

Forum:[Hack Forums](#)

Thread: [How to use Certutil to generate SHA-256 Hash to compare files](#)

Hackoo - May 14, 2018, 5:08 am

Hi ?

Many sites publish a [hash/checksum] for files you download.

These can be MD5, SHA-1, SHA256 or SHA512 and each are a string of [numbers/letters] that make up a unique "fingerprint" of the file downloaded.

The vendor creates the [hash/checksum] when they upload it and publish it.

When the customer downloads it, they can validate what they downloaded was the exact same file that the publisher uploaded.

Example : How to use SHA-256 Hash to Verify Your Downloads Haven't Been Modified

Let's compare a downloaded hash by going to a website that displays the checksum for a download.

For this test, we will be using the download page of [VLC media player for Windows](#).

On their site, they helpfully display their checksum in an SHA-256 hash format by clicking the "Display Checksum" button.

Stay on this webpage, as we'll need to compare the hash against that number shortly.

Each operating system has many different programs for checking/calculating this. Windows has a utility built in called Certutil

So, i created this batch file to compare files SHA-256 hashes using Certutil in command line.

PHP Code

```
<?php
@echo off
Color 0A & Mode 95,6
Title Using Certutil Command Line to Compare SHA256 HASHES Files by Hackoo 2018
set "ScriptName=%~nx0"
if "%~1"==" " goto error
Set
"SHA256_VLC_v302=30160a607e5ec2e4a2718ea2e37764647f6cfc9c7eb31f58f9f873521726695a"
for /f "delims=" %%H in (
'CertUtil -hashfile "%~1" SHA256 ^| findstr /I /V "%~n1:" ^| findstr /I /V "CertUtil") Do (
Set "SHA256hash=%%H"
)
echo(
echo HASH "%~nx1" = "%SHA256hash%"
echo HASH of SHA256_VLC = "%SHA256_VLC_v302%"
If [%SHA256_VLC_v302%] EQU [%SHA256hash%] (
Color 0A & echo( & echo The File is AUTHENTIC !
) else (
Color 0C & echo( & echo The File is NOT AUTHENTIC !
)
pause>nul & Exit
```

```

:*****
:
:Error
Color 0C & Mode 85,5
echo( & echo(
echo    You should drag and drop a file over this batch file "%ScriptName%"
Timeout /T 5 /nobreak>nul & exit
:*****
:

```

How to use this batch file :

Just open your notepad and copy and paste this code above and save it as SHA256_Certutil.bat and drag and drop your downloaded file : in our case (vlc-3.0.2-win32.exe) over it to get something like this :

Phlox - May 14, 2018, 6:35 am

Fantastic script Hackoo, one person was asking for something like this. I just found the Get-FileHash cmdlet which computes the hash value for a file by using a specified hash algorithm.

"Get-FileHash"

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-6>

Hackoo - May 14, 2018, 7:23 am

(May 14, 2018 06:35 AM)Phlox Wrote: [\[CITE\]](#) Fantastic script Hackoo, one person was asking for something like this. I just found the Get-FileHash cmdlet which computes the hash value for a file by using a specified hash algorithm.

"Get-FileHash"

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-6>

?

I made another script to check MD5 Hashes Checksum to compare two videos files for a member in a french forum that asked me something like this :

NB : Translated with Google Translate

Quote:Hello,

my problem is quite simple, but I do not see how to achieve it ??

I have 2 video files, and I would just like to know if I made a copy under another name of the same file. I know it's not good to remember when you did it yourself, but would you have any idea how to do it?

Knowing the differences between the 2, is not mandatory, because I doubt that it is complex on a video. Just know if it's the same file or not. I thought about the MD5 but I have no idea how we do it, and it may be too complicated for something so simple?

Thank you

Just copy and paste this code into your Notepad and save it as MD5_Files_Compare.bat Then drag and drop your two files one by one on this batch to compare their MD5 HASHES

PHP Code

<?php

```

@echo off
>nul chcp 65001
Color 0A & Mode 110,6
Title Using Certutil Command Line to Compare MD5 HASHES Files by Hackoo 2018
Set "LogFile=%~n0.txt"
Set "MD5hash1="
Set "MD5hash2="
echo(
echo Drag and drop a file N°1 and hit enter key to get its MD5 HASH Checksum
Set /p File1=
for /f "delims=" %%a in ("%File1%") do (
    Set "FilePath1=%%~fa"
    Set "FileName1=%%~nxa"
)

for /f "delims=" %%H in (
'CertUtil -hashfile "%FilePath1%" MD5 ^| findstr /I /V "%FileName1%:" ^| findstr /I /V "CertUtil"' ) Do (
    Set "MD5hash1=%%H"
)
echo HASH of "%FileName1%" = "%MD5hash1%"
Timeout /T 2 /NoBreak>nul
cls
echo(
echo Drag and drop another file N°2 and hit enter key to get its MD5 HASH and to compare it with
"%FileName1%"
Set /p File2=
for /f "delims=" %%b in ("%File2%") do (
    Set "FilePath2=%%~fb"
    Set "FileName2=%%~nxb"
)

for /f "delims=" %%G in (
'CertUtil -hashfile "%FilePath2%" MD5 ^| findstr /I /V "%FileName2%:" ^| findstr /I /V "CertUtil"' ) Do (
    Set "MD5hash2=%%G"
)
echo HASH of "%FileName2%" = "%MD5hash2%"
Timeout /T 2 /NoBreak>nul
cls
echo(
If [%MD5hash1%] EQU [%MD5hash2%] (
    Color 0A
    echo THE TWO FILES ARE AUTHENTIC !
    echo MD5 HASH of "%FileName1%" = "%MD5hash1%"
    echo MD5 HASH of "%FileName2%" = "%MD5hash2%"
) else (
    Color 0C
    echo THE TWO FILES ARE NOT AUTHENTIC !
    echo MD5 HASH of "%FileName1%" = "%MD5hash1%"
    echo MD5 HASH of "%FileName2%" = "%MD5hash2%"
)
(
    If [%MD5hash1%] EQU [%MD5hash2%] (
        echo THE TWO FILES ARE AUTHENTIC !
    )
)

```

```

echo MD5 HASH of "%FileName1%" = "%MD5hash1%"
echo MD5 HASH of "%FileName2%" = "%MD5hash2%"
) else (
echo THE TWO FILES ARE NOT AUTHENTIC !
echo MD5 HASH of "%FileName1%" = "%MD5hash1%"
echo MD5 HASH of "%FileName2%" = "%MD5hash2%"
)
)>"%LogFile%"
Timeout /T 4 /NoBreak>nul & Start "" "%LogFile%"
Exit

```

?

HFDone - May 14, 2018, 7:52 am

you just check if its equ you dont echo the hash

if you want to echo the hash you need to use delims and trim the spaces

Code for /f "delims=" %%x in ('CertUtil -hashfile "%~1" SHA256 ^| findstr /i /v "exe:" ^| findstr /i /v "CertUtil") do set x=%%x
and it can be done without find ?

(May 14, 2018 06:35 AM)Phlox Wrote: [\[CITE\]](#) Fantastic script Hackoo, one person was asking for something like this. I just found the Get-FileHash cmdlet which computes the hash value for a file by using a specified hash algorithm.

"Get-FileHash"

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-6>
ps v4 and up

Hackoo - May 14, 2018, 10:38 am

(May 14, 2018 07:52 AM)HFDone Wrote: [\[CITE\]](#) you just check if its equ you dont echo the hash

if you want to echo the hash you need to use delims and trim the spaces

Code for /f "delims=" %%x in ('CertUtil -hashfile "%~1" SHA256 ^| findstr /i /v "exe:" ^| findstr /i /v "CertUtil") do set x=%%x
and it can be done without find ?

ps v4 and up

Thank you very much HFDone for your great remark ?

So i edit my two scripts based on your remark of course ?

Please, feel free to re-check my last edit and tell me if are optimized or not ?

Thank you again for your assistance ?

HFDone - May 14, 2018, 10:49 am

(May 14, 2018 10:38 AM)Hackoo Wrote: [\[CITE\]](#) Thank you very much HFDone for your great remark ?

So i edit my two scripts based on your remark of course ?

Please, feel free to re-check my last edit and tell me if are optimized or not ?

Thank you again for your assistance ?

you still need to trim the spaces

what i mean is that what if i just want to get file hash

```

Code for /f "delims=" %%x in ('CertUtil -hashfile "%~1" SHA256 ^| findstr /i /v "%~n1:" ^| findstr /i /v
"CertUtil") do set x=%%x
rem trim spaces
echo %x: =%
and for all the hashes you can
Code for %%a in (MD5 SHA1 SHA256 SHA512) do (
... the code above
)
and without find
Code for /f "skip=1 delims=" %%x in ('CertUtil -hashfile "%~1" SHA256') do set x=%%x & goto e
:e
echo %x: =%

```

?CARUs L?VE?™ - May 14, 2018, 12:49 pm

This is a fantastic script hackoo! I actually have MANY uses for this and it certainly will come in handy. Thank you for the release!

Hackoo - May 14, 2018, 2:12 pm

(May 14, 2018 10:49 AM)HFDone Wrote: [\[CITE\]](#) and for all the hashes you can

Code for %%a in (MD5 SHA1 SHA256 SHA512) do (

... the code above

)and without find

Code for /f "skip=1 delims=" %%x in ('CertUtil -hashfile "%~1" SHA256') do set x=%%x & goto e

:e

echo %x: =%

(May 14, 2018 12:49 PM)?CARUs L?VE?™ Wrote: [\[CITE\]](#) This is a fantastic script hackoo! I actually have MANY uses for this and it certainly will come in handy. Thank you for the release!

Thank you ?CARUs for your feed back ? and don't forget to rate it ?

This script can get all HASHES (MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512) from a file by drag and drop over this batch script and save results into a text file ? ?

PHP Code

```
<?php
```

```
@echo off
```

```
Color 0A & Mode 136,8
```

```
Title Get [MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512] HASHES from file by drag and
drop using Certutil by Hackoo 2018
```

```
set "ScriptName=%~nx0"
```

```
if "%~1"==" " goto error
```

```
Set "LogFile=%~nx1_HASHES.txt"
```

```
If Exist "%LogFile%" Del "%LogFile%"
```

```
setlocal enabledelayedexpansion
```

```
for %%a in (MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512) do (
```

```
Set /a i+=1
```

```
Set "HASH[!i!]=%%a"
```

```
)
```

```
for /L %%j in (1,1,%%i) do (
```

```
for /f "skip=1 delims=" %%x in ('CertUtil -hashfile "%~1" !HASH[%%j]! ^| findstr /i /v "CertUtil") do (
```

```
set "HASH=%%x"
```

```
set "HASH=!HASH: =!"
```

```
)
```

```

echo !HASH[%%j]!==HASH!
echo !HASH[%%j]!==HASH!>>"%LogFile%"
)
Timeout /T 4 /NoBreak>nul & Start "" "%LogFile%" & Exit
:*****
:Error
Color 0C & Mode 80,5
echo( & echo(
echo    You should drag and drop a file over this batch file "%ScriptName%"
Timeout /T 5 /nobreak>nul & exit
:*****

```

Sir-Teabag - May 14, 2018, 7:54 pm

Awesome job Hackoo!

I would suggest that you use the set /p option to ask the user for the hash to compare to though, instead of it being VLC by default. ?

HFDone - May 15, 2018, 1:00 am

```

Code for %%a in (MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512) do (
    for /f "skip=1 delims=" %%x in ('CertUtil -hashfile "%~1" %%a ^| findstr /i /v "CertUtil") do set
x=%%x
    echo %%a !x: =!
)

```

Hackoo - May 15, 2018, 1:27 am

(May 15, 2018 01:00 AM)HFDone Wrote: [\[CITE\]](#) Code for %%a in (MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512) do (for /f "skip=1 delims=" %%x in ('CertUtil -hashfile "%~1" %%a ^| findstr /i /v "CertUtil") do set x=%%x echo %%a !x: =!) Thank you for your help Bro ? ?

PHP Code

```

<?php
@echo off
Color 0A & Mode 136,10
Title GET ( MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512 ) HASHES from file by drag and
drop using Certutil by Hackoo 2018
set "ScriptName=%~nx0"
if "%~1"==" " goto error
Set "LogFile=%~nx1_HASHES.txt"
If Exist "%LogFile%" Del "%LogFile%"
SetLocal EnableDelayedExpansion
echo(
for %%a in (MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512) do (
    for /f "skip=1 delims=" %%H in ('CertUtil -hashfile "%~1" %%a ^| findstr /i /v "CertUtil") do set H
=%%H
    echo %%a=!H: =!
(echo %%a=!H: =!)>>"%LogFile%"

```

```

)
Timeout /T 4 /NoBreak>nul & Start "" "%LogFile%" & Exit
..*****
:Error
Color 0C & Mode 104,5
echo( & echo(
echo      You should drag and drop a file over this batch file "%ScriptName%"
Timeout /T 5 /nobreak>nul & exit
..*****

```

?

Phlox - May 15, 2018, 4:34 am

Very nice Hackoo, its a very small script as well, keep up the good work!

HFDone - May 15, 2018, 8:26 am

now you can add option to pass hash arg for checking if its equ

Hackoo - May 16, 2018, 7:38 am

(May 14, 2018 07:54 PM)Sir-Teabag Wrote: [\[CITE\]](#) Awesome job Hackoo!
 I would suggest that you use the set /p option to ask the user for the hash to compare to though,
 instead of it being VLC by default. ?
 Hi ?
 I used InputBox with a vbscript file instead of Set /P just give a try and tell me the result ? ?

(May 15, 2018 08:26 AM)HFDone Wrote: [\[CITE\]](#) now you can add option to pass hash arg for
 checking if its equ

I added this feature : Check the SHA256 CheckSum on VirusTotal.com

Checkit.bat ([Click to View](#))

PHP Code

```
<?php
```

```
@echo off
```

```
mode 80,10 & color 0A & setlocal enabledelayedexpansion
```

```
Title Using Certutil Command Line to Compare SHA256 HASHES Files by Hackoo 2018
```

```
Set "LogFile=%~n0.txt"
```

```
Set "VBSFILE=%TMP%\%~n0.vbs"
```

```
if /i exist "%TMP%\%~n0.vbs" del /q "%TMP%\%~n0.vbs"
```

```
(
```

```
echo Dim Input, fso, file
```

```
echo Set fso = CreateObject^("Scripting.FileSystemObject")
```

```
echo If ^(fso.FileExists^("out.file")^)^ Then
```

```
echo    fso.DeleteFile^("out.file")
```

```
echo End If
```

```
echo Input = inputbox^("Copy and paste SHA256 hash :", "Copy and paste SHA256 hash" , ""^)
```

```
echo If Input = "" Then
```

```
echo    WScript.Quit
```

```
echo End If
```

```
echo Set file = fso.OpenTextFile^("out.file", 2, true^)
```

```
echo file.write^(Input^)
```

```
echo file.Close
```



```
call "%VBSFILE%"
```

```
del /q "%VBSFILE%"
```

```

if /i NOT exist out.file exit
set /p VAR=<"out.file"
Del "out.file">nul 2>&1
echo Input=!VAR!
echo Drag and drop your file and hit enter key to compute its SHA256 HASH Checksum
Set /p "File="
for /f "delims=" %%a in ("%File%") do Set "FilePath=%%~fa"
for /f "skip=1 delims=" %%H in ('CertUtil -hashfile "%FilePath%" SHA256 ^| findstr /i /v "CertUtil"'
) do set "H=%%H"
Set "SHA256=!H: =!"
)
echo !SHA256! & Timeout /T 2 /NoBreak>nul
cls
echo(
If [!VAR!] EQU [!SHA256!] (
    Color 0A
    echo [!VAR!]
    echo IS EQUAL TO
    echo [!SHA256!]
    echo THE FILE IS AUTHENTIC
) else (
    Color 0C
    echo THE FILE IS NOT AUTHENTIC
    echo [!VAR!]
    echo IS NOT EQUAL TO
    echo [!SHA256!]
)
(
If [!VAR!] EQU [!SHA256!] (
    echo [!VAR!]
    echo IS EQUAL TO
    echo [!SHA256!]
    echo THE FILE IS AUTHENTIC
) else (
    echo THE FILE IS NOT AUTHENTIC
    echo [!VAR!]
    echo IS NOT EQUAL TO
    echo [!SHA256!]
)
)>"%LogFile%"
Timeout /T 4 /NoBreak>nul & Start "" "%LogFile%"
Start "Chek SHA256 on VIRUSTOTAL" "https://www.virustotal.com/#/file!/SHA256!"
Exit

```

?

HFDone - May 16, 2018, 1:05 pm

dont know why you prefer vbs over simple set as you anyway need to pass the hash
also you can just set the hash form clipboard and drop the file