

# 1. Task1

## 1.1 Result

```
0000000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 èR·NIFS·
0000000010 00 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00 ····ø··?·ÿ····
0000000020 00 00 00 00 80 00 80 00-FF 07 80 0C 00 00 00 00 ······ÿ······
0000000030 00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00 ········
0000000040 F6 00 00 00 01 00 00 00-DA 7F 27 48 A0 27 48 94 ò·····Û·'H·'H·
0000000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····úÄ·Ð·|úhÄ·
0000000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·È···f·>·N
0000000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·'As·UI·r·û
0000000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC U·u·+Ä·u·éÿ···i
0000000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h·'H·····ò·f·
00000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä·X·rá;··uÛs
00000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Ä·····Z3Ü·+E
00000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fy·····Äÿ···è
00000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+ËwI,·»í·f#Äu·
00000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·û·r··
00000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR·h·fSfSf
0000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h,·fa·Í·3A¿
0000000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··ò·úó·ép···f·
0000000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f;··f·····fh··
0000000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh·h···B··
0000000140 00 16 1F 8B F4 CD 13 66-59 5B 5A 66 59 66 59 1F ····òí·fy[ZfYfY·
0000000150 0F 82 16 00 66 FF 06 11-00 03 16 0F 00 8E C2 FF ····fy······Äÿ
0000000160 0E 16 00 75 BC 07 1F 66-61 C3 A1 F6 01 E8 09 00 ··u··faÄ;ò·è··
0000000170 A1 FA 01 E8 03 00 F4 EB-FD 8B F0 AC 3C 00 74 09 jú···òéÿ·ð·<·t·
0000000180 B4 0E BB 07 00 CD 10 EB-F2 C3 0D 0A 41 20 64 69 ··»·Í·èòÄ·A di
0000000190 73 6B 20 72 65 61 64 20-65 72 72 6F 72 20 6F 63 sk read error oc
00000001a0 63 75 72 72 65 64 00 0D-0A 42 4F 4F 54 4D 47 52 curredd···BOOTMGR
00000001b0 20 69 73 20 63 6F 6D 70-72 65 73 73 65 64 00 0D is compressed··
00000001c0 0A 50 72 65 73 73 20 43-74 72 6C 2B 41 6C 74 2B ·Press Ctrl+Alt+
00000001d0 44 65 6C 20 74 6F 20 72-65 73 74 61 72 74 0D 0A Del to restart··
00000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 ········
00000001f0 00 00 00 00 00 00 8A 01-A7 01 BF 01 00 00 55 AA ······$·¿···U·
0000000200 07 00 42 00 4F 00 4F 00-54 00 4D 00 47 00 52 00 ··B·O·O·T·M·G·R·
0000000210 04 00 24 00 49 00 33 00-30 00 00 D4 00 00 00 24 ··$·I·3·0·-·Ô···$
0000000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 ········
0000000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 ········
0000000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 ········
0000000250 00 00 00 00 00 00 E9 C0-00 90 05 00 4E 00 54 00 ······èÄ···N·T·
0000000260 4C 00 44 00 52 00 07 00-42 00 4F 00 4F 00 54 00 L·D·R···B·O·O·T·
0000000270 54 00 47 00 54 00 07 00-42 00 4F 00 4F 00 54 00 T·G·T···B·O·O·T·
0000000280 4E 00 58 00 54 00 00 00-00 00 00 00 00 00 00 N·X·T·······
0000000290 00 00 00 00 00 00 00 00-00 00 0D 0A 41 6E 20 6F ········An o
00000002a0 70 65 72 61 74 69 6E 67-20 73 79 73 74 65 6D 20 perating system
00000002b0 77 61 73 6E 27 74 20 66-6F 75 6E 64 2E 20 54 72 wasn't found. Tr
00000002c0 79 20 64 69 73 63 6F 6E-6E 65 63 74 69 6E 67 20 y disconnecting
00000002d0 61 6E 79 20 64 72 69 76-65 73 20 74 68 61 74 20 any drives that
00000002e0 64 6F 6E 27 74 0D 0A 63-6F 6E 74 61 69 6E 20 61 don't···contain a
00000002f0 6E 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 n operating syst
0000000300 65 6D 2E 00 00 00 00 00-00 00 00 00 00 00 00 em·······
0000000310 00 00 00 00 00 00 00 00-9A-02 66 0F B7 06 0B 00 66 ······f·····f
0000000320 0F B6 1E 0D 00 66 F7 E3-66 A3 52 02 66 8B 0E 40 ·q···f+áfîR·f·@
0000000330 00 80 F9 00 0F 8F 0E 00-F6 D9 66 B8 01 00 00 00 ··ü·····òUf,····
0000000340 66 D3 E0 EB 08 90 66 A1-52 02 66 F7 E1 66 A3 86 f0Äè···f;R·f+áfî·
0000000350 02 66 0F B7 1E 0B 00 66-33 D2 66 F7 F3 66 A3 56 ·f·····f30f+òfîV
0000000360 02 E8 A2 04 66 8B 0E 4E-02 66 89 0E 26 02 66 03 ·èe·f·N·f·-·s·f·
0000000370 0E 86 02 66 89 0E 2A 02-66 03 0E 86 02 66 89 0E ··f···*·f·····f··
0000000380 2E 02 66 03 0E 86 02 66-89 0E 3E 02 66 03 0E 86 ·f·····f··>·f···
0000000390 02 66 89 0E 46 02 66 B8-90 00 00 00 66 8B 0E 26 ·f·F·f,·····f···s
00000003a0 02 E8 90 09 66 0B C0 0F-84 BF FD 66 A3 32 02 66 ·è·f·Ä·¿ÿfî2·f·
00000003b0 B8 A0 00 00 00 66 8B 0E-2A 02 E8 77 09 66 A3 36 ,···f···*·èw·fî6
00000003c0 02 66 B8 B0 00 00 66 8B 0E 2E 02 E8 65 09 66 ·f,·*···f···,èe·f·
00000003d0 A3 3A 02 66 A1 32 02 66-0B C0 0F 84 8C FD 67 80 £:·f;2·f·Ä···ÿg·
00000003e0 78 08 00 0F 85 83 FD 67-66 8D 50 10 67 03 42 04 x·····ÿgf·P·g·B·
00000003f0 67 66 0F B6 48 0C 66 89-0E 92 02 67 66 8B 48 08 gf·¶H·f·····gf·H·
0000000400 66 89 0E 8E 02 66 A1 8E-02 66 0F B7 0E 0B 00 66 f·····f;···f·····f
```

## 2. Task2

### 2.1 Result

```
PS C:\Users\zamao\DigitalForensics\Activity3\Part2> exiftool 1.zip
ExifTool Version Number      : 12.69
File Name                    : 1.zip
Directory                    :
File Size                    : 38 kB
File Modification Date/Time   : 2023:11:09 13:30:00+00:00
File Access Date/Time        : 2023:11:09 13:30:57+00:00
File Creation Date/Time      : 2023:11:09 13:30:57+00:00
File Permissions              : -rw-rw-rw-
File Type                    : PPTX
File Type Extension          : pptx
MIME Type                    : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version         : 20
Zip Bit Flag                 : 0x0006
Zip Compression              : Deflated
Zip Modify Date              : 1980:01:01 00:00:00
Zip CRC                      : 0x805bd1fd
Zip Compressed Size          : 465
Zip Uncompressed Size        : 3259
Zip File Name                : [Content_Types].xml
Preview Image                : (Binary data 7389 bytes, use -b option to extract)
Total Edit Time              : 0
Words                        : 3
Application                  : Microsoft Macintosh PowerPoint
Presentation Format           : On-screen Show (4:3)
Paragraphs                   : 2
Slides                       : 1
Notes                        : 0
Hidden Slides                : 0
MM Clips                     : 0
Scale Crop                   : No
Heading Pairs                 : Theme, 1, Slide Titles, 1
Titles Of Parts              : Office Theme, Nifty Presentation
Company                      :
Links Up To Date             : No
Shared Doc                   : No
Hyperlinks Changed           : No
App Version                  : 14.0000
Title                        : Nifty Presentation
Creator                      : Nancy
Last Modified By             : Jim
Revision Number              : 9
```

```
Directory                    :
File Size                    : 38 kB
File Modification Date/Time   : 2023:11:09 13:30:00+00:00
File Access Date/Time        : 2023:11:09 13:30:57+00:00
File Creation Date/Time      : 2023:11:09 13:30:57+00:00
File Permissions              : -rw-rw-rw-
File Type                    : PPTX
File Type Extension          : pptx
MIME Type                    : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version         : 20
Zip Bit Flag                 : 0x0006
Zip Compression              : Deflated
Zip Modify Date              : 1980:01:01 00:00:00
Zip CRC                      : 0x805bd1fd
Zip Compressed Size          : 465
Zip Uncompressed Size        : 3259
Zip File Name                : [Content_Types].xml
Preview Image                : (Binary data 7389 bytes, use -b option to extract)
Total Edit Time              : 0
Words                        : 3
Application                  : Microsoft Macintosh PowerPoint
Presentation Format           : On-screen Show (4:3)
Paragraphs                   : 2
Slides                       : 1
Notes                        : 0
Hidden Slides                : 0
MM Clips                     : 0
Scale Crop                   : No
Heading Pairs                 : Theme, 1, Slide Titles, 1
Titles Of Parts              : Office Theme, Nifty Presentation
Company                      :
Links Up To Date             : No
Shared Doc                   : No
Hyperlinks Changed           : No
App Version                  : 14.0000
Title                        : Nifty Presentation
Creator                      : Nancy
Last Modified By             : Jim
Revision Number              : 9
Create Date                  : 2015:10:08 18:33:33Z
Modify Date                  : 2015:10:08 19:30:53Z
PS C:\Users\zamao\DigitalForensics\Activity3\Part2>
```

```

Revision Number      : 9
Create Date         : 2015:10:08 18:33:33Z
Modify Date        : 2015:10:08 19:30:53Z
PS C:\Users\zamao\DigitalForensics\Activity3\Part2> exiftool 2.zip
ExifTool Version Number : 12.69
File Name             : 2.zip
Directory             : .
File Size              : 29 kB
File Modification Date/Time : 2023:11:09 13:30:00+00:00
File Access Date/Time   : 2023:11:09 13:30:57+00:00
File Creation Date/Time  : 2023:11:09 13:30:57+00:00
File Permissions       : -rw-rw-rw-
File Type              : XLSX
File Type Extension    : xlsx
MIME Type              : application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Zip Required Version   : 20
Zip Bit Flag           : 0x0006
Zip Compression        : Deflated
Zip Modify Date        : 1980:01:01 00:00:00
Zip CRC                : 0x408e483b
Zip Compressed Size    : 364
Zip Uncompressed Size  : 1220
Zip File Name          : [Content_Types].xml
Preview Image          : (Binary data 21104 bytes, use -b option to extract)
Creator                : Katherine
Last Modified By       : Kaiser Soze
Revision Number        : 12
Create Date            : 2015:10:08 21:34:00Z
Modify Date            : 2015:10:08 22:14:18Z
Application            : Microsoft Macintosh Excel
Doc Security           : None
Scale Crop             : No
Heading Pairs          : Worksheets, 1
Titles Of Parts        : Sheet1
Company                :
Links Up To Date       : No
Shared Doc             : No
Hyperlinks Changed     : No
App Version            : 14.0300
PS C:\Users\zamao\DigitalForensics\Activity3\Part2>

```

```

Hyperlinks Changed     : No
App Version            : 14.0300
PS C:\Users\zamao\DigitalForensics\Activity3\Part2> exiftool 3.zip
ExifTool Version Number : 12.69
File Name             : 3.zip
Directory             : .
File Size              : 13 kB
File Modification Date/Time : 2023:11:09 13:30:00+00:00
File Access Date/Time   : 2023:11:09 13:30:57+00:00
File Creation Date/Time  : 2023:11:09 13:30:57+00:00
File Permissions       : -rw-rw-rw-
File Type              : DOCX
File Type Extension    : docx
MIME Type              : application/vnd.openxmlformats-officedocument.wordprocessingml.document

Zip Required Version   : 20
Zip Bit Flag           : 0x0006
Zip Compression        : Deflated
Zip Modify Date        : 1980:01:01 00:00:00
Zip CRC                : 0x46981d62
Zip Compressed Size    : 378
Zip Uncompressed Size  : 1422
Zip File Name          : [Content_Types].xml
Title                 : Internal_title
Creator                : Charles Galileo
Last Modified By       : Michael Robinson
Revision Number        : 3
Create Date            : 2013:12:12 15:42:00Z
Modify Date            : 2015:10:08 19:29:00Z
Template               : Normal.dotm
Total Edit Time        : 1 minute
Pages                  : 1
Words                  : 102
Characters             : 582
Application            : Microsoft Macintosh Word
Doc Security           : None
Lines                  : 4
Paragraphs             : 1
Scale Crop             : No
Company                :
Links Up To Date       : No
Characters With Spaces : 683
Shared Doc             : No

```

```

File Size : 13 kB
File Modification Date/Time : 2023:11:09 13:30:00+00:00
File Access Date/Time : 2023:11:09 13:30:57+00:00
File Creation Date/Time : 2023:11:09 13:30:57+00:00
File Permissions : -rw-rw-rw-
File Type : DOCX
File Type Extension : docx
MIME Type : application/vnd.openxmlformats-officedocument.wordprocessingml.doc
ument
Zip Required Version : 20
Zip Bit Flag : 0x0006
Zip Compression : Deflated
Zip Modify Date : 1980:01:01 00:00:00
Zip CRC : 0x46981d62
Zip Compressed Size : 378
Zip Uncompressed Size : 1422
Zip File Name : [Content_Types].xml
Title : Internal_title
Creator : Charles Galileo
Last Modified By : Michael Robinson
Revision Number : 3
Create Date : 2013:12:12 15:42:00Z
Modify Date : 2015:10:08 19:29:00Z
Template : Normal.dotm
Total Edit Time : 1 minute
Pages : 1
Words : 102
Characters : 582
Application : Microsoft Macintosh Word
Doc Security : None
Lines : 4
Paragraphs : 1
Scale Crop : No
Company :
Links Up To Date : No
Characters With Spaces : 683
Shared Doc : No
Hyperlinks Changed : No
App Version : 14.0000
PS C:\Users\zamao\DigitalForensics\Activity3\Part2>

```

## 2.2 Analysis

I use Exiftool to query metadata. Exiftool is a command-line tool. You can enter "exiftool" followed by a space and the file you want to query in the command prompt (cmd) to retrieve information.

## 3 Task3

### 3.1 Result

Document 1: This is just a test file: 5

Document 2: PDF

Document 3: XHTML

Document 4: doc, xls, ppt, msi or msg

Document 5: doc, xls, ppt, msi or msg

Document 6: PDB

Document 7: email

Document 8: doc, xls, ppt, msi or msg

Document 9: doc, xls, ppt, msi or msg

### 3.2 Analysis

I opened these files using FTK and examined their content in hexadecimal format. Based on my understanding of the file system, I was able to identify the majority of file types. However, for files 3 and 7, I couldn't find corresponding file signatures. I determined their file types based on the string content. As for files 4, 5, 8, and 9, which are of Windows types, I couldn't specify their exact file formats; I could only identify them as belonging to one of the following types: doc, xls, ppt, msi, or msg.

## 4 Task 4

```
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> fsstat -f ntfs
".\DiskPartitionRawImage.dd"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: A2A4F4DDA4F4B4BF
OEM Name: NTFS
Volume Name: Drive
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 87381
First Cluster of MFT Mirror: 131071
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 128
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 262142
Total Sector Range: 0 - 2097150

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)       Size: No Limit  Flags: Non-resident
$FILE_NAME (48)            Size: 68-578  Flags: Resident,Index
$OBJECT_ID (64)            Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit  Flags: Non-resident
$VOLUME_NAME (96)          Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)                Size: No Limit  Flags:
$INDEX_ROOT (144)          Size: No Limit  Flags: Resident
$INDEX_ALLOCATION (160)     Size: No Limit  Flags: Non-resident
$BITMAP (176)              Size: No Limit  Flags: Non-resident
$REPARSE_POINT (192)       Size: 0-16384  Flags: Non-resident
$EA_INFORMATION (208)      Size: 8-8    Flags: Resident
$EA (224)                  Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536   Flags: Non-resident

OEM Name: NTFS
Volume Name: Drive
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 87381
First Cluster of MFT Mirror: 131071
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 128
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 262142
Total Sector Range: 0 - 2097150

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)       Size: No Limit  Flags: Non-resident
$FILE_NAME (48)            Size: 68-578  Flags: Resident,Index
$OBJECT_ID (64)            Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit  Flags: Non-resident
$VOLUME_NAME (96)          Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)                Size: No Limit  Flags:
$INDEX_ROOT (144)          Size: No Limit  Flags: Resident
$INDEX_ALLOCATION (160)     Size: No Limit  Flags: Non-resident
$BITMAP (176)              Size: No Limit  Flags: Non-resident
$REPARSE_POINT (192)       Size: 0-16384  Flags: Non-resident
$EA_INFORMATION (208)      Size: 8-8    Flags: Resident
$EA (224)                  Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536   Flags: Non-resident
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>
```

```

$EA (224) Size: 0-65536 Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536 Flags: Non-resident
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs ".\DiskPartitionRawImage.dd" 0
MFT Entry Header Values:
Entry: 0 Sequence: 1
$LogFile Sequence Number: 2121493
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 16384 Actual Size: 16384
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-1) Name: N/A Non-Resident size: 131072 init_size: 131072
87381 87382 87383 87384 87385 87386 87387 87388
87389 87390 87391 87392 87393 87394 87395 87396
87397 87398 87399 87400 87401 87402 87403 87404
87405 87406 87407 87408 87409 87410 87411 87412
Type: $BITMAP (176-5) Name: N/A Non-Resident size: 4104 init_size: 4104
87380 128479
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs ".\DiskPartitionRawImage.dd" 1
MFT Entry Header Values:
Entry: 1 Sequence: 1
$LogFile Sequence Number: 2101459
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFTMirr
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 4096 Actual Size: 4096
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $DATA (128-1) Name: N/A Non-Resident size: 4096 init_size: 4096
131071
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $DATA (128-1) Name: N/A Non-Resident size: 4096 init_size: 4096
131071
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 7
MFT Entry Header Values:
Entry: 7 Sequence: 7
$LogFile Sequence Number: 0
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0 ()
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Boot
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 8192 Actual Size: 8192
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-2) Name: N/A Resident size: 76
Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 100
Type: $DATA (128-1) Name: N/A Non-Resident size: 8192 init_size: 8192
0 1
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 100
Type: $DATA (128-1) Name: N/A Non-Resident size: 8192 init_size: 8192
0 1
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 3
MFT Entry Header Values:
Entry: 3 Sequence: 3
$LogFile Sequence Number: 2102601
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0 ()
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Volume
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 0 Actual Size: 0
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-1) Name: N/A Resident size: 80
Type: $SECURITY_DESCRIPTOR (80-2) Name: N/A Resident size: 100
Type: $VOLUME_NAME (96-4) Name: N/A Resident size: 10
Type: $VOLUME_INFORMATION (112-5) Name: N/A Resident size: 12
Type: $DATA (128-3) Name: N/A Resident size: 0
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

Type: $DATA (128-3) Name: N/A Resident size: 0
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 4
MFT Entry Header Values:
Entry: 4 Sequence: 4
$LogFile Sequence Number: 2102571
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0 ()
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $AttrDef
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 36864 Actual Size: 36000
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 100
Type: $DATA (128-4) Name: N/A Non-Resident size: 2560 init_size: 2560
120225
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

120225
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> 6
6
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 6
MFT Entry Header Values:
Entry: 6 Sequence: 6
$LogFile Sequence Number: 2101599
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Bitmap
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 32768 Actual Size: 32768
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 80
Type: $DATA (128-1) Name: N/A Non-Resident size: 32768 init_size: 32768
131082 131083 131084 131085 131086 131087 131088 131089
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 80
Type: $DATA (128-1) Name: N/A Non-Resident size: 32768 init_size: 32768
131082 131083 131084 131085 131086 131087 131088 131089
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 8
MFT Entry Header Values:
Entry: 8 Sequence: 8
$LogFile Sequence Number: 2101669
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 0 Actual Size: 0
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 82
Type: $DATA (128-2) Name: N/A Resident size: 0
Type: $DATA (128-1) Name: $Bad Non-Resident size: 1073737728 init_size: 0
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> istat -f ntfs "
.\DiskPartitionRawImage.dd" 9
MFT Entry Header Values:
Entry: 9 Sequence: 9
$LogFile Sequence Number: 2109402
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 257 (S-1-5-18)
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System, Index View
Name: $Secure
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 0 Actual Size: 0
Created: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
File Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
MFT Modified: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)
Accessed: 2011-09-28 02:28:17.758000000 (Pacific Summer Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-7) Name: N/A Resident size: 80
Type: $DATA (128-8) Name: $SDS Non-Resident size: 263832 init_size: 263832
120160 120161 120162 120163 120164 120165 120166 120167
120168 120169 120170 120171 120172 120173 120174 120175
120176 120177 120178 120179 120180 120181 120182 120183
120184 120185 120186 120187 120188 120189 120190 120191
120192 120193 120194 120195 120196 120197 120198 120199
120200 120201 120202 120203 120204 120205 120206 120207
120208 120209 120210 120211 120212 120213 120214 120215
120216 120217 120218 120219 120220 120221 120222 120223
120224
Type: $INDEX_ROOT (144-11) Name: $SDH Resident size: 56
Type: $INDEX_ROOT (144-14) Name: $SII Resident size: 56

```

```

-/d * 100-144-1: MSI97a47.tmp
V/V 128: $OrphanFiles
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> fls -d "DiskPar
titionRawImage.dd"
-/d * 100-144-1: MSI97a47.tmp
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> fls -d "DiskPar
titionRawImage.dd"
-/d * 100-144-1: MSI97a47.tmp
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

```

titionRawImage.dd"
-/d * 100-144-1: MSI97a47.tmp
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023> img_stat "DiskP
artitionRawImage.dd" 6
Error stat(ing) image file (raw_open: image "6" - No such file or directory)
PS C:\Users\zamao\Documents\DigitalForensics\HandsonActivity3\OneDrive_1_11-7-2023>

```

# 5 Task 5

## 5.1 Result

