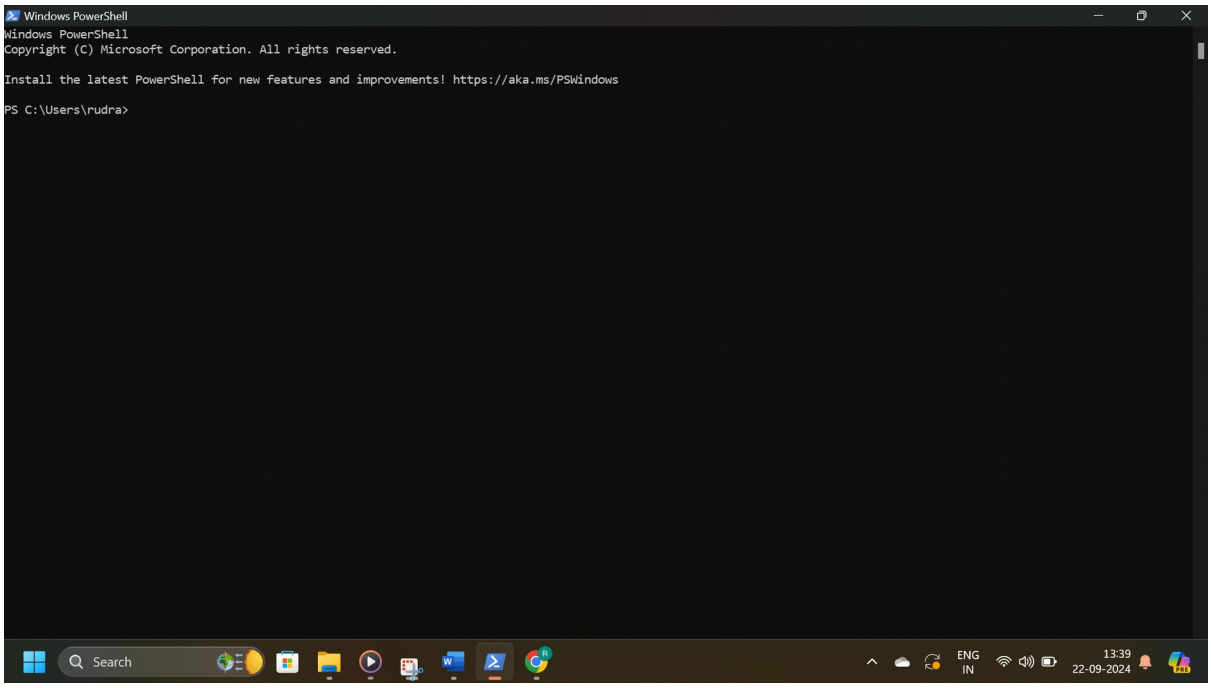
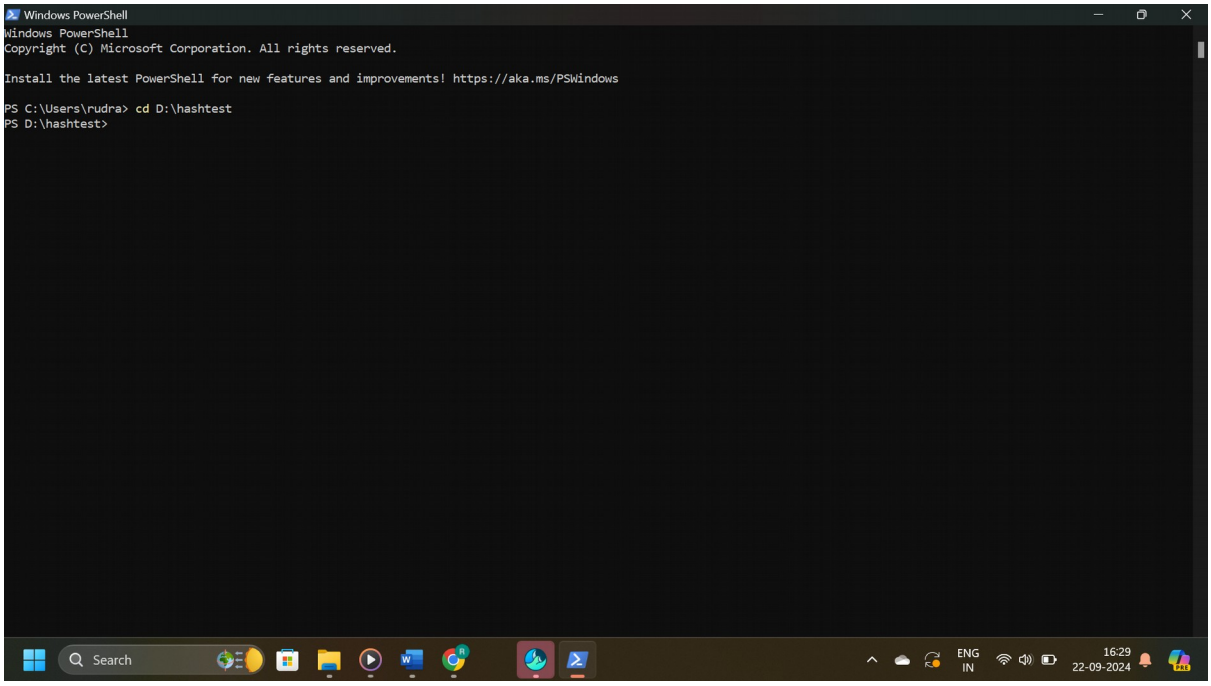
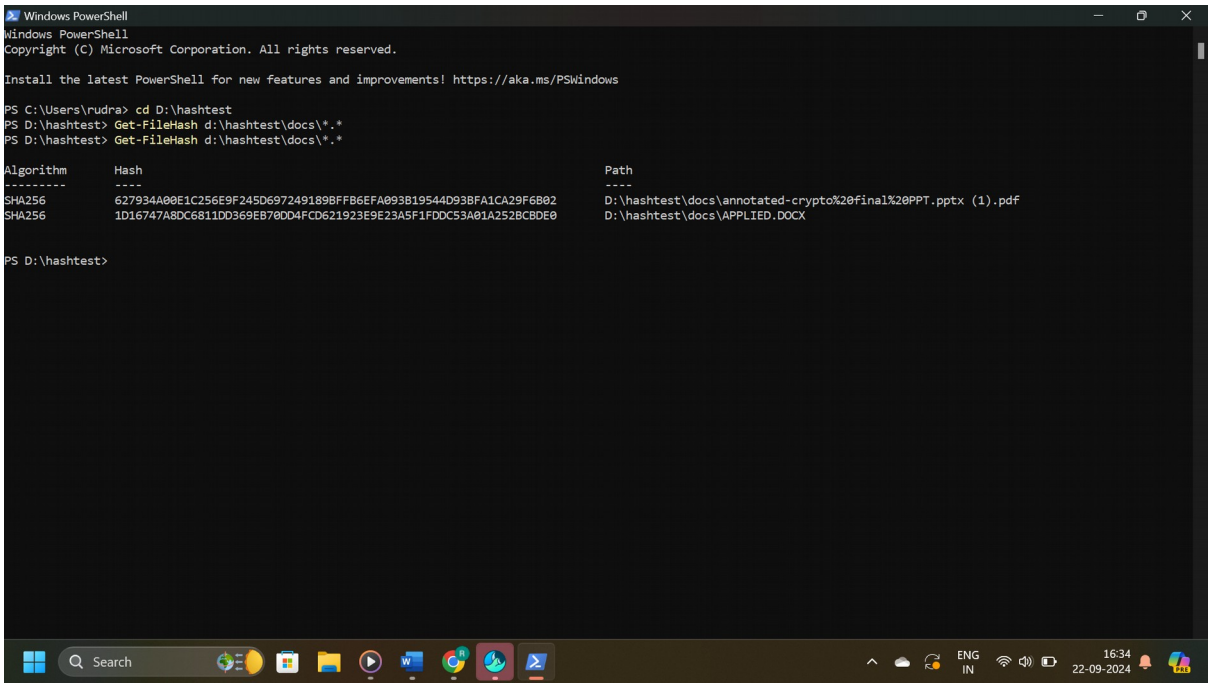
Name: Rudrama Devi CP

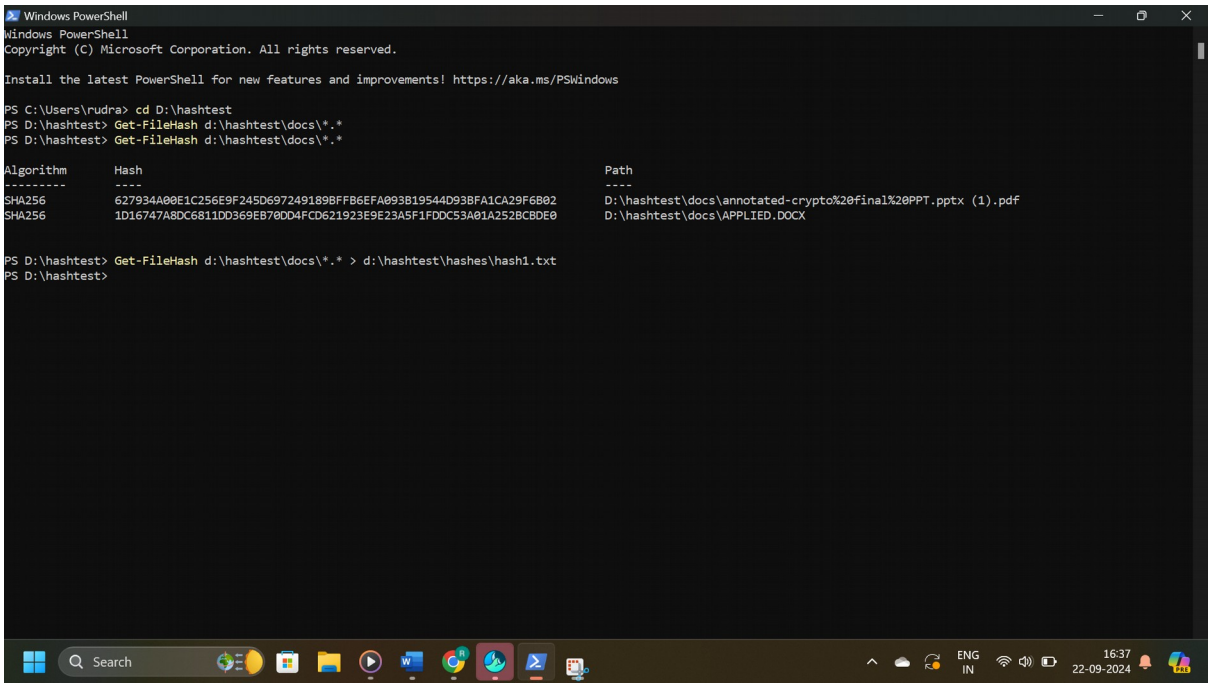
ID:16344164

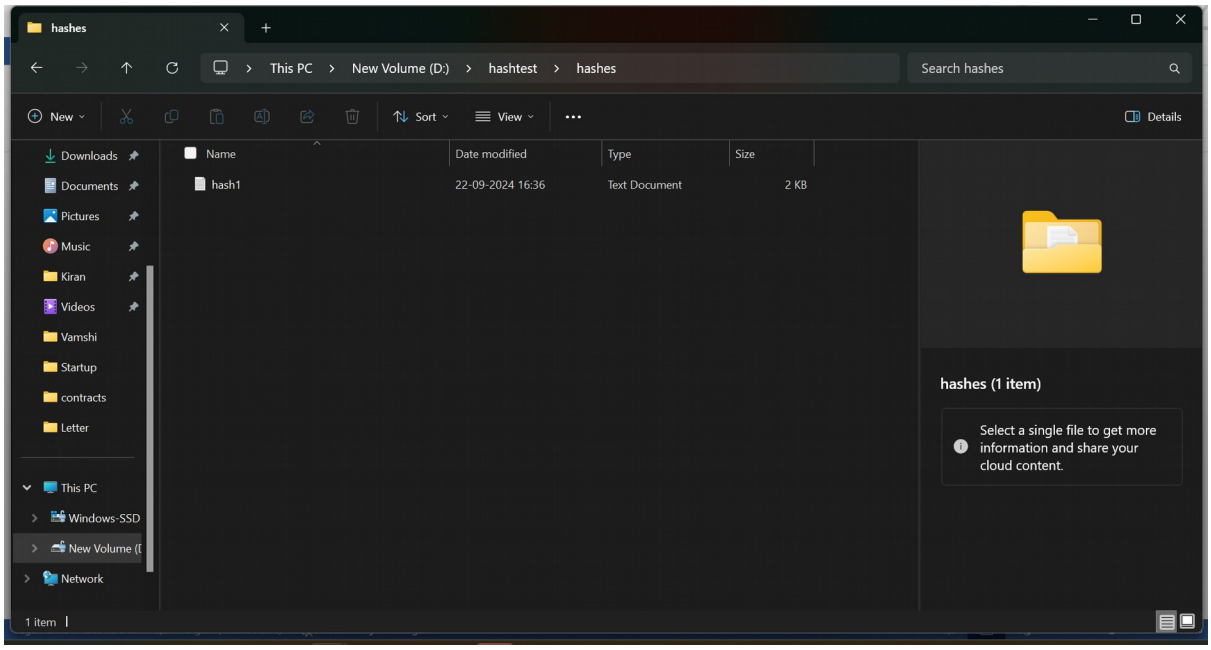
Simple File Integrity Monitoring with PowerShell Get-FileHash

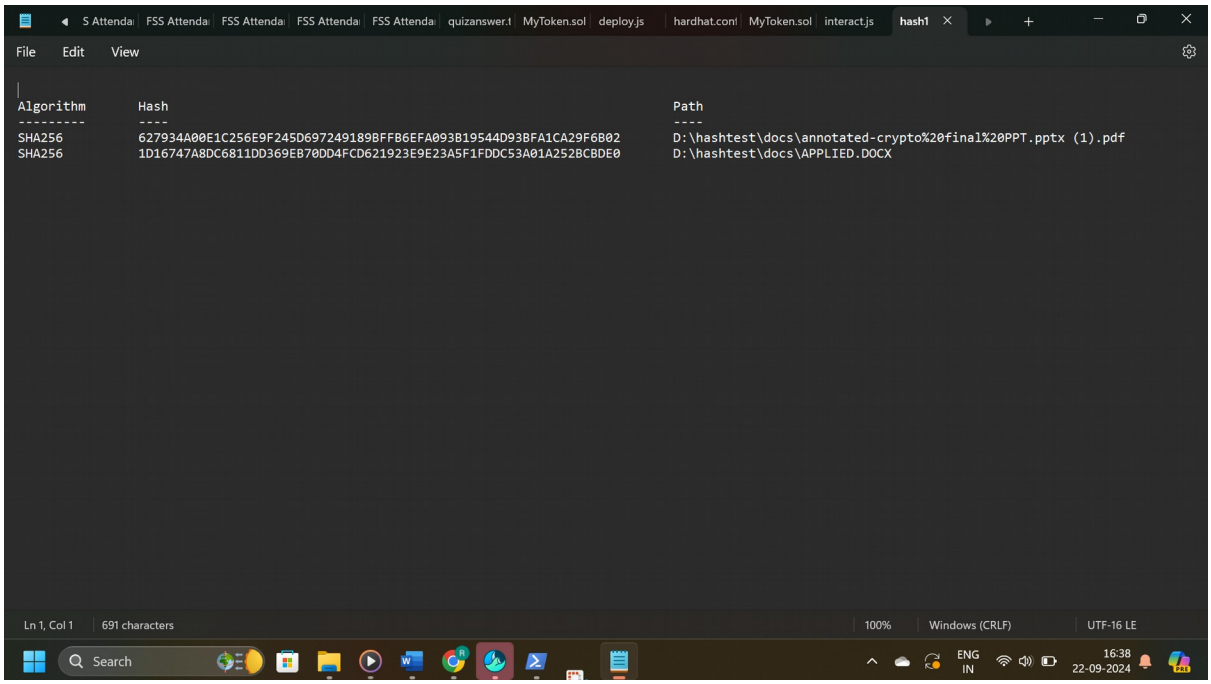


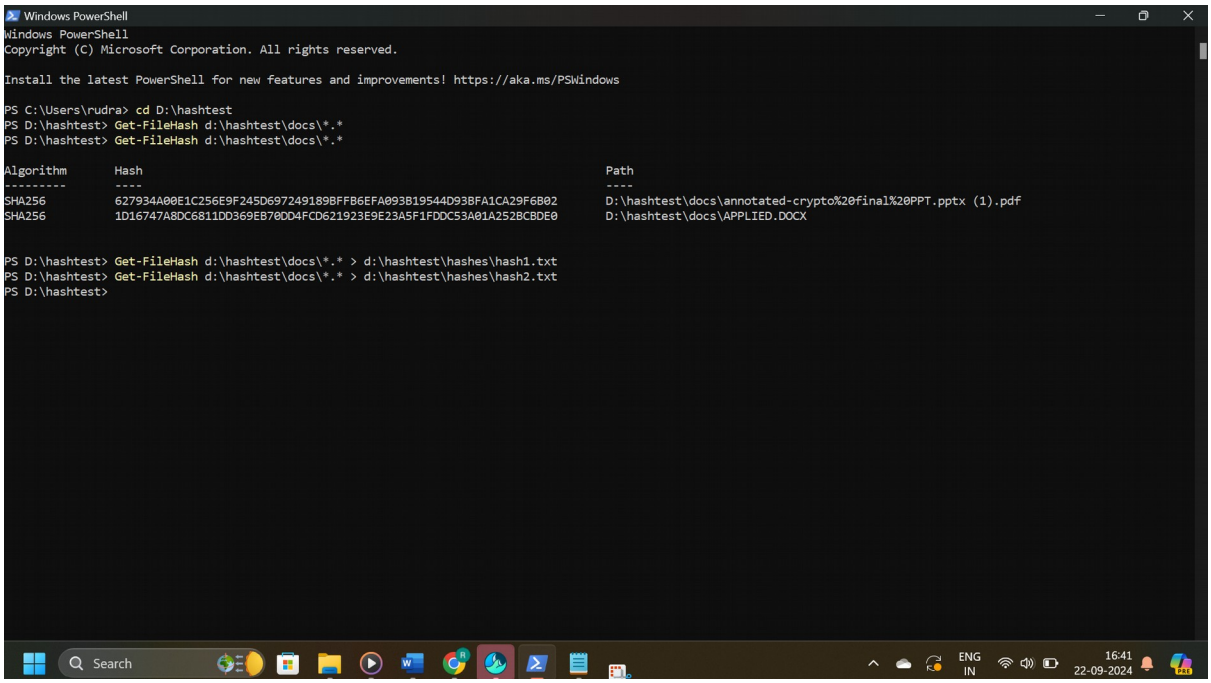


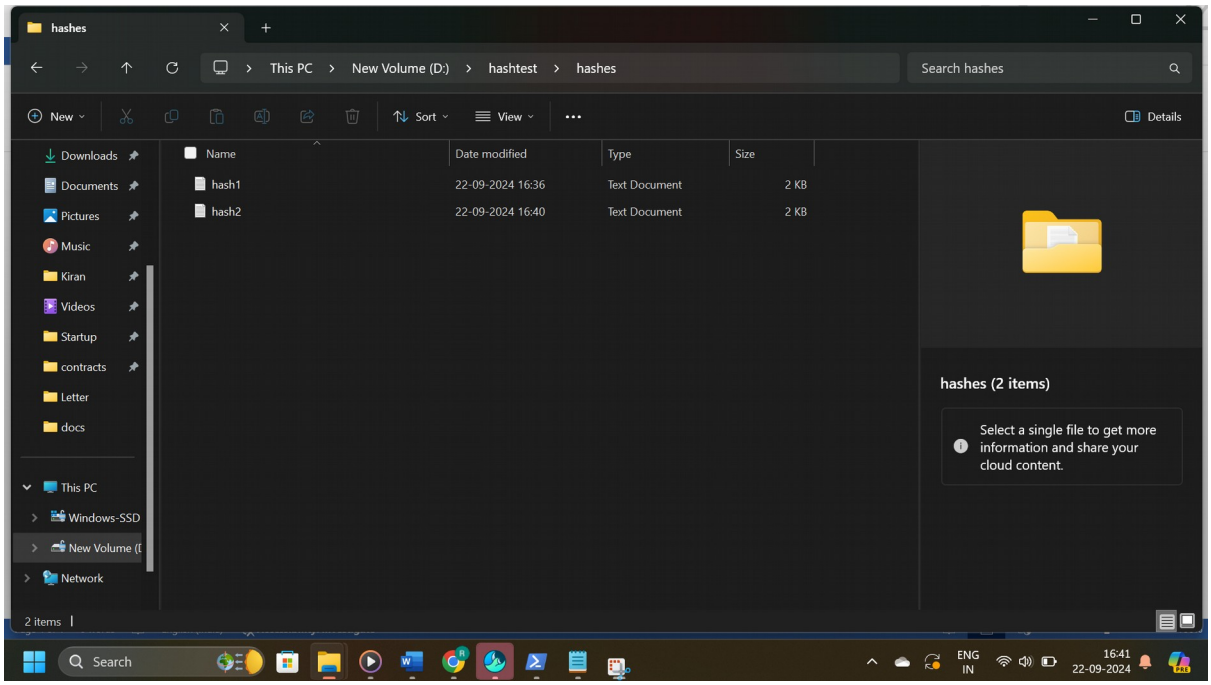

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\rudra> cd D:\hashtest
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
Algorithm Hash Path
SHA256 627934A00E1C256E9F245D697249189BFFB6EFA093B19544D93BFA1CA29F6B02 D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256 1D16747A8DC6811DD369EB70DD4FCD621923E9E23A5F1FDDC53A01A252BCBDE0 D:\hashtest\docs\APPLIED.DOCX
PS D:\hashtest>
Search
ENG
IN
16:34
22-09-2024

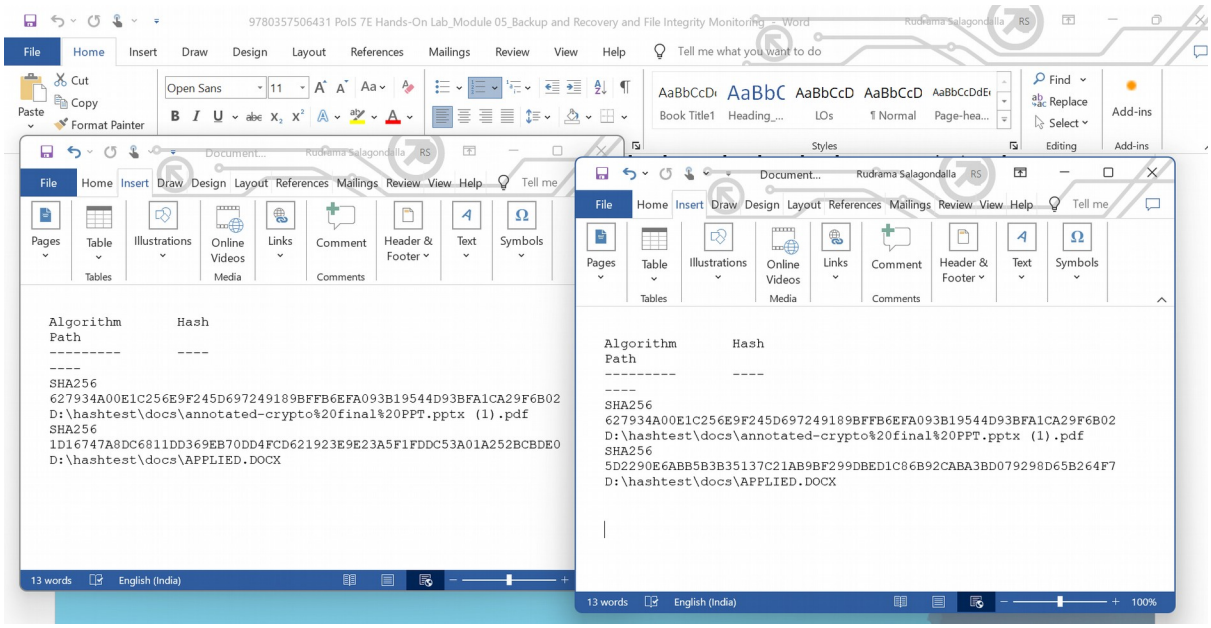

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\rudra> cd D:\hashtest
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
Algorithm Hash Path
SHA256 627934A00E1C256E9F245D697249189BFFB6EFA093B19544D93BFA1CA29F6B02 D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256 1D16747A8DC6811DD369EB70DD4FCD621923E9E23A5F1FDDC53A01A252BCBDE0 D:\hashtest\docs\APPLIED.DOCX
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.* > d:\hashtest\hashes\hash1.txt
PS D:\hashtest>
Search
ENG
IN
16:37
22-09-2024

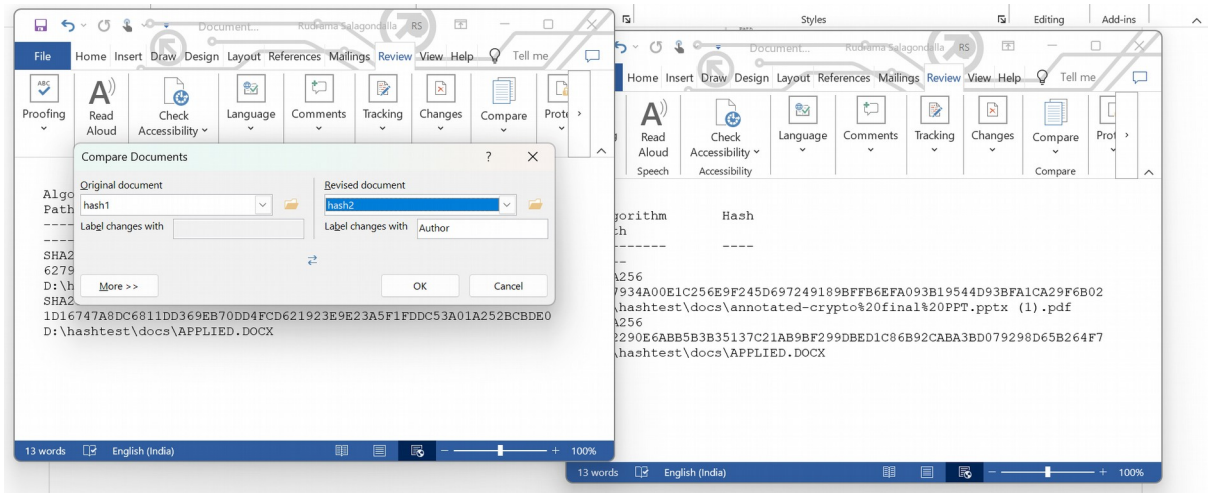

hashes
This PC
New Volume (D:)
hashtest
hashes
Search hashes
New
Sort
View
Details
Downloads
Documents
Pictures
Music
Kiran
Videos
Vamshi
Startup
contracts
Letter
This PC
Windows-SSD
New Volume ([
Network
Name
Date modified
Type
Size
hash1
22-09-2024 16:36
Text Document
2 KB
hashes (1 item)
Select a single file to get more information and share your cloud content.
1 item

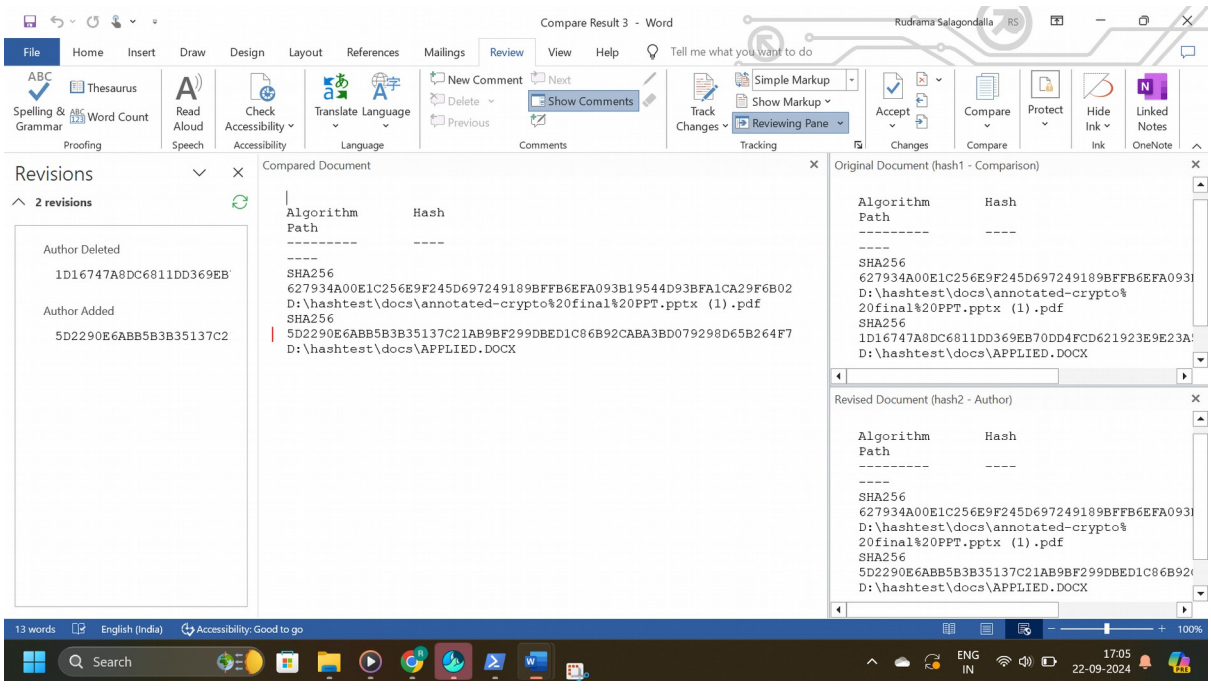

File
Edit
View
Algorithm Hash Path
SHA256 627934A00E1C256E9F245D697249189BFFB6EFA093B19544D93BFA1CA29F6B02 D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256 1D16747A8DC6811DD369EB70DD4FCD621923E9E23A5F1FDDC53A01A252BCBDE0 D:\hashtest\docs\APPLIED.DOCX
Ln 1, Col 1
691 characters
100%
Windows (CRLF)
UTF-16 LE
Search
ENG
IN
16:38
22-09-2024


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\rudra> cd D:\hashtest
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.*
Algorithm Hash Path
SHA256 627934A00E1C256E9F245D697249189BFFB6EFA093B19544D93BFA1CA29F6B02 D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256 1D16747A8DC6811DD369EB70DD4FCD621923E9E23A5F1FDDC53A01A252BCBDE0 D:\hashtest\docs\APPLIED.DOCX
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.* > d:\hashtest\hashes\hash1.txt
PS D:\hashtest> Get-FileHash d:\hashtest\docs*.* > d:\hashtest\hashes\hash2.txt
PS D:\hashtest>
Search
ENG IN
16:41 22-09-2024

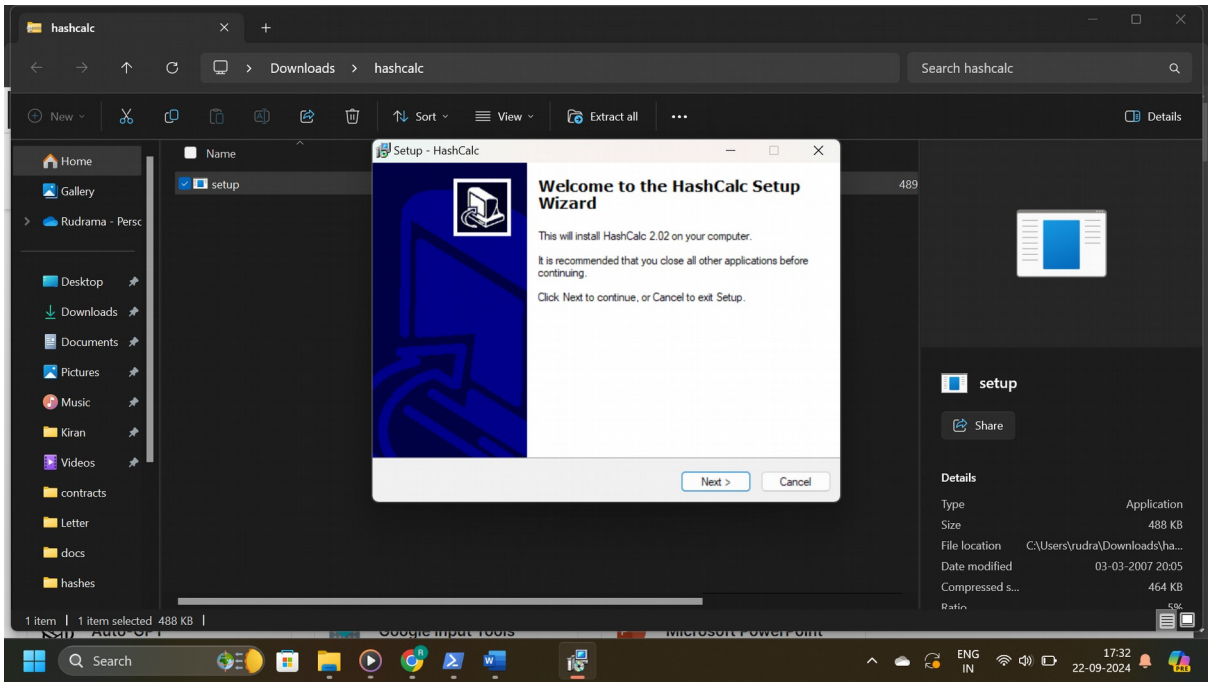

hashes
This PC › New Volume (D:) › hashtest › hashes
Search hashes
New
Sort
View
Details
Downloads
Documents
Pictures
Music
Kiran
Videos
Startup
contracts
Letter
docs
This PC
Windows-SSD
New Volume ([
Network
Name
Date modified
Type
Size
hash1 22-09-2024 16:36 Text Document 2 KB
hash2 22-09-2024 16:40 Text Document 2 KB
hashes (2 items)
Select a single file to get more information and share your cloud content.
2 items
Search
ENG IN
16:41 22-09-2024

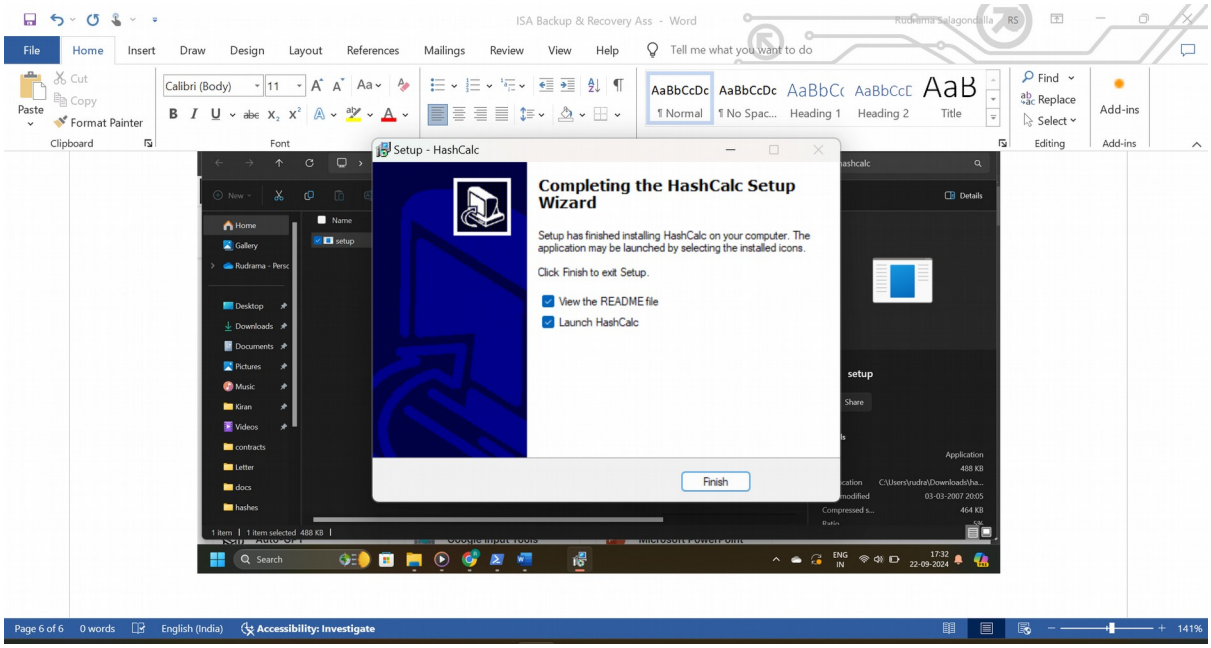

Algorithm Hash
Path
SHA256
627934A00E1C256E9F245D697249189BFFB6EFA093B19544D93BFA1CA29F6B02
D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256
1D16747A8DC6811DD369EB70DD4FCD621923E9E23A5F1FDDC53A01A252BCBDE0
D:\hashtest\docs\APPLIED.DOCX
SHA256
5D2290E6ABB5B3B35137C21AB9BF299DBED1C86B92CABA3BD079298D65B264F7
D:\hashtest\docs\APPLIED.DOCX

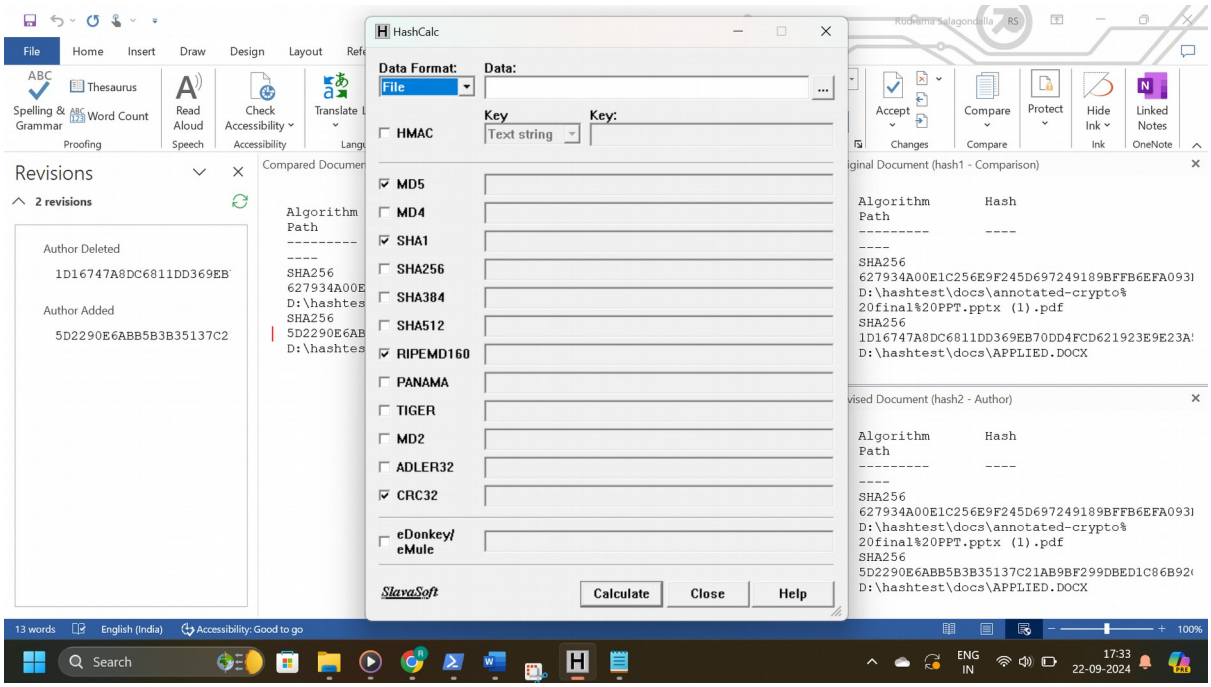

Compare Documents
Original document
hash1
Label changes with
Revised document
hash2
Label changes with
Author
More >>
OK
Cancel

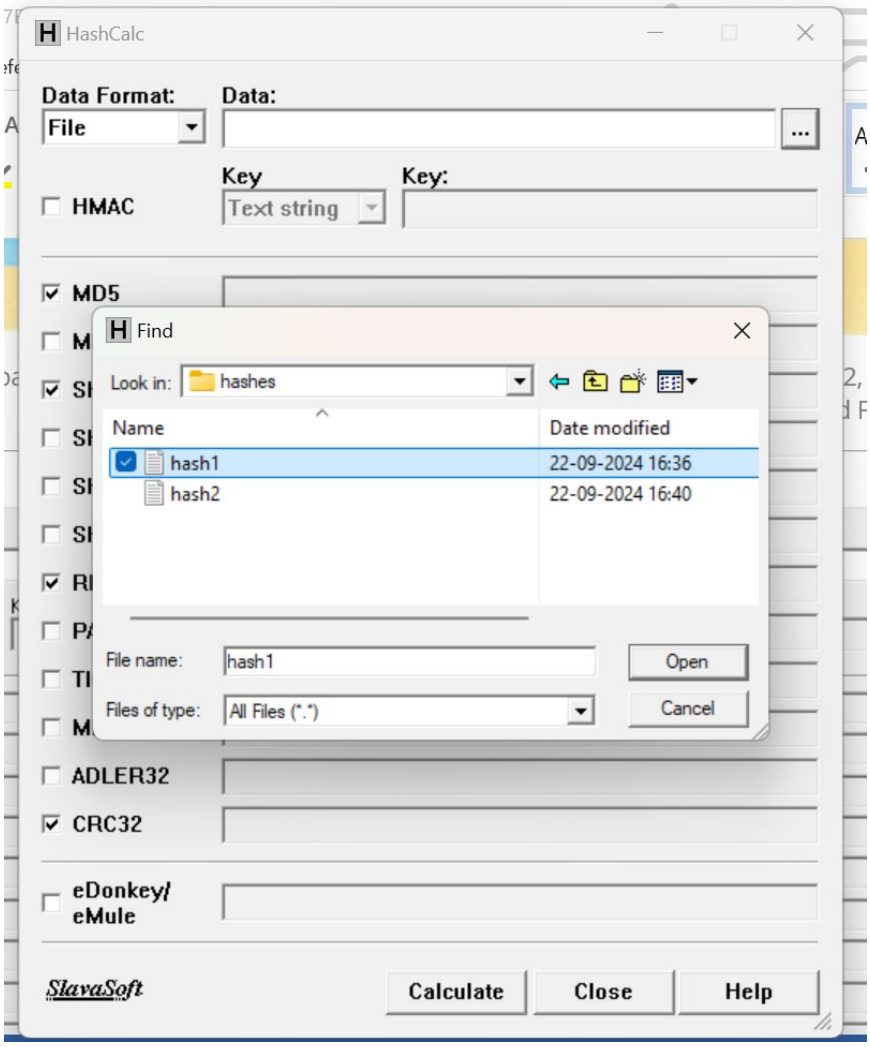

Revisions
2 revisions
Author Deleted
1D16747A8DC6811DD369EB
Author Added
5D2290E6ABB5B3B35137C2
Compared Document
Original Document (hash1 - Comparison)
Revised Document (hash2 - Author)

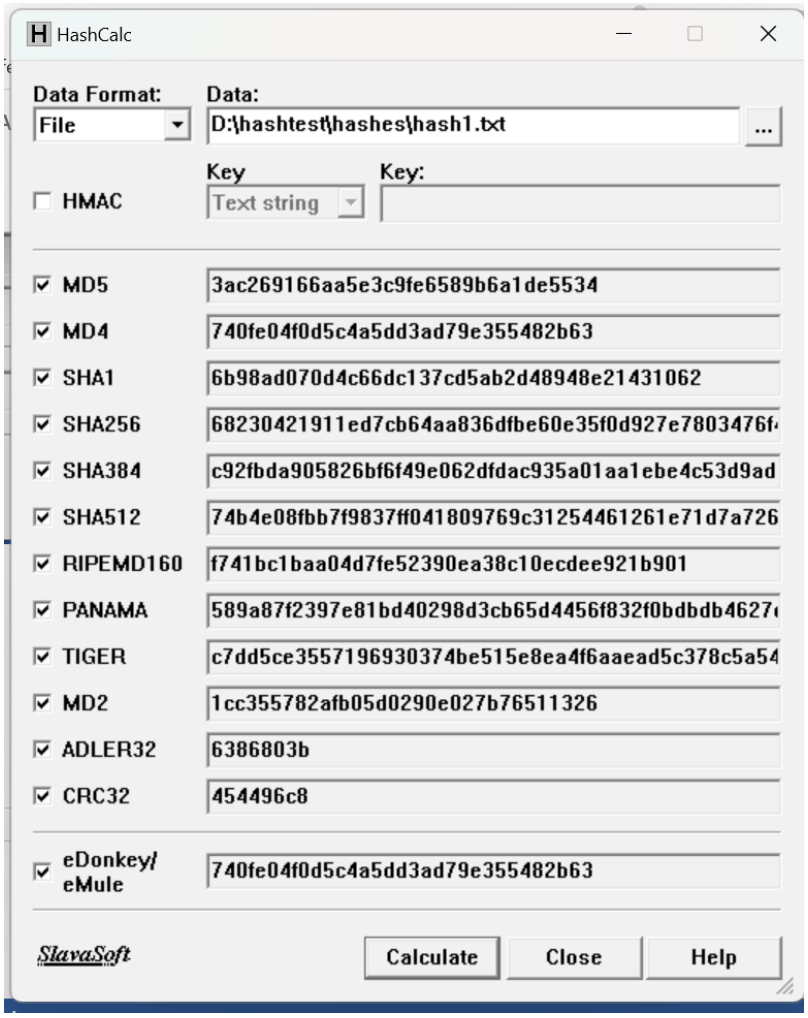
Simple File Integrity Monitoring with HashCalc



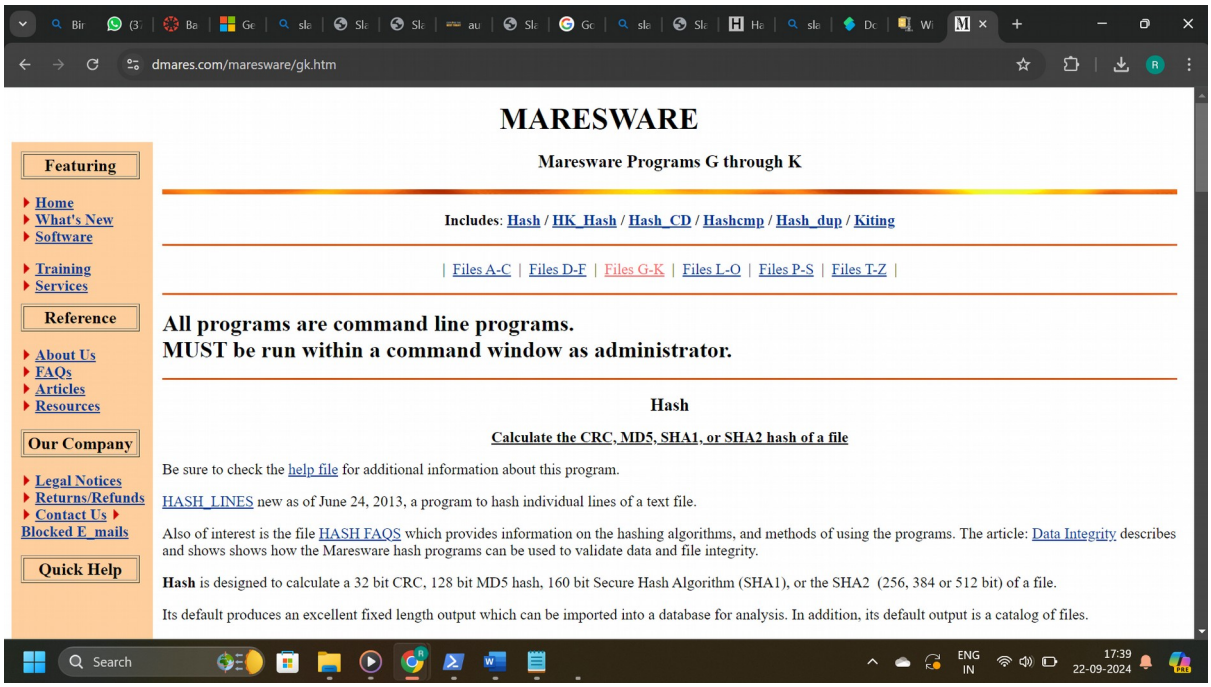


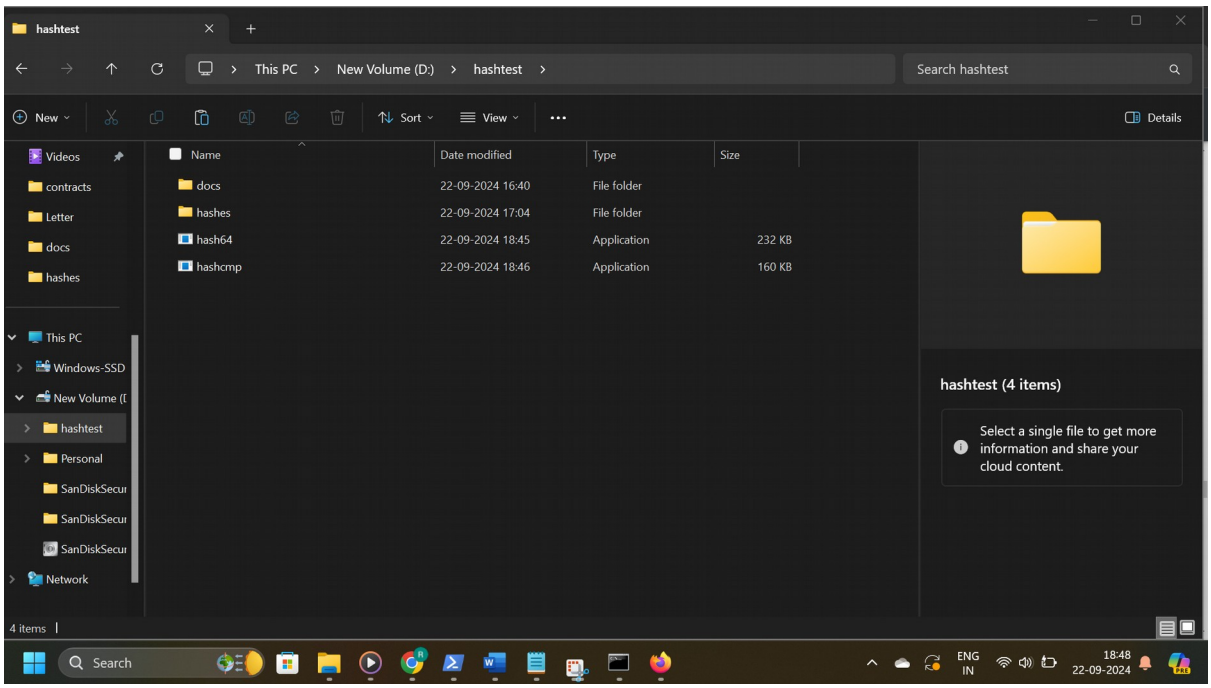

HashCalc
Data Format:
File
Data:
Key
Text string
Key:
HMAC
MD5
MD4
SHA1
SHA256
SHA384
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
Revisions
2 revisions
Author Deleted
1D16747A8DC6811DD369EB
Author Added
5D2290E6ABB5B3B35137C2
Algorithm Hash
Path
SHA256
627934A00E1C256E9F245D697249189BFFB6EFA093
D:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf
SHA256
1D16747A8DC6811DD369EB70DD4FCD621923E9E23A
D:\hashtest\docs\APPLIED.DOCX
SHA256
5D2290E6ABB5B3B35137C21AB9BF299DBED1C86B92
D:\hashtest\docs\APPLIED.DOCX


HashCalc
Data Format:
File
Data:
Key
Text string
Key:
HMAC
MD5
ADLER32
CRC32
eDonkey/ eMule
SlavaSoft
Calculate
Close
Help
Find
Look in:
hashes
Name
Date modified
hash1
22-09-2024 16:36
hash2
22-09-2024 16:40
File name:
hash1
Open
Files of type:
All Files (*.*)
Cancel


HashCalc
Data Format:
File
Data:
D:\hashtest\hashes\hash1.txt
...
HMAC
Key
Text string
Key:
MD5
3ac269166aa5e3c9fe6589b6a1de5534
MD4
740fe04f0d5c4a5dd3ad79e355482b63
SHA1
6b98ad070d4c66dc137cd5ab2d48948e21431062
SHA256
68230421911ed7cb64aa836dfbe60e35f0d927e7803476f
SHA384
c92fbda905826bf6f49e062dfdac935a01aa1ebe4c53d9ad
SHA512
74b4e08fbb7f9837ff041809769c31254461261e71d7a726
RIPEMD160
f741bc1baa04d7fe52390ea38c10ecdee921b901
PANAMA
589a87f2397e81bd40298d3cb65d4456f832f0bdbdb4627
TIGER
c7dd5ce3557196930374be515e8ea4f6aaead5c378c5a54
MD2
1cc355782afb05d0290e027b76511326
ADLER32
6386803b
CRC32
454496c8
eDonkey/ eMule
740fe04f0d5c4a5dd3ad79e355482b63
SlavaSoft
Calculate
Close
Help

Using Maresware Hash64 and Hashcmp to Monitor File Integrity

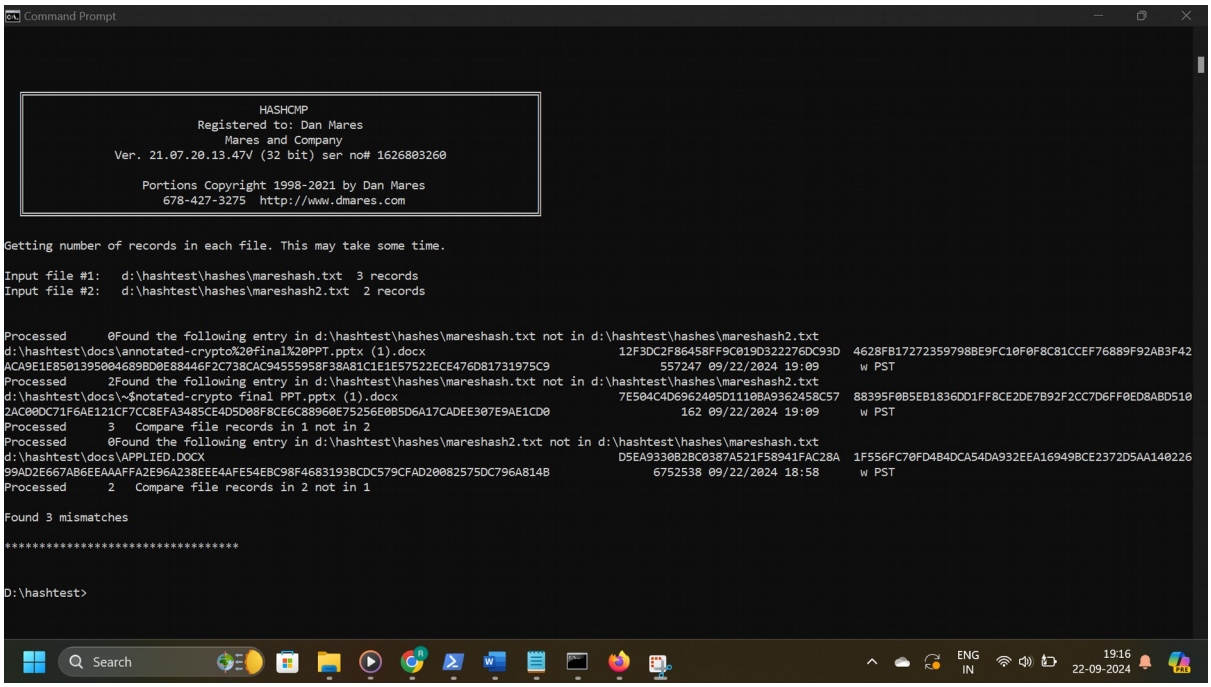




```
D:\hashtest>hash64 -p d:\hashtest\docs\ -256

Started Mon Sep 23 01:53:00 2024 GMT, 18:53 Pacific Standard Time (PST/PDT:8*)

  Last Access Date UPDATE is turned ON


 -------- BEGIN PROCESSING MD5 -----------
  PATH                                                                                                MD5
     SHA2 - 256                SIZE  MDATE      MTIME   TZ
d:\hashtest\docs\annotated-crypto%20final%20PPT.pptx (1).pdf                                DB50EEE7848E662267F232F0767FC201  BF12B45B73D8C412CE361492C86E715C53B74F10D62E04490
A97FDD286BA539BA165CA82D29F017AE7F503C469B6C78DA04C58DC3B6AC4CBB5BEB342312F213D        702292 04/24/2024 13:12      w PST
d:\hashtest\docs\APPLIED.DOCX                                                               FF08A746E1D478CBFD31C9322412F563  304AE499D7334E8853E47F4E184A5271D528619C560146F65
179B67F95DF8A9B46FCD989BFED9A4F1AB06831C11CA5B166219DA84036E6806047A8130FB9FF15        6750474 09/22/2024 16:40      w PST
 -------- END PROCESSING MD5 -----------

  0 directories, 2 files, 7,452,766 bytes, 7.45 MB
  Drive Freespace 4,175,335,424
  Elapsed:  0 hrs. 0 mins. 0 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash.txt

  0 directories, 2 files, 7,452,766 bytes, 7.45 MB
  Drive Freespace 4,175,335,424
  Elapsed:  0 hrs. 0 mins. 0 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash.txt

  0 directories, 2 files, 7,452,733 bytes, 7.45 MB
  Drive Freespace 4,175,335,424
  Elapsed:  0 hrs. 0 mins. 0 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash.txt
```



```
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash.txt

  0 directories, 2 files, 7,452,733 bytes, 7.45 MB
  Drive Freespace 4,175,335,424
  Elapsed:  0 hrs. 0 mins. 0 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash.txt

  0 directories, 2 files, 7,454,830 bytes, 7.45 MB
  Drive Freespace 4,175,335,424
  Elapsed:  0 hrs. 0 mins. 0 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hash64 -p d:\hashtest\docs\ -256 > d:\hashtest\hashes\mareshash2.txt

  0 directories, 2 files, 7,454,830 bytes, 7.45 MB
  Drive Freespace 4,175,331,328
  Elapsed:  0 hrs. 0 mins. 1 secs.
  Last Access Date UPDATE is: turned ON


D:\hashtest>hashcmp d:\hashtest\hashes\mareshash.txt d:\hashtest\hashes\mareshash2.txt
```



Self-Reflection and Response:

Have you chosen to make a backup copy of your computer system? In the space below, explain why or why not. What steps did you take (or will you take in the future) to research and implement your method?

I've decided to backup my computer system since they provide a safeguard against unintentional deletion, corruption, data loss, and hardware failure scenarios, all of which could jeopardize sensitive information. They act as a defense for our settings, programs, documents, and data. In addition to local backups kept on external hard drives, I intend to use cloud backup services like Google Drive and Amazon S3.

Can you think of another reason, not mentioned in the lab, for using the File Integrity monitor featers found in PowerShell? Describe how you might use it.

utilizing Event Logging: PowerShell's robust event logging features enable you to record file integrity events and maintain an extensive audit trail, which is one of the additional advantages of utilizing File Integrity Monitor. This information is very helpful for both forensic investigation and compliance reporting.

Remote Monitoring: PowerShell may be used to monitor file integrity via a network, which is useful for organizations with distributed systems or several servers.

Were you able to install and use the hashing tools from MaresWare? What was your experience using these tools?

Yes, I was able to successfully install and use the Maresware hashing tools. These instruments are frequently used to guarantee the accuracy of files and data. Users can confirm that files haven't been altered or corrupted during transmission or storage by using Maresware hashing tools to generate hash values for files.