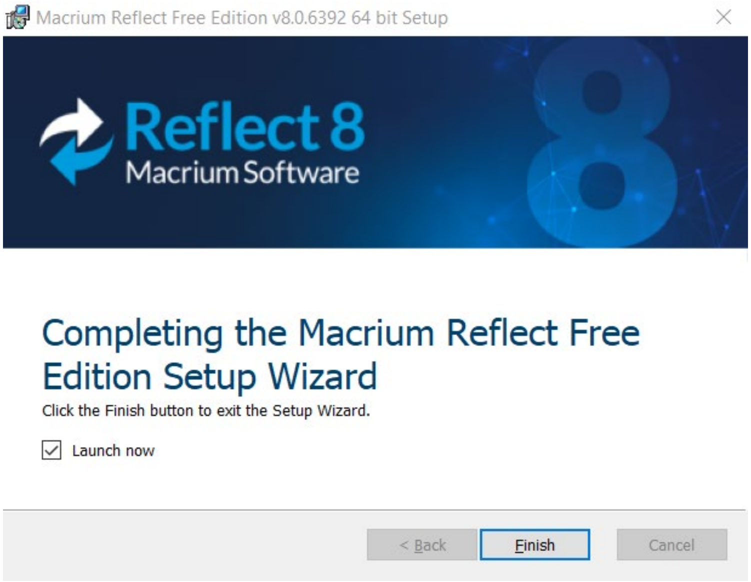
Muhammad Izham Bin Norhamadi (B032020039)

Lab 12

1. Creating a Disk Image Backup



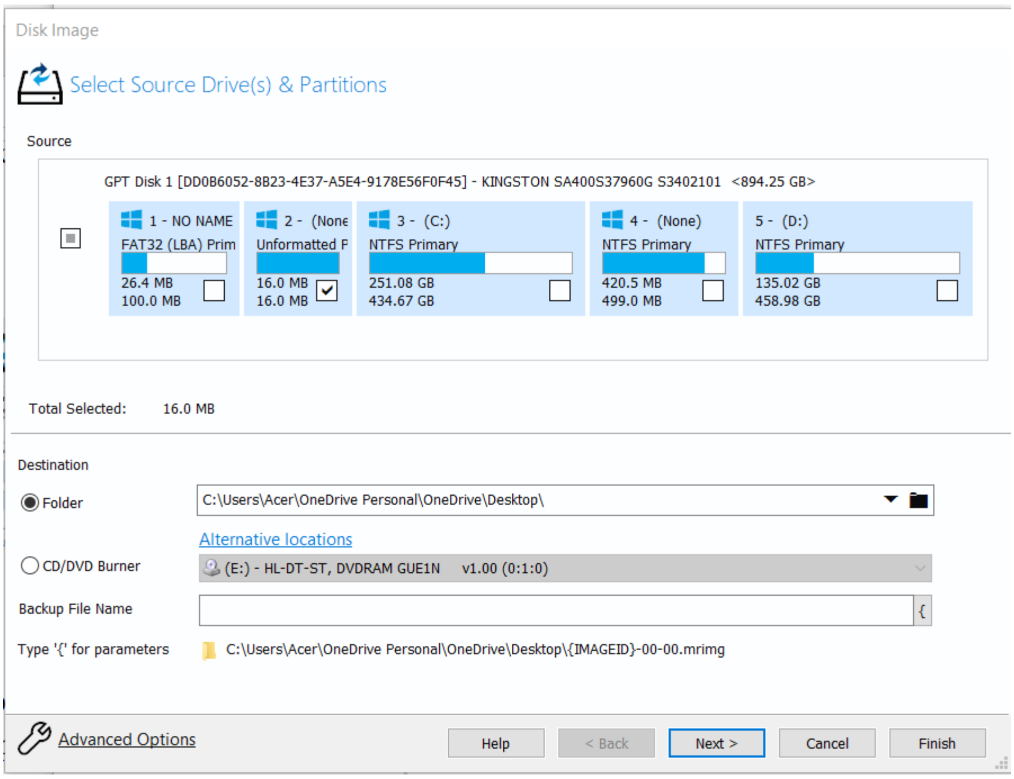
Macrium Reflect Free Edition v8.0.6392 64 bit Setup

Completing the Macrium Reflect Free Edition Setup Wizard

Click the Finish button to exit the Setup Wizard.

☑ Launch now

Figure 1 Macrium Reflect Installer



Disk Image

Select Source Drive(s) & Partitions

Source

GPT Disk 1 [DD0B6052-8B23-4E37-A5E4-9178E56F0F45] - KINGSTON SA400S37960G S3402101 <894.25 GB>

1 - NO NAME	2 - (None	3 - (C:)	4 - (None)	5 - (D:)
FAT32 (LBA) Prim	Unformatted F	NTFS Primary	NTFS Primary	NTFS Primary
26.4 MB 100.0 MB □	16.0 MB 16.0 MB ☑	251.08 GB 434.67 GB □	420.5 MB 499.0 MB □	135.02 GB 458.98 GB □

Total Selected: 16.0 MB

Destination

● Folder C:\Users\Acer\OneDrive Personal\OneDrive\Desktop\

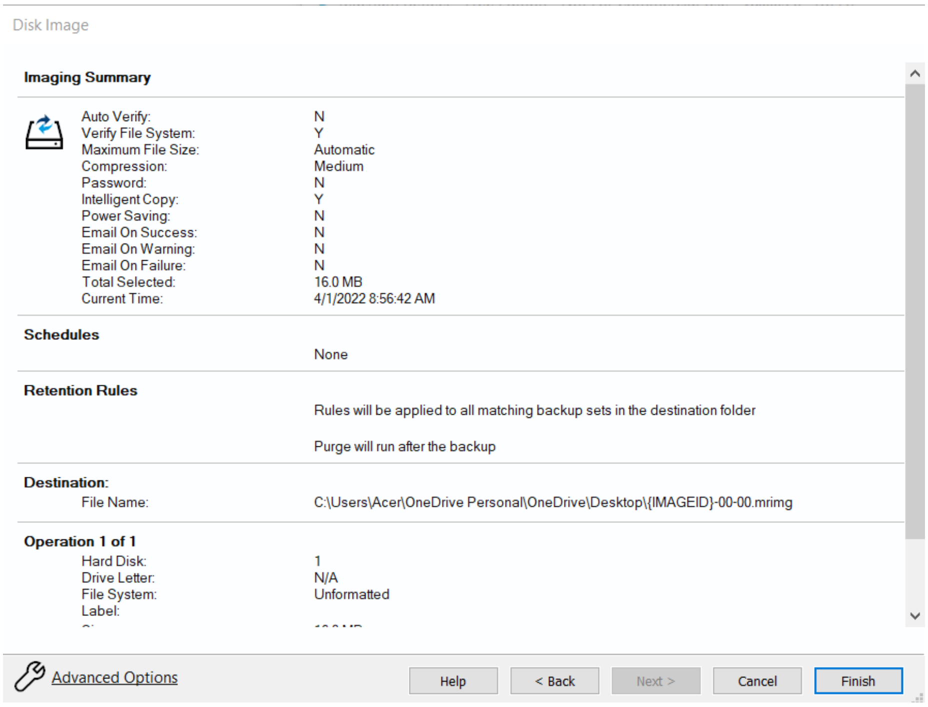
Alternative locations

○ CD/DVD Burner (E:) - HL-DT-ST, DVDRAM GUE1N v1.00 (0:1:0)

Backup File Name

Type '{' for parameters C:\Users\Acer\OneDrive Personal\OneDrive\Desktop\{IMAGEID}-00-00.mrimg

Figure 2 Macrium Reflect Disk Image



Imaging Summary

Auto Verify:	N
Verify File System:	Y
Maximum File Size:	Automatic
Compression:	Medium
Password:	N
Intelligent Copy:	Y
Power Saving:	N
Email On Success:	N
Email On Warning:	N
Email On Failure:	N
Total Selected:	16.0 MB
Current Time:	4/1/2022 8:56:42 AM

Schedules

None

Retention Rules

Rules will be applied to all matching backup sets in the destination folder

Purge will run after the backup

Destination:

File Name:	C:\Users\Acer\OneDrive Personal\OneDrive\Desktop\{IMAGEID}-00-00.mrimg

Operation 1 of 1

Hard Disk:	1
Drive Letter:	N/A
File System:	Unformatted
Label:	

Figure 3 Macrium Reflect Image Summary

1.1 Differentiate Full, Differential and Incremental retention rules.

Full Backup: Stores all information present

Differential Backup: Stores only the difference between last full backup and the current state of data

Incremental Backup: Stores the difference between the current state of data and state of data from previous successful backup

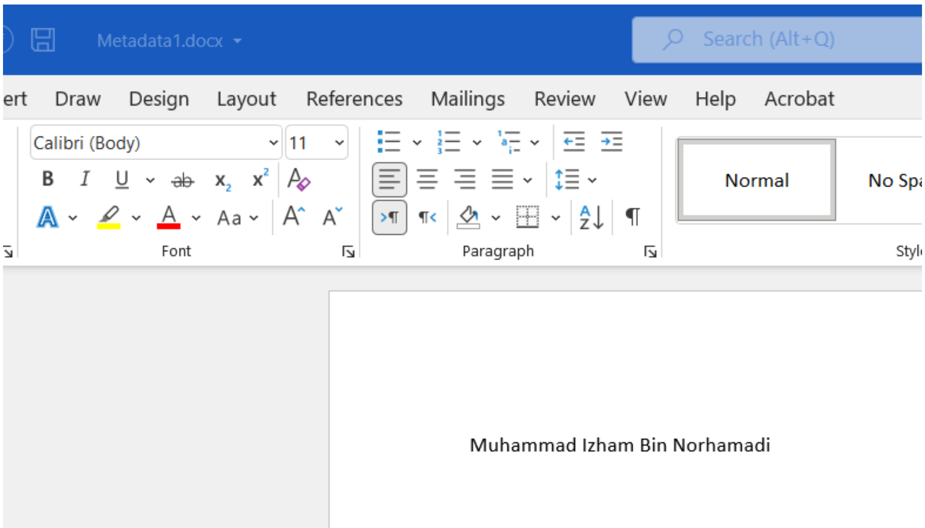
1.2 Differentiate between disk cloning and disk imaging. What is the advantages of disk imaging?

Disk Cloning: Creates an exact functional one-to-one copy of hard drive

Disk Imaging: Creates an compressed archive of hard drive

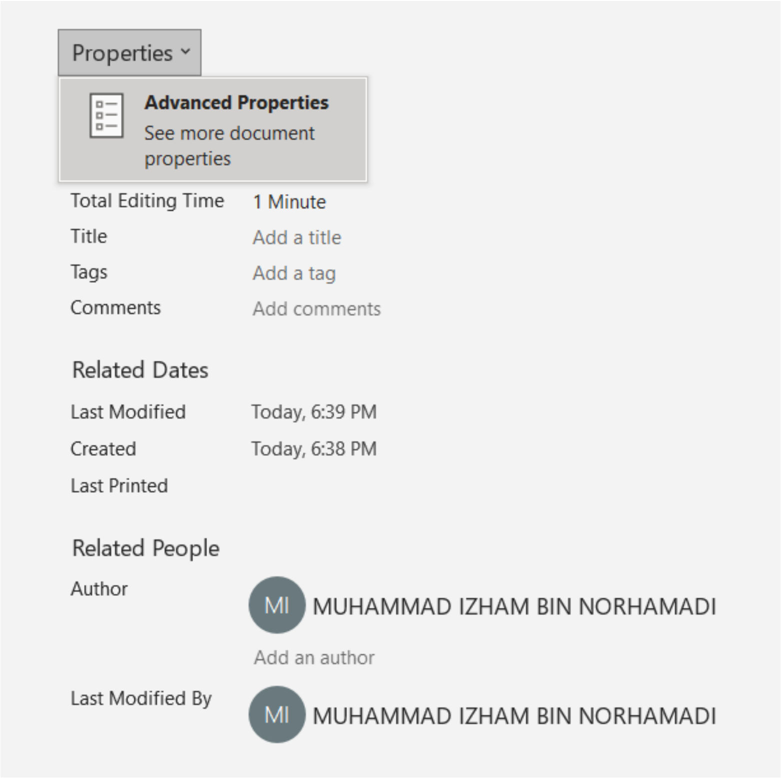
Advantages of disk imaging: Multiple disk images can be stored on other storage than hard drives such as optical media and flash drive

3. Entering and Viewing Metadata



Muhammad Izham Bin Norhamadi

Figure 4 Metadata1.docx



Total Editing Time	1 Minute
Title	Add a title
Tags	Add a tag
Comments	Add comments

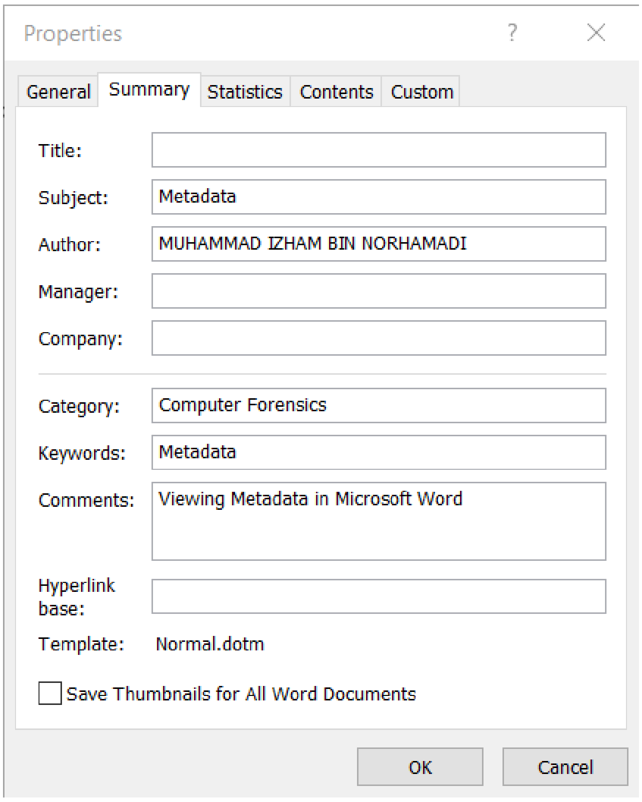
Related Dates

Last Modified	Today, 6:39 PM
Created	Today, 6:38 PM
Last Printed	

Related People

Author	MI MUHAMMAD IZHAM BIN NORHAMADI Add an author
Last Modified By	MI MUHAMMAD IZHAM BIN NORHAMADI

Figure 5 Microsoft Word Advanced Properties



Title:

Subject: Metadata

Author: MUHAMMAD IZHAM BIN NORHAMADI

Manager:

Company:

Category: Computer Forensics

Keywords: Metadata

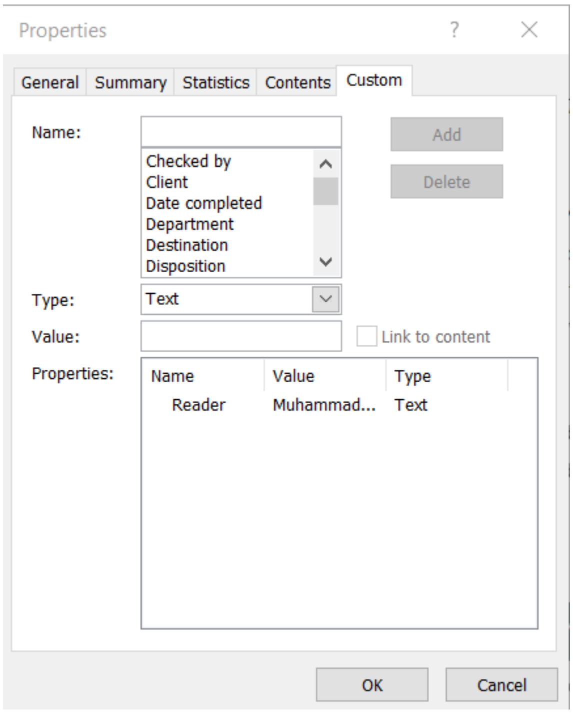
Comments: Viewing Metadata in Microsoft Word

Hyperlink base:

Template: Normal.dotm

□ Save Thumbnails for All Word Documents

Figure 6 Property Fields



Name:

Checked by
Client
Date completed
Department
Destination
Disposition

Type: Text

Value:

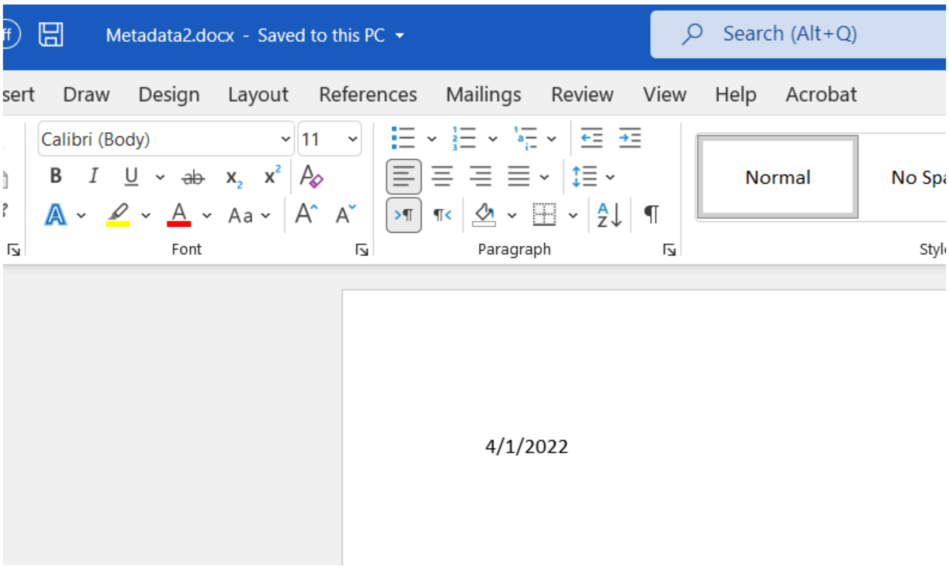
□ Link to content

Properties:

Name	Value	Type
Reader	Muhammad...	Text

Figure 7 Custom Properties

Muhammad Izham Bin Norhamadi (B032020039)



4/1/2022

Figure 8 Metadata2.docx

3.1. How could a computer forensics specialist use this metadata when examining this file?

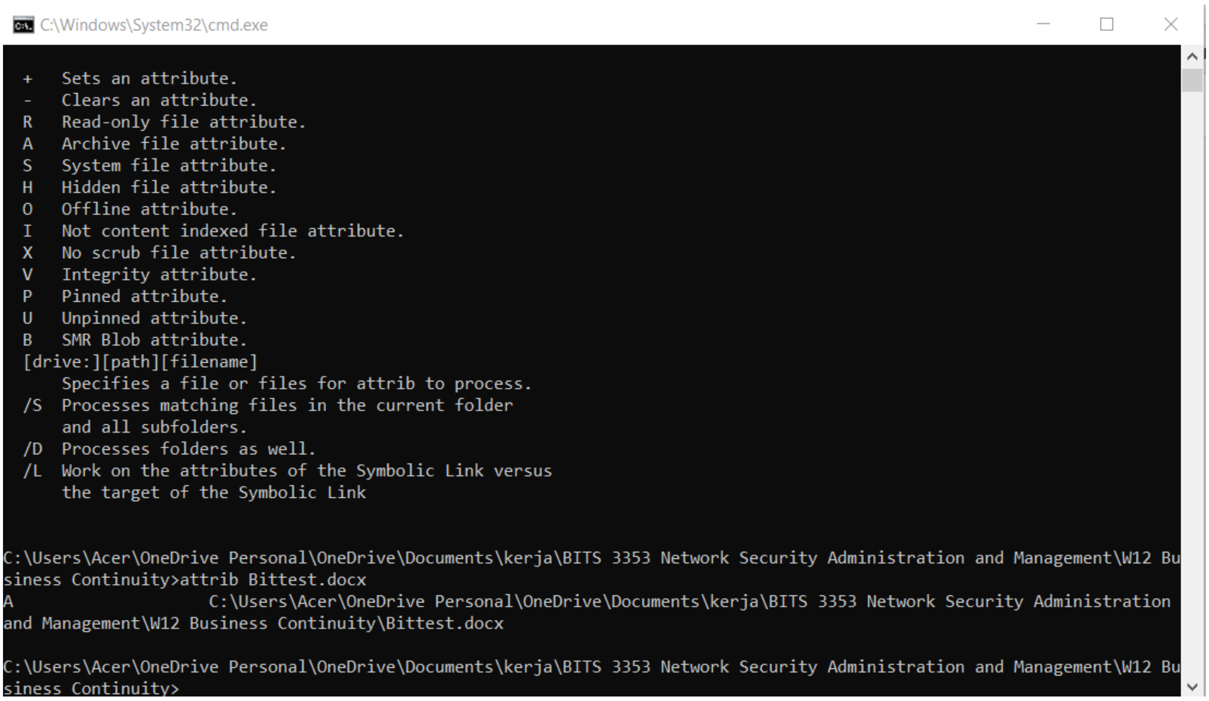
- Metadata can be used by forensics specialist to understand the history of an electronic file such as when it was created, modified, and accessed

3.2 What properties carried over to Metadata2.docx from Metadata1.docx, even though the contents of the file were erased? Why did this happen? Could a computer forensics specialist use this technique to examine metadata, even if the contents of the document were erased?

- Metadata field such as subject, author name, and keywords. Metadata persists so that finding and working with a particular files easier. Yes, the forensics specialists can use this method of examining metadata

Muhammad Izham Bin Norhamadi (B032020039)

4. Viewing and Changing the Backup Archive Bit

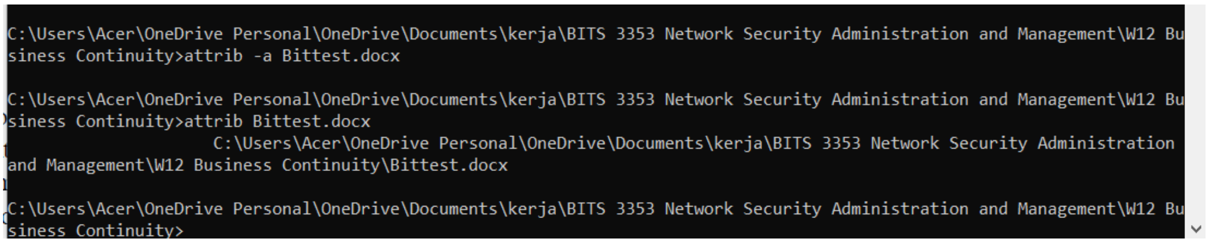


```
  +   Sets an attribute.
  -   Clears an attribute.
  R   Read-only file attribute.
  A   Archive file attribute.
  S   System file attribute.
  H   Hidden file attribute.
  O   Offline attribute.
  I   Not content indexed file attribute.
  X   No scrub file attribute.
  V   Integrity attribute.
  P   Pinned attribute.
  U   Unpinned attribute.
  B   SMR Blob attribute.
  [drive:][path][filename]
      Specifies a file or files for attrib to process.
  /S  Processes matching files in the current folder
      and all subfolders.
  /D  Processes folders as well.
  /L  Work on the attributes of the Symbolic Link versus
      the target of the Symbolic Link


C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration and Management\W12 Bu
siness Continuity>attrib Bittest.docx
A                    C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration
and Management\W12 Business Continuity\Bittest.docx

C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration and Management\W12 Bu
siness Continuity>
```

Figure 9 A Attribute Bittest.docx



```
C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration and Management\W12 Bu
siness Continuity>attrib -a Bittest.docx

C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration and Management\W12 Bu
siness Continuity>attrib Bittest.docx
                     C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration
and Management\W12 Business Continuity\Bittest.docx

C:\Users\Acer\OneDrive Personal\OneDrive\Documents\kerja\BITS 3353 Network Security Administration and Management\W12 Bu
siness Continuity>
```

Figure 10 Attribute Bittest.docx removed