`
65	101	41	01000001	A	97	141	61	01100001	a
66	102	42	01000010	B	98	142	62	01100010	b
67	103	43	01000011	C	99	143	63	01100011	c
68	104	44	01000100	D	100	144	64	01100100	d
69	105	45	01000101	E	101	145	65	01100101	e
70	106	46	01000110	F	102	146	66	01100110	f
71	107	47	01000111	G	103	147	67	01100111	g
72	110	48	01001000	H	104	150	68	01101000	h
73	111	49	01001001	I	105	151	69	01101001	i
74	112	4A	01001010	J	106	152	6A	01101010	j
75	113	4B	01001011	K	107	153	6B	01101011	k
76	114	4C	01001100	L	108	154	6C	01101100	l
77	115	4D	01001101	M	109	155	6D	01101101	m
78	116	4E	01001110	N	110	156	6E	01101110	n
79	117	4F	01001111	O	111	157	6F	01101111	o
80	120	50	01010000	P	112	160	70	01110000	p
81	121	51	01010001	Q	113	161	71	01110001	q
82	122	52	01010010	R	114	162	72	01110010	r
83	123	53	01010011	S	115	163	73	01110011	s
84	124	54	01010100	T	116	164	74	01110100	t
85	125	55	01010101	U	117	165	75	01110101	u
86	126	56	01010110	V	118	166	76	01110110	v
87	127	57	01010111	W	119	167	77	01110111	w
88	130	58	01011000	X	120	170	78	01111000	x
89	131	59	01011001	Y	121	171	79	01111001	y
90	132	5A	01011010	Z	122	172	7A	01111010	z
91	133	5B	01011011	[	123	173	7B	01111011	{
92	134	5C	01011100	\	124	174	7C	01111100	|
93	135	5D	01011101	]	125	175	7D	01111101	}
94	136	5E	01011110	^	126	176	7E	01111110	~
95	137	5F	01011111	_	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-

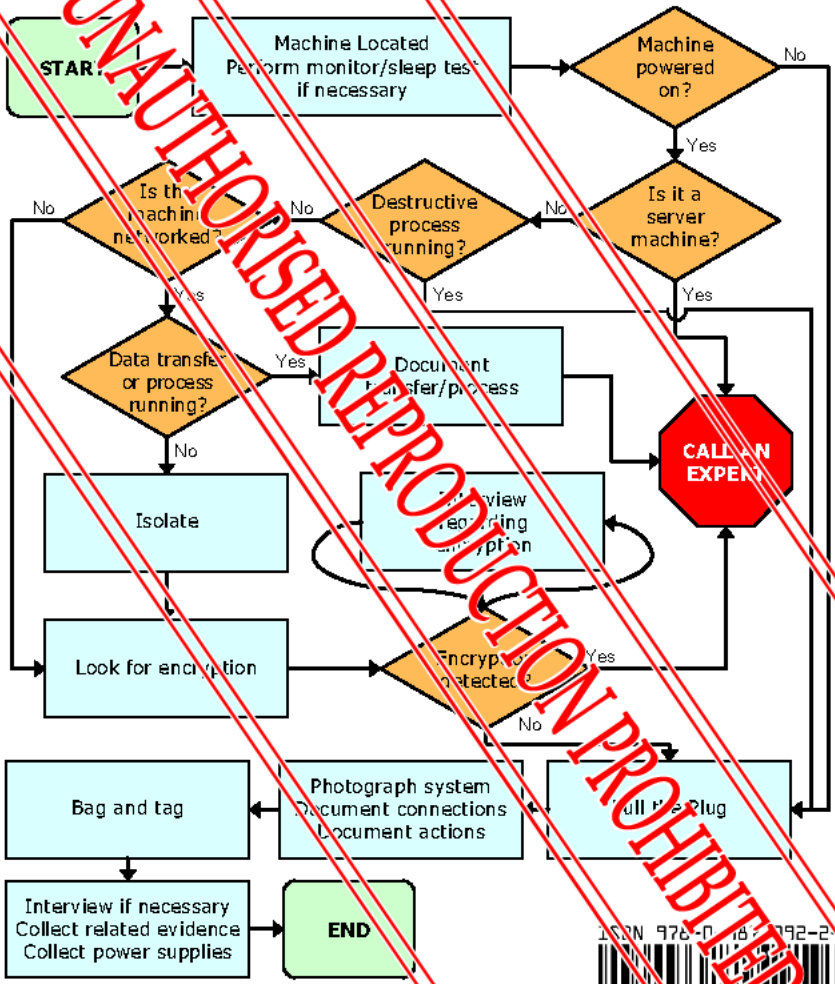
ASCII CHART - 192 to 255

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	º
197	305	C5	11000101	»
198	306	C6	11000110	¼
199	307	C7	11000111	½
200	310	C8	11001000	¾
201	311	C9	11001001	¿
202	312	CA	11001010	À
203	313	CB	11001011	Á
204	314	CC	11001100	Â
205	315	CD	11001101	Ã
206	316	CE	11001110	Ä
207	317	CF	11001111	Å
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-

FIRST RESPONDER - Evidence Seizure Triage Flowchart



UNAUTHORISED REPRODUCTION PROHIBITED

Copyright © 2012 International Association of Computer Investigative Specialists (IACIS®)
(Flowchart included with the permission of IACIS®)

ISBN 978-0-[illegible]-[illegible]792-2-[illegible]
9 780997 309 28