

Anderson Cheat Sheet August - 2025			Header Contains: Case info, Acquisition info, Notes, etc. Data Blocks CRC's Acquisition Hash			
Dec	Hex	Bin				
0	0	0000				
1	1	0001	MD5: 128 bits	CRC: 32 bits	SHA1: 160 bits	
2	2	0010	File Signature Analysis - X-Ways			
3	3	0011	Signature	Extension	Comparison	Results
4	4	0100	Listed	Listed	Match	Confirmed
5	5	0101	Not Listed	Listed	Incorrect	Not Confirmed
6	6	0110	Not Listed	Not Listed	N/A	Not in List
7	7	0111	Listed	No Ext	N/A	Newly Identified
8	8	1000	Listed	Listed	Incorrect	Mismatch Detected
9	9	1001	Partially Overwritten / Broken			Irregular
10	A	1010	File Size Less Than 8 Bytes			Insignificant
11	B	1011	Prior to Refine Volume Snapshot			Not Verified
12	C	1100	Bit	Byte	Name	Binary
13	D	1101	1	1/8	Bit	1
14	E	1110	4	1/2	Nibble	0000
15	F	1111	8	1	Byte	0000-0000
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
el: file type specific encryption/DRM
e?: high entropy, possibly fully encrypted
(Res): Resource fork
(SEFS): 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

Windows 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
Mac / Linux Terminal Commands	
Recent Logins	last
Network Info	netstat
Computer Name	hostname
X-Ways	Hot Keys / Shortcuts
Remove Sorting	Shift + Left Click on the Sorted Column
Sorting / Filtering	Control + H
General Options	F5
GREP Examples	
Browser Search:	/search\?.{5,50}
Email Address:	@.{3,15}\.[a-z]{3}
SSNs:	[^#][0-8]##[^\.\x20]([1-9#]) (0[1-9])[\.\x20]####[^#]

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