regio IT

Desinfec't

Dokumentation

Stand 2020

Inhalt

Allgemeine Informationen zu Desinfec’t

MacGyver hat es, Schweizer Offiziere haben es. Die Rede ist hier von einem Multitool, welches heutzutage bei keinem Computernutzer mehr fehlen sollte. Wir sprechen aber nicht von dem bekannten Schweizer Offiziersmesser, sondern von dem äußerst effektiven Notfall-System „Desinfec´t“.
Mit zahlreichen wirklich guten Tools wird hierbei unter die Haube des laufenden Computersystems gegriffen. Im schlimmsten Fall können verlorene Daten bzw. über forensische Methoden eigentlich unwiederbringliche Dateien wiederhergestellt werden. Der Live-USB-Stick stellt u.a. vier Open Source Virenscanner (ESET, F-Secure, Sophos und Kaspersky) zu Verfügung, die Sie beim kleinsten Verdacht einer Vireninfektion im „Offline Modus“ bei der Beseitigung unterstützen.
Im Unterschied zu einem installierten Virenscanner startet die Desinfec't über einen Live-USB-Stick oder einem USB-Stick und analysiert das möglicherweise infizierte Windows-System bevor es aktiv gestartet wird. Schädlinge haben keine Chance sich über ein aktives Windowssystem zu verstecken.

heise.de: *„Mit der aktuellen Version von Desinfec't können Sie Schädlinge vom Kaliber Emotet noch effektiver aufspüren und erledigen.“*

Diese Anleitung wurde mit der zu diesem Zeitpunkt aktuellen „Heise Desinfec’t 2020“ erstellt. Weitere Informationen und den Bezug der aktuellen „Desinfec´t“ entnehmen Sie den Quellangaben.

FAZIT: Das **Desinfec’t Projekt** wird seit ca. 16 Jahren von der c’t (heise.de) publiziert. Als „Schweizer Offiziersmesser für Jedermann“ sollte die **Desinfec’t** in keiner Schublade fehlen. Über viele nützliche Funktionen kann das Notfall-System durchaus die schlimmsten Szenarien im EDV-Alltag verhindern. Weitere Informationen und den Bezug der „Desinfec´t 2020“ entnehmen Sie den Quellangaben.

Bootbaren Desinfec't USB-Stick erstellen

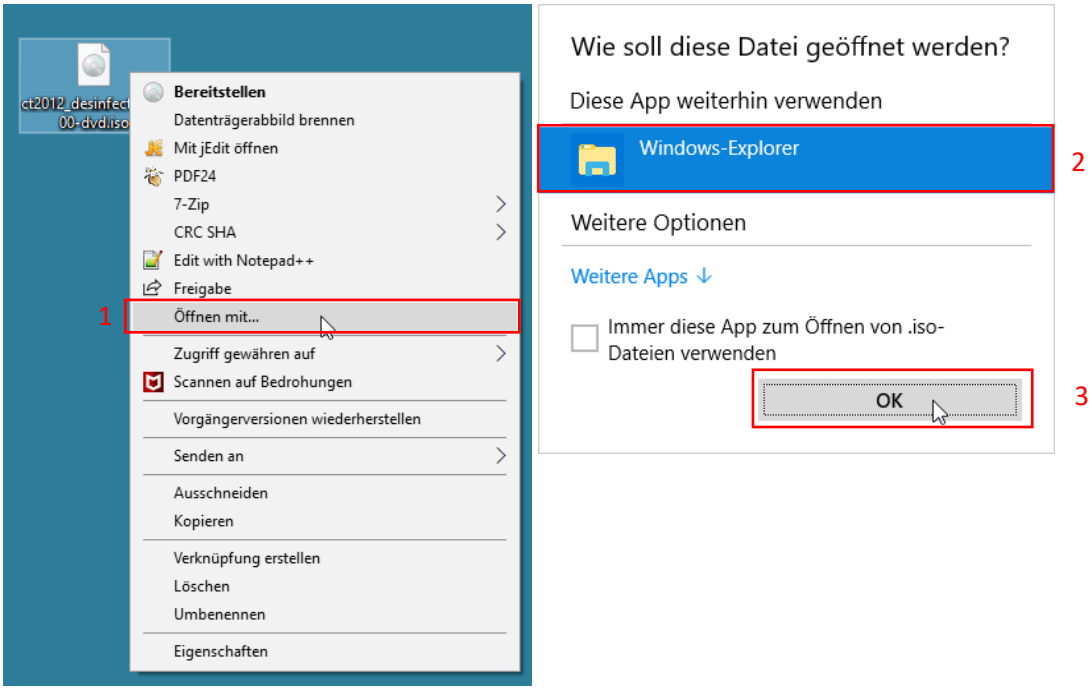
Information zum Erstellen von einem Desinfec't USB-Stick

- Ein Desinfec't USB-Stick nicht auf einem PC erstellen, welcher eventuell mit Viren verseucht ist.
- Alle Geräte bis auf Bildschirme, Maus, Tastatur und den zu installierenden USB-Stick vom Computer trennen.
- Die ISO-Datei (ct2012_desinfect… .iso) und die Dokumentation auf den Desktop kopieren.
- Den Bereich Hilfe aufrufen, wenn Sie bei der Installation Probleme haben.

Erstellung des Desinfec't USB-Sticks

- Was brauche ich um einen Desinfec't USB-Stick zu erstellen?
  - Mindestens 16 GB großen USB-Stick (am besten einen 3.0 USB-Stick oder besser)
  - Desinfec't ISO
  - Windows Computer mit Administrator rechten

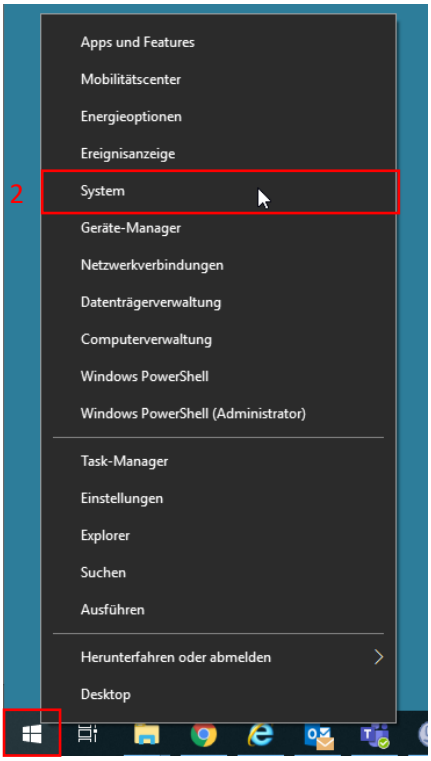
1. ISO mit einem **Doppelklick öffnen** (linke Taste auf der Maus)
   a. Falls Windows den Brennassistenten oder ein anderes Programm startet dann mit **Rechtsklick (rechte Taste auf der Maus) > Öffnen mit… > Windows Explorer > OK** klicken.



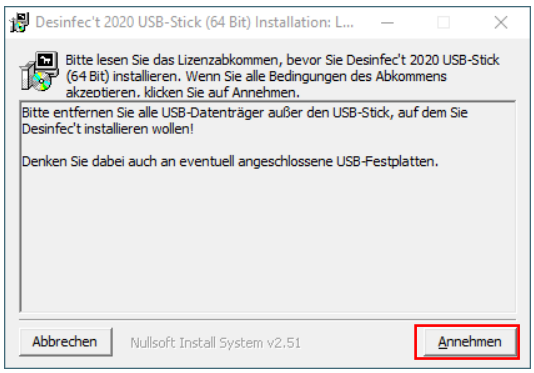
2. In dem geöffneten Fenster die „*Desinfect2USB_64_Bit.exe*“ **ausführen**, Warnmeldung mit „*OK*“ **bestätigen** und ggf. mit Adminkennung anmelden.
    a. Bei einem 32 Bit System die „*Desinfect2USB_32_Bit.exe*“ **ausführen**.

   Herausfinden welchen Systemtyp Sie haben:

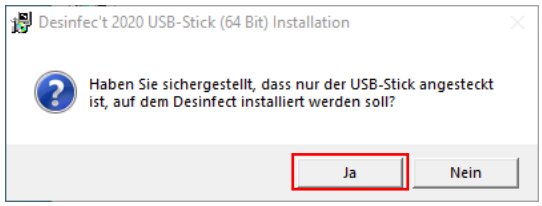
   Systeminformation unter **Rechtsklick auf das Windows Logo > System > Systemtyp**



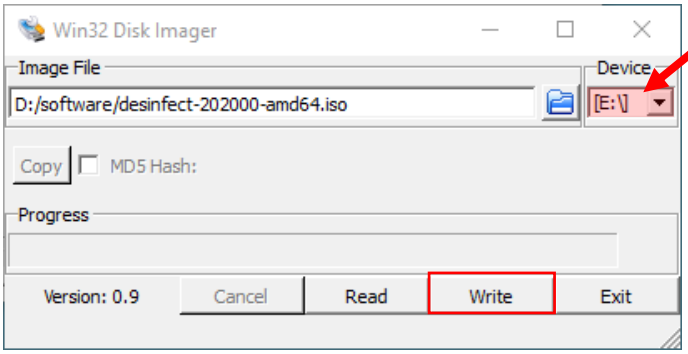
3. USB-Stick **anschließen**, wenn er noch nicht angeschlossen ist.
4. Lizenzabkommen lesen ☺ und auf „*Annehmen*“ **klicken**.



5. Auf „*Ja*“ **klicken**.

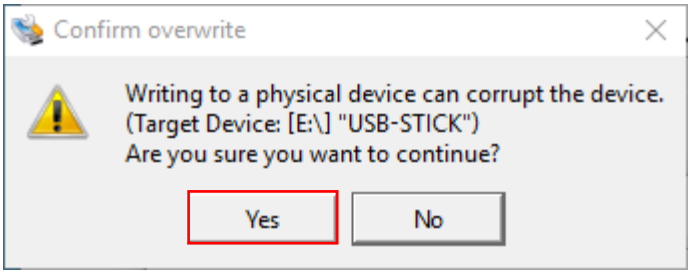


6. Überprüfen ob der richtige USB-Stick ausgewählt wurde und auf „*Write*“ **klicken**.

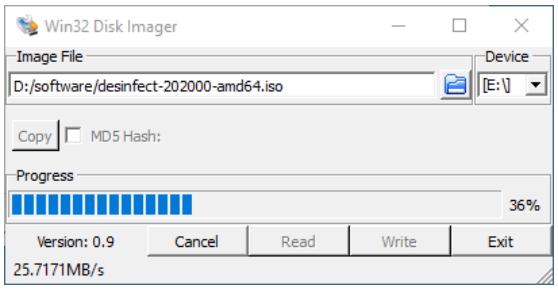


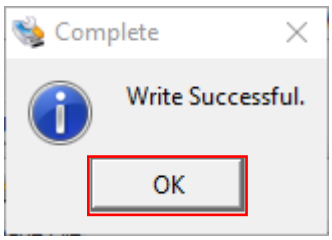
Name des USB-Stick, wo Sie Desinfec't installieren.

7. WICHTIG: Alle Daten die sich auf dem USB-Stick befinden werden gelöscht! Warnmeldung mit „*Yes*“ **bestätigen**.

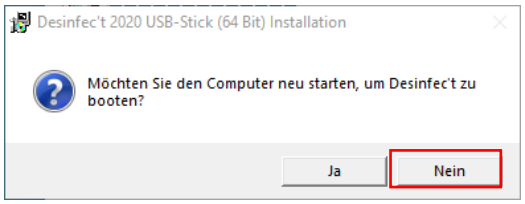


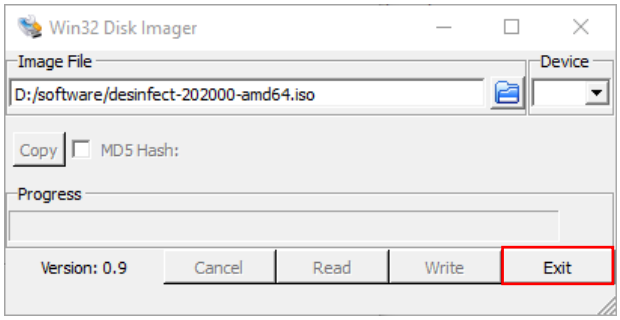
8. Desinfec't wird auf den USB-Stick geschrieben. Erstellung dauert ca. 3 Min. und wird nach Fertigstellung mit einem Fenster bestätigt (Das „Write Succsessful.-Fenster“ kann sich eventuell hinter einem anderen Fenster verbergen/verstecken).

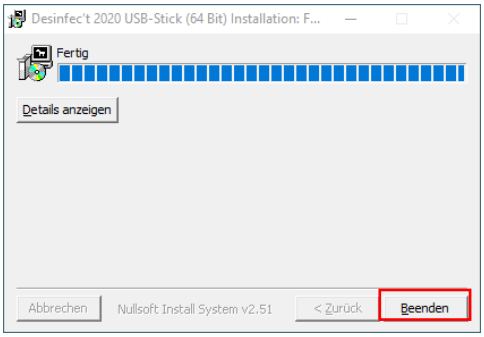




9. Auf „*Nein*“, „Exit“ und „Beenden“ **klicken** (der USB-Stick wird danach automatisch ausgeworfen).







10. Fertig!

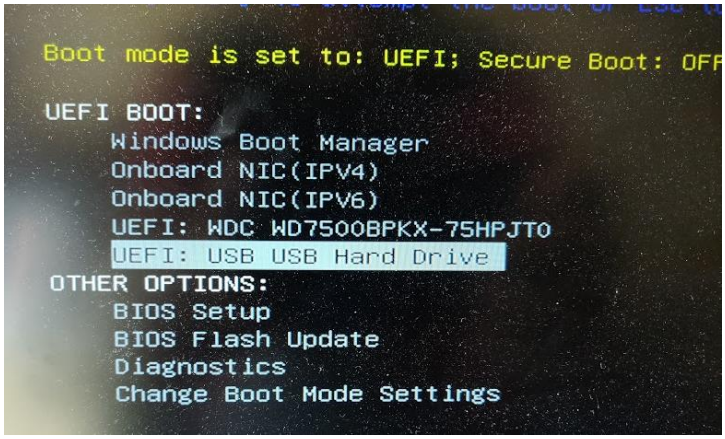
Computer scannen

Der zu überprüfende Computer sollte über eine aktive Internetverbindung verfügen, damit die Signaturen der Virenscanner aktualisiert werden können. Allerdings kann Desinfec’t nur mit einer Dezentralen Internetverbindung wie z.B. ein Mobiler Hotspot überprüft werden. Wenn der Computer keine Internetverbindung hat, ist der USB-Stick über einen anderen Rechner zu aktualisieren siehe Anleitung „Computer ohne Internetverbindung scannen“. Damit Sie einen Computer nach Viren überprüfen können, müssen Sie wie im Teil „Bootbaren Desinfec’t USB-Stick erstellen“ beschrieben einen Desinfec’t USB-Stick erstellt haben um von diesem USB-Stick starten zu können.

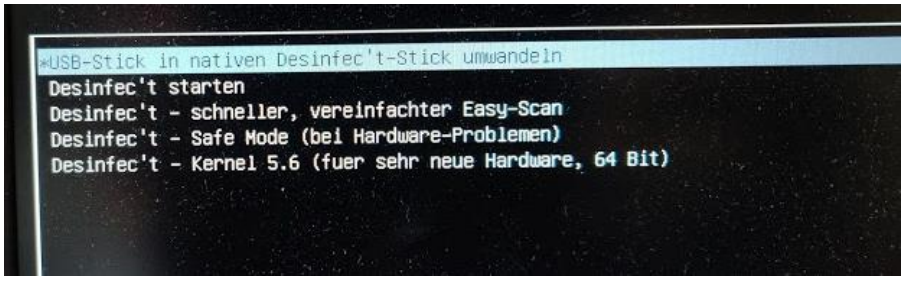
Den Bereich Hilfe aufrufen, wenn Sie beim Computer scannen Probleme haben.

Vom Desinfec’t Medium starten/booten

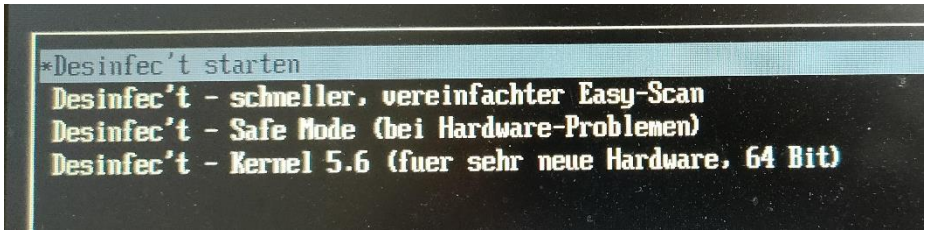
1. Desinfec’t USB-Stick an einen USB-Anschluss an dem zu überprüfendem Computer **anschließen** (bei einem USB 3.0 Stick oder besser, in den USB3.0 Anschluss einstecken).
2. Den Computer starten und die Taste drücken, mit der man ins Boot Menü kommt.
    a. Je nach Hersteller variiert die Taste. Meist **F1**, **F2**, **F8**, **F11** oder **F12**.
        i. Bei Dell **F12**
        ii. Bei Lenovo zuerst die „**ENTER**“ Taste und danach die „**F12“**-Taste **drücken**.
3. USB-Stick aus Boot Menü mit den Pfeiltasten auswählen und mit „**ENTER**“ Bestätigen.



4. Mit **Enter** den Punkt „*USB-Stick in nativen Desinfec’t-Stick umwandeln*“ **bestätigen**.



5. Nun sollte Desinfec’t vom USB-Stick starten/booten (Dies kann einige Minuten dauern).
6. Beim Nächten mal „*Desinfec’t starten*“ **auswählen**.

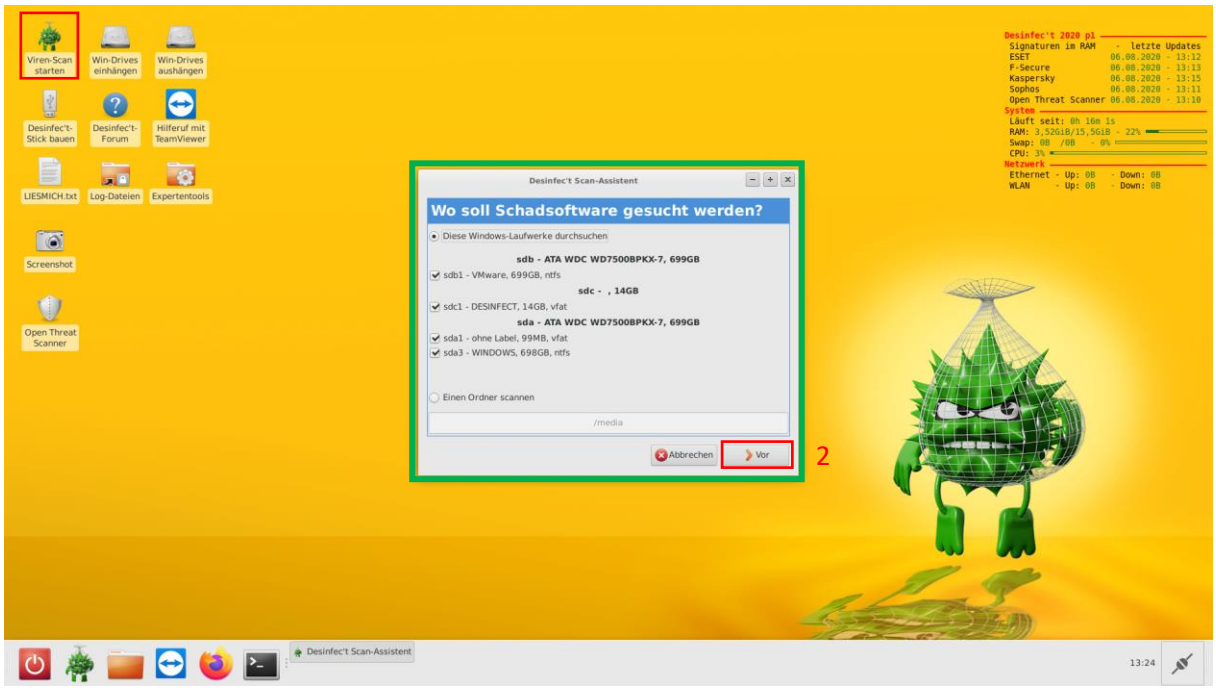


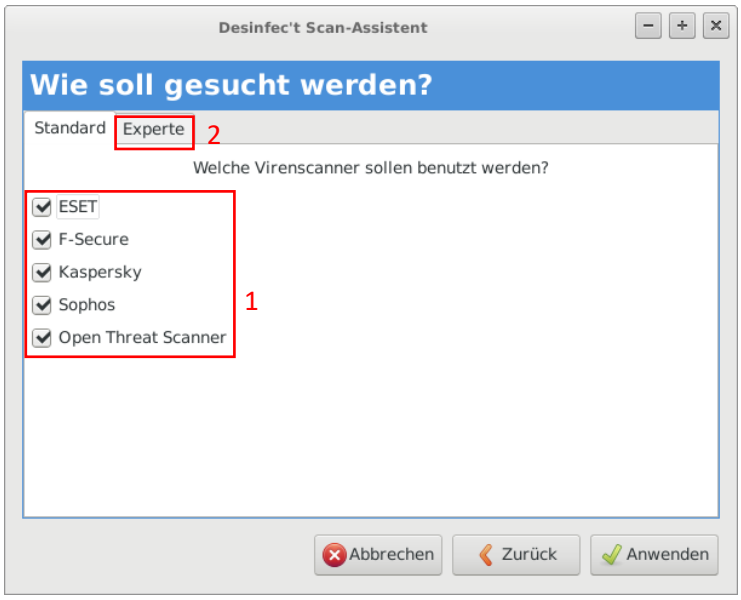
7. Beim Start in Desinfec’t werden Sie gefragt, ob Sie ein Projektordner erstellen möchten. Falls Sie keinen Projektordner erstellen möchten, können Sie das Fenster „Projektordner“ schließen. Die Information was ein Projektordner ist, entnehmen Sie aus dem Bild.

Computer mit Internetverbindung scannen

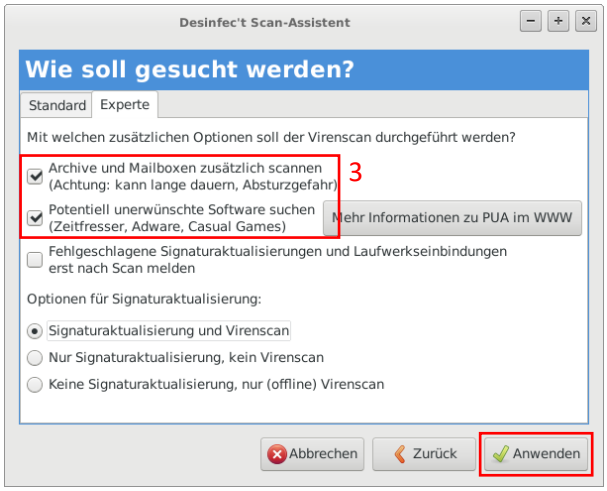
- Die Signaturen können nur über eine dezentrale Internetverbindung aktualisiert werden.
  z.B. Mobiler Hotspot

1. **Doppelklick** auf „*Viren-Scan starten*“ und auf „*Vor*“ **klicken**.
   a. Wenn man ein oder mehrere spezifische Laufwerke oder Ordner mit Desinfec’t überprüfen möchte, lässt sich das in dem Fenster „*Wo soll Schadsoftware gesucht werden?*“ (grün markiert) einstellen.
2. Alle Häkchen anwählen und auf den Tab „*Experte*“ **klicken**.

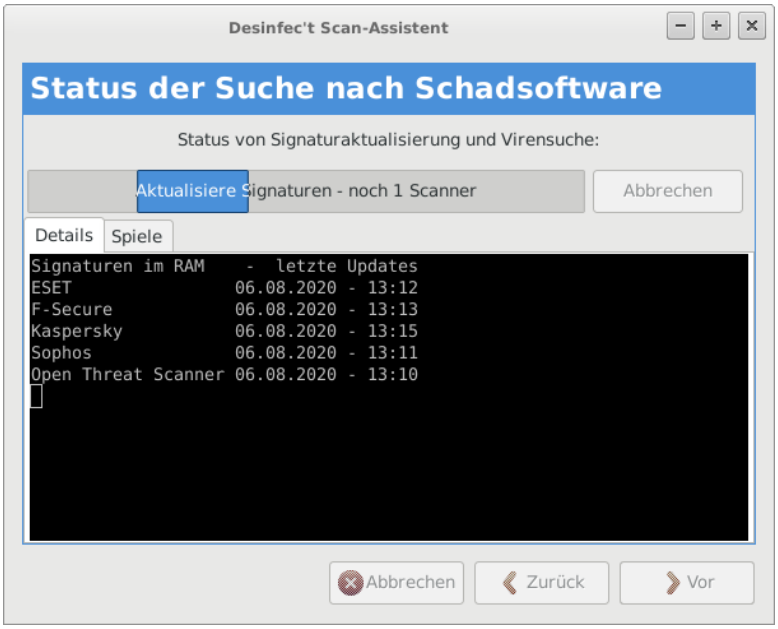




3. Die **Häkchen setzten** bei *„Archive und Mailboxen zusätzlich scannen“* und *„Potenziell unerwünschte Software suchen“*.
4. Auf *„Anwenden“* **klicken**.



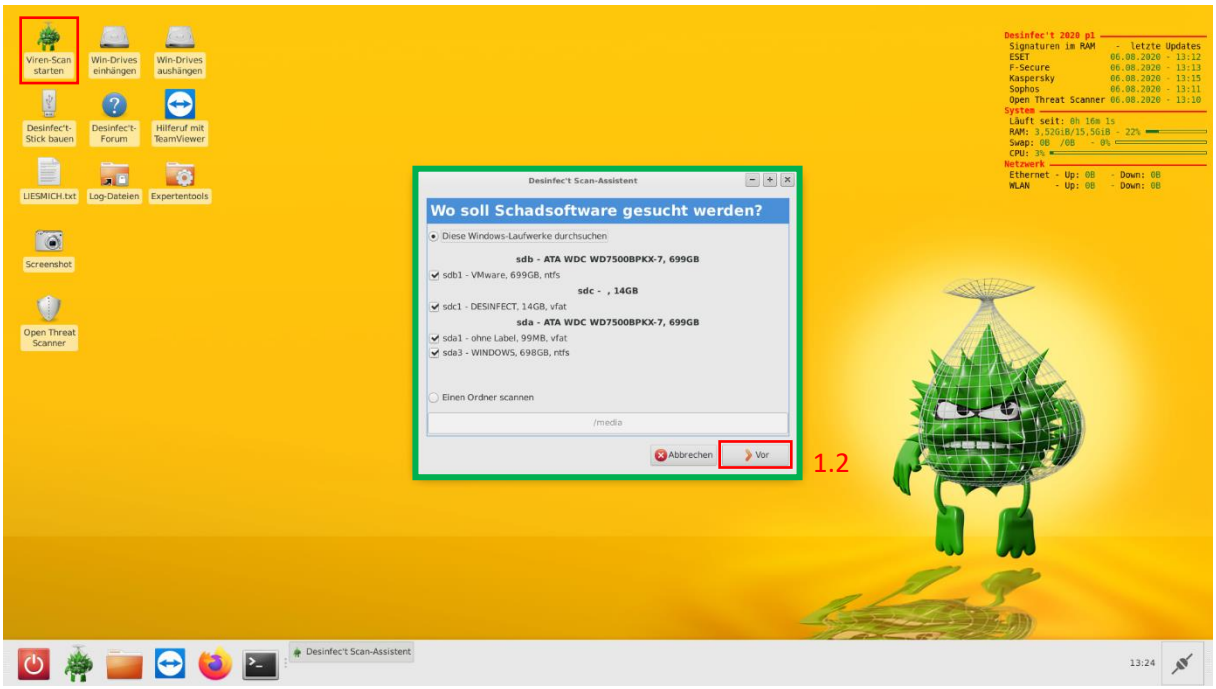
5. Desinfec’t aktualisiert zuerst die ausgewählten Virenscanner. Danach wird der Virenscan durchgeführt. Die Zeit für den Virenscan kann sehr stark variieren, da Faktoren wie SSD, Festplatte, USB-Stick, Größe des Speichermediums und wie viele Dateien sich auf dem Datenträger befinden die Zeit beeinflussen können.

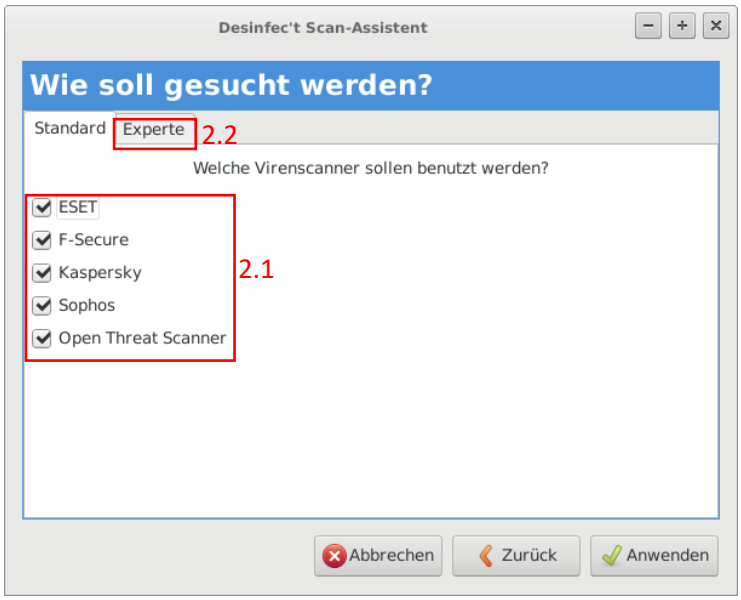


Computer ohne Internetverbindung scannen

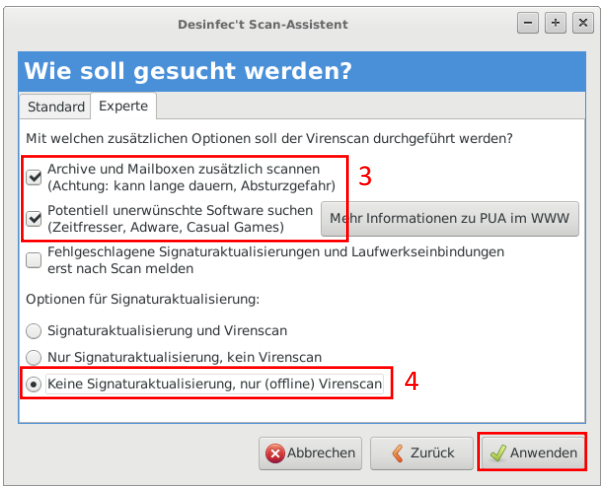
- Vor **jedem** Virenscan empfiehlt es sich die Signaturen auf dem Desinfec't Stick zu aktualisieren. HIER KLICKEN um zum Teil zu kommen, wie man die Signaturen aktualisiert.

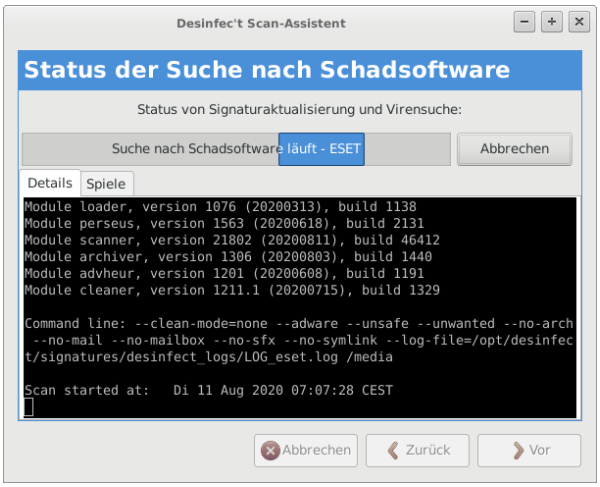
1. **Doppelklick** auf „*Viren-Scan starten*“ und auf „*Vor*“ **klicken**.
   a. Wenn man ein oder mehrere spezifische Laufwerke oder Ordner mit Desinfec't überprüfen möchte, lässt sich das in dem Fenster „*Wo soll Schadsoftware gesucht werden?*“ (grün markiert) einstellen.
2. Alle Häkchen anwählen und auf den TAB „*Experte*“ **klicken**.



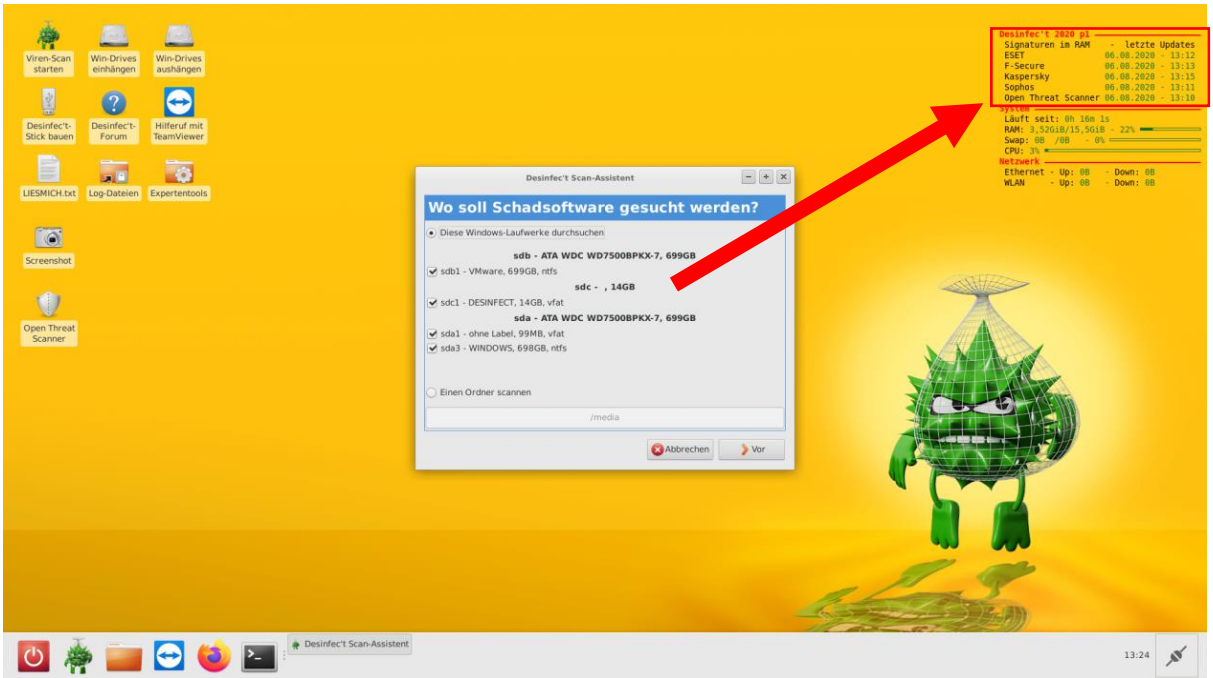


3. Die Häkchen bei „*Archive und Mailboxen zusätzlich scannen*“ und „*Potenziell unerwünschte Software suchen*“ **setzten**.
4. Den Punkt „*Keine Signaturaktualisieren, nur (offline) Virenscan*“ **auswählen**.
5. Auf „*Anwenden*“ **klicken**.
6. Nun sucht Desinfec’t nach Viren.





7. Oben rechts lässt sich einsehen, wann zuletzt die Signaturen geupdated wurden.

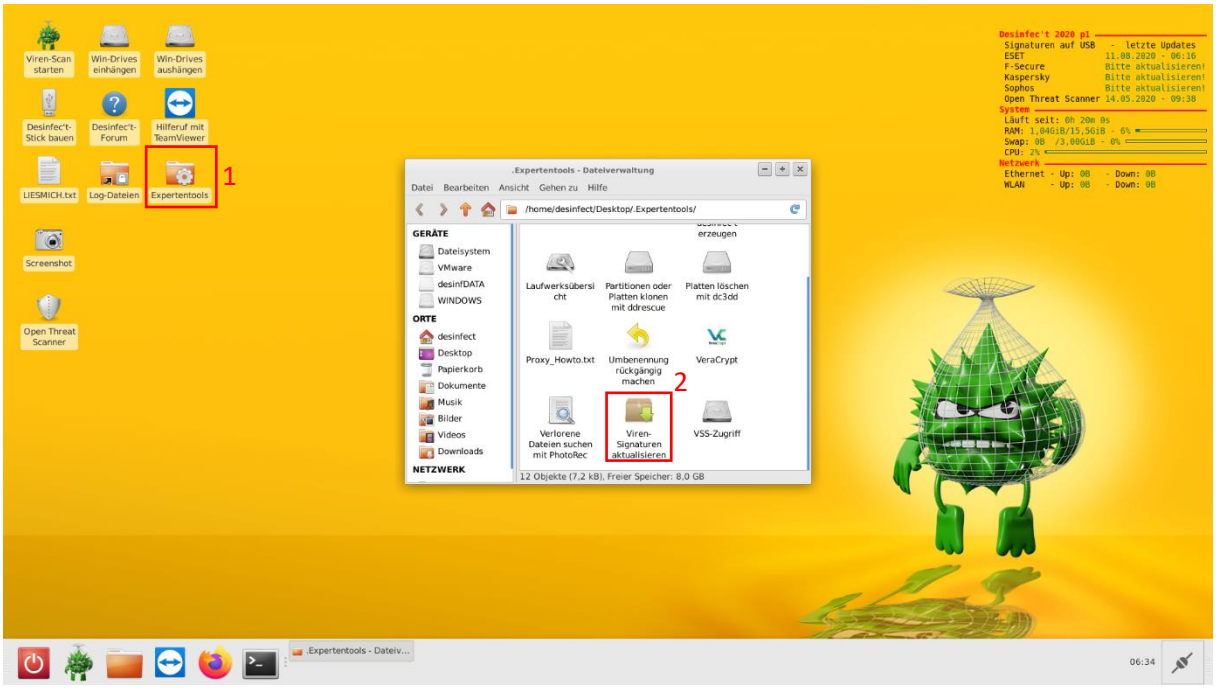


Signaturen der Virenscanner auf dem USB-Stick aktualisieren.

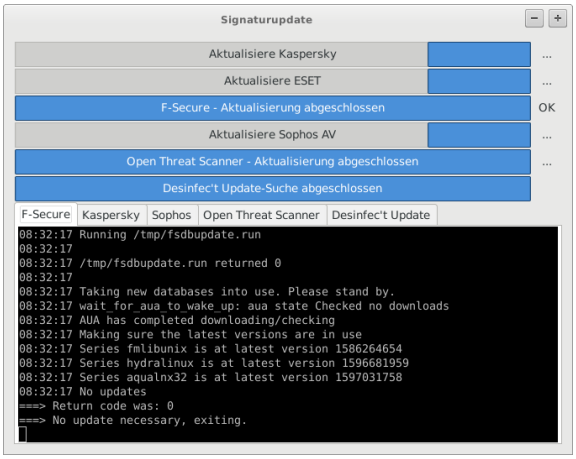
- Um die Signaturen zu aktualisieren benötigt Desinfec't/ der PC eine dezentrale Internetverbindung (z.B. Mobiler Hotspot).

Variante 1:

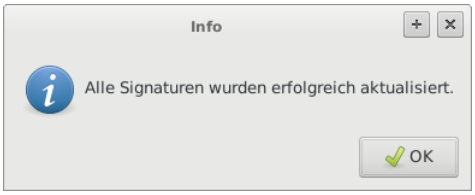
1. „*Expertentools*“ **öffnen**.
2. In dem Fenster runterscrollen und auf „*Viren-Signaturen aktualisieren*“ **klicken**.



3. Nun aktualisiert Desinfec't die Signaturen.

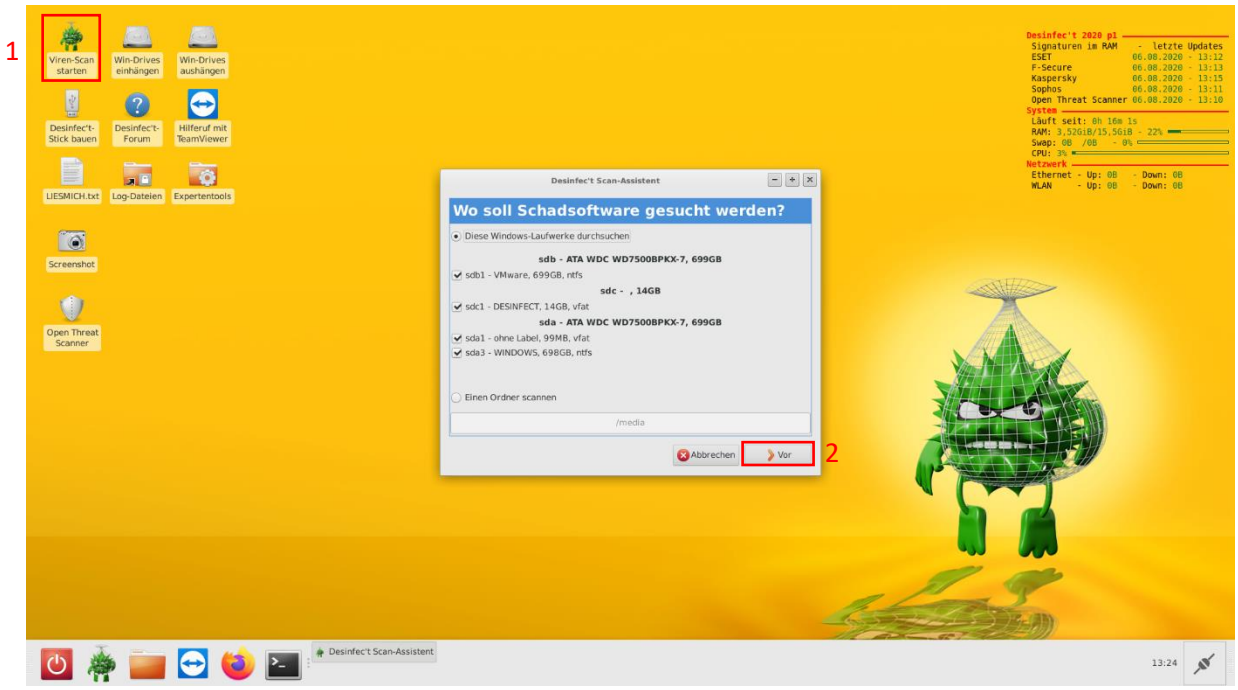


Bestätigungsfenster nachdem alle Virenscanner erfolgreich aktualisiert wurden:

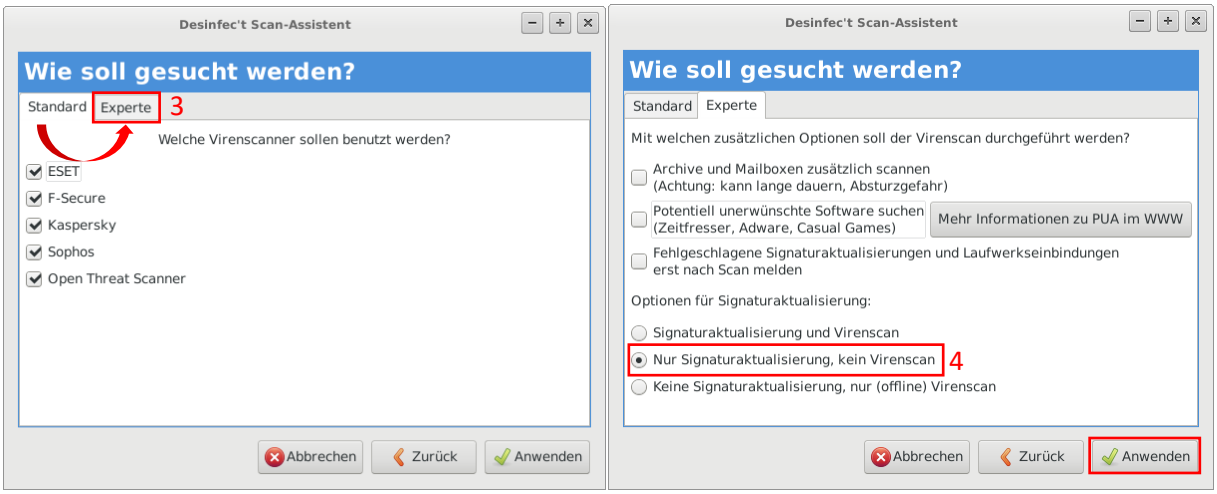


Variante 2:

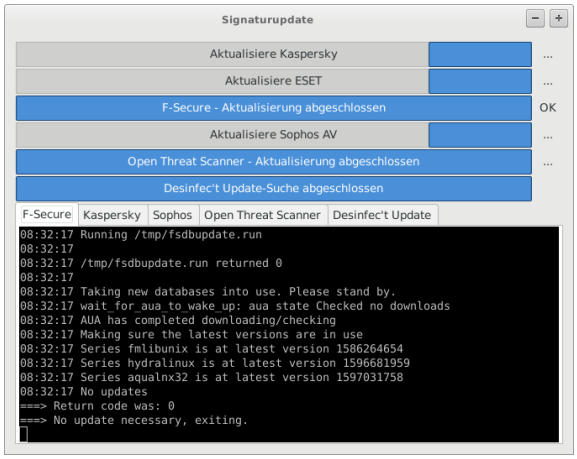
1. Auf „*Viren-Scan starten*“ **klicken**.
2. Auf „*Vor*“ **klicken**.



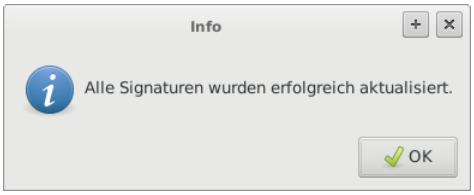
3. Vom Tab „*Standard*“ auf „*Experte*“ **klicken**.
4. Den Punkt „*Nur Signaturaktualisierung, kein Virenscan*“ **auswählen**.
5. Auf „*Anwenden*“ **klicken**.



6. Nun aktualisiert Desinfec’t die Signaturen.



Bestätigungsfenster nachdem alle Virenscanner erfolgreich aktualisiert wurden:

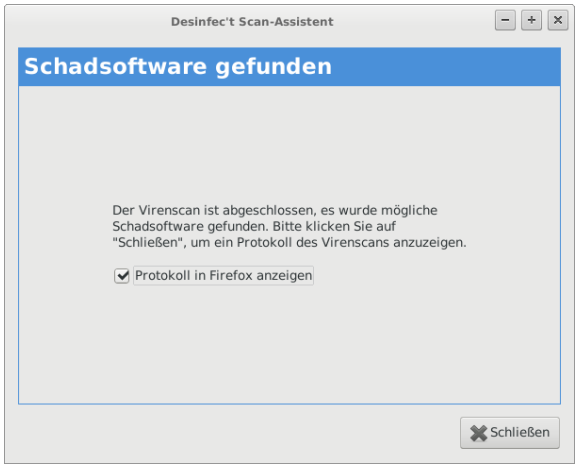


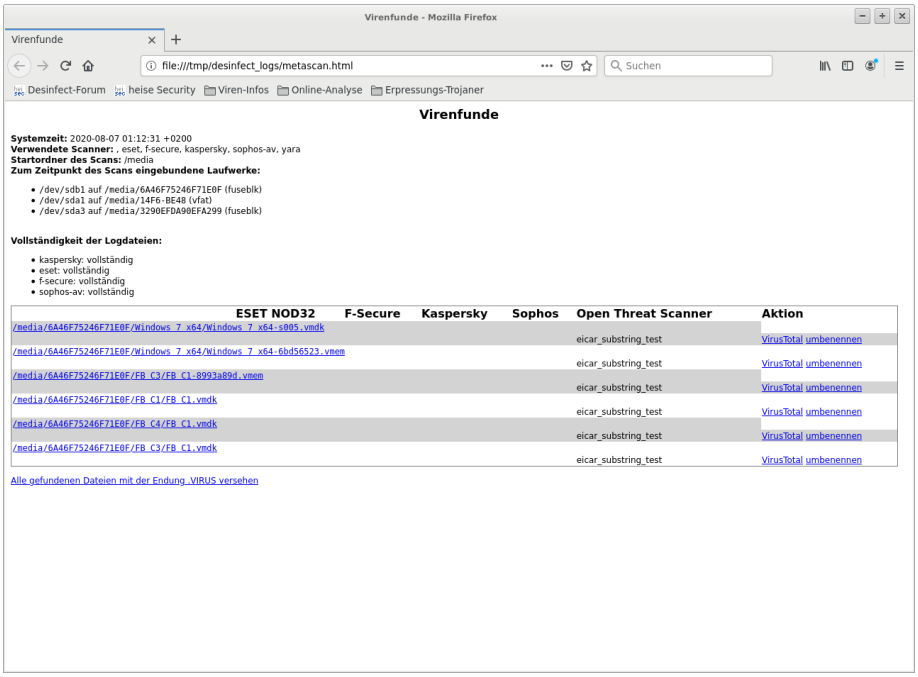
Nach dem Virenscan

Bei Virenfund

So sieht es aus, wenn Desinfec’t einen oder mehrere Viren gefunden hat:

1. Das **Häkchen** „*Protokoll in Firefox anzeigen*“ **setzen**.
2. „*Schließen*“ **klicken**.

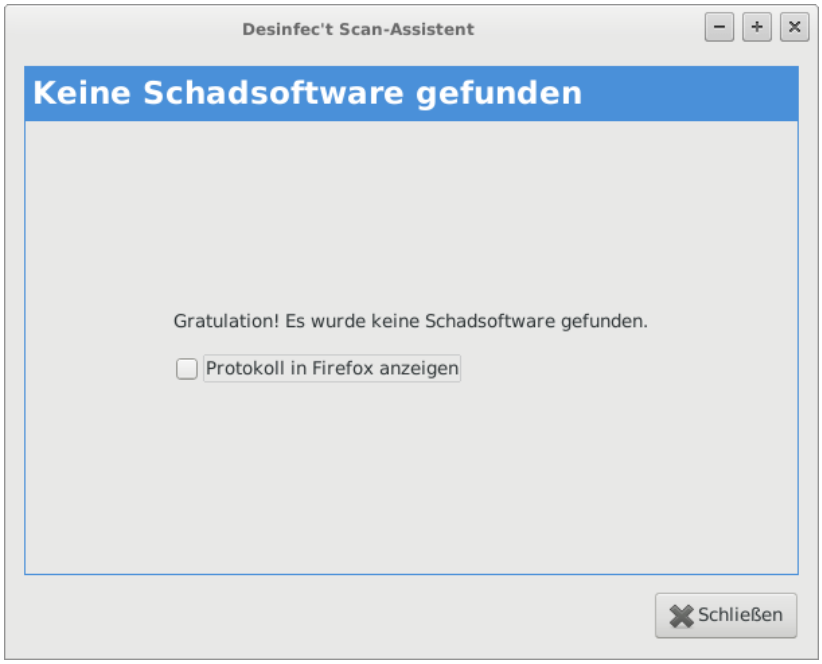




Bei einem Virenfund sofort die **IT-Sicherheit** oder **Hotline** informieren, den Computer **nicht** mehr **in Windows hochfahren** und das **Netzwerkkabel trennen**!

Bei keinem Virenfund

So sieht es aus, wenn Desinfec’t keine Viren gefunden hat:



Herzlich Glückwunsch! Desinfec’t hat keine Viren/Schadsoftware gefunden. Es kann allerdings sein, dass Sie sich einen Virus oder eine andere Schadsoftware eingefangen haben, welche noch in keiner der fünf Datenbanken der Virensignaturen vorhanden ist. Daher sollte der Rechner einige Tage später erneut mit aktualisierten Signaturen offline überprüft werden.

Hilfe

Bei Fragen oder Problemen hilft Ihnen das Desinfec't Forum oder Desinfec't FAQ.

Quellangaben

Artikel: https://www.heise.de/security/meldung/Das-Sicherheitstool-der-c-t-Redaktion-Desinfec-t-2020-ist-da-4724635.html

Weitere Artikel: https://www.heise.de/suche/?q=desinfect&sort_by=date&rm=search

Video zur Desinfec't 2020: https://www.heise.de/ct/artikel/nachgehakt-Desinfec-t-2020-4724909.html

Desinfec't 2020: https://shop.heise.de/id-16720

Feedback

Ich hoffe ich konnte Ihnen mit dieser Dokumentation weiterhelfen.

Wenn Sie einen Verbesserungsvorschlag für diese Dokumentation haben, können Sie mir gerne eine E-Mail mit dem Titel „**FEEDBACK Desinfec’t Doku 2020**“ an security@regioit.de zuschicken.