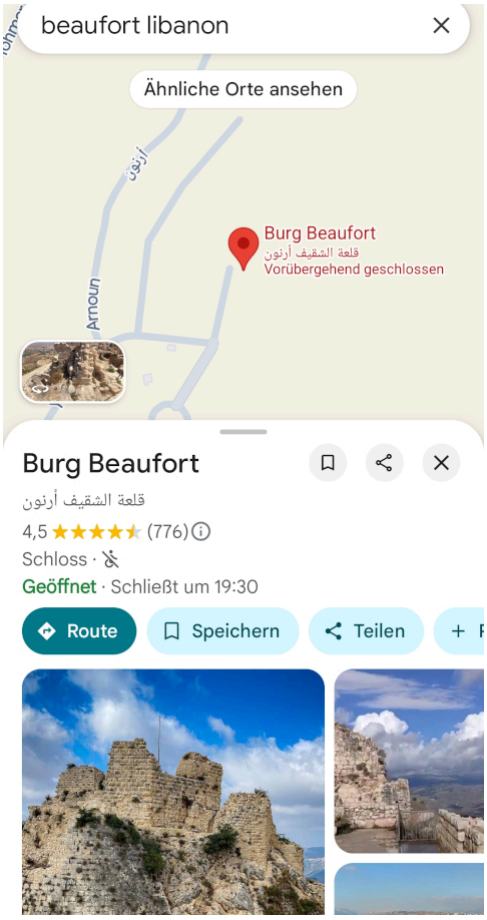
Vorübergehend geschlossen



Die IDF hat Burg Beaufort im Libanon eingenommen.

„Beaufort war die einzige größere Kreuzritterburg, die der Eroberungswelle Saladins in den Jahren 1187 bis 1189 standhielt, der die Burg mehrmals belagerte. Dabei überlistete der Burgherr Rainald von Sidon Saladin, indem er die Übergabe versprach, die Burg jedoch heimlich reparierte.“

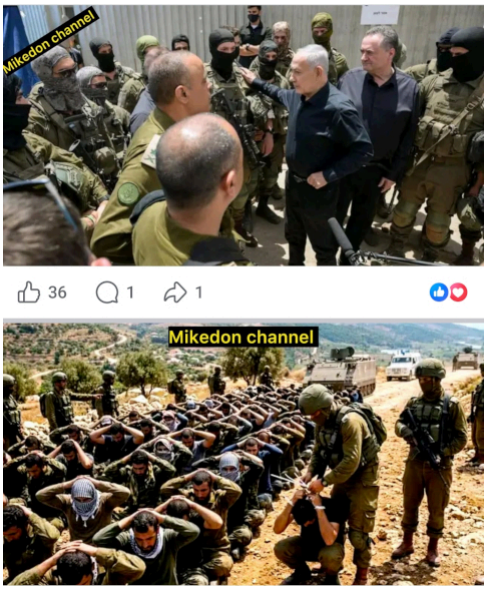
Rainald sprach übrigens fließend Arabisch.

Hinweis: Wenn man mich ~~verarschen~~ auf den Arm nehmen will, muss man das schon geschickter anstellen. Das Bild ganz unten, das Hisbollah-Terroristen im Libanon zeigen soll, ist garantiert nicht echt. Die tragen sogar ihre „Palästinenser“-Tücher noch.

Der Betreiber des Kanals ~~ist aus Lagos, Nigeria~~: „I am a

businessman living in Guangzhou, China.“ Schon klar.

ChatGPT bestätigt meine Vermutung:



„Ich kann nicht mit Sicherheit sagen, ob das Bild echt oder KI-generiert ist, aber ich sehe mehrere Merkmale, die mich skeptisch machen:

Auffälligkeiten, die für KI sprechen könnten

Die Menschenmenge wirkt ungewöhnlich gleichförmig

► Viele Personen haben nahezu identische Körperhaltungen.
► Die Arme über dem Kopf bilden ein fast perfektes Muster, wie man es oft bei KI-generierten Menschenmengen sieht.

Gesichter im Hintergrund sind kaum klar erkennbar

► Besonders in den mittleren Reihen wirken viele Gesichter verwaschen oder unnatürlich vereinfacht. Das ist ein typisches Problem von KI-Bildern, vor allem bei größeren Personengruppen.

Unklare Details an Händen und Armen

► Einige Hände scheinen ineinander überzugehen.
► An mehreren Personen ist schwer zu erkennen, welche Arme zu welchem Körper gehören.

Der Soldat rechts vorne

► Seine Ausrüstung wirkt auf den ersten Blick plausibel. Allerdings erscheinen einzelne Gurte und Taschen etwas unlogisch angeordnet. Das allein beweist nichts, ist aber ein typisches KI-Indiz.

Licht und Schärfe

► Die Szene wirkt insgesamt sehr kontrastreich und dramatisch.
► Moderne KI-Bilder haben oft genau diesen „hyperrealistischen Nachrichtenfoto-Look“.

Was für ein echtes Foto spricht

Fahrzeuge und Landschaft

► Die gepanzerten Fahrzeuge und die Straße sehen weitgehend konsistent aus.
► Keine offensichtlichen KI-Fehler wie schwebende Räder oder unmögliche Perspektiven.
► Keine extremen Anatomiefehler
► Ich sehe keine sechs Finger, verschmolzenen Gesichter oder andere grobe Fehler, die bei KI häufig vorkommen.
► Das Motiv selbst: Solche Bilder existieren tatsächlich aus realen Konflikten. Das Motiv ist also nicht von vornherein unrealistisch.“

Unter Kühlenden [Update]

Ich weiß, was ich heute unter anderem gemacht habe, wenn ich in meinen Kühlschrank schaue…

Update: Ich weiß, was ich heute gegessen habe, wenn ich auf meinen Teller schaue…

Unter Taxidermisten

Ich hatte heute nach mehreren Monaten wieder mal eine Schicht im Naturkundemuseum.

Mit einem jüngeren Besucher kam ich exakt vor dem Tyrannosaurus Rex ins Gespräch: Es stellte sich heraus, dass er jeden Morgen kurz nach zwei aufstand, um bei einem Bäcker zu arbeiten und in seiner Freizeit dem Hobby nachging, 3-D-Modelle zu bauen. Er zeigte mir ein paar beeindruckende Fotos von selbst gebauten Tierköpfen, die auch als Dekoration in Horrorfilmen nützlich gewesen wären.

Ich fragte ~~Hal~~ die KI nach dem, was wir kurz diskutierten: Was hältst du von der These, dass die heutigen Techniken der Tierpräparation von 3-D-Drucken in Kombination mit KI abgelöst werden?

Warum KI und 3D-Druck Tierpräparate ersetzen könnten

Moderne Verfahren entwickeln sich schnell:

► Ein Tier kann mit hochauflösenden Scannern digital erfasst werden.
► Fehlende Bereiche lassen sich mit KI rekonstruieren.
► Körper, Muskeln, Hautstrukturen und Federn können per 3D-Druck erzeugt werden.
► Farbdruckverfahren werden immer realistischer.
► Beschädigte oder seltene Exemplare müssen nicht mehr präpariert werden.

Für Museen hat das einige Vorteile:

► Keine Verwesung oder Schädlingsprobleme.
► Keine empfindlichen organischen Materialien.
► Beliebig viele identische Kopien.
► Leichter Transport und Versicherung.
► Keine ethischen Fragen bezüglich geschützter Arten.

Warum echte Präparate dennoch bleiben werden

Ein echtes Präparat besitzt Eigenschaften, die eine Replik

nicht hat:

► Es ist das tatsächliche Tier.
► Wissenschaftliche Untersuchungen (DNA, Federn, Haare, Gewebe) bleiben möglich.
► Historische Sammlungen haben einen dokumentarischen Wert.
► Viele Besucher empfinden Originale als authentischer.

Das ist vergleichbar mit Kunstwerken: Hochwertige Reproduktionen können einem Gemälde optisch sehr nahe kommen, ersetzen aber für viele Menschen nicht das Original.

Tharlarion Caravan Loading Station

Da die Weltläufte nichts hergeben, muss ich mir etwas ausdenken – etwas mit Tieren.. Außerdem sollte ich die 382-ste Aufgabe meiner Zeitung in Secondlife spätetens morgen fertig haben. Einer der dortigen Leser steuerte dieses Bild bei (credits: G□□RN H□G□L□□N (gwordn.tripsa), Rune Priest of Torvaldsland).

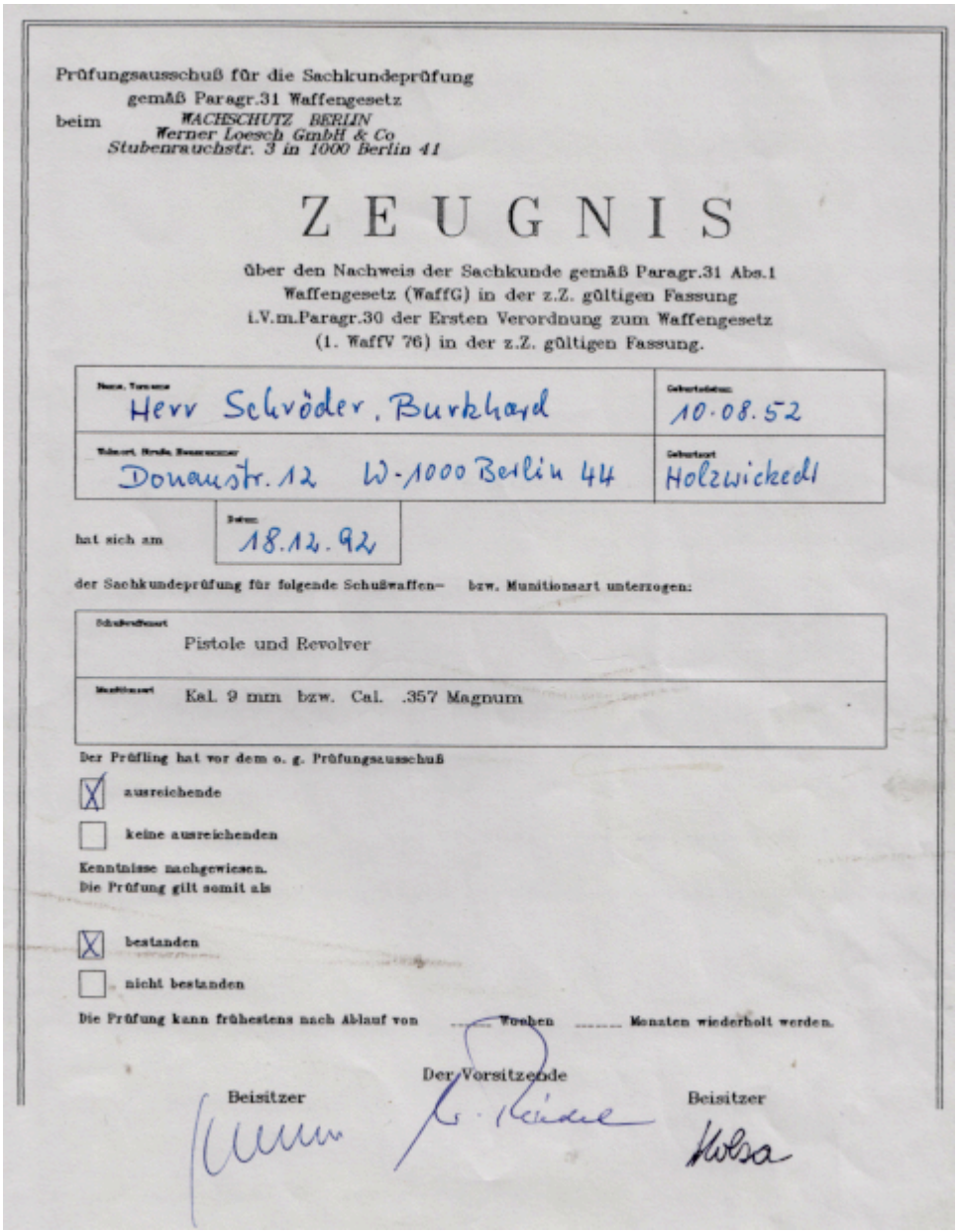
Geprägt

Jugendbildnis, ca. 1977. Man sieht deutlich, dass die Gesichtszüge vom Maoismus und allgemeiner Kapitalismus-Feindlichkeit geprägt wurden.

VW, enhanced

Mein Volkswagen, enhanced. Das Original hatte ich hier am 30.09.2023 schon gepostet. Das Original war ein Polaroid von 1979 oder 1980 und sah auch digitalisisert dementsprechen aus.

Pistole und Revolver



Prüfungsausschuß für die Sachkundeprüfung
gemäß Paragr.31 Waffengesetz
beim WACHSCHUTZ BERLIN
Werner Loesch GmbH & Co
Stubenrauchstr. 3 in 1000 Berlin 41

ZEUGNIS

über den Nachweis der Sachkunde gemäß Paragr.31 Abs.1
Waffengesetz (WaffG) in der z.Z. gültigen Fassung
i.V.m.Paragr.30 der Ersten Verordnung zum Waffengesetz
(1. WaffV 76) in der z.Z. gültigen Fassung.

Herr Schröder, Burkhard	10.08.52
Donaustr. 12 W-1000 Berlin 44	Holzwickedl

hat sich am 18.12.92

der Sachkundeprüfung für folgende Schußwaffen- bzw. Munitionsart unterzogen:

	Pistole und Revolver
	Kal. 9 mm bzw. Cal. .357 Magnum

Der Prüfling hat vor dem o. g. Prüfungsausschuß

[X] ausreichende

[ ] keine ausreichenden

Kenntnisse nachgewiesen.
Die Prüfung gilt somit als

[X] bestanden

[ ] nicht bestanden

Die Prüfung kann frühestens nach Ablauf von ..... Wochen ..... Monaten wiederholt werden.

Beisitzer Der Vorsitzende Beisitzer

Wisst ihr Bescheid.

Geheime zweite Schutzinselprofile

A futuristic smartphone displaying a hidden „Second Space“ profile designed to conceal sensitive data, sci-fi cyber security aesthetic, dual digital identities inside one device, encrypted private zone glowing beneath the normal interface, holographic folders, hidden emails and secret files protected behind biometric locks, layered user profiles visualized as parallel digital realities, dark neon environment, blue and cyan light, cinematic atmosphere, ultra-detailed, cyberpunk style, advanced mobile privacy technology, glowing encryption symbols, realistic high-tech smartphone UI, dramatic volumetric lighting, octane render, 8k –ar 16:9 –stylize 700

Wir müssen es mit der Datencontainerwissenschaft noch weiter treiben, zumal in den Kommentaren Defätismus verbreitet wurde, dem ich entgegenwirken will.

Die Idee, auf mich und meine kleine Hirse gemünzt (ich habe jetzt zwei Xiaomi-Handys): Ist es möglich, das E-Mail-Programm – hier FairEmail – in einem geschützten Container zu betreiben?

Die KI sagt: Ja und nein. Es sei prinzipiell möglich, „aber mit wichtigen Einschränkungen unter Xiaomi Android bzw. HyperOS/MIUI.“

Programme wie EDS können verschlüsselte Container (ähnlich VeraCrypt) bereitstellen. Darin lassen sich Dateien speichern. Schwieriger wird es aber bei kompletten installierten Apps wie FairEmail.

Der entscheidende Punkt: Android installiert Apps normalerweise immer im regulären App-Bereich des Systems. Ein Container wie EDS kann zwar APK-Dateien oder Daten speichern,

aber nicht ohne weiteres eine App „unsichtbar“ im Container betreiben, sodass sie erst nach dem Mounten erscheint.

Vorschlag: eine „Work Profile“-Container benutzen.

Mit Apps wie Shelter, Insular oder Island kann man FairEmail in ein getrenntes Arbeitsprofil installieren. Dieses Profil kann gesperrt werden. Dann verschwindet die App aus dem normalen Bereich, Benachrichtigungen stoppen, und erst nach Entsperren des Profils wird FairEmail sichtbar.

Alle drei Apps – Shelter, Insular und Island – basieren auf derselben Android-Technik: dem sogenannten „Work Profile“ bzw. Arbeitsprofil. Sie erzeugen also keinen echten VeraCrypt-artigen Container, sondern nutzen die von Android eingebaute Trennung verschiedener Profile.

„Das ist auf Xiaomi-Geräten meist die praktikabelste Lösung ohne Root-Zugriff.“

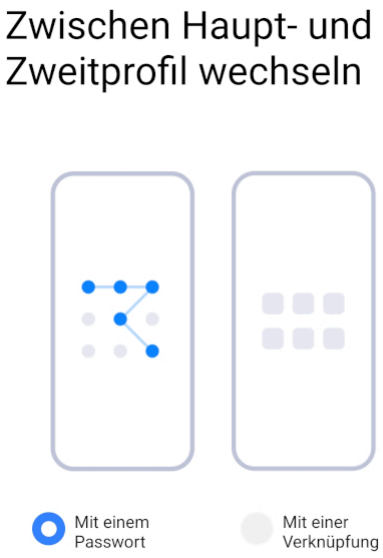
Funktion	**Shelter**	**Insular**	**Island**
Open Source	Ja	Ja	Teilweise / nicht vollständig FLOSS
Basis	Eigenständiges Projekt	Fork von Island	Originalprojekt
Datenschutz-Fokus	Sehr hoch	Hoch	Mittel
Werbung / Tracking	Keine bekannt	Keine bekannt	Teilweise Google-näher
Bedienung	Einfach, technisch	Modern und komfortabel	Sehr komfortabel
Apps einfrieren („Freeze“)	Ja	Ja	Ja
Arbeitsprofil pausieren	Ja	Ja	Ja

Funktion	Shelter	Insular	Island
Kontakte zwischen Profilen blockieren	Gut	Sehr gut	Eher schwach
F-Droid verfügbar	Ja	Ja	Nein
Xiaomi-Kompatibilität	Meist gut	Gut	Schwankt je nach HyperOS-Version
Ressourcenverbrauch	Gering	Mittel	Mittel
Typische Zielgruppe	Privacy- und Security-Nutzer	Privacy mit mehr Komfort	Mainstream- und Komfort-Nutzer
Besonderheit	Sehr transparent und minimalistisch	Guter Mittelweg zwischen Privacy und Bedienung	Viele Komfortfunktionen und App-Klonen
Empfehlung für FairEmail auf Xiaomi	Sehr empfehlenswert	Gut geeignet	Eher Komfortlösung

[Eine Stunde später.] Nein, ist es nicht.

Auf Xiaomi-Smartphones lässt sich Shelter zwar per F-Droid installieren, aber die vollständige Installation wird geblockt. Shelter ist auch im Play Store nicht mehr erhältlich. Shelter und Insula wurden entfernt, „unter anderem wegen Android-/Google-Play-Richtlinien rund um Work Profiles und App-Installation.“

Ich kann natürlich nichts darüber sagen, wie Apps, die per F-Droid installiert wurden, auf Samsung- und anderen Smartphones funktionieren. Bei Xiaomi geht es definitiv nicht.



Also Plan B. Und der wird jetzt richtig kompliziert und nerdig, aber es funktioniert.

Wer sich aber der Hilfe der KI bedienen will, muss starke Nerven haben, weil auf Anhieb alle Antworten falsch sind und dann bedauernd kommt: Ja, tut mir leid, früher war das so, heute ist das nicht mehr der Fall und ähnlicher nervtötender Quatsch.

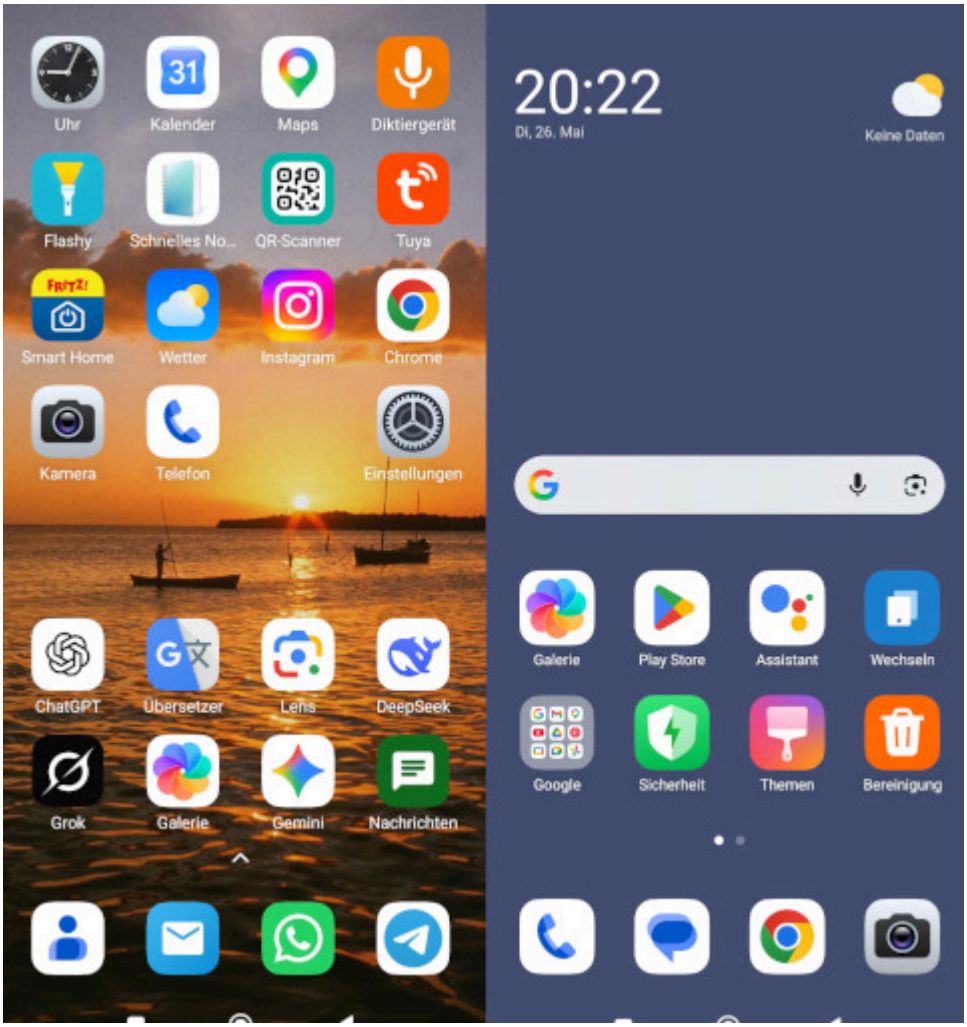
Man muss ein so genanntes Zweitprofil einrichten. (Die Option findet man in den Einstellungen.)

HyperOS hat die Oberfläche von „Second Space“ stark verändert:
– manche Regionen blenden das Icon aus,
– manche zeigen es nur im Zweitprofil,
– manche nur über den Sperrbildschirm.

Das ist an sich nicht kompliziert (wenn man das Feature gefunden hat). Die Panik kommt, wenn es funktioniert und man plötzlich vor einem ganz „fremden“ Handy-Monitor mit nur wenigen Apps sitzt. Wie gelangt man wieder zurück ins Hauptprofil? Es gibt im Zweitprofil einen „Schalter“ (wie eine App) „wechseln“. Aber mitnichten im Hauptprofil.

Man muss tricksen: Den Bildschirm sperren und dann mit dem Passwort oder dem Fingerabdruck des Zweitprofils einloggen.

Niemand weist einen darauf hin, dass man beim Anlegen des zweiten Profils auch andere Passwörter benutzen sollte – sonst funktionier das nicht und man tritt|tippt auf der Stelle.



Ich finde die Idee gut. Es ist fast so wie bei einem *hidden container*: Wenn ein Schnüffler gar nicht weiß, dass es ein zweites Profil gibt, müsste man schon gezielt und lange – mit forensischen Methoden – danach suchen. (Den Button „Wechseln“ habe ich ganz nach hinten verbannt.)

Wie die Übersicht unten zeigt, bieten einige Hersteller diese Option an.

Kompliziert ist bei Xiaomi, Daten von einem Profil zum anderen zu schicken. Ich habe mir beim ersten Mal mit Webmail beholfen. Zukünftig werde ich – wie bisher – einfach FTP benutzen.

Hersteller	Funktion	Art der Trennung	Besonderheiten
Xiaomi	Zweitprofil / Second Space	Sehr stark	Fast wie ein zweites Smartphone mit getrennten Apps, Daten und Konten
Samsung	Secure Folder	Stark	Knox-basierte Hardwareverschlüsselung, separater geschützter Bereich
OnePlus	System Cloner / Private Safe	Mittel bis stark	Separates Benutzerprofil mit eigenen Apps und Daten
OPPO	Privacy Space / System Cloner	Stark	Ähnlich Xiaomis Zweitprofil, inklusive separater Apps und Konten
Vivo	Privacy Space	Mittel	Fokus auf versteckte Apps und private Datenbereiche
Huawei	PrivateSpace	Sehr stark	Komplett getrenntes Profil mit eigenem Passwort und Fingerabdruck
Honor	Parallel Space / Private Space	Mittel	Je nach MagicOS-Version unterschiedlich umfangreich
Google Pixel / Android 15+	Private Space	Mittel	Versteckter App-Bereich mit separater Sperre und eigenem Play Store

Hersteller	Funktion	Art der Trennung	Besonderheiten
Standard-Android vieler Hersteller	Gastmodus / Mehrbenutzer	Sehr stark	Echte Android-Benutzerkonten mit vollständiger Trennung
Beste Sicherheitslösung	Samsung Knox Secure Folder	Sehr stark	Besonders starke Hardware- und Software-Isolation
Beste Alltagstauglichkeit	Xiaomi Zweitprofil	Sehr stark	Sehr komfortabler Wechsel zwischen getrennten Bereichen

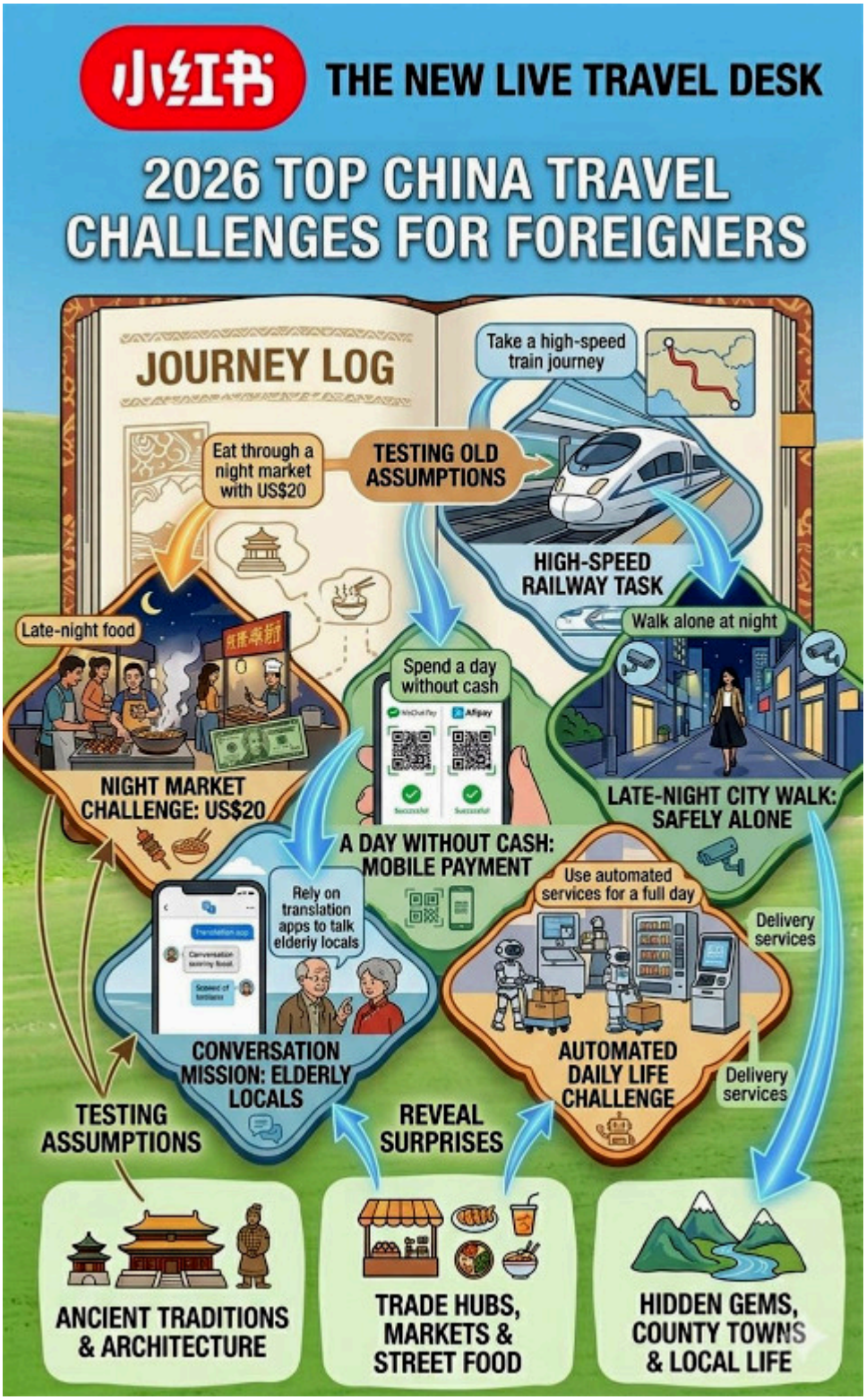
---

Der Osten ist rot!

Die deutsche Entwicklungshilfe zeigt endlich Früchte. Chinesische Raumfahrer, die man Taikonauten nennt, sind auf der chinesischen Weltraumstation gelandet und von der dortigen Mannschaft (sic) gendersprachenfrei empfangen worden.

China steht auf meiner To-Do-Liste, aber noch nicht in diesem Jahr. Vielleicht schon im nächsten? Auf jeden Fall zur

[Liveübertragung im Jahr ~~2023~~ 2030](#)!



Kaltstartangriffe und Hidden Volumes, minderlegal reloaded

Multiple nested encrypted containers, inspired by VeraCrypt, layered vaults inside each other, glowing secure cores, digital locks and keyholes, symbol of strong cryptography, dark background, blue and cyan light, ultra detailed, cinematic lighting, 3d render, octane style –ar 3:2 –s 750 (Midjourney)

Ich habe mich kurz umgesehen, was es an verständlichen Anleitungen gibt, ein *hidden volume* mit Veracrypt anzurichten. Es gibt einige und recht gute (auf Englisch), sogar für Lehrer.

Wenn man weiß, wie Veracrypt funktioniert, ist es fast selbsterklärend.

Merke: *Bevor Sie ein komplettes Laufwerk inklusive Daten verschlüsseln, sollten Sie die Dateien zuvor unbedingt sichern. Zwar arbeitet Veracrypt seit Jahren sehr zuverlässig, doch Fehler können trotzdem passieren.*

Das habe ich noch nie gemacht. So viele Daten, die privat bleiben sollten, habe ich gar nicht. Ich begnüge mich mit Containern und verschlüsselten USB-Sticks (vor allem auf Reisen). Umgekehrt: Wenn man das ganze Laufwerk des Rechners

verschlüsselt, braucht man *keine* Container.

Aber: Wozu sollte man *hidden volumes* überhaupt haben? Für misstrauische Ehepartner?

Ich habe mir ein Szenario überlegt, das vielleicht für Geschäftsleute realistisch ist, die davon ausgehen müssen, dass sie in dem Land, in dem sie gerade sind, gezwungen werden, den Inhalt ihrer Rechner den neugierigen Augen der dortigen Sicherheitsbehörden preiszugeben, etwa China und Hongkong, USA, Großbritannien, Kanada. (Fährt hier jemand oft nach Russland? Weiterlesen!)

Ich muss ein bisschen ausholen. Vor Jahren habe ich ein Vortrag in einem großen Rüstungskonzern über Sicherheit und Recherche gehalten und einer der Teilnehmer fragt, ob von ihrer Firma etwas im Darknet zu finden sei. Nichts leichter als das.

Man muss natürlich die Realität berücksichtigen; In welcher Firma ist es erlaubt, den Tor-Browser zu installieren und in dunkelsten Ecken des Netzes herumzusurfen? Ich habe schon in internationalen Konzernen gearbeitet, die sich IT-mäßig als Hochsicherheitstrakt – ohne jedwede Fremdgeräte – gaben, aber natürlich lagen alle Daten bei Microsoft in der Cloud.

Ich fand damals irgendwelche internen Preislisten der Firma im Darknet und löste eine gewissen Panik aus nach dem Motto:

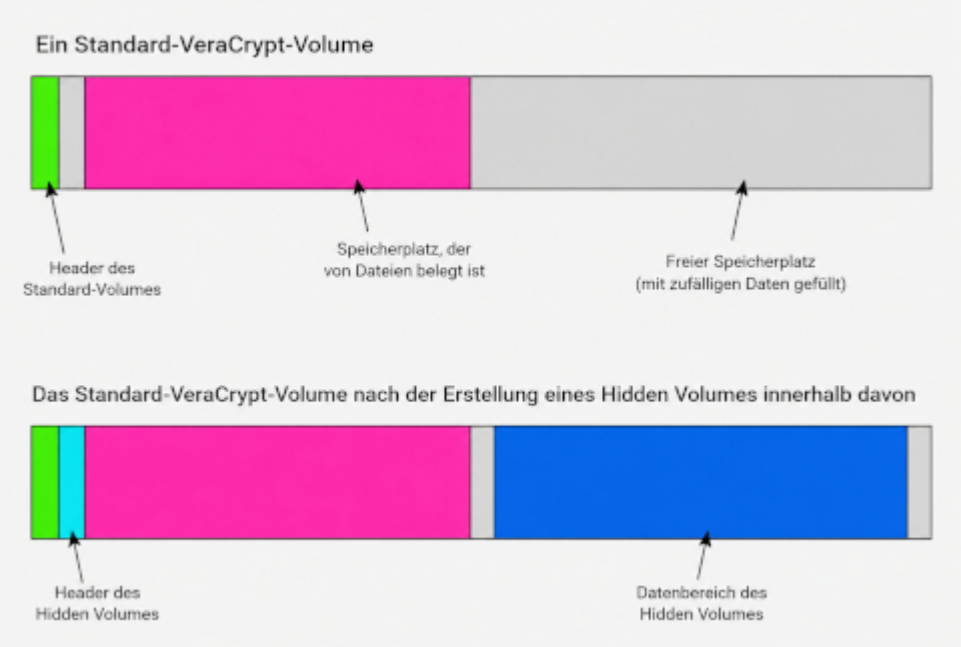
Kriegt man das wieder da weg?

Nehmen wir an, wie schicken dem potenziellen Geschäftskunden keine verschlüsselte E-Mails, sondern möchte bestimmt Dokumente, die viel wert sind, persönlich diskutieren. Und die Konkurrenz sollte davon auch nichts erfahren.

Es fängt schon bei den *basics* an und mit der – bei Microsoft-Hassern – legendären Schlagzeile „Microsoft Word bytes Tony Blair in the butt“. Oder jemand erstellte ein PDF für uns mit eingebettetem Javascript, das beim Aufrufen dieses und jenes aus dem Internet lädt. „Wenn es mehrere Möglichkeiten gibt, eine Aufgabe zu erledigen, und eine davon in einer Katastrophe endet oder sonst wie unerwünschte Konsequenzen nach sich zieht, dann wird es jemand genau so machen.“

Wir haben uns bemüht das zu vermeiden, und wollen zwei Dutzend Dokumente absolut sicher verbergen, auch wenn die Briten, Russen und US-Amerikaner unseren Laptop bei der Einreise auseinandernehmen, die Daumenschrauben rausholen und verkünden: Wenn du uns nicht alle Passwörter verrätst, musst du wieder heim!

Wir machen es richtig schwer. Die Chinesen sagen sogar: Öffnen Sie den Veraclypt-Containel! Und wenn der leer ist, werden sie erst recht misstrauisch.



Wenn wir nicht freiwillig verraten, das da noch in den Tiefen ein *hiden volume* schlummert, sind wir auf der sicheren Seite – mit kleineren Einschränkungen, die zu beachten wären.

Segment	**Bedeutung**	**Erklärung**
Header des Standard-Volumes	Startbereich des normalen VeraCrypt-Volumes	Enthält die verschlüsselten Informationen, mit denen VeraCrypt das äußere Volume öffnen kann.
Speicherplatz, der von Dateien belegt ist	Sichtbare Dateien im äußeren Volume	Hier liegen die normalen, harmlosen Dateien, die beim Öffnen mit dem äußeren Passwort sichtbar werden.

Segment	Bedeutung	Erklärung
Freier Speicherplatz	Scheinbar leerer Bereich	Dieser Bereich ist mit Zufallsdaten gefüllt. Dadurch ist nicht erkennbar, ob er wirklich leer ist oder ein Hidden Volume enthält.
Header des Hidden Volumes	Startbereich des versteckten Volumes	Wird nur mit dem Passwort des Hidden Volumes erkannt. Für Außenstehende sieht er wie Zufallsdaten aus.
Datenbereich des Hidden Volumes	Geheimer Speicherbereich	Hier liegen die eigentlichen geheimen Dateien. Ohne das richtige Passwort ist dieser Bereich nicht vom übrigen Zufallsdatenbereich zu unterscheiden.

Wer das noch nie gemacht hat und des Lesens von kurzen Texten mächtig ist: Bei VeraCrypt wird ein Hidden Container (bei mir unter Linux) über die grafische Oberfläche genauso geöffnet wie ein normaler Container.

Zunächst startet man VeraCrypt über das Anwendungsmenü und klickt anschließend auf *select file (Veracrypt gibt es auch auf Deutsch), um die Container-Datei auszuwählen. Danach markiert man einen freien Slot (oder „Laufwerk)) und klickt auf mount*.

Entscheidend ist allein das eingegebene Passwort: Wird das

Passwort des **äußeren Containers** (oder *volume*) eingegeben, öffnet VeraCrypt das normale äußere Volume; wird dagegen das Passwort des **Hidden Volumes** eingegeben, wird automatisch das versteckte Volume geöffnet.

Es gibt dafür keinen besonderen Menüpunkt und auch keine separate Datei für das Hidden Volume, da sich beide Bereiche innerhalb derselben verschlüsselten Containerdatei befinden.

Nach erfolgreichem Einhängen erscheint das Volume wie ein normales Laufwerk im Dateimanager. Wichtig ist außerdem, dass beim Öffnen des äußeren Volumes Schreibzugriffe das versteckte Volume beschädigen können. Deshalb sollte man beim Mounten des äußeren Volumes in den „Mount Options“ die Funktion „Protect hidden volume against damage caused by writing to outer volume“ aktivieren und zusätzlich das Passwort des Hidden Volumes angeben.

Bei VeraCrypt bleibt ein Hidden Volume auch dann unsichtbar, wenn man beim Öffnen des äußeren Containers die Funktion *mount all devices* beziehungsweise „Alle Datenträger einhängen“ verwendet: Das versteckte Volume ist technisch kein eigenes Laufwerk und keine eigene Datei. Äußeres Volume und Hidden Volume befinden sich innerhalb derselben verschlüsselten Containerdatei oder Partition. VeraCrypt erkennt daher nicht zwei getrennte Datenträger, sondern nur einen einzigen verschlüsselten Container. Welcher Bereich tatsächlich geöffnet wird, entscheidet ausschließlich das eingegebene Passwort.

Technisch ist das Hidden Volume zwar nicht von zufälligen verschlüsselten Daten zu unterscheiden. In der Praxis entstehen aber unter Umständen Hinweise durch das Verhalten des Nutzers oder durch „Daten-Beifang“ außerhalb des Containers.

Multiple nested encrypted containers, inspired by VeraCrypt, layered vaults inside each other, glowing secure cores, digital locks and keyholes, symbol of strong cryptography, dark background, blue and cyan light, ultra detailed, cinematic lighting, 3d render, octane style –ar 3:2 –s 750 (Gemini)

Ein Risiko: Das äußere Volume wirkt ungewöhnlich leer. Wenn ein großer Container vorhanden ist, sich darin aber nur wenige harmlose Dateien befinden und gleichzeitig nur wenig freier Speicher angezeigt wird, kann dies Verdacht erregen. Deshalb empfiehlt VeraCrypt, das äußere Volume mit glaubwürdigen Dummy-Dateien zu füllen, damit der belegte Platz plausibel erscheint.

Ich würde als Geschäftsmann daher in den äußeren Container Duplikate aller meiner geheimen Dokumente legen, aber mit falschen Zahlen und Angaben, am besten noch mit „streng geheim“ markiert, und beim erzwungenen Öffnen des (äußeren) Containers händeringend in Tränen ausbrechen.

ChatGPT warnt: Auch Metadaten außerhalb des Containers können problematisch sein. Beispielsweise können Dateimanager, Backup-Programme oder Cloud-Synchronisationsdienste Hinweise liefern, dass bestimmte Dateien häufiger benutzt werden, als es der sichtbare Inhalt des äußeren Volumes vermuten lässt. Ebenso können temporäre Dateien, Vorschaubilder, zuletzt geöffnete Dokumente oder Einträge in der Shell-History

verraten, dass mit sensiblen Daten gearbeitet wurde.

Ein weiteres Risiko liegt in forensischen Analysen des Systemspeichers. Wenn ein Hidden Volume geöffnet ist, können Schlüsselmaterial oder Dateinamen zeitweise im RAM vorhanden sein. Wird ein laufendes System beschlagnahmt oder ein sogenannter Cold-Boot-Angriff durchgeführt, könnten Ermittler Hinweise auf ein geöffnetes verstecktes Volume finden. Deshalb schützt VeraCrypt vor allem ruhende Daten (Data at rest), nicht unbedingt ein bereits laufendes und entsperrtes System.

Ich habe natürlich einen unschlagbaren Vorteil – solange niemand mein Blog liest: Bei meinem Alter werden Grenzbeamte sich vermutlich fragen, ob ich den Unterschied zwischen einem Betriebssystem und einem Browser kennte. Und ich werde harmlos lächeln und mich angemessen verbeugen.

Unter Nicht-Migranten

Das Ministerium für Wahrheit – auch bekannt als „Tagesschau“ – gibt bekannt: Deutsche heißen jetzt „Nicht-Migranten“.

Meine Urgrosseltern Anna Emilie Kukuk und Gustav Reinhold Schröder, revisited

Meine Urgroßmutter Anna Emilie Kukuk, Bäuerin (geb. 22.5.1864 in Elsendorf, Westpreußen heute Dąbrowa Wielka, Polen) und mein Urgroßvater Gustav Reinhold Schröder, Bauer (geb. 14.5.1859 in Mittenwalde, heute Dąbrowa Mała, Polen) bei ihrer Diamantenen Hochzeit am 11.12.1942. Mein Urgroßvater war damals 84, meine Urgroßmutter fünf Jahre jünger.

Das untere Foto hatte ich schon am 22.02.2013 publiziert. Die obere Version wurde mit ChatGPT verbessert.

Kennt sich jemand mir Orden aus? Es ist kaum etwas zu erkennen. ChatGPT hat zwar zahlreiche Vorschläge, muss aber auch passen.

Plausible Abstreitbarkeit

Ein Artikel von mir im Journalistenblatt 2/2026.

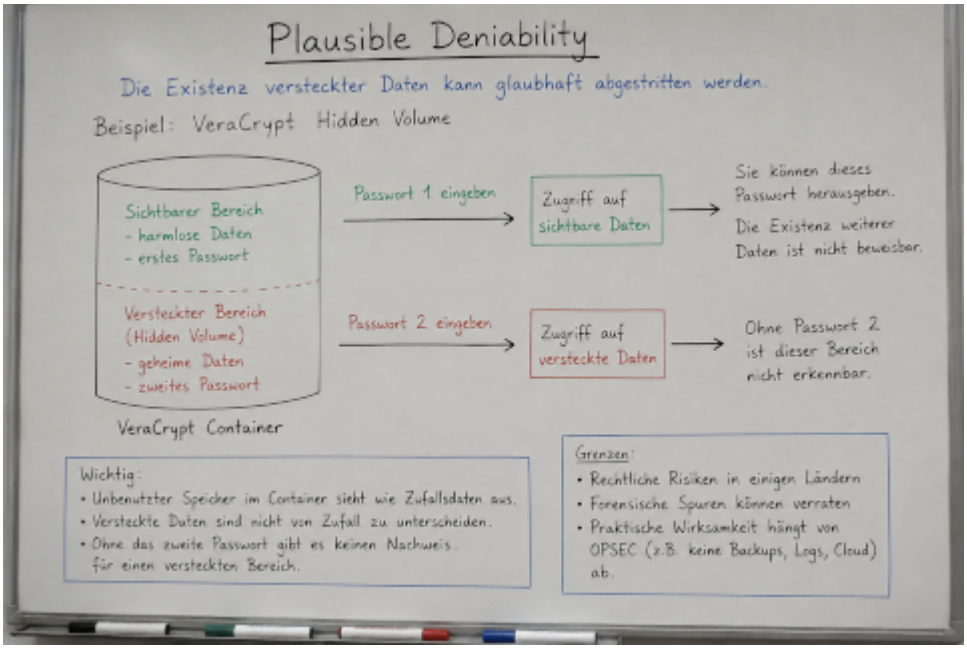
Reisen wir nach Hongkong, China, Neuseeland oder Russland? Es macht keinen Unterschied, was die Neugier der jeweiligen Sicherheitskräfte angeht. Man muss alle elektronischen Geräte bei der Einreise entsperren und alle Passwörter herausrücken. (vgl. Übersicht unten, Stand April 2026). Das gilt nicht nur für Leute, die Ilhan Omar heißen oder einen Islamistenbart tragen.

Das Konsulat der USA in Hongkong warnt zum Beispiel: Am 23. März 2026 änderte die Regierung von Hongkong die Durchführungsbestimmungen zum National Security Law. Es ist nun strafbar, sich zu weigern, der Hongkonger Polizei Passwörter mitzuteilen oder Entschlüsselungshilfe zu leisten, um Zugriff auf sämtliche persönlichen elektronischen Geräte zu ermöglichen, einschließlich Mobiltelefonen und Laptops. Die Geräte können auch beschlagnahmt werden, sind die Grenzbeamten misstrauisch geworden.

Geschäftsleute und Journalisten, die Daten und Dokumente

ungern in falsche Hände sehen wollen, können das Risiko minimieren, indem sie auf einer Auslandsreise ein „leeres“ Laptop mitnehmen und ein Zweithandy benutzen, auf dem nichts Privates zu finden ist, und dann vor Ort alles neu installieren und von der eigenen Cloud herunterladen. Das ist aber unpraktisch und umständlich.

Kategorie	Staat	Rechtslage	Konsequenz bei Verweigerung	Besonderheiten
Strafbarer Passwort-Zwang	Hongkong	Passwortherausgabe gesetzlich erzwingbar	Geldstrafe oder Haft möglich	Gilt auch bei Transit
Strafbarer Passwort-Zwang	China	Weitreichende Sicherheitsgesetze	Strafverfolgung möglich	Besonders streng bei politischen Inhalten
Strafbarer Passwort-Zwang	Vereinigtes Königreich	Anti-Terror-Gesetze erlauben Passwortforderung	Strafbar bei Verweigerung	Auch ohne konkreten Verdacht möglich
Strafbarer Passwort-Zwang	Neuseeland	Zoll darf Entsperrung verlangen	Geldstrafe bei Weigerung	Gilt speziell bei Einreise
Faktischer Zwang	Vereinigte Staaten	Geräte dürfen durchsucht werden	Einreise kann verweigert werden	Besonders bei Nicht-Staatsbürgern
Faktischer Zwang	Kanada	Grenzbehörden dürfen Geräte prüfen	Probleme/Verzögerung möglich	Rechtslage im Wandel
Faktischer Zwang	Australien	Durchsuchung ohne richterlichen Beschluss	Verweigerung führt zu Problemen	Weitreichende Zollbefugnisse
Faktischer Zwang	Russland	Sicherheitsbehörden mit umfassenden Befugnissen	Einreiseprobleme möglich	Praxis teils streng umgesetzt



Mit dem Zwang, alle Passwörter herauszugeben, verhält es sich wie mit Zensur jedweder Art: Das trifft nur die Dummen und Faulen, nie die Richtigen. Man kann das alles umgehen, und muss noch nicht einmal IT- oder Kryptografie-Experte sein.

Die Aufgabe ist also nicht nur, Inhalte zu verbergen, sondern auch, das Verbergen zu verbergen.

Das Problem: Es dürfte bekannt sein, dass alles, was man schützen will, in verschlüsselte Verycrypt-Container gehört. Dafür gibt es zahllose und sogar leicht verständliche Tutorials. Aber: Weil es jeder weiß, wird ein Grenzbeamter, der sich auskennt, beim Entsperren eines Laptops diese Container entdecken und dann auffordern, ihm den Inhalt zu zeigen. Die Aufgabe ist also nicht nur, Inhalte zu verbergen, sondern auch, das Verbergen zu verbergen.

Das ist gar nicht so kompliziert, wie es sich anhört. Das Prinzip nennt man „Plausible Deniability“ (plausible Abstreitbarkeit). Wenn man mit Veracrypt einen „hidden container“ anlegt, hat man einen sichtbaren Container (der wie eine Dateiordner aussieht), indem sich ein weiterer Ordner (Container) verbirgt, der aber unsichtbar ist und auch ein anderes Passwort hat. Wenn man gezwungen wird, das Passwort herauszugeben, gibt man das des äußeren Containers an, der

legitime, unkritische Daten enthält – der versteckte Dateiordner bleibt unsichtbar. Das funktioniert mit allem Betriebssystemen und auch externen Speichern wie USB-Sticks.

Das Problem sind natürlich die E-Mail-Programme auf Smartphones und Rechnern. Man könnte sogar gezwungen werden, verschlüsselte E-Mails zu öffnen. Noch schlimmer ist, dass alle Kontakte offen gelegt wären.

Auch dafür gibt es eine Lösung – hier eine Übersicht:

System	**Anleitung**
Windows	1. VeraCrypt installieren. 2. Einen verschlüsselten Container erstellen. 3. Den Container als Laufwerk einbinden, zum Beispiel V:. 4. Das Mailprofil oder die portable Version des Mailprogramms in den Container verschieben. 5. Das Mailprogramm nur starten, wenn der Container eingebunden ist. 6. Nach der Nutzung das Mailprogramm schließen und den Container aushängen.
Ubuntu / Linux	1. VeraCrypt installieren. 2. Einen Container anlegen und mounten, zum Beispiel nach /media/veracrypt1. 3. Das Thunderbird-Profil in diesen Container verschieben. 4. Thunderbird mit dem Profil im Container starten, z. B. mit: thunderbird -profile /media/veracrypt1/thunderbird-profile 5. Nach dem Arbeiten Thunderbird beenden und den Container wieder aushängen.

System	Anleitung
macOS	1. VeraCrypt installieren oder alternativ ein verschlüsseltes DMG-Image mit dem Festplattendienstprogramm anlegen. 2. Den Container oder das verschlüsselte Image öffnen. 3. Das Mailprofil in den verschlüsselten Bereich verschieben. 4. Das Mailprogramm nur von dort bzw. mit diesem Profil starten. 5. Nach der Nutzung das Mailprogramm beenden und das Image bzw. den Container schließen.
Hinweis	Der Schutz wirkt nur, solange der Container geschlossen ist. Wenn der Container geöffnet und das Mailprogramm aktiv ist, können die Inhalte natürlich gelesen werden. Für mehr Sicherheit sollten außerdem temporäre Dateien, Suchindizes, Ruhezustand und unverschlüsselte Backups beachtet werden.

Bereich	Anleitung
Ziel	Die lokal gespeicherten E-Mails sollen nicht offen auf dem Smartphone liegen, sondern möglichst in einem verschlüsselten Bereich gespeichert werden.

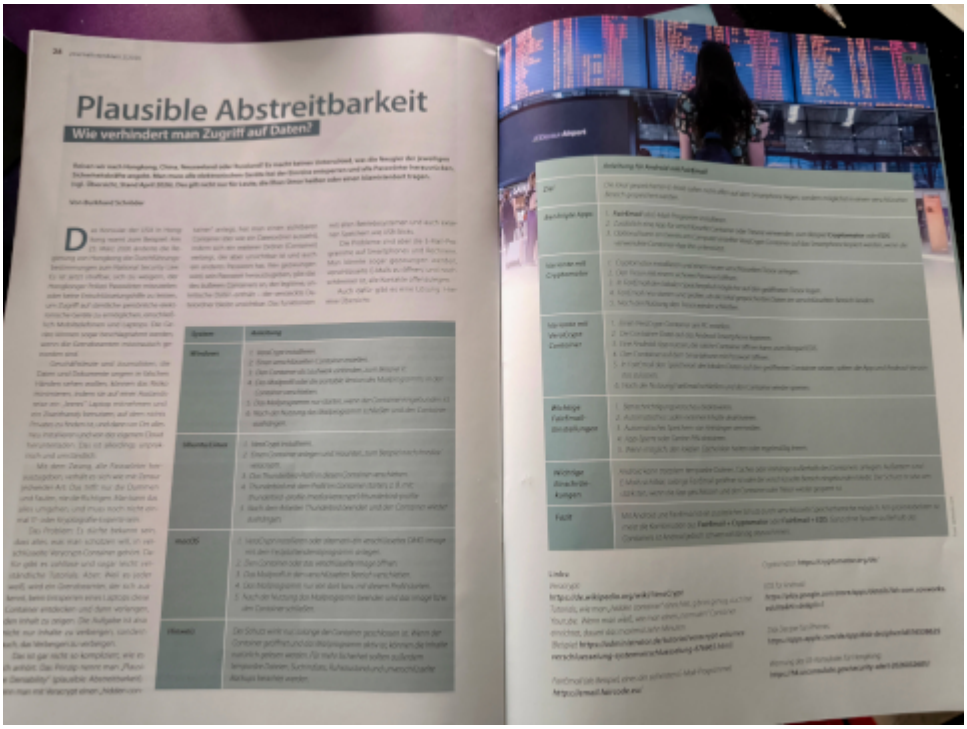
Bereich	Anleitung
Benötigte Apps	1. FairEmail als E-Mail-Programm installieren. 2. Zusätzlich eine App für verschlüsselte Container oder Tresore verwenden, zum Beispiel Cryptomator oder EDS. 3. Optional kann ein bereits am Computer erstellter VeraCrypt-Container auf das Smartphone kopiert werden, wenn die verwendete Container-App ihn unterstützt.
Variante mit Cryptomator	1. Cryptomator installieren und einen neuen verschlüsselten Tresor anlegen. 2. Den Tresor mit einem sicheren Passwort öffnen. 3. In FairEmail den lokalen Speicherpfad möglichst auf den geöffneten Tresor legen. 4. FairEmail neu starten und prüfen, ob die lokal gespeicherten Daten im verschlüsselten Bereich landen. 5. Nach der Nutzung den Tresor wieder schließen.

Bereich	Anleitung
Variante mit VeraCrypt-Container	1. Einen VeraCrypt-Container am PC erstellen. 2. Die Container-Datei auf das Android-Smartphone kopieren. 3. Eine Android-App nutzen, die solche Container öffnen kann, zum Beispiel EDS. 4. Den Container auf dem Smartphone mit Passwort öffnen. 5. In FairEmail den Speicherort der lokalen Daten auf den geöffneten Container setzen, sofern die App und Android-Version das zulassen. 6. Nach der Nutzung FairEmail schließen und den Container wieder sperren.
Wichtige FairEmail-Einstellungen	1. Benachrichtigungsvorschau deaktivieren. 2. Automatisches Laden externer Inhalte deaktivieren. 3. Automatisches Speichern von Anhängen vermeiden. 4. App-Sperre oder Geräte-PIN aktivieren. 5. Wenn möglich, den lokalen Cache klein halten oder regelmäßig leeren.

Bereich	Anleitung
Wichtige Einschränkungen	Android kann trotzdem temporäre Dateien, Caches oder Anhänge außerhalb des Containers anlegen. Außerdem sind E-Mails sichtbar, solange FairEmail geöffnet ist oder der verschlüsselte Bereich eingebunden bleibt. Der Schutz ist also am stärksten, wenn die App geschlossen und der Container oder Tresor wieder gesperrt ist.
Fazit	Mit Android und FairEmail ist ein zusätzlicher Schutz durch verschlüsselte Speicherbereiche möglich. Am praktikabelsten ist meist die Kombination aus FairEmail + Cryptomator oder FairEmail + EDS. Ganz ohne Spuren außerhalb des Containers ist Android jedoch schwer vollständig abzuschirmen.

Wer nichts zu verbergen und eine Webcam im Schlafzimmer installiert hat, muss nichts tun.

Gute Reise!



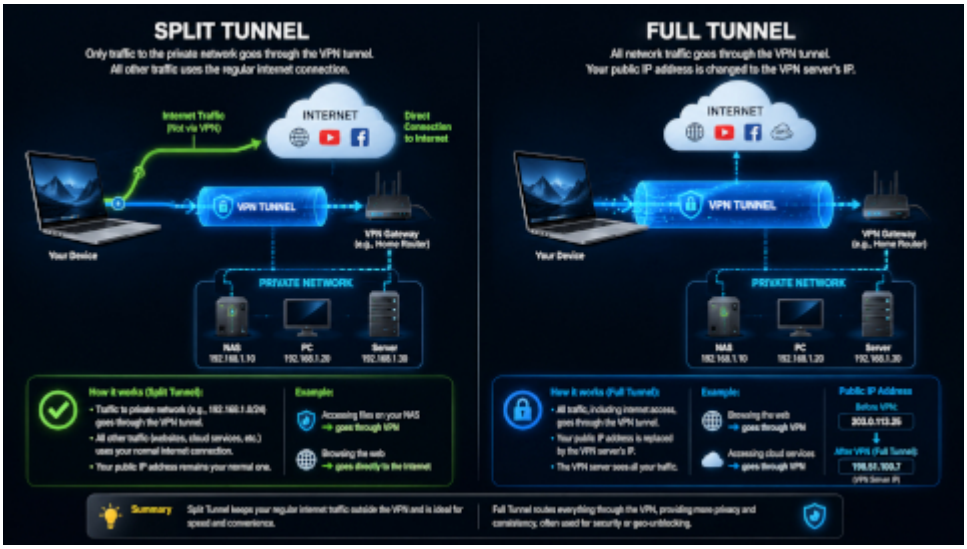
Links:

– Veracrypt
– Tutorials, wie man *hidden container* einrichtet, gibt es genug, auch bei Youtube. Wenn man weiß, wie man einen „normalen“ Container einrichtet, dauert das maximal zehn Minuten. Beispiel: Vollständiges Veracrypt Tutorial: Volumes – Hidden Volumes – Systemverschlüsselung.
– FairEMail – als Beispiel, eines der sichersten E-Mail-Programme)
– Cryptomator
– EDS für Android
– Disk Deciper für iPhones

Neukölln in einem Foto

Der QR-Code von den Plakaten war vor einer Sekunde abgerissen worden, vom wem, weiß ich aber nicht…

Split Tunneling



A modern cybersecurity infographic illustrating the difference between Split Tunneling and Full VPN Tunneling. On the left side, show a laptop connected to a VPN tunnel where only traffic to a home network and private servers passes through the encrypted tunnel, while normal internet traffic bypasses it directly to the web. Label this “Split Tunnel”. On the right side, show a “Full Tunnel” where all internet traffic, including websites and cloud services, is routed completely through the VPN tunnel, changing the user’s public IP address. Use glowing blue VPN tunnels, network diagrams, internet cloud icons, routers, and data streams. Professional IT illustration style, dark background with neon blue and cyan highlights, highly detailed, clean layout, futuristic networking concept art, cinematic lighting –ar 16:9 –v 7 (ChatGPT)

Ich hatte neulich ein interessantes IT-Problem: *Ich bin mit einem Ubuntu Laptop in einem Firmennetz online, wenn ich Wireguard einschalte, komme ich nicht aber mehr online. Kann es sein, dass der Admin des Firmennetzes VPN bzw. Wireguard zu meiner eigenen Fritz!Box unterbindet?*

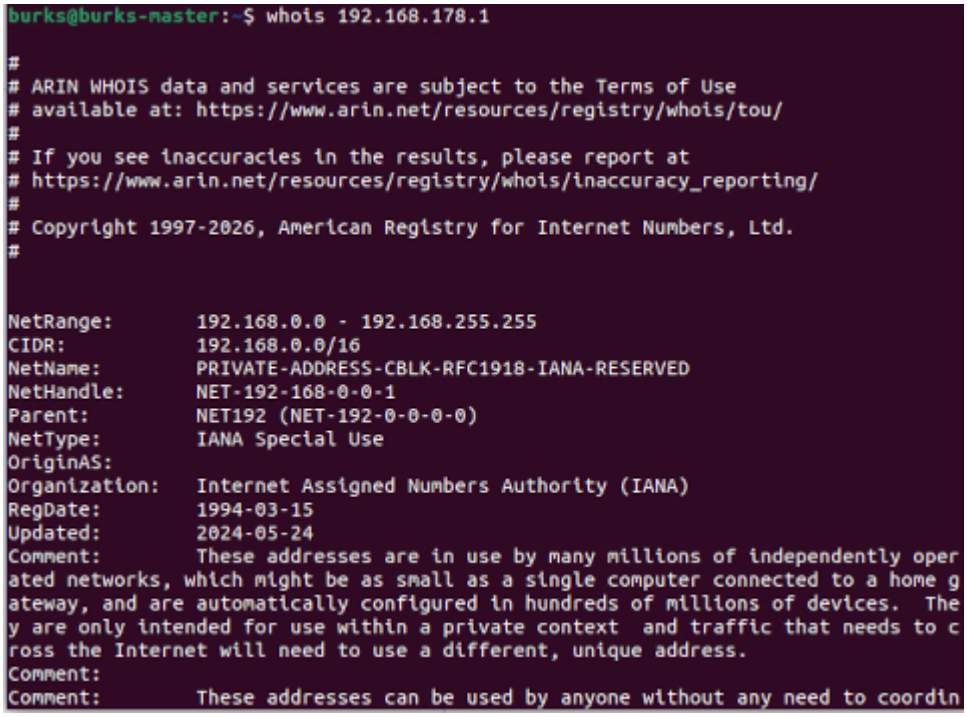
Daraus ergab sich eine längere „Unterhaltung“ mit viel Gefummel, und das Problem konnte ich noch nicht lösen. Ich weiß aber, wie es ginge, habe nur keine Lust dazu. Da ich aber im November außerhalb Europas sein werden, könnte es sein, dass ich doch etwas machen muss, weil dort das Internet streng zensiert wird.

Midjourney erzeugt bei identischem Prompt nur symbolischen Unfug ohne Erkenntniswert.

Ja, das ist gut möglich. Viele Firmennetze blockieren oder filtern VPN-Verbindungen – besonders unbekannte oder private VPNs wie eine eigene FRITZ!Box-WireGuard-Verbindung.

Typische Ursachen:
→ Die Firewall blockiert den WireGuard-Port (standardmäßig UDP 51820).
→ UDP-Traffic wird generell eingeschränkt.
→ Das Firmennetz erlaubt nur HTTP/HTTPS über Proxy.
→ Deep Packet Inspection erkennt und blockiert VPN-Traffic.
→ Das Firmennetz verhindert „Split Tunneling“ oder private Tunnel absichtlich aus Sicherheitsgründen.

Dass „gar nichts mehr geht“, sobald WireGuard aktiv ist, deutet oft auf eines dieser Probleme hin:
→ Der Tunnel baut sich nicht korrekt auf
→ dann routet Ubuntu trotzdem alles durch das VPN und verliert Internetzugang.
DNS wird über den Tunnel geschickt, funktioniert aber nicht
→ Webseiten wirken „offline“, obwohl IP-Verbindungen evtl. noch gehen.
Die Firma blockiert genau den UDP-Verkehr zur Fritzbox
→ Handshake kommt nie zustande.



Ping geht, aber DNS nicht. Also liegt das Problem vermutlich daran. Was haltet ihr von den Ratschlägen der KI?

Wenn Ping auf IPs geht, aber DNS nicht:
→ DNS-Problem im Tunnel.

Oft hilft bei Firmennetzen:
→ WireGuard auf einen anderen UDP-Port legen (z. B. 53, 123 oder 443 UDP)
→ Auf der Fritzbox einen alternativen Port konfigurieren
→ PersistentKeepalive = 25
→ Split Tunneling statt AllowedIPs = 0.0.0.0/0
Beispiel: AllowedIPs = 192.168.178.0/24

```
resolvectl status

Global
               Protocols: -LLMNR -mDNS -DNSOverTLS
DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (wlp0s12f0)
```

```
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
DNSSEC=no/unsupported
Current DNS Server: 8.8.4.4
       DNS Servers: 8.8.8.8 8.8.4.4

Link 4 (wg_config)
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
DNSSEC=no/unsupported
Current DNS Server: 192.168.178.1
                    DNS   Servers:   192.168.178.1
fd93:9136:e393:0:7642:7fff:fe2c:f103
        DNS Domain: fritz.box ~.
```

Das erklärt das Verhalten ziemlich eindeutig. Dein WireGuard-Tunnel setzt den DNS auf deine FRITZ!Box:
Current DNS Server: 192.168.178.1

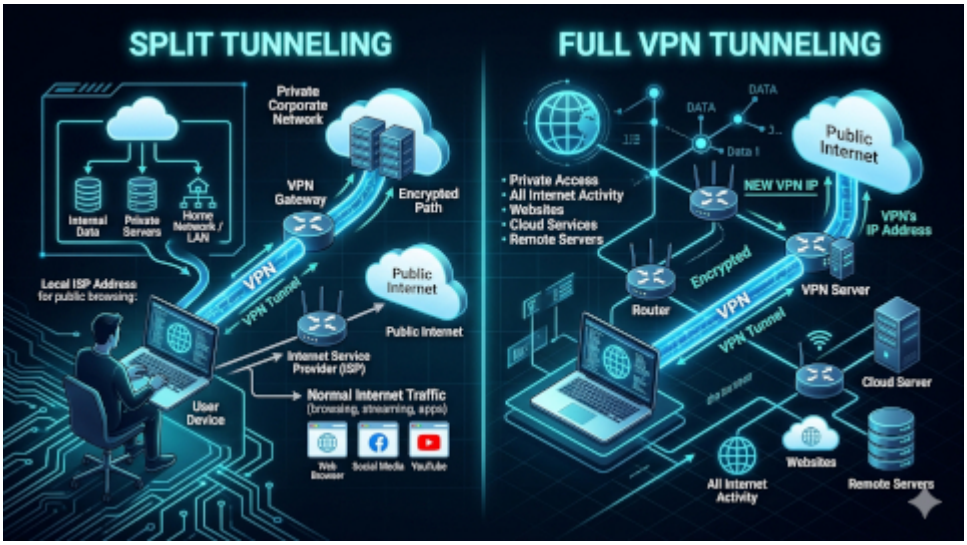
Sobald WireGuard aktiv wird, versucht Ubuntu also:
→ alle DNS-Anfragen an deine Fritzbox zuhause zu schicken durch den VPN-Tunnel
→ Wenn der Tunnel aber im Firmennetz nicht richtig funktioniert oder UDP teilweise blockiert wird, erreicht dein Laptop die Fritzbox-DNS nicht mehr zuverlässig.

Darum:
→ DNS → kaputt
→ Webseiten → „offline“
→ SERVFAIL von 127.0.0.53

Der entscheidende Punkt:
Dein normales WLAN (wlp0s12f0) hat funktionierende Google-DNS:
→ 8.8.8.8
→ 8.8.4.4

Aber WireGuard überschreibt das mit:
192.168.178.1
„Das ist typisch bei Fritzbox-WireGuard-Konfigurationen.“

ChatGPT empfiehlt split tunneling: Das sei in Firmennetzen fast immer die stabilere Lösung. Das hülfe mir aber nicht gegen Internet-Zensur…



Identischer Prompt, Gemini-Version

Sie werden ersetzt. Widerstand ist zwecklos.

Sehr geehrtes Zentralorgan für Oberstudienräte! Mein Arbeitsplatz ist sicher und wird nicht ersetzt!

Von irgendwem Gekapertes

Womöglich eine Erlanger Gleichstellungsbeauftragte mit Lebensabschnittsgefährtem beim Spaziergang im Walderlebniszentrum Tennenlohe (Symbolbild)

Noch einmal zu Joana und anderem. Man freut sich, wenn die eigenen Vorurteile bestätigt werden. Erlangen hat (hatte?) gleich zwei Gleichstellungsbeauftragte, die genau so aussehen, wie man sich Gleichstellungsbeauftragte vorstellt, wenn sie bestimmte Lieder anhören.

Das ehemalige Nachrichtenmagazin schreibt: „Die Stadt Erlangen betonte gegenüber den »Nürnberger Nachrichten« [natürlich ohne einen Link zur Quelle zu setzen], dass es sich bei den zwölf Songs nicht um eine Verbotsliste handele. »Die Liste ist als Orientierung und Sensibilisierung gedacht. Unser gemeinsames Ziel mit Wirtinnen, Wirten und Schaustellerbetrieben ist ein friedliches und respektvolles Fest für alle«, heißt es. Einfacher gesagt: Die Gleichstellungsstelle macht das, was eine Gleichstellungsstelle halt so macht.“

„Im vergangenen Jahr hatte es Berichte über sexuelle Belästigung auf dem Volksfest gegeben, womöglich angeheizt durch frauenfeindliche Songtexte“. Womöglich. Womöglich werden islamische Messerstecher auch durch einschlägige Computerspiele angeheizt. Womöglich fällt irgendwo ein Baum um, daher sollten Spaziergänger in Baumnähe immer einen Helm tragen.

Meine Verschwörungstheorie ist: Die Erlanger AfD hat den Gleichstellungsbeauftragten vorher ein paar Geldscheine zugesteckt mit der Bitte, doch mal eine Liste von Musikstücken zusammenzustellen, die Gleichstellungsbeauftragten auf keinen Fall gefallen würde und diese natürlich an die Presse weiterzugeben, wegen „Transparenz, Vielfalt und Öffentlichkeit“ und so.

„2024 hat man sich mit Festwirten und Musikern zudem darauf geeinigt, das inzwischen häufig von Rechten gekaperte Lied L’Amour Toujours nicht mehr zu spielen.“

Deswegen sollte die deutsche Nationalhymne auch nie mehr gespielt werden. Am besten sogar verbieten.

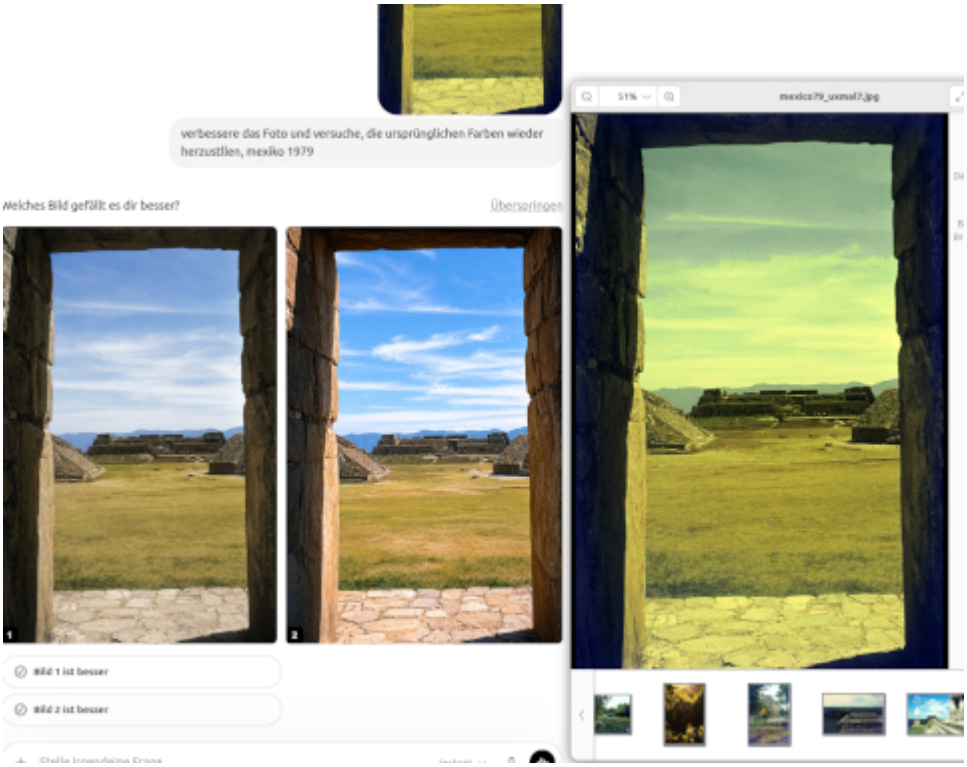
Der weiße Berg und Uxmal, KI revisited und der vergebliche Versuch, etwas in die Zukunft zu retten

Das Original-Foto

Zu meiner Überraschung fand ich das obige Foto auf dem Blog gar nicht. Habe ich es bisher nicht veröffentlicht? Monte Albán war ehemalige Hauptstadt und das religiöse Zentrum der Zapoteken im heutigen Mexiko in der Nähe von Oaxaca. Das Foto habe ich am 14.10.1979 gemacht. Über Monte Alban hatte ich am 13.07.2012 und am 02.07.2023 etwas geschrieben.

Uxmal das Original-Foto, hier veröffentlicht am 06.08.2022. Fotografiert in Yucatan, Mexiko, am 17.10.1979.

Ich war etwas komplizierter als gedacht, die Fotos (die schon ein eingescannte Dias waren) zu restaurieren.



Offenbar haben künstliche Intelligenzen ein Problem, „verbessern“ und „verändern“ unterscheiden zu können. Geminis Versionen von Monte Alban waren zwar auch gut, aber beim ersten Mal halluzinierte die KI eine große Touristengruppe auf den kleinen Hügel im Hintergrund in der Mitte. Die fiktiven Personen waren so klein, dass ich sie beinahe nicht gesehen hätte. Wir waren damals allein – andere Touristen wären kontraproduktiv und sowieso komplett gelogen.

Version ChatGPT von Monte Alban

Bei Uxmal wurden mir zwei Versionen vorgeschlagen. Die zweite hatte den Himmel verändert und war geringfügig besser, ich wählte dennoch der Authentizität werden die erste.

Uxmal, Version Gemini

Natürlich ist das alles völlig sinnlos. Wer interessiert sich für Fotos, die vor einem halben Jahrhundert geschossen wurden?

Ich habe zwar Nachfahren, die meinen gesamten Krempel erben werden, aber die rufen vermutlich gleich einen Entrümplungsdienst.

Etwas irgendjemandem hinterlassen zu wollen, ist evolutionär eine Übersprungshandlung des Zeugens von Nachkommen. So sehe ich das. Die Nachgeborenen lernen nicht aus den Fehlern, die man selbst gemacht hat.

Ich werde ganz egoistisch dennoch alle (ca. 3000) Bilder noch einmal durchforsten und auch die Reise-Tagebücher, die ich, als ich begann, die Fotos hier zu veröffentlichen (2010? Die auf spiggel.de – der Vor-Version dieses Blogs – waren nicht eingesannt), gar nicht berücksichtigt hatte – auf die Idee kam ich erst später. Kann sein, dass das Publikum demnächst Bilder vorgesetzt bekommt, die es schon kennt, nur etwas *enhanced*…

Nonnenklostervieréck [2. Update]

Ich bin sehr motiviert, meine alten Fotos von der KI aufmöbeln zu lassen (vgl. oben und unten).

Dazu schrieb ich am 14.11.2022: Das letzte Foto aus der Ruinenstadt Uxmal in Mexiko, am 17.10.1979. Ich habe lange gesucht, um ein ähnliches Foto zu finden, aber vergeblich. Es hat sich nicht viel geändert. Die Ruine gehört zum Nunnery Quadrangle (Cuadrangulo De Las Monjas).

Unter Exorzisten

Die bürgerliche Hauptstadtpresse berichtet: *Gleich 32 Autoren, die ihre Bücher bislang im Westend Verlag veröffentlicht haben, verkünden in einem offenen Brief an die Geschäftsführung des in Frankfurt ansässigen Verlags, dass sie diesen verlassen werden. „Wir distanzieren uns hiermit von der Neuausrichtung Ihres Verlagsprogramms." (…)*

Mit der „Neuausrichtung" ist gemeint, dass der Verlag, der sich bislang „ausdrücklich als Plattform für kritische, linke Perspektiven auf gesellschaftliche Entwicklungen" verstanden hat, wie es bis vor kurzem auf der Verlagsseite stand, nun auch Bücher von Autoren wie Wolfgang Kubicki und Ulf Poschardt verlege, mithin sich rechten Positionen öffne.

Die haben doch nicht mehr alle Tassen im Schrank. Die gefühlt „linken" Damen und Herrn Autoren sind noch nicht einmal mehr in der Lage, jemanden in ihrer virtuellen Nähe zu dulden, der nicht ihrer stromlinienförmigen Meinung entspricht, ohne ein exorzistisches Reinigungsritual zu zelebrieren.