IT-Security (ITS) B1

DIKU, E2023

Today’s agenda

1: Forensics

Forensics defined

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found on digital devices

Applied in a **corporate**, **civil**, or **criminal** setting (originated in law enforcement)

Applied to a **security** investigation or **personnel** investigation

In security investigations, forensics either means a **root cause or impact analysis** of a cyber-attack, often post-mortem, **or simply techniques** used in the process of uncovering, understanding, and responding to a security incident

In security, **DFIRMA** = digital forensics + incident response + malware analysis

DFIRMA in practice

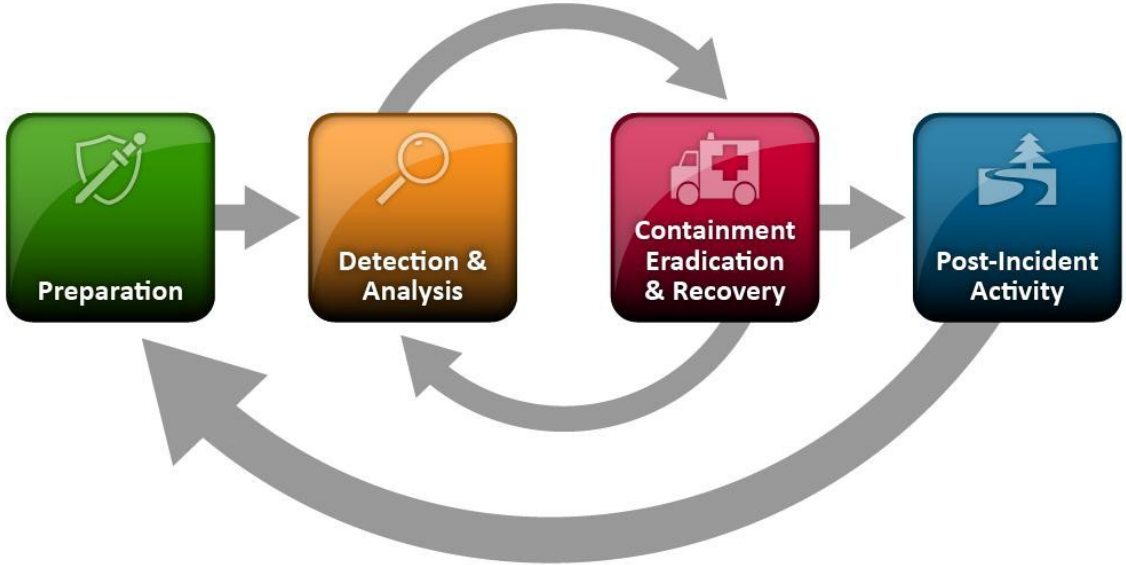
```
while true:
        intrusion analysis

        if intrusion suspected:
                preliminary analysis

                if intrusion verified:
                        repeat until incident fully contained:
                                forensic analysis
                                malware anaysis
                                incident response

        update plans
```

Recap: Intrusion detection



Many forms of forensics

Digital forensics =

- Computer forensics
- Memory forensics
- Network forensics
- Mobile forensics
- Etc. forensics

Memory forensics

Memory forensics

From Wikipedia:

“Memory forensics is forensic analysis of a computer's **memory dump**.

Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive.”

First, get a copy

Live acquisition

- Different techniques

Live analysis

- Direct analysis of the running kernel

Dead acquisition

- Hibernation files, page files

Virtualization - thank you

What to find in memory?

- Running processes
- Listening sockets
- Open connections
- Encryption keys
- Credentials
- Memory only malware
- Closed connections
- Terminated processes
- Open file handles
- Deobfuscated code

Memory forensic analysis process

1: Find rogue processes

2: Analyse DLLs

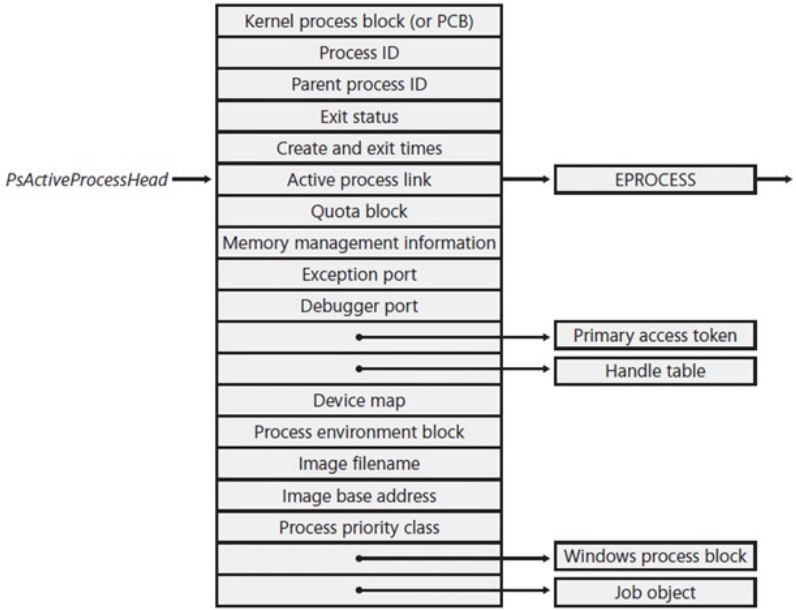
3: Review network artefacts

4: Look for evidence of code injections

5: Dump suspicious processes → further analysis

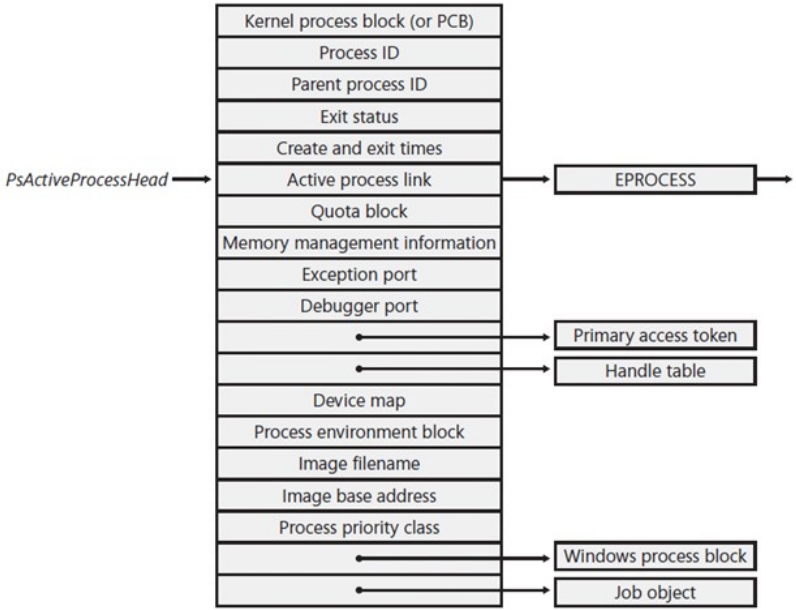
How to find processes (on Windows)

EPROCESS objects in memory:

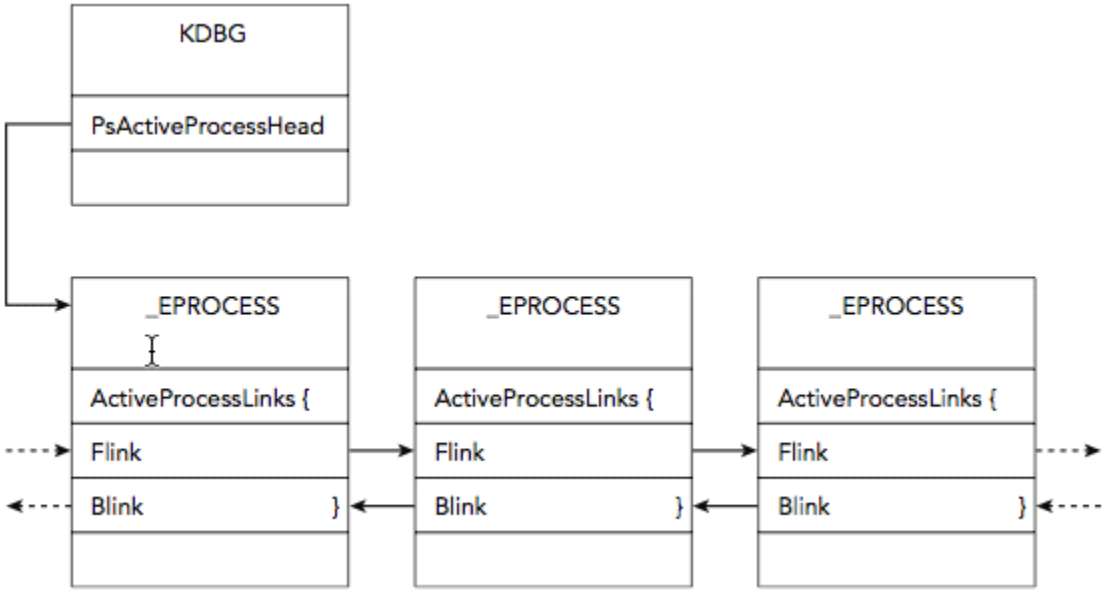


How to find processes (on Windows)

Scan for EPROCESS objects:



Process enumeration (on Windows)



Key concept in memory forensics:

Walking a list, or **scanning for objects**

Step 1 revisited: Find rogue processes

Those that:

Hide

Have odd parents

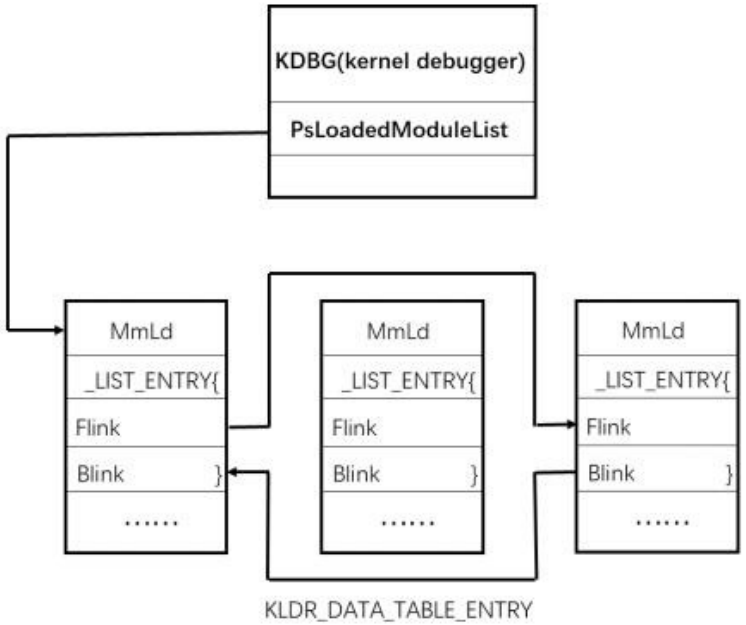
Do network comm but shouldn’t

Have unusually many handles open

Contain maliciously injected code

…

Direct kernel objection manipulation (DKOM)



Example:

Stuxnet

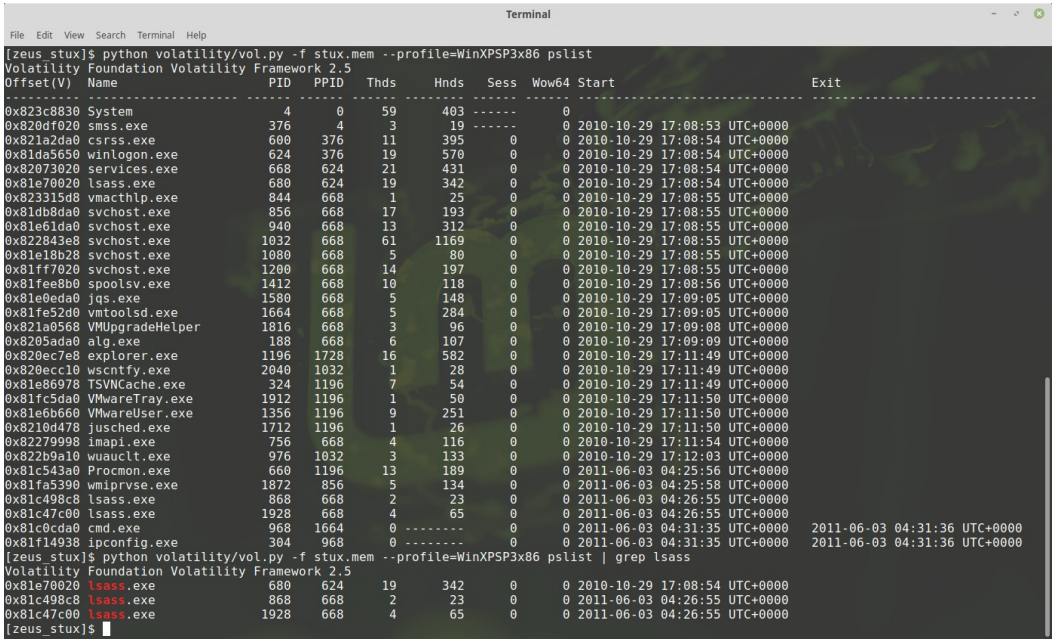
Stuxnet


DO WE HAVE A BACKUP?
Stuxnet VIRUS
CHAPPATTE
Int'l Herald Tribune

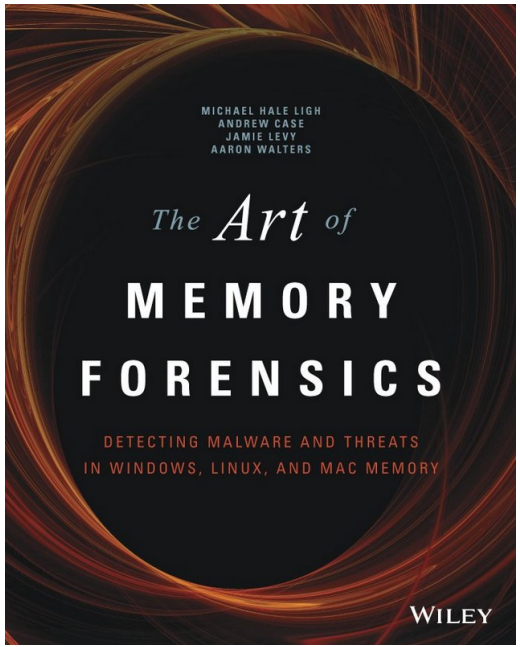
Stuxnet

Natanz Nuclear Facility in Iran

Volatility and Stuxnet



Further reading



Disk (or, file system) forensics

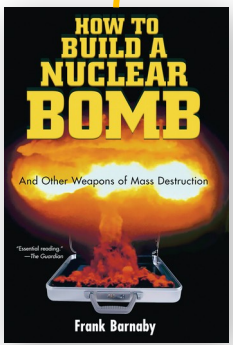
”Vi fik ham. Bombeplanen lå på hans bærbar.”

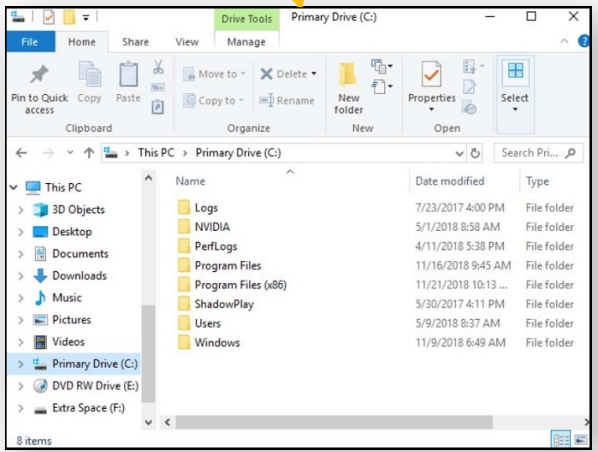

Western Digital
www.westerndigital.com
500GB
SATA / 16MB Cache
WD5000AAKX
WD Caviar Blue
00452768
EVIDENCE
(TO BE OPENED BY AUTHORIZED PERSONNEL ONLY)
NOTE
CASE NUMBER:
DESCRIPTION OF ENCLOSED EVIDENCE:
SUBMITTING AGENCY:
TELEPHONE NUMBER:
EVIDENCE RECORDED BY:
VICTIM'S FULL NAME:
SUSPECT'S FULL NAME:
EVIDENCE BAG SEALED BY:
DATE SEALED:
TIME SEALED:
CHAIN OF CUSTODY
FOR CRIME LAB PERSONNEL ONLY
FINAL DISPOSAL ACTION
CUT BELOW DOTTED LINE TO OPEN

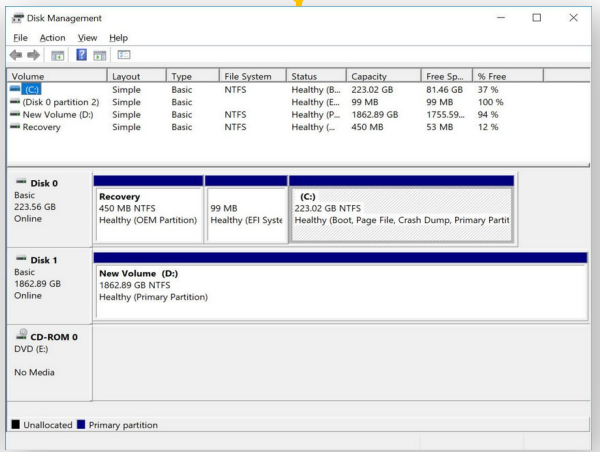

Franz Jäger Berlin
1964

Copy

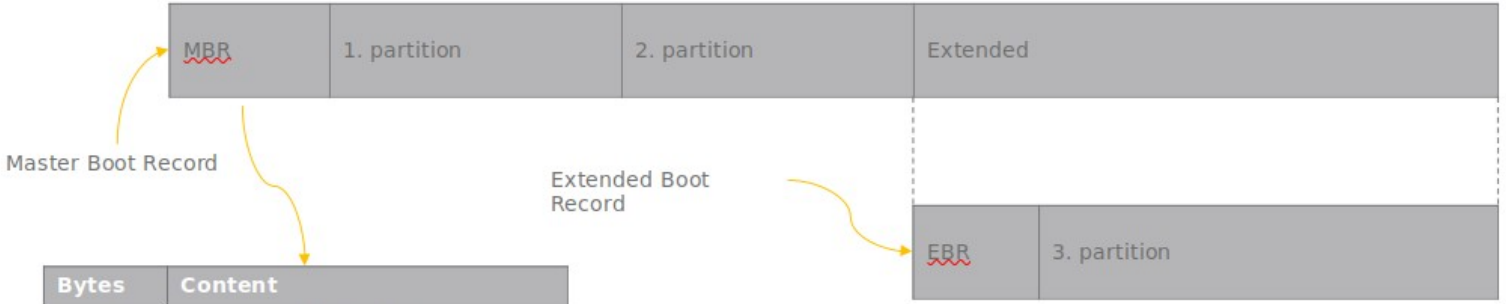
Og beregn hashværdi


HOW TO BUILD A NUCLEAR BOMB
And Other Weapons of Mass Destruction
Frank Barnaby


Drive Tools
Primary Drive (C:)
File
Home
Share
View
Manage
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
This PC
Primary Drive (C:)
Search Pri...
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Primary Drive (C:)
DVD RW Drive (E:)
Extra Space (F:)
Name
Date modified
Type
Logs 7/23/2017 4:00 PM File folder
NVIDIA 5/1/2018 8:58 AM File folder
PerfLogs 4/11/2018 5:38 PM File folder
Program Files 11/16/2018 9:45 AM File folder
Program Files (x86) 11/21/2018 10:13 ... File folder
ShadowPlay 5/30/2017 4:11 PM File folder
Users 5/9/2018 8:37 AM File folder
Windows 11/9/2018 6:49 AM File folder
8 items


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Sp... % Free
(C:) Simple Basic NTFS Healthy (B... 223.02 GB 81.46 GB 37 %
(Disk 0 partition 2) Simple Basic Healthy (E... 99 MB 99 MB 100 %
New Volume (D:) Simple Basic NTFS Healthy (P... 1862.89 GB 1755.59... 94 %
Recovery Simple Basic NTFS Healthy (... 450 MB 53 MB 12 %
Disk 0
Basic
223.56 GB
Online
Recovery
450 MB NTFS
Healthy (OEM Partition)
99 MB
Healthy (EFI Syste
(C:)
223.02 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partit
Disk 1
Basic
1862.89 GB
Online
New Volume (D:)
1862.89 GB NTFS
Healthy (Primary Partition)
CD-ROM 0
DVD (E:)
No Media
Unallocated
Primary partition

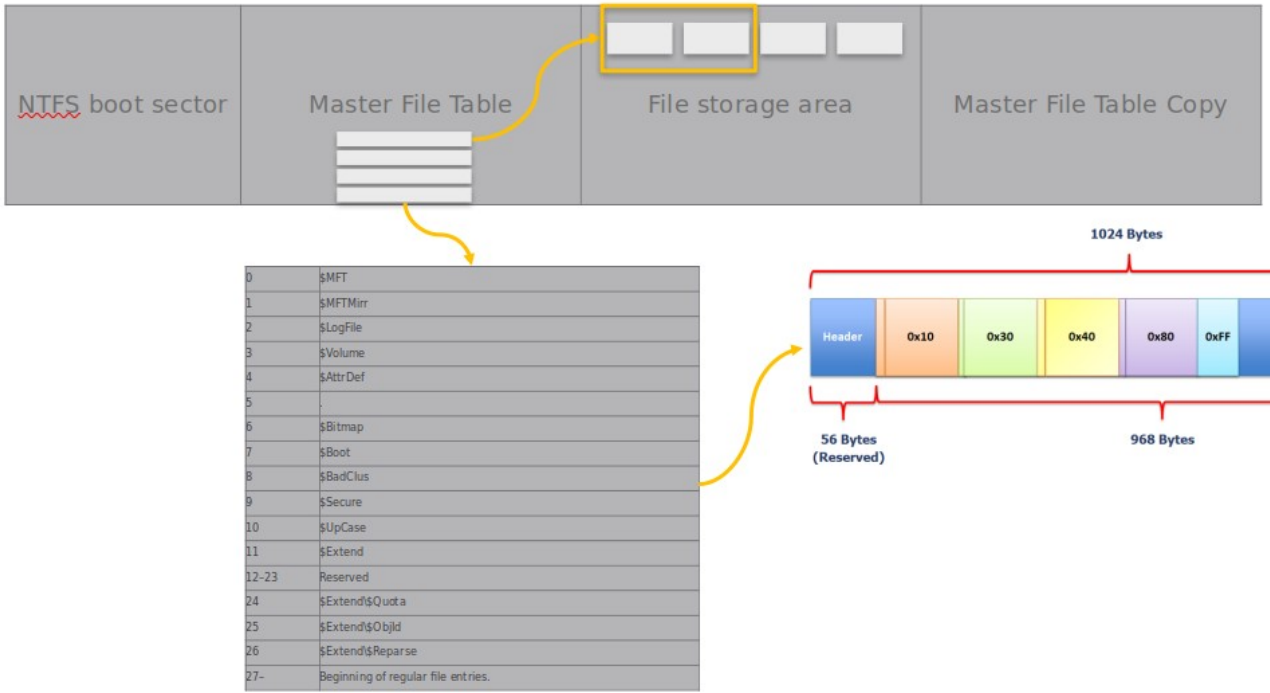

Western Digital
www.westerndigital.com
500GB
WD5000AAKX
WD Caviar Blue

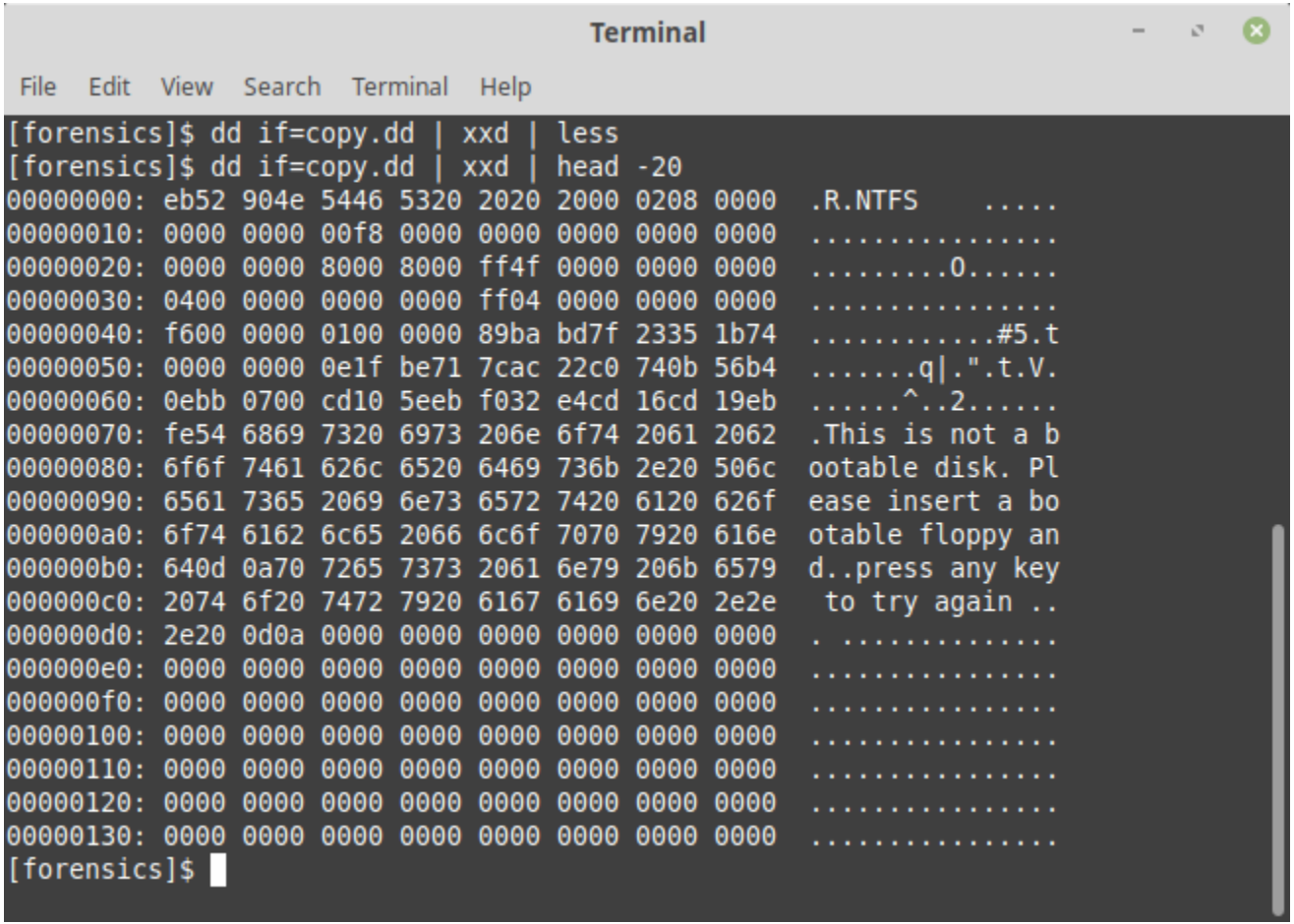


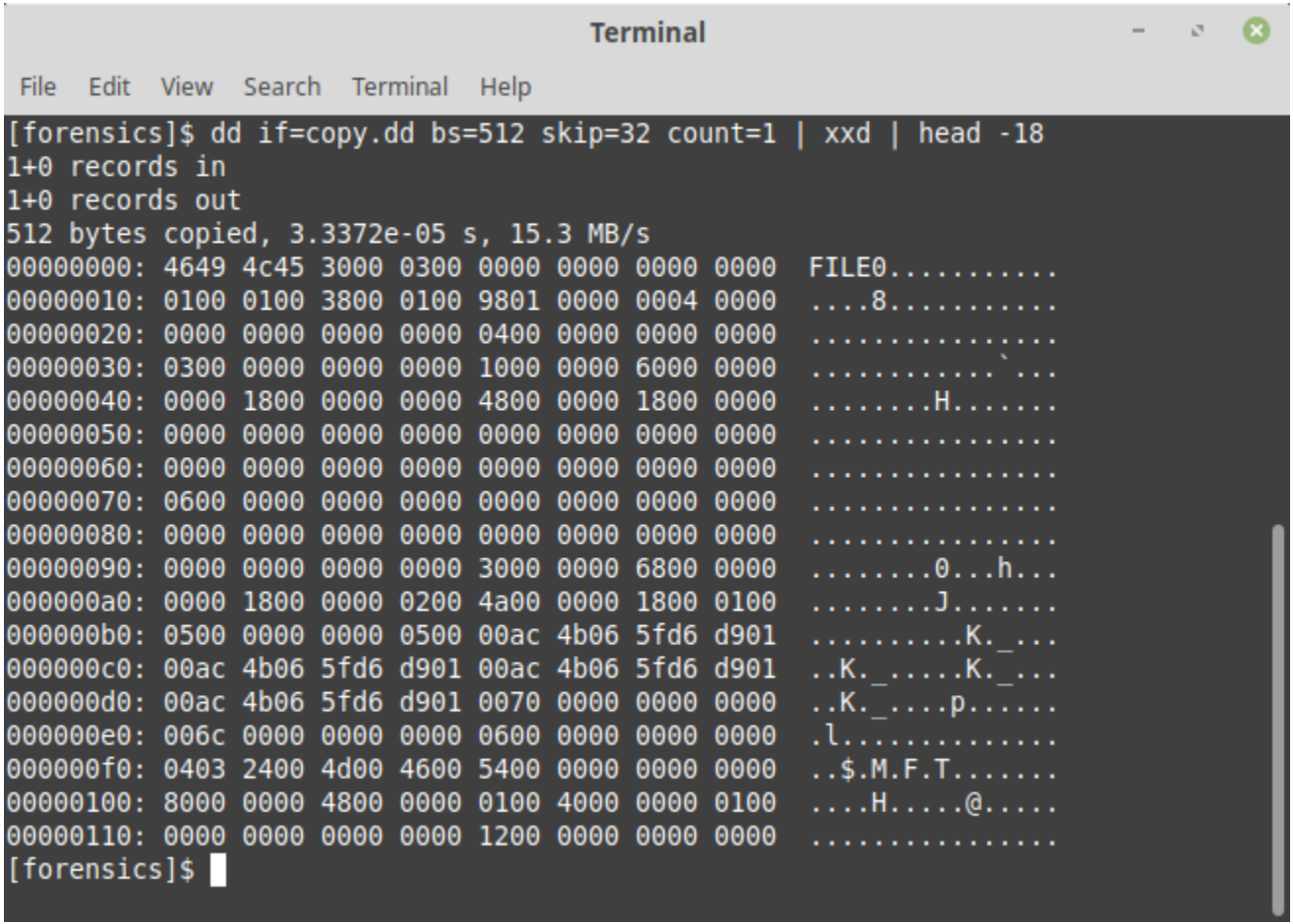
Bytes	Content
0-445	Upstart code, disk signature
446-461	Partition entry 1
462-477	Partition entry 2
478-493	Partition entry 3
494-509	Partition entry 4
510-511	MBR/EBR signature (0xAA55)

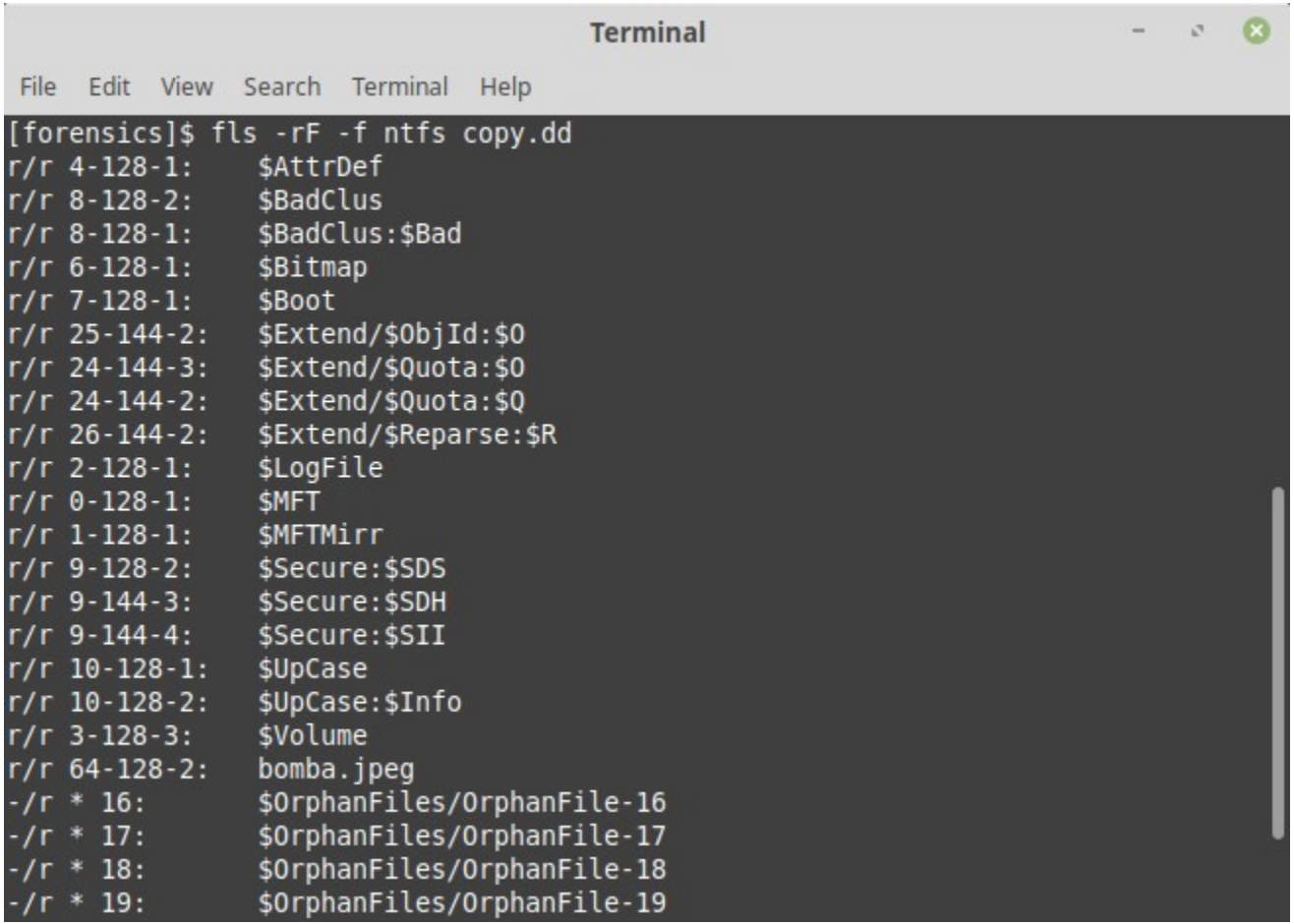
Bytes	Content
0	0x00 not boot, 0x80 boot
1-3	Cylinder-head-sector (CHS) of start sector
4	Partition type
5-7	Cylinder-head-sector (CHS) of end sector
8-11	Logical block addressing (LBA) of start sector
12-15	Number of sectors in partition

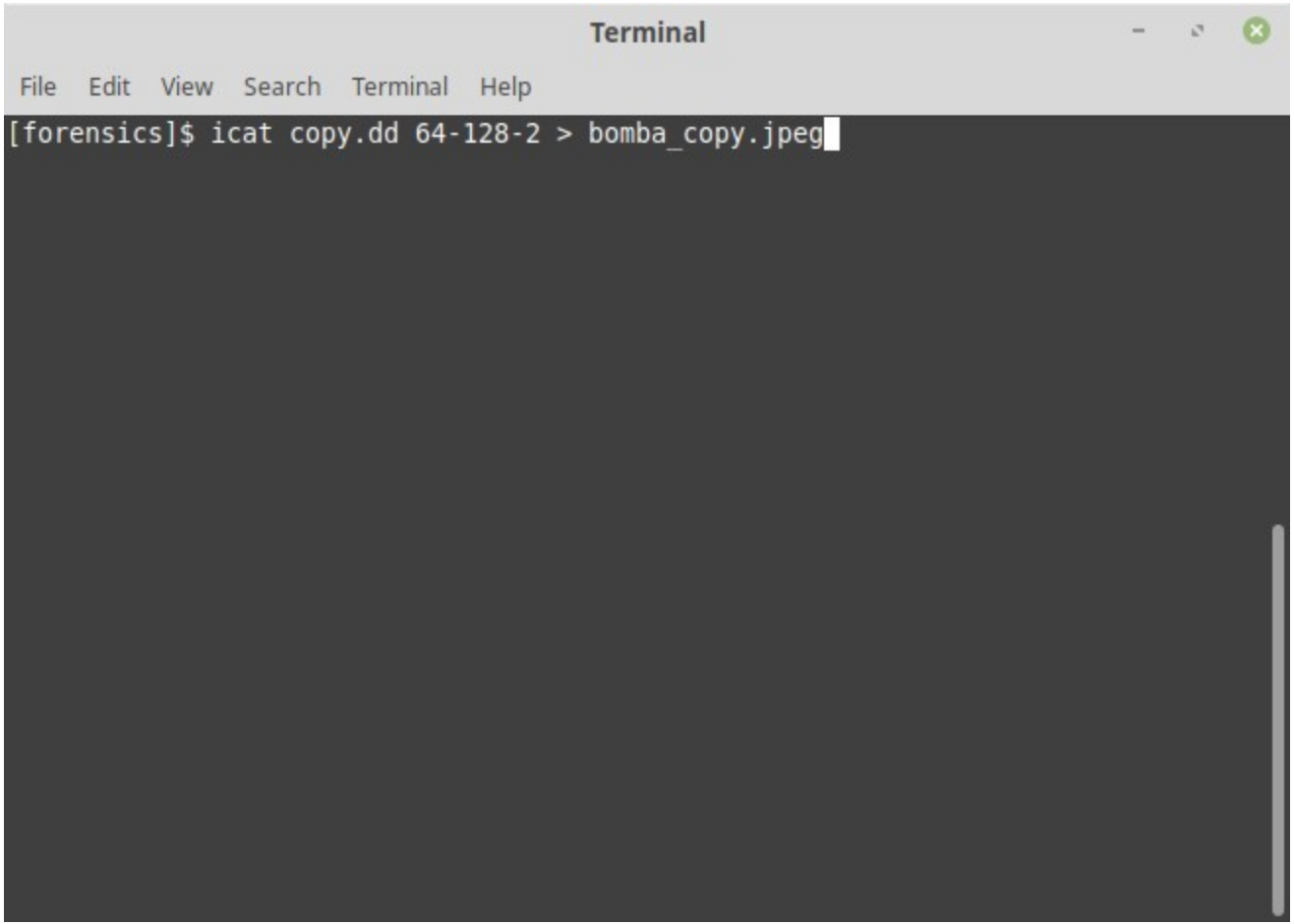
Type	FAT12	FAT16	FAT32	Linux native	Linux swap	Extended	NFTS
Hex value	0x01	0x0E	0x0C	0x83	0x82	0x05	0x07

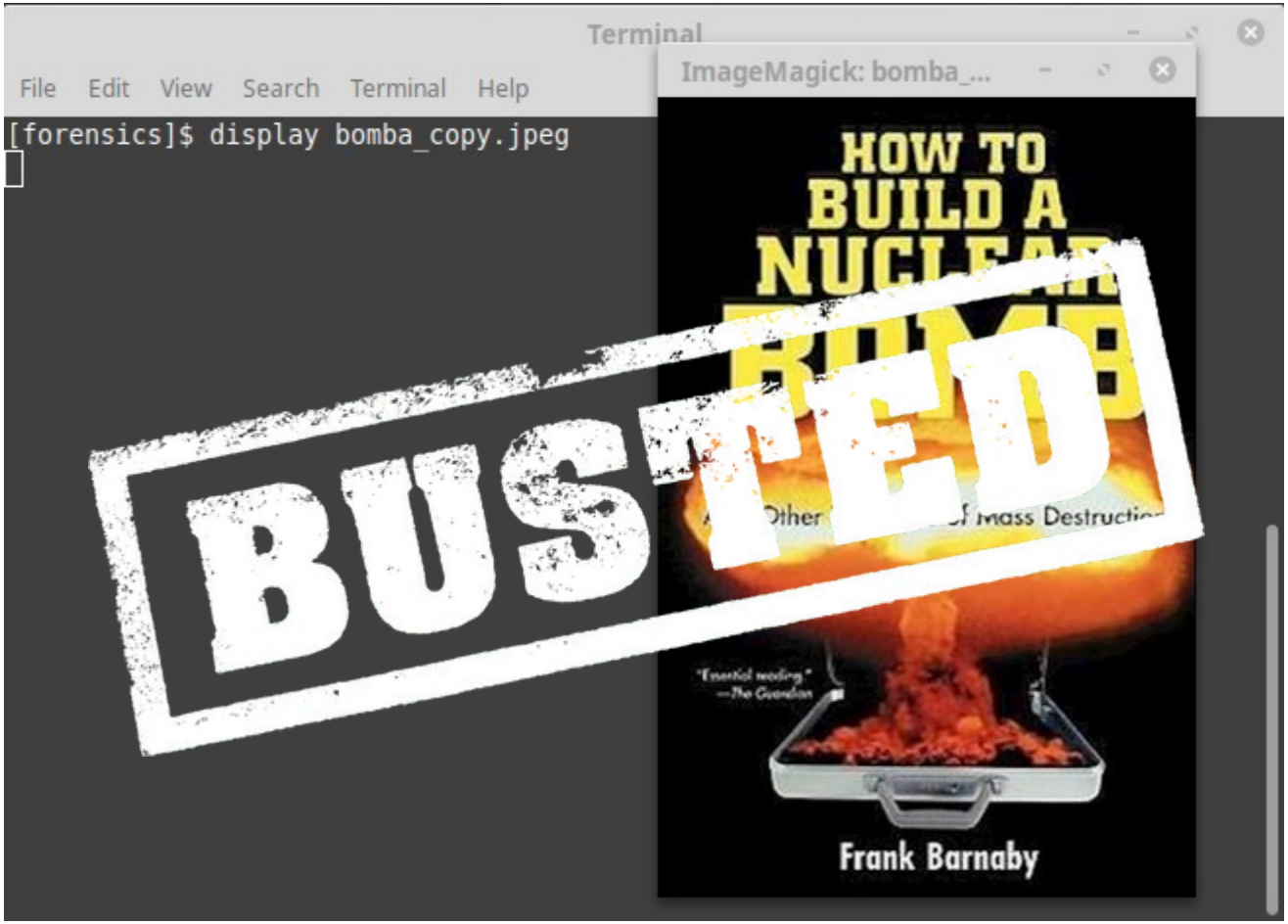

NTFS boot sector
Master File Table
File storage area
Master File Table Copy
0 $MFT
1 $MFTMirr
2 $LogFile
3 $Volume
4 $AttrDef
5 .
6 $Bitmap
7 $Boot
8 $BadClus
9 $Secure
10 $UpCase
11 $Extend
12-23 Reserved
24 $Extend\$Quota
25 $Extend\$ObjId
26 $Extend\$Reparse
27- Beginning of regular file entries.
1024 Bytes
Header
0x10
0x30
0x40
0x80
0xFF
56 Bytes
(Reserved)
968 Bytes


Terminal
File Edit View Search Terminal Help
[forensics]$ dd if=copy.dd | xxd | less
[forensics]$ dd if=copy.dd | xxd | head -20
00000000: eb52 904e 5446 5320 2020 2000 0208 0000 .R.NTFS   .....
00000010: 0000 0000 00f8 0000 0000 0000 0000 0000 ....
00000020: 0000 0000 8000 8000 ff4f 0000 0000 0000 ....O......
00000030: 0400 0000 0000 0000 ff04 0000 0000 0000 ....
00000040: f600 0000 0100 0000 89ba bd7f 2335 1b74 ....#5.t
00000050: 0000 0000 0e1f be71 7cac 22c0 740b 56b4 ....q|."."t.V.
00000060: 0ebb 0700 cd10 5eeb f032 e4cd 16cd 19eb ......^..2......
00000070: fe54 6869 7320 6973 206e 6f74 2061 2062 .This is not a b
00000080: 6f6f 7461 626c 6520 6469 736b 2e20 506c ootable disk. Pl
00000090: 6561 7365 2069 6e73 6572 7420 6120 626f ease insert a bo
000000a0: 6f74 6162 6c65 2066 6c6f 7070 7920 616e otable floppy an
000000b0: 640d 0a70 7265 7373 2061 6e79 206b 6579 d..press any key
000000c0: 2074 6f20 7472 7920 6167 6169 6e20 2e2e   to try again ..
000000d0: 2e20 0d0a 0000 0000 0000 0000 0000 0000 . ...
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000130: 0000 0000 0000 0000 0000 0000 0000 0000 ....
[forensics]$


Terminal
File Edit View Search Terminal Help
[forensics]$ dd if=copy.dd bs=512 skip=32 count=1 | xxd | head -18
1+0 records in
1+0 records out
512 bytes copied, 3.3372e-05 s, 15.3 MB/s
00000000: 4649 4c45 3000 0300 0000 0000 0000 0000 FILE0.....
00000010: 0100 0100 3800 0100 9801 0000 0004 0000 ....8.....
00000020: 0000 0000 0000 0000 0400 0000 0000 0000 ....
00000030: 0300 0000 0000 0000 1000 0000 6000 0000 ....`...
00000040: 0000 1800 0000 0000 4800 0000 1800 0000 ....H.....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000070: 0600 0000 0000 0000 0000 0000 0000 0000 ....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 ....
00000090: 0000 0000 0000 0000 3000 0000 6800 0000 ....0...h...
000000a0: 0000 1800 0000 0200 4a00 0000 1800 0100 ....J.....
000000b0: 0500 0000 0000 0500 00ac 4b06 5fd6 d901 ....K._...
000000c0: 00ac 4b06 5fd6 d901 00ac 4b06 5fd6 d901 ..K._....K._...
000000d0: 00ac 4b06 5fd6 d901 0070 0000 0000 0000 ..K._....p....
000000e0: 006c 0000 0000 0000 0600 0000 0000 0000 .l....
000000f0: 0403 2400 4d00 4600 5400 0000 0000 0000 ..$.M.F.T.....
00000100: 8000 0000 4800 0000 0100 4000 0000 0100 ....H.....@.....
00000110: 0000 0000 0000 0000 1200 0000 0000 0000 ....
[forensics]$


Terminal
File Edit View Search Terminal Help
[forensics]$ fls -rF -f ntfs copy.dd
r/r 4-128-1: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
r/r 25-144-2: $Extend/$ObjId:$O
r/r 24-144-3: $Extend/$Quota:$O
r/r 24-144-2: $Extend/$Quota:$Q
r/r 26-144-2: $Extend/$Reparse:$R
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-2: $Secure:$SDS
r/r 9-144-3: $Secure:$SDH
r/r 9-144-4: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-2: $UpCase:$Info
r/r 3-128-3: $Volume
r/r 64-128-2: bomba.jpeg
-/r * 16: $OrphanFiles/OrphanFile-16
-/r * 17: $OrphanFiles/OrphanFile-17
-/r * 18: $OrphanFiles/OrphanFile-18
-/r * 19: $OrphanFiles/OrphanFile-19


Terminal
File Edit View Search Terminal Help
[forensics]$ icat copy.dd 64-128-2 > bomba_copy.jpeg


Terminal
File Edit View Search Terminal Help
[forensics]$ display bomba_copy.jpeg
ImageMagick: bomba_...
HOW TO
BUILD A
Frank Barnaby
BUSTED

Deleted != destroyed

When a file is deleted, **data still exists** on disk until overwritten

If overwritten, **remnants may still exist** in

- extra copies of the file
- page/swap/hibernation file, or
- elsewhere on the disk due to (de)fragmentation

However, if disk wiped, only just once, recovery infeasible

Think libraries

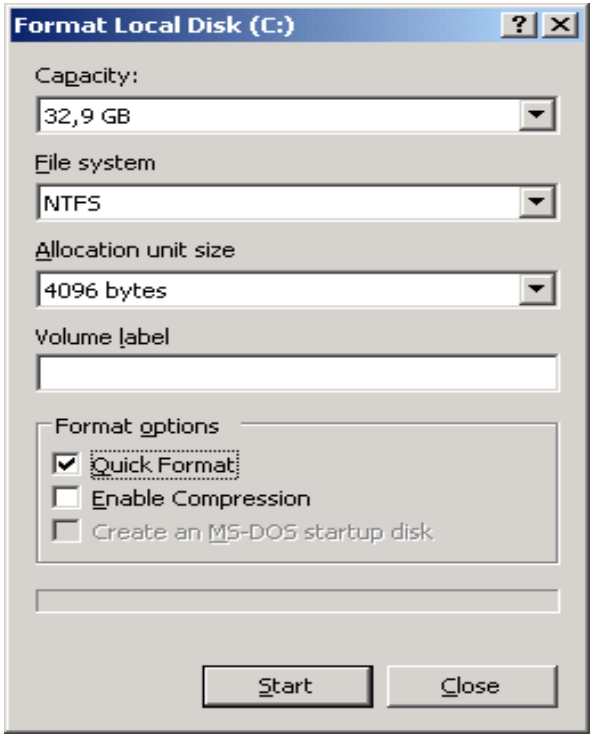
Format is not wiping

Formats create and replace file system structures

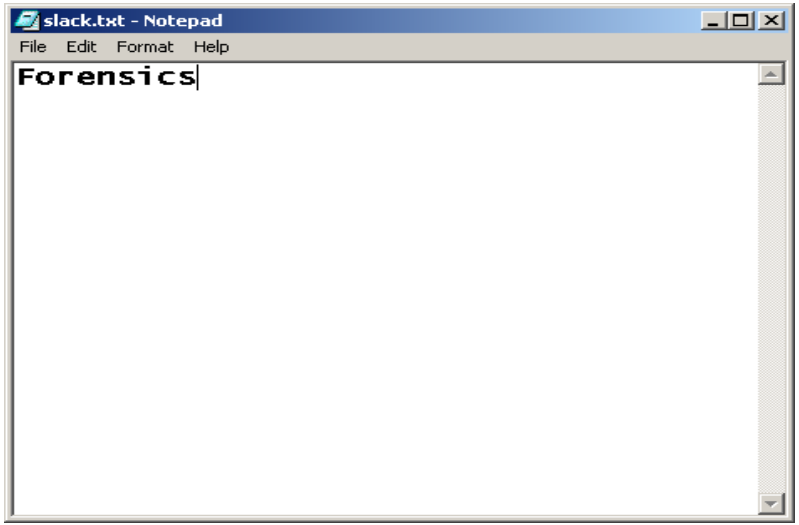
Files are not overwritten

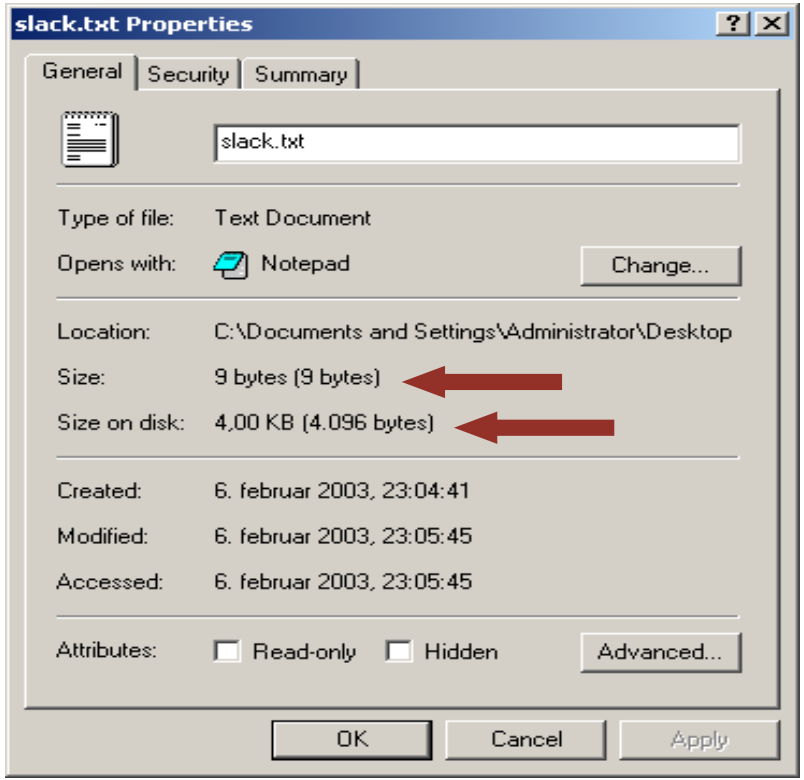
Regular formats take longer as the disk is scanned for bad sectors

Use wiping software for wiping

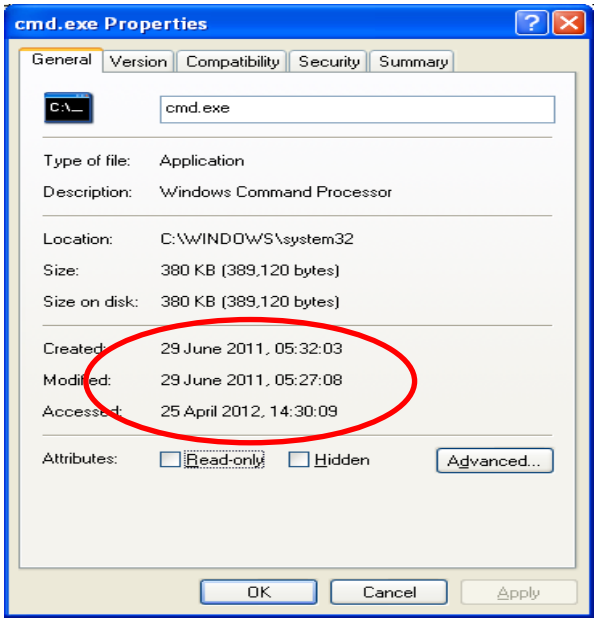


Slack space


slack.txt - Notepad
File Edit Format Help
Forensics

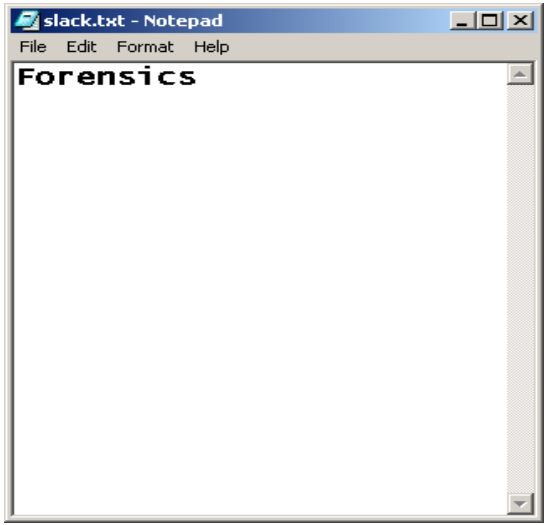

slack.txt Properties
General
Security
Summary
slack.txt
Type of file: Text Document
Opens with: Notepad
Change...
Location: C:\Documents and Settings\Administrator\Desktop
Size: 9 bytes (9 bytes)
Size on disk: 4,00 KB (4.096 bytes)
Created: 6. februar 2003, 23:04:41
Modified: 6. februar 2003, 23:05:45
Accessed: 6. februar 2003, 23:05:45
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

Timeline (Modified, Accessed, Changed)



Searching for file types

Slack.txt



Slack.exe

Slack.pdf

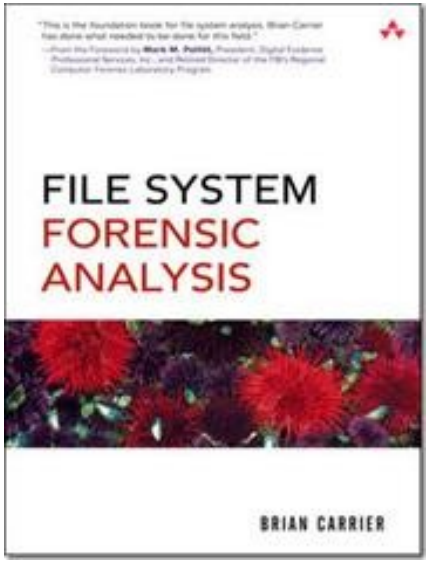
Slack.zip

Slack.dat

Slack.mp3

Slack.dll

Further reading



Wrap-up