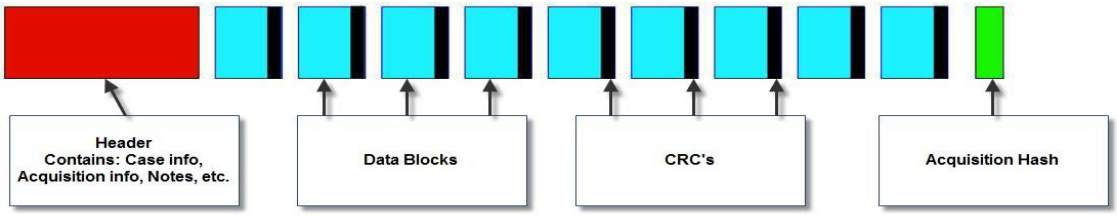
Cheat Sheet
August - 2023

Dec	Hex	Bin
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111



MD5: 128 bits	CRC: 32 bits	SHA1: 160 bits

File Signature Analysis - X-Ways

Signature	Extension	Comparison	Results
Listed	Listed	Match	Confirmed
Not Listed	Listed	Incorrect	Not Confirmed
Not Listed	Not Listed	N/A	Not in List
Listed	No Ext	N/A	Newly Identified
Listed	Listed	Incorrect	Mismatch Detected
Partially Overwritten / Broken			Irregular
File Size Less Than 8 Bytes			Irrelevant
Prior to Refine Volume Snapshot			Not Verified

Bit	Byte	Name	Binary
1	1/8	Bit	1
4	1/2	Nibble	0000
8	1	Byte	0000-0000

GREP Symbols

\uFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y or Z
[^XYZ]	Neither X nor Y nor Z
\[	Literal character
(ab)	Group ab together for ?, +, *, |
{m,n}	Repeat m to n times
a|b	Either a or b
^	Start of a file

Hexadecimal

8	4	2	1	8	4	2	1
0	0	0	0	0	0	0	0

Decimal

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0

File Systems	FAT	ExFAT	NTFS	MBR
1. Track the name of the file	DE	FNER / DE	$MFT	First sector
2. Track the starting cluster	DE	SER	$MFT	Ends in 55 AA
3. Track the fragmentation	FAT	$Bitmap	$MFT	Partition Table
4. Track the status of blocks	FAT	FAT	$Bitmap	64 Bytes in Total

A: to be archived, R: read-only
H: hidden, S: system
X: not indexed (in Windows)
P: NTFS reparse point
O: offline, T: temporary, I: has object ID
#: contents only partially initialized
~: sparse
C: compressed at filesystem level
c: compressed in archive
E: encrypted at filesystem level
e: encrypted in archive
e!: file type specific encryption/DRM
e?: high entropy, possibly fully encrypted
(Res): Resource fork
($EFS): encryption metadata
(INDX): index attribute
(ADS): alternate data stream
(EA): extended attribute
(SC): from volume shadow copy
Δ (delta): cloned with shared allocation (APFS)
(Jrnl): Inode in Ext journal
File mode: l=symlink, c=char. device, b=block device
t=sticky bit, s=socket, p=FIFO
Permissions: user read/write/exec., group rwx, other rwx
(SUID): Set User ID, (SGID): Set Group ID

CMD Commands for On Scene Investigations

What?	Command
Encryption	manage-bde -status
Recovery Key	manage-bde -protectors C: -get
Computer Name	hostname
Network Info	ipconfig /all
Windows Version	winver
Registry	regedit
WMIC	**Windows Management Instrumentation**
Turn it On / Off	wmic / exit
Options	/?
Groups	group list brief
Motherboard	baseboard
BIOS	bios
Boot Order	bootconfig
Win Install Date	os get installdate
Last Boot	os get lastbootuptime
Installed Software	product
Users	useraccount
All Volumes	volume