
LABORATORIJSKA VEŽBA BR. 8

Operativni sistemi

CILJ VEŽBE

- Upoznavanje sa porogramskim paketom Truecrypt
- Izrada standardnog volumena
- Aktiviranje i deaktiviranje volumena
- Zaštita datoteka putem ključ datoteke
- Primena skrivenih volumena

POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom
- Istalirani programski paket Truecrypt

TEORIJSKE OSNOVE

Programski paket Truecrypt

Truecrypt je besplatan program otvorenog koda koji korisnicima nudi funkcionalnost čuvanja podataka na šifrovanim sistemima datoteka. Korisnicima su na raspolaganju sledeći simetrični algoritmi: Blowfish, Twofish, AES, CAST5, Serpent i Triple DES, kao i međusobne kombinacije funkcija šifrovanja (npr. AES-Twofish, AES-Blowfish-Serpent i njima slične).

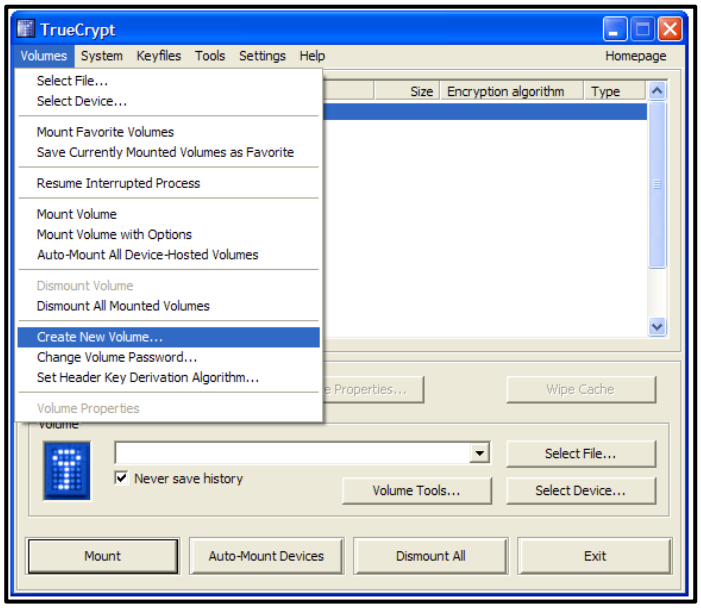
Program Truecrypt možete besplatno preuzeti sa adrese https://truecrypt.en.lo4d.com/windows.
Šifrovani sistemi datoteka mogu se generisati kao volumeni smešteni u nekoj datoteci na postojećem sistemu datoteka ili kao zasebne particije na disku. U oba slučaja, kripto sistem datoteka se aktivira preko logičkih diskova. TrueCrypt omogućava i izradu skrivenih volumena, o kojima će kasnije biti više reči. Podaci se štite lozinkom, **ključ-datotekom** (*keyfile*) ili kombinacijom lozinke sa ključ-datotekom.
Za sada nije dokazano da je u TrueCrypt ugrađena klopka; takođe, program ne priznaje nikakve autoritete koji mogu nasilno dešifrovati vaše podatke niti ostavlja mogućnost administratoru sistema da to uradi – ključ-datoteke se ne distribuiraju u profil korisnika niti na bilo koje drugo mesto, a program je prilično oprezan po pitanju čuvanja lozinki i ključ-datoteka u radnoj memoriji. Korisnik može definisati kombinaciju tastera koja će izazvati deaktiviranje svih šifrovanih sistema datoteka (po potrebi i nasilno) i brisanje memorijskog keša za skladištenje ključeva i lozinki.

Ispitivanje performansi algoritama

Pre nego što generišete neki kripto sistem datoteka, poželjno je da ispitate performanse algoritama. Odaberite **Tools → Benchmark** iz glavnog menija programa i odaberite veličinu bafera (na primer, 50 ili 100 MB). Test se odvija u radnoj memoriji računara i, u zavisnosti od veličine bafera, traje od nekoliko sekundi do nekoliko minuta. Na test računaru, algoritmi Blowfish i Twofish pokazali su se kao najbrži. Ovaj test ne sme da bude jedini kriterijum za izbor algoritma (iako na osnovu njega definitivno možete zaključiti da nije preporučljivo izabrati Triple DES). Međutim, ukoliko se dvoumite između nekoliko algoritma kojima verujete, odaberite brži. Ovo može da bude jako korisno ukoliko imate volumen velikog kapaciteta šifrovan u režimu ulančavanja.

Izrada standardnog volumena

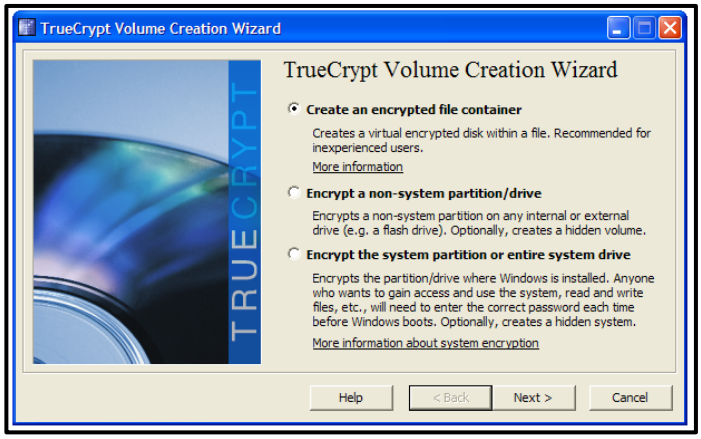
Postupak izrade standardnog volumena u datoteci koji će biti zaštićen lozinkom je jednostavan. Odaberite **Volumes → Create New Volume** iz glavnog menija programa i pratite šta *Volume Creation wizard* traži od vas. Napomena: datoteke kontejneri ne moraju imati nastavak *.tc*, osim ako želite da se volumen poveže sa programom TrueCrypt na nivou Windows Explorera. TrueCrypt će na osnovu podataka koje ste uneli napraviti prazan šifrovani volumen koji kasnije možete aktivirati preko logičkih diskova.



ZADATAK 1.

Kreirajte standardni Truecrypt volumen zaštićen lozinkom.

Odaberite iz padajućeg menija **Volumes → Create New Volume** kao što je prikazano na slici**.**



Otvara se TrueCrypt Volume Creation Wizard.

Odaberite **Create an encrypted file container**, klik na **Next**.

Odaberite Standard TrueCrypt volume, kliknite na **Next**.

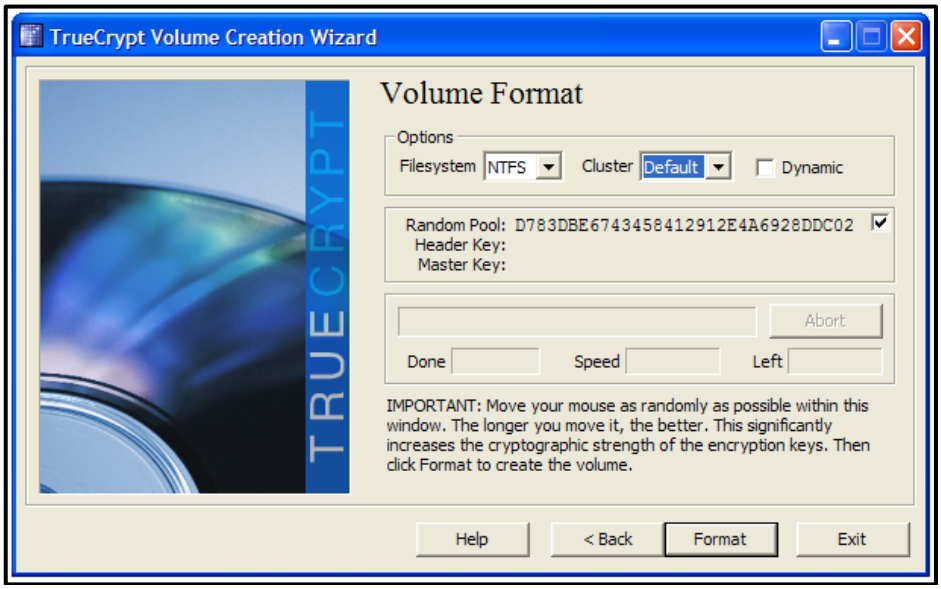
Program pita gde zelite da smestite kontejner. Upisite c:\disk1.tc. Klik na Next.

Odaberite algoritam za šifrovanje Twofish, za hash RIPEMD-160. Klik na Next.

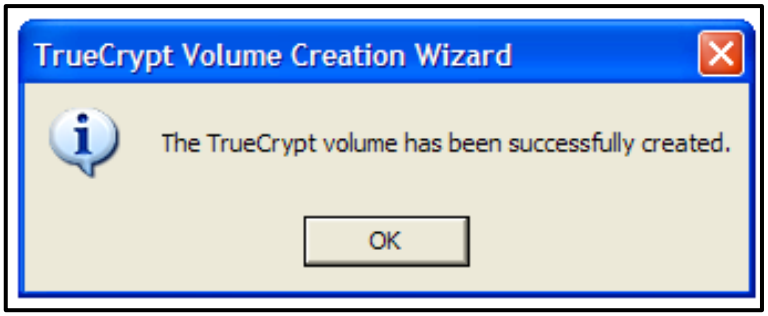
Unesite veličinu diska (volume size). Upišite 10 i odaberite MB. Klik na Next.

Unesite lozinku 123456 (na osnovu nje će se generisati ključ za šifrovanje) u polje Password i potvrdite je u polju Confirm (pogledajte sledeću sliku).

Klik na **Next**. Program vas upozorava da je lozinka kratka i traži da potvrdite da želite da je koristite. Klik na **Yes** potvrdićemo lozinku.
Na sledećem ekranu birate fajl sistem koji će biti kreiran u okviru šifrovanog volumena. Ukoliko radite samo sa Windows OS, birajte NTFS. U suprotnom, odaberite FAT (jednostavnije je na FAT FS izvesti upis ukoliko aktivirate volume na Linux-u). U ovom slučaju odaberite Filesystem: NTFS. Veličinu klastera (Cluster) ostavite kao podrazumevanu vrednost (default).
Dobijate obaveštenje da je volumen uspešno kreiran. Klik na **OK**. Klik na **Format**.



Klik na **Exit** u "TrueCrypt Volume Creation Wizard" prozoru.



Dijalog vam javlja da je volumen kreiran i spreman za rad.

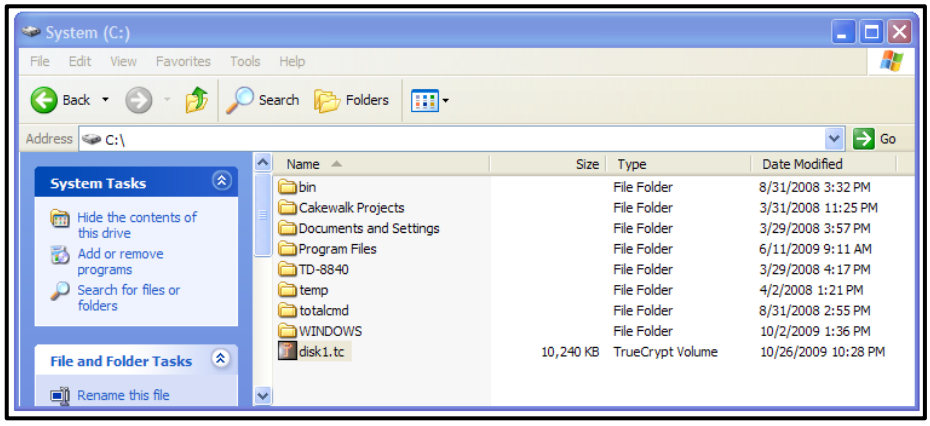
Aktiviranje i deaktiviranje volumena

Pokretanjem datoteke sa nastavkom .tc u Windows Exploreru, otvara se TrueCrypt dijalog za aktiviranje volumena. Šifrovani sistem datoteka aktivira se preko slovne oznake logičkog diska koju vi birate. Od vas se zahteva da unesete lozinku kojom je sistem datoteka zaštićen. Alternativno, volumen možete aktivirati iz TrueCrypt glavnog prozora, pozivanjem opcije **Volumes → Mount Volume** i unošenjem imena datotekea u kojoj se nalazi volumen.

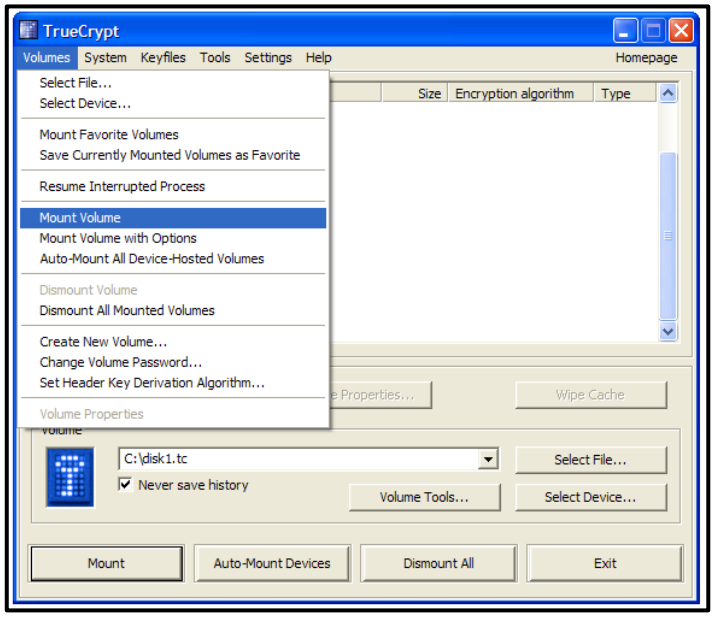
Nakon toga, volumenu pristupate kao lokalnom disku. Volumeni se deaktiviraju iz TrueCrypt glavnog prozora, pomoću opcije **Volumes → Dismount Volume** ili **Volumes → Dismount All Mounted Volumes** (ukoliko želite da deaktivirate sve šifrovane sisteme datoteka). Volumeni se mogu deaktivirati i odgovarajućom kombinacijom tastera, ukoliko je aktivna System Tray ikonica TrueCrypt koja omogućava izvršenje TrueCrypt procesa u pozadini. Ova opcija može biti veoma zgodna, pa se korisnicima preporučuje da ne isključuju ovaj proces. Kombinacije tastera za deaktiviranje i nasilno deaktiviranje definiše sam korisnik.

ZADATAK 2.

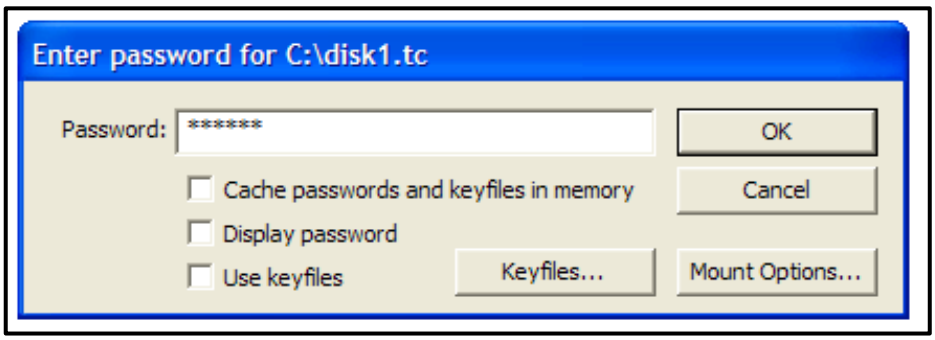
Aktivirajte volumen koji ste malopre kreirali. Pristupite mu i iskopirajte na njega neku datoteku. Odaberite u exploreru fajl c:\disk1.tc i uradite dvoklik na taj fajl. Otvoriće se TrueCrypt prozor. Alternativno, otvorite sami TrueCrypt, pa u delu Volume odaberite **Select file** i pronađite na disku c:\disk1.tc ili jednostavno upišite putanju i ime fajla.



Odaberite neki slobodan logički drajv, na primer K:
Iz menija birajte **Volume -> Mount Volume** ili na dnu prozorčića kliknite na dugme **Mount**.



Pojaviće se prozor "Enter password for C:\disk1.tc".
U polje password upisite lozinku koju ste malopre uneli (123456) i kliknite na OK.



Volumen je sad aktiviran i možete mu pristupiti preko logičkog diska K:
Otvorite disk K: iz explorera i iskopirajte na njega neki fajl.
Volumen deaktivirate tako što otvorite TrueCrypt, odaberete disk K: (drajv preko kog se pristupa aktiviranom volumenu) i sa dna prozora kliknete na **Dismount** (ili iz menija izaberete **Volumes -> Dismount Volume**). Deaktivirajte volumen.

Ključ-datoteke

Ključ-datoteka (*keyfile*) jeste datoteka čiji se sadržaj pomoću specijalnog algoritma "kombinuje" sa lozinkom i na taj način obezbeđuje viši nivo zaštite volumena. Korisnik ne može aktivirati šifrovani volumen zaštićen ključ datotekom ukoliko tu datoteku ne poseduje. U programu se ne insistira na korišćenju ovakve zaštite, ali su u zvaničnom uputstvu navedene prednosti koje ona donosi:

- obezbeđuje zaštitu od programa za krađu lozinki (engl. *keyloggers*) koji skriveno prate šta ste otkucali na tastaturi i to beleže u neku datoteku ili šalju preko Interneta napadaču. Napadač koji otkrije vašu lozinku, neće moći da aktivira volumen jer nema ključ-datoteku;
- povećava kvalitet lozinke, tj. njenu dužinu i složenost, a samim tim i otpornost na napade grubom slilom.

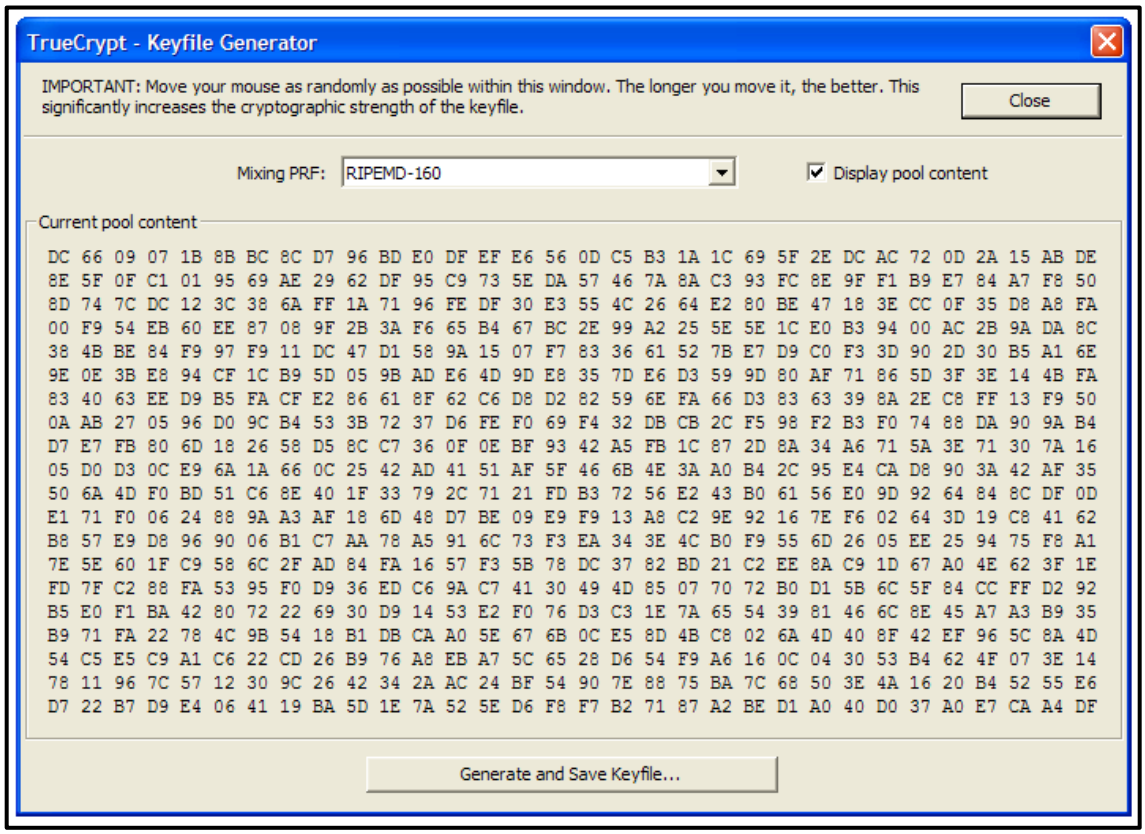
Volumen se može zaštititi jednom datotekom ili većim brojem datoteka. Ukoliko se volumen štiti većim brojem ključ-datoteka, one se mogu redistribuirati većem broju korisnika – u tom slučaju se volumen može aktivirati samo ako svi korisnici istovremeno prilože svoje ključ-datoteke. Prednost ovog načina zaštite jeste smanjenje uticaja ljudskog faktora na redukciju sigurnosti (npr. eliminiše se mogućnost podmićivanja jedne osobe radi ostvarivanja pristupa).
Svaki tip datoteke može se koristiti kao ključ. U zvaničnom uputstvu se preporučuje korišćenje komprimovanih datoteka ili datoteka sa čitljivim, tj. razumljivim sadržajem (.mp3, .jpg, .avi, .zip* i njima slične). TrueCrypt ne modifikuje sadržaje ovakvih datoteka, što znači da korisnik u nekom direktorijumu sa oko 500 mp3 datoteka može čuvati i nekoliko ključeva. Analizom ovih datoteka ne može se utvrditi da li se one koriste kao ključevi ili ne; dodatno, napadač koji po inerciji pretražuje skrivena mesta (npr. profil, USB fleš disk i slično) najverovatnije neće pretpostaviti da je ključ mp3 datoteka.
Navodimo i dve važne napomene vezane za ključ-datoteke:

- Ukoliko se volumen štiti ključ-datotekom, program ne insistira na korišćenju lozinke. Međutim, korišćenje lozinke sa ključ-datotekom obezbeđuje vrlo visok nivo zaštite volumena.
- Poželjno je da ukupna veličina svih datoteka kojima se štiti volumen bude veća od 20 bajtova kako bi se sprečila mogućnost napada grubom silom. Ovo je naročito značajno ukoliko se volumen štiti samo ključ-datotekom, bez lozinke.
- Pazite da ne izgubite ključ-datoteku. Ukoliko je izgubite, podaci na šifrovanom volumenu koji je njome zaštićen biće nedostupni.

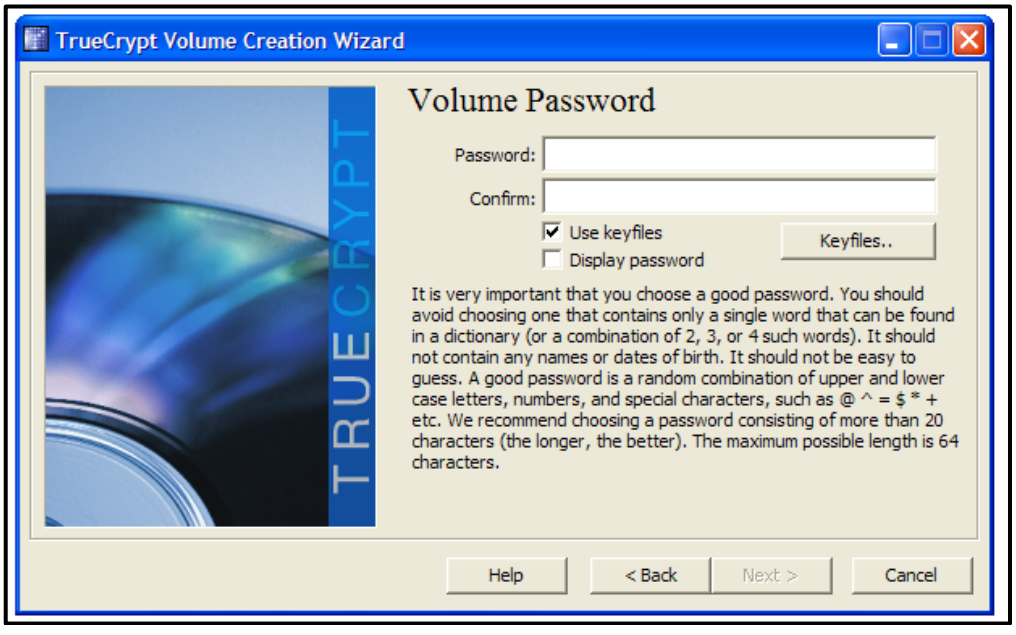
ZADATAK 3.

Kreirajte prvo ključ datoteku a zatim standardni volumen zaštićen datotekom.
Iz padajućeg menija birate **Tools → Keyfile** generator.

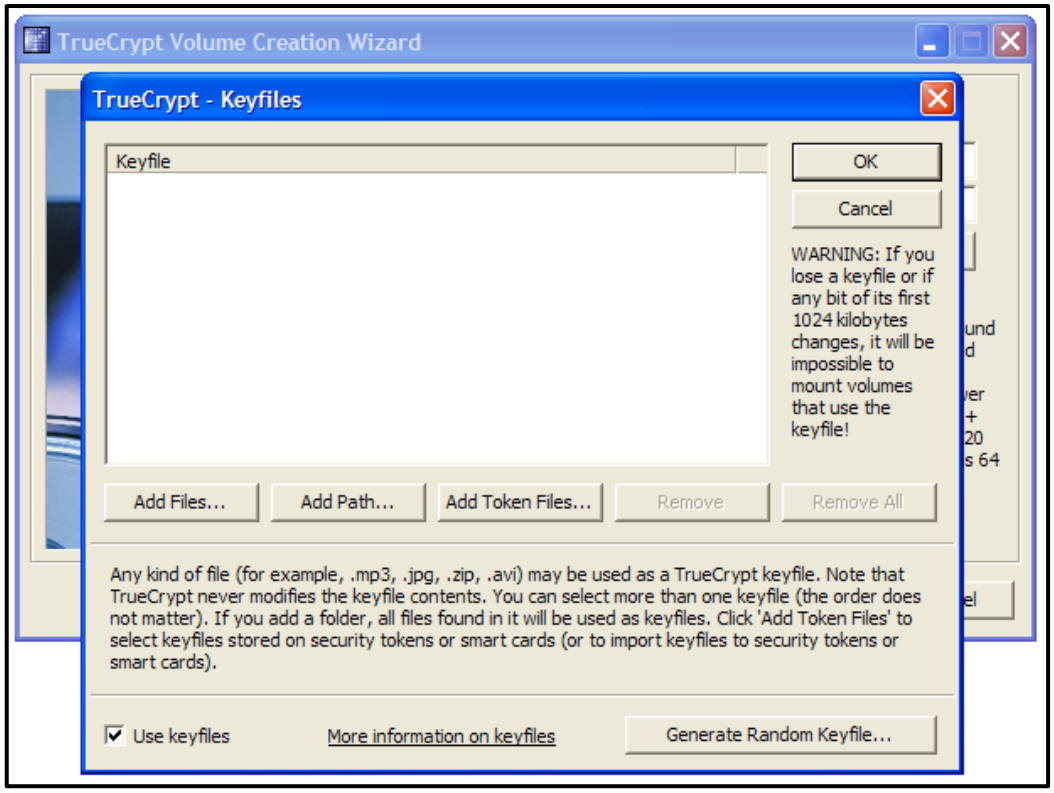
Napravite malo slučajnosti mišem – promrdajte ga malo levo desno.



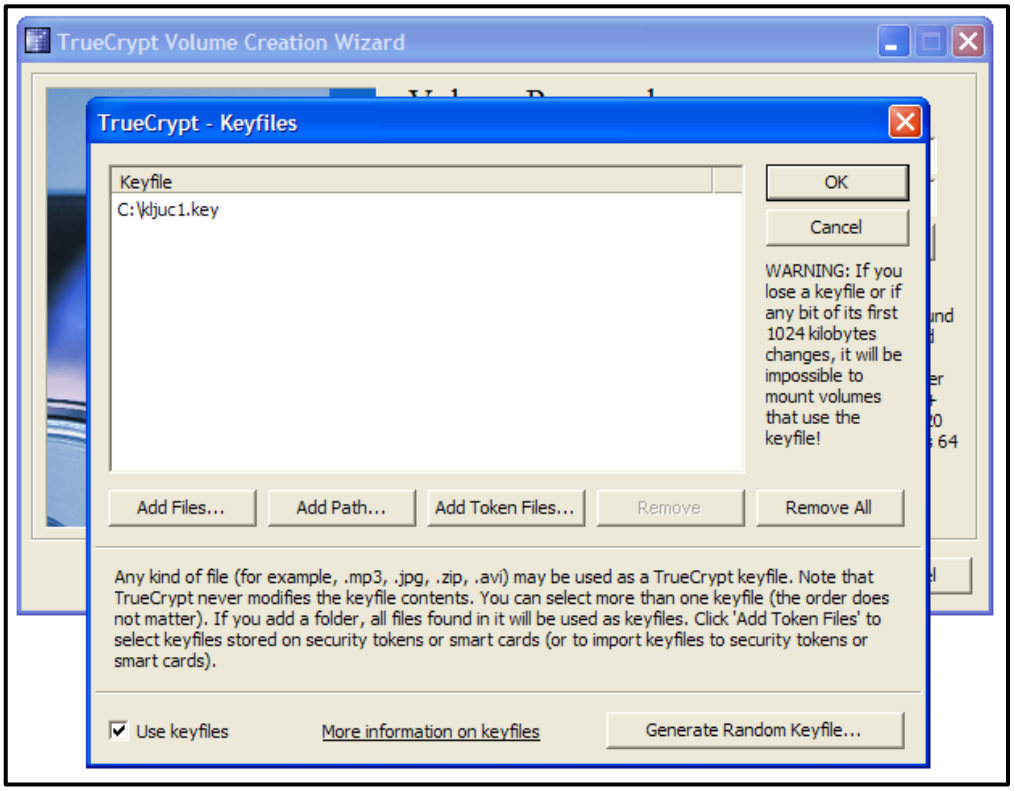
Kilk na **Generate and Save Keyfile**. Snimite ključ kao C:\ljuc1.key. Klik na **Close**.
Slično kao i u prvom primeru kreiranja volumena kreirajte novi kontejner. Birajte iz menija **Volumes → Create New Volume**. Otvara se TrueCrypt Volume Creation Wizard. Odaberite **Create an encrypted file container**, klik na **Next**. Odaberite Standard TrueCrypt volume, klik na **Next**. Program pita gde želite da smestite kontejner. Upišite c:\disk2.tc. Klik na **Next**. Odaberite algoritam za šifrovanje Twofish i za hash RIPEMD-160. Klik na **Next**. Unesite veličinu diska (volume size). Upišite 10 i odaberite MB. Klik na **Next**.
Sada umesto lozinke navodite da želite da volumen zaštitite ključ datotekom. Štiklirajte opciju Use Keyfiles kao na sledećoj slici.



Kliknite na dugme **Keyfiles**. Otvoriće se prozor "TrueCrypt - Keyfiles".



Klik na **Add Files**. Pronađite i odaberite fajl c:\kljuc1.key koji ste prethodno generisali.
U prozoru TrueCrypt - Keyfiles kilikite na **OK**.



Klik na **Next**.
Odaberite Filesystem: NTFS. Veličinu klastera (Cluster) ostavite kao podrazumevanu vrednost (default).
Klik na **Format**. Dobijate obaveštenje da je volumen uspešno kreiran. Kliknite na **OK** na prozoru za obaveštenje.
Klik na **Exit** u "TrueCrypt Volume Creation Wizard" prozoru. Aktivirajte sad ovaj volumen.
Odaberite u exploreru fajl c:\disk2.tc i uradite dvoklik na taj fajl. Otvoriće se TrueCrypt prozor.

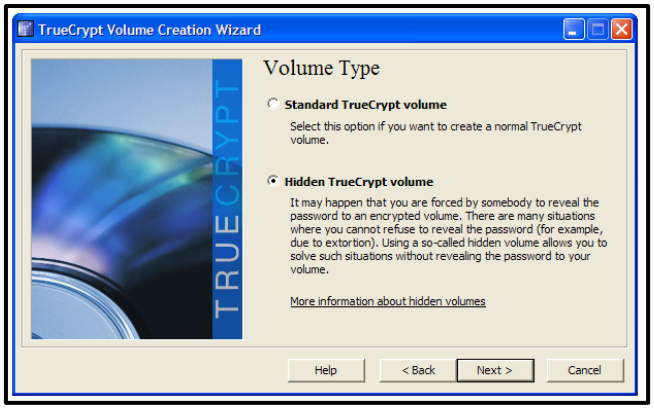
Odaberite neki slobodan logički drajv, na primer K:. Iz menija birajte **Volume -> Mount Volume** ili na dnu prozorčića kliknite na dugme **Mount**. Pojavice se prozor "Enter password for C:\disk2.tc".
Umesto lozike naznačite programu da je volumen zašticen ključ datotekom. Kliknite na dugme **Keyfiles**. Otvoriće se prozor "TrueCrypt - Keyfiles". Kao i malopre, klik na **Add Files**. Pronađite i odaberite fajl c:\ljuc1.key kojim je volumen zaštićen. Posedovanje ovog fajla je slično kao da znate lozinku kojom je volumen ili neki šifrat zaštićen. Doduše ovde govorimo o zaštiti informacije pomoću nečega što imate a ne nečega što znate, kao što je lozinka. Međutim, za sada prihvatite to kao nešto jako slično poznavanju lozinke.
U prozoru "TrueCrypt - Keyfiles" kilikite na **OK**. U prozoru "Enter password for C:\disk2.tc" kliknite na **OK**. Volumen je sad aktiviran i možete mu pristupiti preko logickog diska K:. Otvorite disk K: iz explorera i iskopirajte na njega neki fajl. Deaktivirajte volumen.

Skriveni volumeni

Postoji nekoliko tipova kriptoanalitičkih napada. Jedan od efikasnijih napada je napad potkupljivanjem, ucenom, krađom i sličnim aktivnostima (tzv "*rubberhose*"). Postoje situacije u kojima ne možete odbiti da napadaču predate ključ ili lozinku (ne možete reći ne simpatičnom čovečuljku sa pištoljem, zar ne?).
Korišćenje skrivenih volumena jedan je od načina kojim se možete odbraniti od ovakvih napada.

U okviru praznog prostora spoljašnjeg volumena, koji se prilikom izrade popunjava pseudoslučajnim podacima, TrueCrypt generiše skriveni, unutrašnji volumen (engl. *hidden volume*). Deo praznog prostora u kom je napravljen skriveni volumen ne razlikuje se ni po čemu od ostatka praznog prostora. Čak i ako aktivirate spoljašnji volumen, nemoguće je dokazati postojanje unutrašnjeg volumena. Preporučuje se da na spoljašnji volumen iskopirate neke podatke koji će napadaču stvoriti iluziju pravog sadržaja čije je otkrivanje cilj njegovog napada. U većini slučajeva dovoljno je da u spoljašnji volumen iskopirate datoteku sa lažnim lozinkama i nekoliko bezvrednih dokumenata ili slika koje, navodno, želite da sakrijete, ali čije otkrivanje ne sme imati nikakve posledice. Ovi dokumenti će biti dostupni svakome ko vas primora da mu predate lozinku i/ili ključ-datoteku.
Poverljive datoteke čuvaju se na skrivenom volumenu, čijeg postojanja napadač nije svestan. Lozinka skrivenog volumena mora se razlikovati od lozinke spoljašnjeg volumena koji služi kao maska za prevaru napadača. Skriveni volumen se aktivira slično spoljašnjem – pri tome, program aktivira volumen za koji navedete lozinku. TrueCrypt će najpre pokušati da dešifruje zaglavlje spoljašnjeg volumena. Ukoliko u tome uspe, tj. ako ste naveli lozinku kojom je zaštićen spoljašnji volumen, biće vam dostupni podaci koji nisu osetljivi. Ukoliko je dešifrovanje zaglavlja spoljašnjeg volumena neuspešno, tj. ako je uneta pogrešna lozinka, TrueCrypt će pokušati da dešifruje zaglavlje skrivenog volumena (obično se nalazi u trećem bloku s kraja spoljašnjeg volumena). Ako u tome uspe, tj. ukoliko ste naveli lozinku kojom je zaštićen skriveni volumen, biće vam dostupni pravi podaci.

ZADATAK 4.



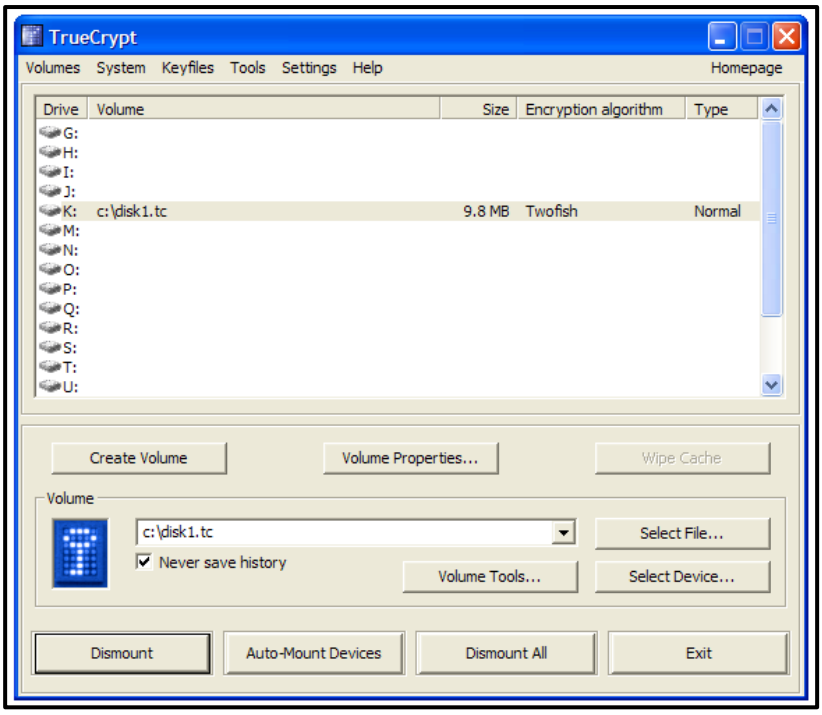
U standardnom volumenu iz prvog primera koji je zaštićen lozinkom 123456 kreirajte skriveni volumen koji će biti zaštićen kombinacijom iste lozinke i ključ datoteke generisane u drugom primeru.

Postupak:

Koristimo spoljašnji kontejner c:\disk1.tc u koji je već smeštena neka datoteka.

Birajte iz menija **Volumes -> Create New Volume**. Otvara se TrueCrypt Volume Creation Wizard.

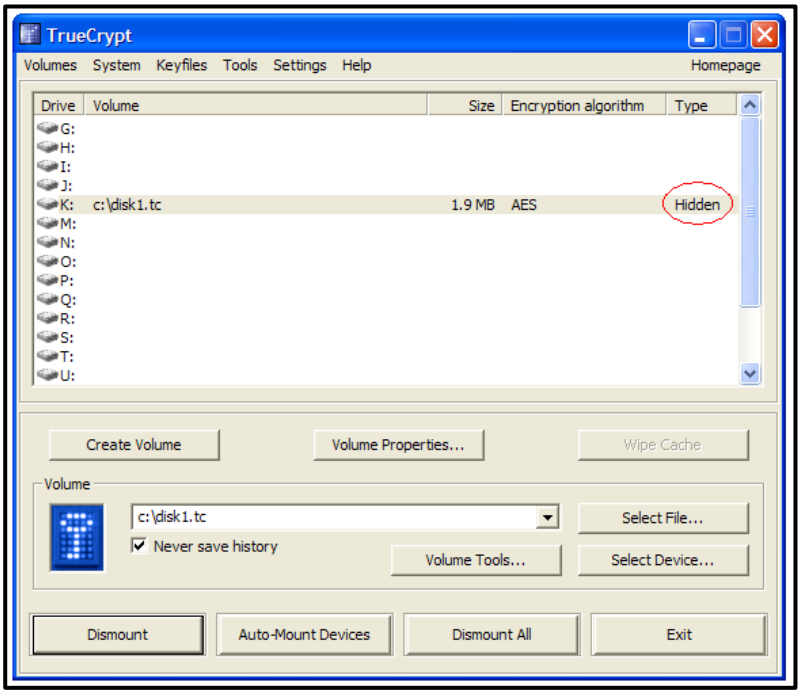
Odaberite **Create an encrypted file container**, klik na **Next**. Odaberite **Hidden TrueCrypt volume**, klik na **Next.**



Odaberite **Direct mode** jer kreirate novi volumen u postojećem. Klik na **Next**. Program pita za lokaciju spoljašnjeg volumena. Upišite c:\disk1.tc. Klik na **Next**. Program dalje pita za lozinku za spoljašnji volumen (Outter Volume Password). Unesite 123456 i kliknite na **Next**. Program upozorava da je FAT fajl sistem bolji u spoljašnjem volumenu ukoliko želite da pravite i skriveni (manje otpada na FS *overhead*). Nadalje se postupak svodi na kreiranje skrivenog volumena. Kliknite na **Next**.

Odaberite algoritam za šifrovanje (npr AES) i heš (npr RIPEMD-160). Klik na **Next**. Zadajte veličinu volumena 2MB i kliknite na **Next**. Zaštitite spoljašnji volumen istom lozinkom 123456 i ključem c:\kljuc1.key. Unesite lozinku 123456 u polja Password i Confirm. Štiklirajte **Use Keyfiles**. Kliknite na dugme **Keyfiles**. Otvoriće se prozor "TrueCrypt - Keyfiles".

Kao i malopre, klik na **Add Files**. Odaberite fajl c:\kljuc1.key kojim je volumen zaštićen. U prozoru "TrueCrypt - Keyfiles" kilikite na **OK**. Kliknite na **Next** u Wizardu i opet ćete dobiti upozorenje da je lozinka kratka. Sada ga ignorišite, ali ako šifrujete nešto bitno, nemojte ga ignorisati. Dakle, sada može klik na **Yes** kako bi potvrdili lozinku. Za fajl sistem sada morate odabrati FAT. Veličinu klastera ostavite na podrazumevanu vrednost (default). Klik na **Format** pa na **Exit**.



Aktivirajte spoljasnji volumen lozinkom 123456. Koji se fajl(ovi) nalaze na njemu?

Aktivirajte unutrašnji volumen lozinkom 123456 i ključem c:\kljuc1.key. Da li na njemu postoje isti fajlovi kao i na spoljašnjem?