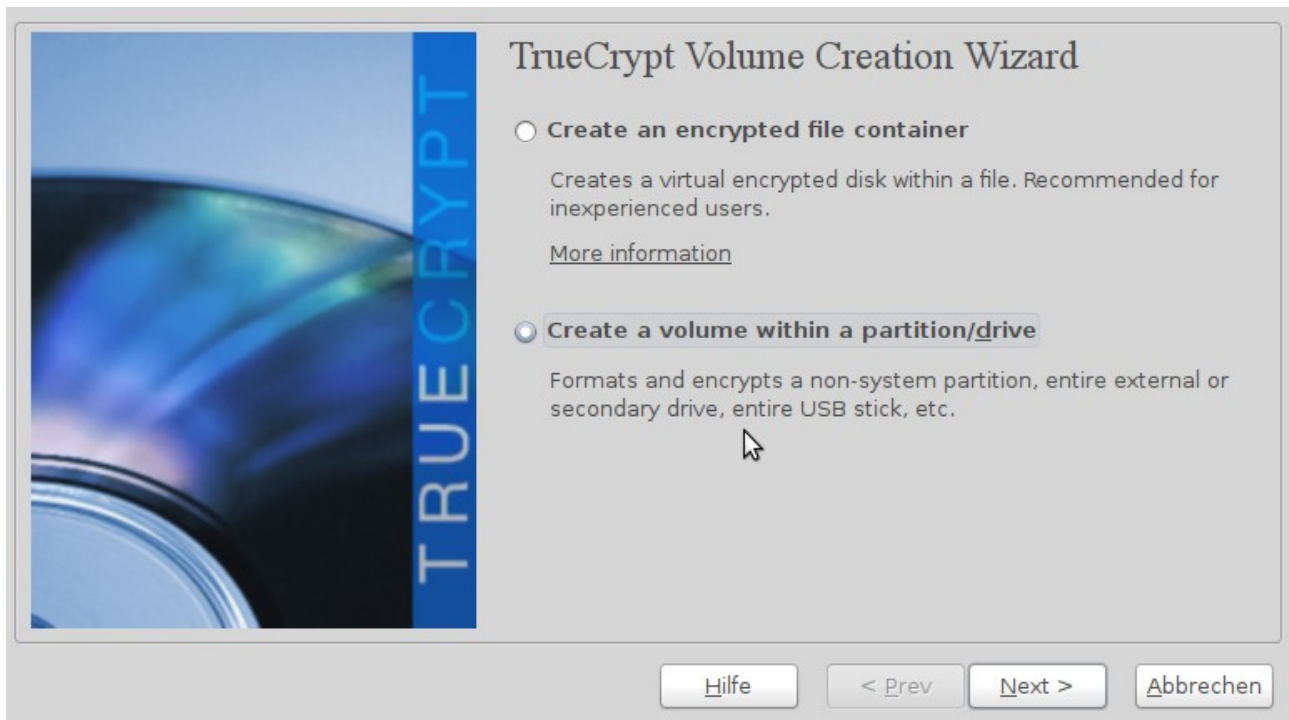


## Trügerische Sicherheit durch Verschlüsselung

Oftmals taucht der Wunsch nach verschlüsselten Daten und Devices auf, so dass viele Anwender zur beliebten Software „Truecrypt“ greifen.

Truecrypt ist für verschiedenen Betriebssysteme erhältlich und ist Open Source.

Unterschiedliche Möglichkeiten der Verschlüsselung werden angeboten und man kann ganze Festplatten, USB Sticks oder auch Teilbereiche in Kontainer verschlüsseln.



Im Szenario wurde dazu ein USB Stick verwendet, mit dem bereits Daten transportiert wurden, verschlüsselt oder unverschlüsselt. Die Daten, die sich auf dem Stick befanden, wurden nach dem Transport gelöscht, um Speicherplatz wieder frei zu geben. Das hier eine echte Löschung nicht statt findet, dürfte vielen noch klar sein. Also lassen sich die Daten mittels forensische Hilfsmittel wieder herstellen.

Jetzt wurde der USB Stick mit Truecrypt „Quick Format“ neu formatiert und mit einem frischen Passwort versehen. Hierbei ist es besonders wichtig zu wissen, dass *nicht* alle Daten überschrieben werden und die Verschlüsselung somit noch nicht vollkommen greift. Daten die dort vorher auf dem jetzt neu verschlüsselten Device waren, sind unter forensischen Aspekten wieder herstellbar.

Dies führt zu einer trügerischen Sicherheit, denn selbst in einem verschlüsselten Device sind gelöschte Daten, die nicht explizit überschrieben wurden, wieder herstellbar.

Im Szenario wurde anschließend getestet, wie sich das Device unter forensischen Gesichtspunkten verhält, nachdem mittels Truecrypt eine vollständige Formatierung und neue Verschlüsselung durchgeführt wurde.

Fast alle Datenblöcke sind überschrieben worden, jedoch *nicht* alle!

