

Checksumme vergleichen

Checksum vergleichen

“ mit Hilfe von Powershell

Checksum / Prüfsumme berechnen / ermitteln

Anleitung für Windows und Linux

Hier erfährst du was Checksum bedeutet und wie du unter Windows und unter Linux (Ubuntu/Lubuntu) den Checksum einfach ermittelst. Mit einem Vergleich der Checksummen prüfst du eine heruntergeladene Datei auf Integrität, d.h. du stellst damit sicher, dass du die Originaldatei erhalten hast.

- Kurzinfo 1: [Was ist Checksum / Prüfsumme?](#)
- Kurzinfo 2: [Wozu ist Checksum nützlich?](#)
- Windows 10 Möglichkeit 1: [Checksum mittels Powershell unter Windows 10 ermitteln](#)
- Windows 10 Möglichkeit 2: [Checksum mittels 7-Zip Kontextmenü CRC SHA unter Windows 10 ermitteln](#)
- Ubuntu / Lubuntu Möglichkeit 1: [Checksum mittels Terminal unter Linux Ubuntu-Lubuntu verifizieren](#)

Was ist Checksum / Prüfsumme?

Ein Checksum (Prüfsumme) ist ein digitaler Fingerabdruck einer Datei. Genau wie ein Fingerabdruck einer Person einzigartig ist, ist auch der digitale Fingerabdruck, also die Checksum einer Datei, einzigartig. Solange der Inhalt einer Datei nicht verändert wurde, bleibt der

Fingerabdruck (die Checksum) jeder Datei auch unverändert. Wird jedoch der Inhalt (nicht der Dateiname) einer Datei auch nur minimal verändert, so ändert sich auch der digitale Fingerabdruck dieser Datei.

Wozu ist das nützlich?

Wenn ich eine Datei erstelle und dir per E-Mail, Download etc. zur Verfügung stelle, dann kann es sein, dass diese Datei auf dem Weg zu dir manipuliert/verändert wurde. Und hier hilft die Checksum bzw. die Prüfsumme. Ich ermittle aus der Datei die ich dir zusenden möchte die Checksum und teile dir diese Checksum mit.

Und sobald du die Datei empfangen hast, ermittelst du auf deinem PC zu der Datei auch die Checksum und vergleichst die beiden Checksumen miteinander. Sind sie identisch, so wurde die Datei nicht verändert. Sind diese Checksumen nicht identisch, so wurde der Inhalt dieser Datei auf dem Weg zu dir verändert.

Natürlich ist die Sicherstellung der korrekten Checksum bei unwichtigen Dateien wie Bilder und mp3 Musik nicht wirklich notwendig. Solange das Bild der Erwartung entspricht und die Musik das gewünschte Lied abspielt, ist es völlig egal, ob die Checksumen identisch sind oder nicht.

Das sieht jedoch bei wichtigen Programmen wie zB. bei Krypto-Brieftaschen (Wallets) ganz anders aus. Wenn jemanden z.B. 5,5 Bitcoin (**aktueller Wert: 103.450,71 EUR**), 50 Litecoin (**aktueller Wert: 2.618,08 EUR**) oder 100 Monero (**aktueller Wert: 14.038,05 EUR**) auf seiner Krypto-Adresse besitzt, der sollte genauer Prüfen ob das heruntergeladene Wallet-Programm tatsächlich auf dem Downloadweg nicht verändert / manipuliert wurde. Kurz gesagt, wichtige Programme/Dateien sollten immer auf Integrität geprüft werden.

Wie wichtig es ist eine Wallet-Datei vor der Installation über den Hashwert auf Integrität zu prüfen, zeigt der am 19.11.2019 bekannt gewordener Fall der Monero cli Wallet. Wer zwischen dem 19.11. und dem 20.11.2019 die Monero cli Wallet heruntergeladen und ohne zu prüfen auch installiert hat, hat sich eine Wallet mit Malware installiert. Diese Wallet hat die Seed entwendet, was dazu führte, dass die Moneros für immer weg waren.

Checksum unter Windows 10 ermitteln

Mittels Powershell / Eingabeaufforderung (cmd)

Als erstes öffne die Powershell. Drücke dazu gleichzeitig die Tastenkombination **[Windowstaste] + [R]**. Es öffnet sich ein kleines Fenster. Gebe hier "powershell" (ohne Anführungszeichen) ein und drücke Enter.

In dieser Anleitung wird Powershell verwendet. Das selbe funktioniert auch mit der Eingabeaufforderung "cmd".

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\Users\chaincheck>
```

In diesem Beispiel wollen wir die Checksum der Datei "Beam-Wallet-3.1.5765.exe" ermittelt. Diese Datei befindet sich im Downloads-Ordner.

Hier nutzen wir den Hash-Algorithmus sha256, da die Checksum der Datei auf der Beam-Webseite auch mit diesen Hash-Algorithmus erstellt wurde. Entsprechend geben wir in der Powershell folgendes ein (ohne \$ Zeichen) und drücken Enter:

```
$ CertUtil -hashfile .\Downloads\Beam-Wallet-3.1.5765.exe sha256
```

Es erscheint der sha256 Checksum der Datei Beam-Wallet-3.1.5765.exe. In diesem Fall "e23146aed1607239329f614d68dd147af69cb0d3c42920b73cc7781ee5266c8b". Mit der Maus kann diese Checksum markiert und durch drücken der Enter Taste in die Zwischenablage kopieren werden.

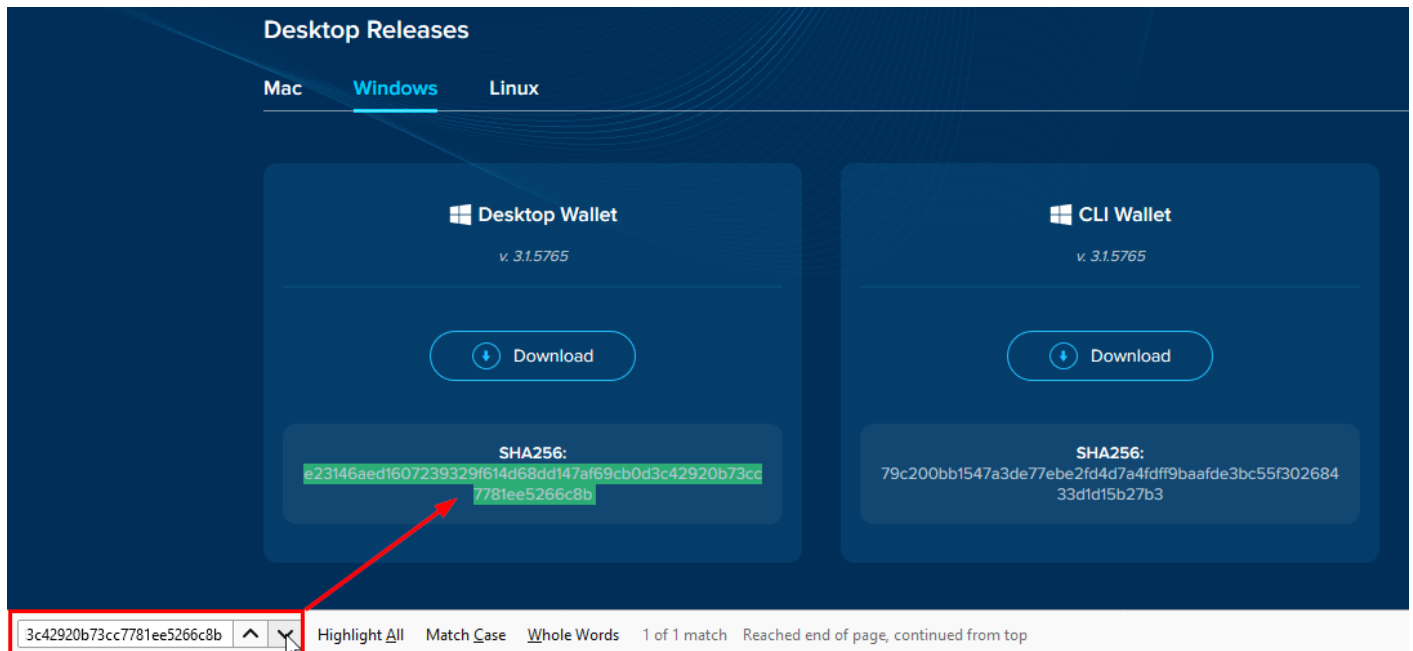
```
Windows PowerShell

PS C:\Users\chaincheck>
PS C:\Users\chaincheck>
PS C:\Users\chaincheck> CertUtil -hashfile .\Downloads\Beam-Wallet-3.1.5765.exe sha256
SHA256-Hash von .\Downloads\Beam-Wallet-3.1.5765.exe:
e23146aed1607239329f614d68dd147af69cb0d3c42920b73cc7781ee5266c8b
CertUtil: -hashfile-Befehl wurde erfolgreich ausgeführt.
PS C:\Users\chaincheck>
```

Jetzt muss nur noch geprüft werden, ob die auf dem eigenem Rechner ausgegebene Checksum die selbe ist, wie auf der Download-Seite. Kopiere den Checksum und gehe dazu auf die Download-

Seite. Drücke dort *STRG+F* und dann *STRG+V* um nach dem Zeichensatz in der Zwischenablage zu suchen.

Ist die Checksum identisch, dann kann davon ausgegangen werden, dass die heruntergeladene Datei die Originaldatei ist.



Checksum unter Windows 10

Mittels 7-zip Kontextmenü CRC SHA ermitteln

Wer das Datenkomprimierungs-Programm 7-Zip unter Windows installiert hat, der kann auch über das Windows Kontextmenü schnell die Checksum einer Datei überprüfen.

Dazu einfach die Datei mit der rechten Maustaste anklicken. Es öffnen sich das Kontaxtmenü in diesem der Unterpunkt "CRC SHA" erscheint. Hier muss nur noch der gewünschte Checksum entsprechend ausgewählt werden:

Als Ergebnis erhalten wir den Checksum zu dieser Datei. Dieser Zeichensatz ist leider nicht kopierbar.

Checksum unter Linux (Ubuntu/Lubuntu) ermitteln

Mittels Linux Terminal

Um den Checksum Unter Linux (Ubuntu/Lubuntu usw.) zu ermitteln, wird der gesuchte Hash-Algorithmus einfach vor der Datei eingegeben.

Möchten wir z.B. für die Datei "Beam-Wallet-3.1.5765.exe" den Hash-Algorithmus **sha256** ermitteln, so müssen wir im Ubuntu/Lubuntu Terminal folgendes eingeben:

```
$ sha256sum Beam-Wallet-3.1.5765.exe
```

Und für **MD5** geben wir folgendes ein:

```
$ md5sum Beam-Wallet-3.1.5765.exe
```

usw.

```
$ sha1sum Beam-Wallet-3.1.5765.exe
```

Bei crc32 dann wieder ohne sum anhängen:

```
$ crc32 Beam-Wallet-3.1.5765.exe
```

Das sind die Möglichkeiten die Checksum bzw. die Prüfsumme zu ermitteln.

Fehlt eine eventuell noch bessere oder einfachere Möglichkeit die Checksum zu ermitteln? Dann schreibe mir bitte, damit ich diese Anleitung anpassen kann.

Revision #1

Created 17 August 2023 10:37:56 by Hermann

Updated 17 August 2023 10:40:09 by Hermann