CARNET

Šifriranje diska

NCERT-PUBDOC-2018-1-351

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

U današnje vrijeme svjedoci smo sve većeg broja sigurnosnih incidenata koji rezultiraju krađom povjerljivih podataka i koji nanose značajnu financijsku štetu žrtvama. Osim izravnih udaljenih napada preko mreže, vrlo često do gubitka podataka može doći i jednostavnom krađom prijenosnih računala koja sadrže povjerljive podatke ili sadrže podatke koji se mogu iskoristiti za olakšavanje daljnjih napada na glavnu infrastrukturu organizacije. Svojim prodorom u sve sfere ljudskog života računala su postala nužna i izvan radnog mjesta, a svojom rastućom prenosivošću omogućila su da ih uvijek imamo uza sebe. Posljedica ovoga je uvelike povećana opasnost od gubitka računala i na njima pohranjenih podataka. Šteta nastala gubitkom podataka često može višestruko nadilaziti vrijednost samog računala, a u slučaju odgovornih osoba velikih poduzeća ili zaposlenika u vladinim agencijama, krađa podataka može biti i glavni razlog krađe računala.

Postojeće metode i alati za sprječavanje neovlaštenog udaljenog pristupa računalu, iako učinkovite u borbi protiv hakerskih napada, u ovakvim su slučajevima potpuno neučinkovite. Fizičko posjedovanje računala napadaču omogućava lako zaobilaženje svih zaštita te vađenjem tvrdog diska i zatim njegovim umetanjem u računalo pod svojom kontrolom jednostavno postiže cilj. Više nije dovoljno samo spriječiti pristup i čitanje s medija za pohranu već treba onemogućiti da napadač čitanjem dođe do podataka u upotrebljivom obliku. To se postiže šifriranjem podataka.

Osim kao mjera zaštite podataka u slučaju krađe računala, šifriranje diska mogu zahtijevati i propisi koji reguliraju načine pohrane i zaštite poslovnih, povjerljivih, tajnih ili osobnih podataka krajnjih korisnika koji se čuvaju i obrađuju unutar neke organizacije. Jednako tako, šifriranje podataka koristi se kao mjera umanjivanja štete i odgovornosti u slučajevima krađe podataka neovlaštenim udaljenim pristupom jer se gubitak šifriranih podataka smatra manjim sigurnosnim incidentom.

1.1 Što je šifriranje diska?

Šifrirati se mogu datoteke i poruke, a i cijeli medij, na primjer disk. Šifriranje diska je tehnika kojom se cijeli disk ili njegovi dijelovi šifriraju kriptografskim algoritmom, čime se onemogućava čitanje podataka bez poznavanja tajnog ključa. Za razliku od šifriranja pojedinačnih datoteka, šifriranjem cijelog diska u potpunosti se štite svi korisnički podaci, uključujući i metapodatke. Na taj se način izbjegava opasnost da korisnik nepažnjom zaboravi zaštititi neke osjetljive podatke ili da napadač pristupi povjerljivim podacima kojih korisnik nije niti bio svjestan, kao što su npr. pohranjene lozinke Web preglednika, privremene datoteke ili spremnici, dnevnici rada i sl.

Kako bi se omogućio nesmetani rad sustava i pokretanje operacijskog sustava računala sa šifriranog diska, potrebno je ili koristiti odvojeni disk za pokretanje operacijskog sustava ili ostaviti jedan mali dio diska nešifriranim kako bi se s njega mogao pokrenuti alat za unos korisničke lozinke i otključavanje ostatka diska. Svi ostali podaci na disku zaštićuju se kriptografskim ključem.

2 Tehnička pozadina šifriranja diska

Jednostavan pristup šifriranju diska odvijao bi se na sljedeći način:

- Korisnik odabere lozinku za šifriranje
- Cijeli disk se šifrira koristeći tu lozinku izravno kao ključ

No u stvarnosti, kako bi šifriranje diska bilo sigurno i praktično, postupak je znatno složeniji.

Kada bi se cijeli disk šifrirao u komadu, primjerice kao što se datoteke obično šifriraju, tada bi se on morao kod korištenja u cijelosti i dešifrirati. Zbog veličine diska to je u pravilu nepraktično – potpuno dešifriranje današnjih diskova čija se veličina mjeri u terabajtima bi trajalo satima, ako ne i više.

Zato se prilikom šifriranja diska on prvo dijeli na blokove pa se svaki blok zasebno šifrira. Na taj je način moguće brzo dešifrirati individualne blokove i držati njihov sadržaj u radnoj memoriji, bez potrebe da se dešifrira cijeli disk. To zapravo odgovara i uobičajenom korištenju diska – računalo prilikom korištenja ne čita njegov sadržaj u cijelosti, već čita pojedinačne blokove koji mu u tom trenutku trebaju.

Uz to, u pravilu se lozinka koju korisnik upisuje ne koristi izravno kao ključ. Uobičajeni postupak je zapravo sljedeći:

- Ključ za šifriranje diska nasumično se generira.
    - U konačnici se sastoji od 128 ili više nasumičnih bitova.
    - On se naziva **ključem za šifriranje podataka** (eng. *data encryption key* – **DEK**).
- Disk se šifrira tim ključem za šifriranje podataka (DEK).
- Sada bi korisnik morao zapamtiti taj dugački nasumični ključ što bi bilo vrlo neupotrebljivo u praksi. Najbolje je taj ključ zapisati na sam medij koji se njime šifrira, na dogovoreno mjesto. Međutim, tada bi napadač mogao iskoristiti ključ.
- Zbog toga se ključ prije zapisivanja šifrira.
    - Za to šifriranje koristi se **ključ za šifriranje ključa** (eng. *key encryption key* – **KEK**).
- Taj se ključ dobiva iz lozinke koja je puno kraća i koju sam korisnik izabere tako da ju može lagano zapamtiti.
- Lozinka koju korisnik upiše koristi se kao ulazni podatak za funkciju izvođenja ključa (eng. *key derivation function*).
    - Ta funkcija obavlja tzv. rastezanje ključa (eng. *key stretching*).
    - Izlaz funkcije je ključ (KEK) od 128 ili više bitova.

- Ključ za šifriranje podataka (DEK) se šifrira ključem za šifriranje ključa (KEK) i zapisuje na početak diska.

Kako bi korisnik mogao koristiti disk, prilikom pokretanja računala odvija se sljedeći postupak (tzv. otključavanje diska):

1. Korisnik upisuje lozinku.
2. Lozinka se ubacuje u funkciju izvođenja ključa i generira se ključ za šifriranje ključa (KEK).
3. Pomoću tog generiranog ključa dešifrira se zapisani ključ za šifriranje podataka (DEK).
4. Ključ za šifriranje podataka (DEK) ostaje u radnoj memoriji računala do njegovog gašenja i koristi se za dešifriranje podataka na disku.

Složenost ovog postupka opravdava njegova postignuća. Kao prvo, korištenje ključa za šifriranje podataka (DEK) koji ne ovisi nikako o lozinki omogućava lako mijenjanje lozinke te korištenje različite lozinke za svakog korisnika.

Ako korisnik odluči promijeniti lozinku, nije potrebno dešifrirati i ispočetka šifrirati cijeli disk novim ključem, već je dovoljno šifrirati ključ za šifriranje podataka (DEK) ključem za šifriranje ključa (KEK) izvedenim iz nove lozinke i zapisati ga na početak diska.

Ako računalo koristi više korisnika, svaki od njih može koristiti vlastitu lozinku te posredno i vlastiti ključ za šifriranje ključa (KEK). I dalje postoji samo jedan ključ za šifriranje podataka (DEK) s kojim je šifriran disk. Kada postoji više korisnika, potrebno je šifrirati taj ključ za šifriranje podataka (DEK) sa svakim od ključeva za šifriranje ključa (KEK) i rezultat tih šifriranja zapisati na početak diska. Kada korisnik upiše svoju lozinku, program pokuša dešifrirati svaki od tih zapisa dok ne uspije, tj. dok ne naiđe na upravo onaj zapis koji je šifriran ključem za šifriranje ključa (KEK) od tog korisnika.

Kao drugo, najslabija karika u lancu sigurnosti šifriranja diska često je lozinka koju je korisnik odabrao. Korisnici često biraju loše, predvidljive lozinke tako da je u pravilu najlakši način za dešifriranje diska napad višestrukim pokušavanjem (eng. *brute force*) dešifriranja nizom potencijalnih lozinki. Taj napad nije moguće u potpunosti spriječiti – ako korisnik odabere lozinku koju je dovoljno lako pogoditi, napadač će uvijek moći doći do podataka. No tu vrstu napada moguće je usporiti tako da uspješan napad traje primjerice pet godina umjesto pet dana.

Ključ je usporavanja tih napada prethodno spomenuta funkcija izvođenja ključa (eng. *key derivation function*) koja obavlja tzv. rastezanje ključa (eng. *key stretching*). Pojednostavljeno objašnjenje te funkcije je sljedeće:

- Funkcija kao ulaz prima korisnikovu lozinku
- Zatim, nad njom računa velik broj (npr. milijun) iteracija neke kriptografske funkcije računanja sažetka (eng. *cryptographic hash function*)

- I konačno, kao izlaz vraća rezultat te operacije.

Gledajući tu funkciju izvan ovog konteksta, ona radi beskoristan posao – samo troši vrijeme. No u ovom slučaju, to je izrazito korisno. Ona troši vrijeme na taj način da napadač tijekom napada za svaku lozinku s kojom pokušava dešifrirati podatke mora obaviti veliku količinu vremenski zahtjevnog posla (npr. milijun iteracija kriptografske funkcije računanja sažetka). Korisniku to trošenje vremena ne smeta jer taj posao mora obaviti samo jednom prilikom svakog paljenja računala, dok napadač to vrijeme mora potrošiti za svaku potencijalnu lozinku.

2.1 Hardversko i softversko šifriranje diska

Dvije su osnovne vrste rješenja za šifriranje diska: hardversko šifriranje ugrađeno u sam uređaj i softversko rješenje uporabom programskog alata za šifriranje diska. Glavna prednost hardverskog šifriranja je lakoća primjene za krajnjeg korisnika. Podaci se šifriraju automatski na samom uređaju tako da osim omogućavanja šifriranja i izbora lozinke, nije potrebno poduzimati dodatne korake. Budući da je posao šifriranja podataka prepušten specijaliziranom procesoru ugrađenom u sam disk, hardverska rješenja ne opterećuju glavni procesor računala te su često brža u radu.

Softverska rješenja temelje se na uporabi softvera za šifriranje diska kojeg je potrebno instalirati na računalo. Cijenom su ovakva rješenja daleko pristupačnija jer osim što se isti alat u pravilu može koristiti za šifriranje više diskova, postoje i provjerena besplatna rješenja. Ovisno o konkretnom alatu, konfiguracija šifriranja može biti složena, no današnji operacijski sustavi većinom dolaze s ugrađenim rješenjima namijenjenima jednostavnom i lakom korištenju.

Sa sigurnosnog aspekta, hardverska rješenja nude prednosti u obrani od nekih vrsta napada jer se glavni ključ nikada ne nalazi u memoriji računala već je šifriranje u cijelosti pod nadzorom posebnog hardvera. Uz to, u hardverska rješenja mogu biti ugrađene dodatne zaštite od napada višestrukim pokušajima tako da uređaj nakon određenog broja neuspjelih pokušaja zabrani pristup ili čak uništi podatke. Efikasnost tih zaštita ovisi o tome koliko je lako rastaviti sam disk i izravno pristupiti šifriranim podacima i šifriranom ključu za šifriranje podataka (DEK).

Sigurnost softverskih rješenja ovisi o sigurnosti samog računala jer je neovlaštenim upadom u računalo u radu moguće doći u posjed kriptografskog ključa ili na neki drugi način izvršiti napad na sigurnost podataka. S druge strane, softversko rješenje omogućuje odabir rješenja otvorenog koda. Kriptografija je složeno područje prepuno zamki i izrada sigurnog kriptografskog alata iznimno je složen i zahtjevan posao. Ozbiljni sigurnosni propusti događali su se i iskusnim proizvođačima (1), a nažalost, postoje i slučajevi namjernog snižavanja razine zaštite (2) ili čak ugradnja tajnih ulaza (eng. *backdoor*). Korištenjem softverskog rješenja otvorenog koda moguće je uvidom u izvorni kod do neke mjere utvrditi sigurnost rješenja. Alat čiji je izvorni kod javno dostupan, kojeg su analizirali i nastavljaju analizirati brojni stručnjaci te koji je i nakon toga općeprihvaćen kao siguran, zasigurno je dobar izbor za zaštitu podataka. Ovo nipošto ne znači da su sva rješenja zatvorenog koda nužno nesigurna, ali ostaje nepobitna činjenica da se njihova sigurnost ne može neovisno dokazati već je potrebno u potpunosti vjerovati proizvođaču.

3 Nedostaci šifriranja diska

Glavni nedostatak zaštite podataka šifriranjem diska je činjenica da su podaci zaštićeni samo kada je računalo ugašeno. Nakon što korisnik unese ispravnu lozinku tijekom pokretanja računala, kriptografski ključ za dešifriranje podataka drži se u memoriji računala kako bi se omogućio nesmetani rad i pristup podacima. Ako napadač ostvari fizički ili udaljeni pristup pokrenutom računalu, šifriranje diska neće spriječiti neovlašteni pristup podacima.

Zbog toga što se kriptografski ključ nalazi u memoriji, zaključavanje računala povratkom na zaslon za prijavu korisnika ne štiti podatke u potpunosti. Brojni forenzički alati omogućuju stvaranje preslike memorije računala korištenjem nekog od priključaka s izravnim pristupom memoriji, kao što su PCI, PCI Express, Thunderbolt, ExpressCard ili FireWire, čime napadač izravno dolazi u posjed ključa pohranjenog u memoriji. Priključke koji se ne koriste poželjno je isključiti u postavkama BIOS-a kako bi se smanjio broj mogućih izvora napada.

Presliku memorije moguće je dobiti i iskorištavanjem svojstva memorijskih čipova da nakon nestanka napona još kratko vrijeme zadržavaju svoj sadržaj. Naglim snižavanjem temperature čipova ovo se vrijeme može produljiti i do nekoliko minuta, što omogućava tzv. napad hladnog pokretanja (eng. *cold boot attack*). Nakon naglog hlađenja memorijskih čipova, napadač gasi računalo te zatim memorijske čipove priključuje na računalo posebno pripremljeno za stvaranje preslike glavne memorije ili jednostavno pokreće napadano računalo s prijenosnog medija na kojem se nalazi operacijski sustav s alatima za forenzičko kopiranje memorije.

Kako bi se izbjegli ovi nedostaci, računalo ne treba ostavljati uključenim bez nadzora te treba onemogućiti gašenje računala metodom spavanja i hibernacije. Pri spavanju, glavna memorija računala zadržava sav sadržaj, što omogućava ranije spomenute napade. Prilikom hibernacije računalo se gasi, ali prethodno sadržaj memorije pohranjuje na disk. Sigurnost podataka izravno ovisi o načinu na koji alat za šifriranje upravlja ovim procesom. Ukoliko alat prije gašenja računala šifrira i pohranjeni sadržaj memorije, podaci su zaštićeni. Ako se pak on ostavi nešifriran, računalo je zapravo izloženo povećanom riziku jer je hibernacija odradila dio posla za napadača i unaprijed mu pripremila datoteku s preslikom memorije u kojoj može pronaći kriptografski ključ za dešifriranje svih podataka.

Posebnu pažnju treba posvetiti i sigurnosti ostalih korisničkih računa na računalu. Zbog činjenice da se za šifriranje podataka na disku koristiti samo jedan kriptografski ključ, svi korisnici računala nakon uspješne prijave u pravilu imaju potpuni pristup ključu. Za postizanje željene razine zaštite potrebno je dosljedno se pridržavati pravila o minimalnoj složenosti korisničke lozinke.

Na kraju, potrebno je imati u vidu i činjenicu kako nije moguće postići potpunu sigurnost. Uz dovoljno motivacije, pripreme i vremena za nesmetano djelovanje, fizički pristup računalu napadaču pruža brojne mogućnosti napada.

Jedan od napada koje napadač može izvesti je tzv. napad zle sluškinje (eng. *evil maid attack*) (3) (4). Ime napada dolazi od scenarija u kojem žrtva ostavi svoje računalo u hotelskoj sobi i u njenoj odsutnosti „zla sluškinja“ koja ima pristup sobi neometano mijenja računalo. „Zla sluškinja“, tj. napadač, mijenja nešifrirani dio diska koji služi za početno pokretanje računala

(objašnjen u odjeljku 1.1) tako da kada korisnik upiše svoju lozinku, ona se pošalje napadaču ili zapiše negdje gdje ju napadač kasnije može pročitati.

Za uspješan napad nije potrebno ni mijenjati sadržaj diska – budući da se sigurnost šifriranja oslanja na sigurnost lozinke za otključavanje, ugradnjom hardverskog uređaja za snimanje pritisnutih tipki (eng. *keylogger*) ili postavljanjem skrivenih kamera napadač može saznati korisničku lozinku. Onog trenutka kada napadač sazna lozinku, korisnik se više ne može oslanjati na bilo kakvu zaštitu podataka prilikom krađe ili neovlaštenog pristupa disku.

4 Zaključak

Šifriranje diska korisna je mjera zaštite podataka od neovlaštenog čitanja dok je računalo ugašeno. U ovom dokumentu objašnjena je tehnička pozadina šifriranja diska, pobrojani su nedostaci tog postupka te su u nastavku dokumenta u prilogu opisani postupci korištenja široko dostupnih alata za šifriranje cijelog diska na najčešće korištenim operacijskim sustavima.

Kao i brojne druge sigurnosne mjere, šifriranje diska nije savršeno, no uz razumijevanje postupka šifriranja diska te njegovih prednosti i nedostataka moguće je podići zaštitu svojih podataka na vrlo visoku razinu. Danas su alati za šifriranje diska u pravilu integrirani s postojećim operacijskim sustavima, lako ih je koristiti i gotovo da ne utječu na brzinu rada sustava tako da je šifriranje cijelog diska korisna i pristupačna opcija za sve korisnike koji žele zaštititi svoje podatke.

5 Literatura

1. **Alendal, Gunnar, Kison, Christian i modg.** got HW crypto? On the (in) security of a Self-Encrypting Drive series. s.l. : IACR Cryptology ePrint Archive 2015, 2015.
2. **Gasior, Geoff.** 256-bit AES encryption broken in SandForce SSD controllers. *The Tech Report.* [Mrežno] 11. lipanj 2012. [Citirano: 1. prosinac 2017.] https://techreport.com/news/23096/256-bit-aes-encryption-broken-in-sandforce-ssd-controllers.
3. **Schneier, Bruce.** "Evil Maid" Attacks on Encrypted Hard Drives. *Schneier on Security.* [Mrežno] 23. listopad 2009. [Citirano: 1. prosinac 2017.] https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.
4. **Rutkowska, Joanna.** Evil Maid goes after TrueCrypt! *The Invisible Things Lab's blog.* [Mrežno] 16. listopad 2009. [Citirano: 1. prosinac 2017.] http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html.
5. **ArchWiki.** Disk encryption. [Mrežno] 21. studeni 2017. [Citirano: 1. prosinac 2017.] https://wiki.archlinux.org/index.php?title=Disk_encryption&oldid=497724.

6 Prilog – korištenje alata za šifriranje diska

Ovo poglavlje opisuje kako šifrirati cijeli disk pomoću široko dostupnih alata. Opisani su alati za Windows, Mac OS X i Linux operacijske sustave:

- BitLocker
- FileVault
- Linux Unified Key Setup (cryptsetup, dm-crypt)
- VeraCrypt

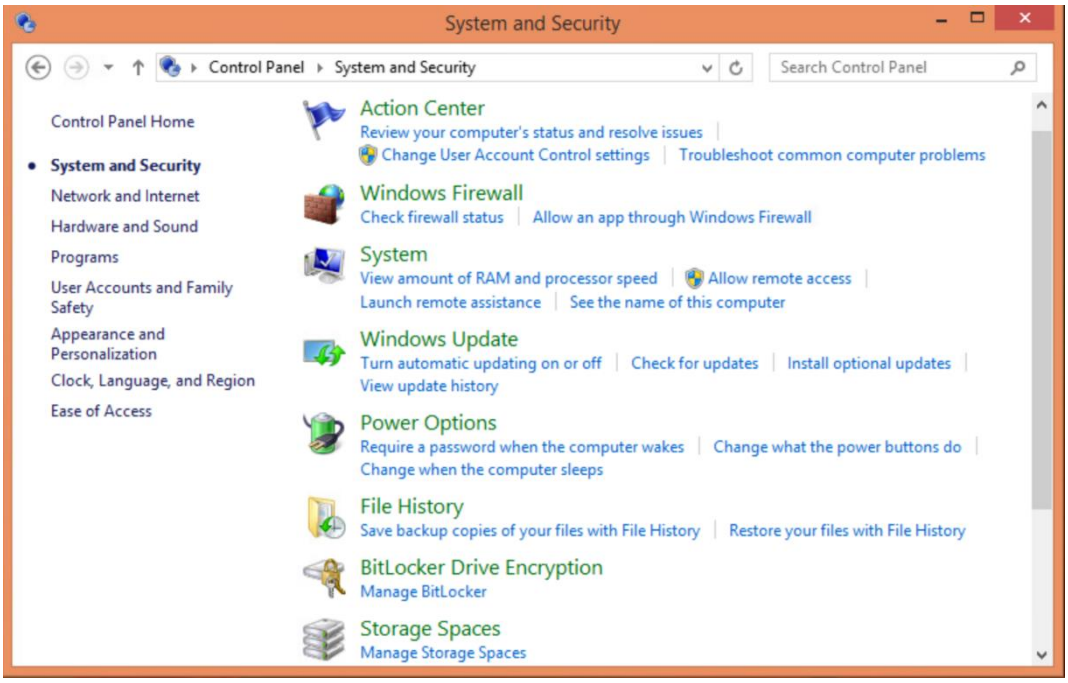
6.1 BitLocker

BitLocker je softver za šifriranje diska integriran u Microsoft Windows operacijski sustav. Koristi AES algoritam za šifriranje u CBC ili XTS načinu rada s ključem od 128 ili 256 bita.

BitLocker je dostupan u sljedećim inačicama Microsoft Windows operacijskog sustava:

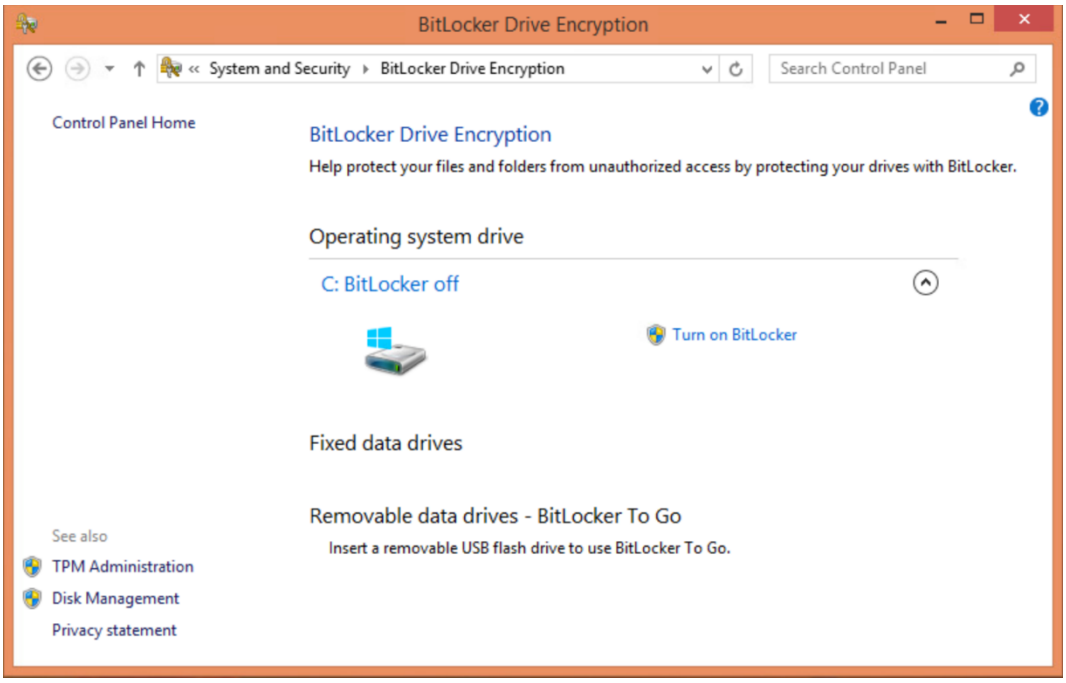
- Windows Vista i Windows 7 – Enterprise i Ultimate inačice
- Windows 8 i 8.1 – Enterprise i Pro inačice
- Windows 10 – Enterprise, Pro i Education inačice
- Windows Server 2008 i novije Windows Server inačice

U nastavku je opisan postupak šifriranja cijelog diska pomoću BitLocker-a.



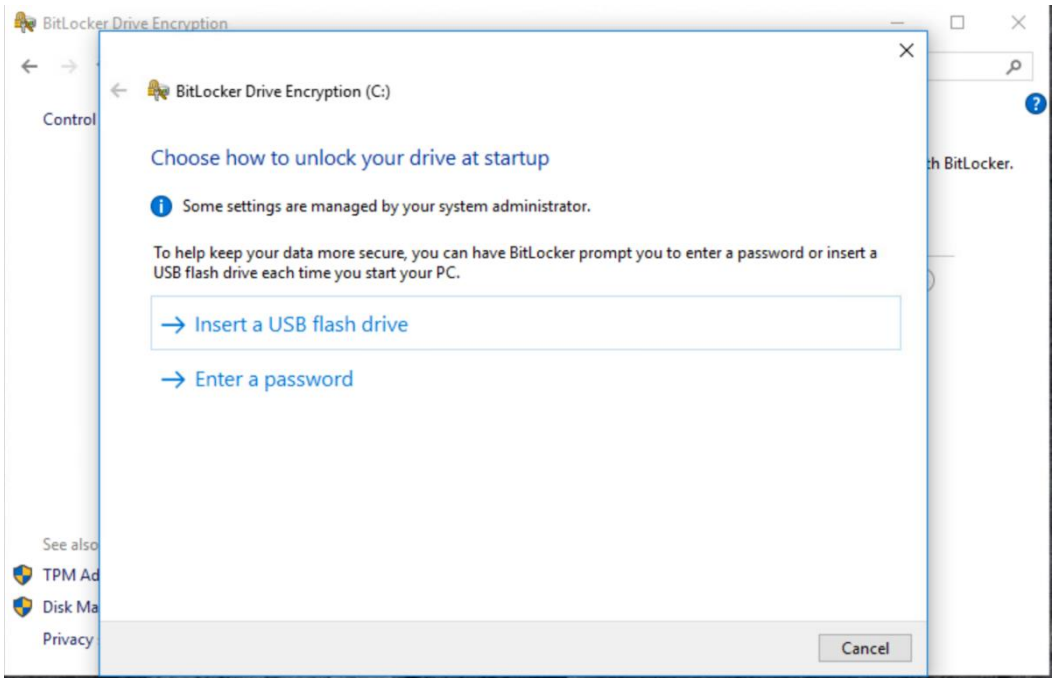
Korak 1:

Ako korisnik ima jednu od navedenih inačica Microsoft Windows operacijskog sustava koja sadrži BitLocker, moguće ga je uključiti otvaranjem Upravljačke ploče (*Control Panel*) i odabirom Sustava i sigurnosti (*System & Security*). Konačno, potrebno je odabrati *BitLocker Drive Encryption*.



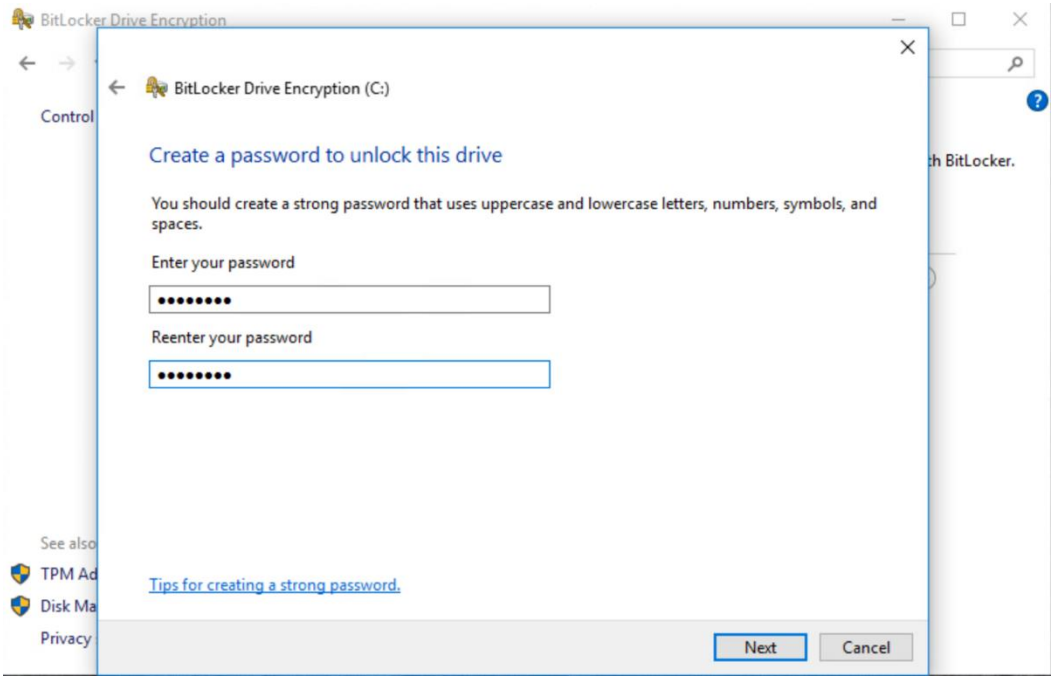
Korak 2:

U BitLocker izborniku potrebno je odabrati *Turn on BitLocker* čime se provjerava jesu li svi uvjeti za šifriranje diska zadovoljeni.



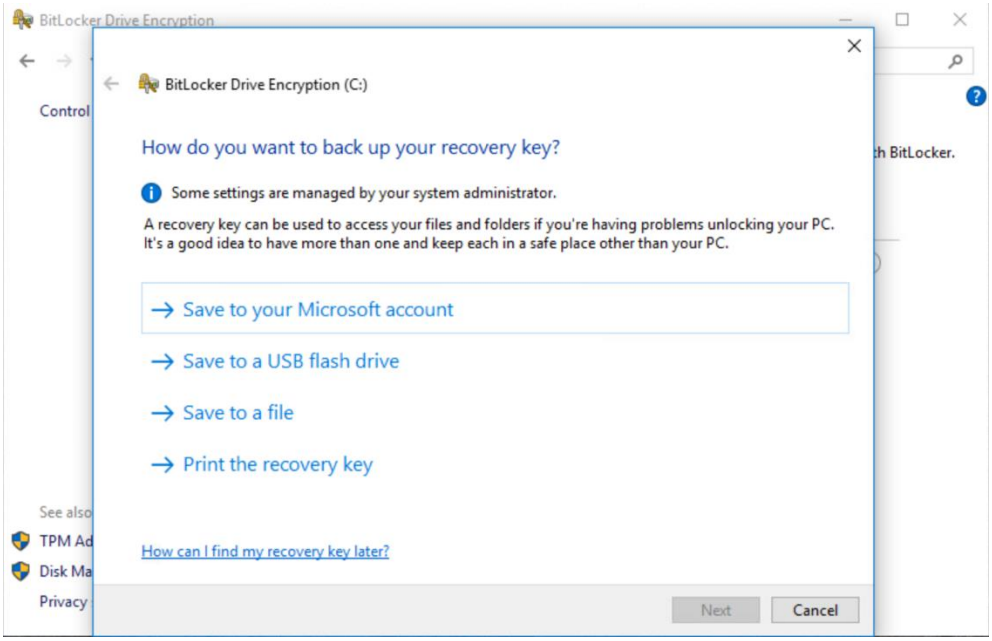
Korak 3:

Ako je provjera uspješna, potrebno je odabrati način na koji će se otključati disk prilikom pokretanja operacijskog sustava. Moguće opcije su USB medij ili lozinka. „USB medij“ znači da će se na USB memoriju pohraniti ključ. Za otključavanje diska potrebno je u računalo svaki put priključiti USB. Ove upute opisuju korištenje lozinke za otključavanje diska.



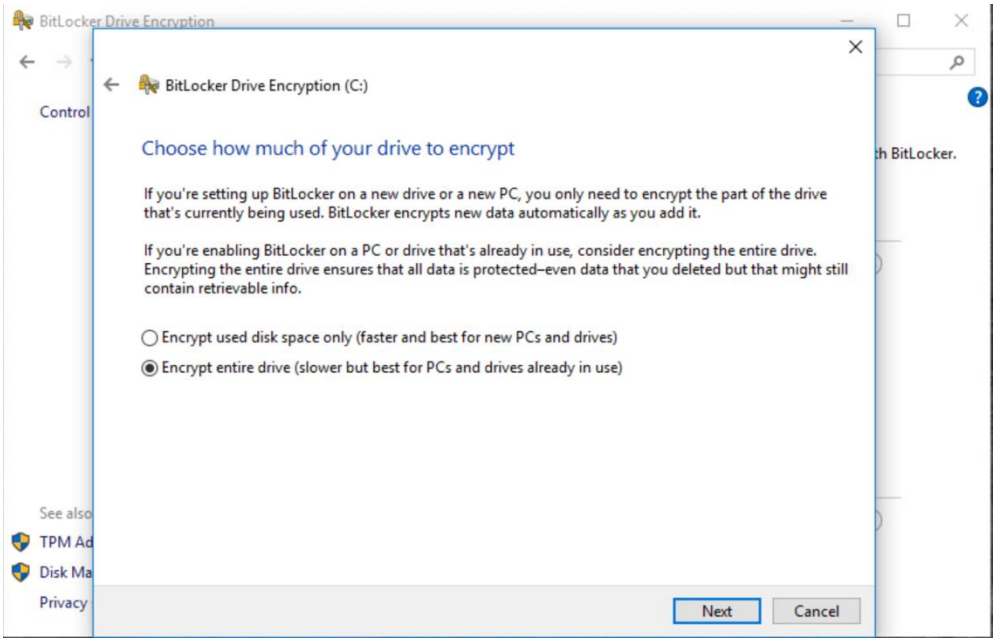
Korak 4:

Potrebno je odabrati i unijeti lozinku (pod pretpostavkom da je odabran taj način).



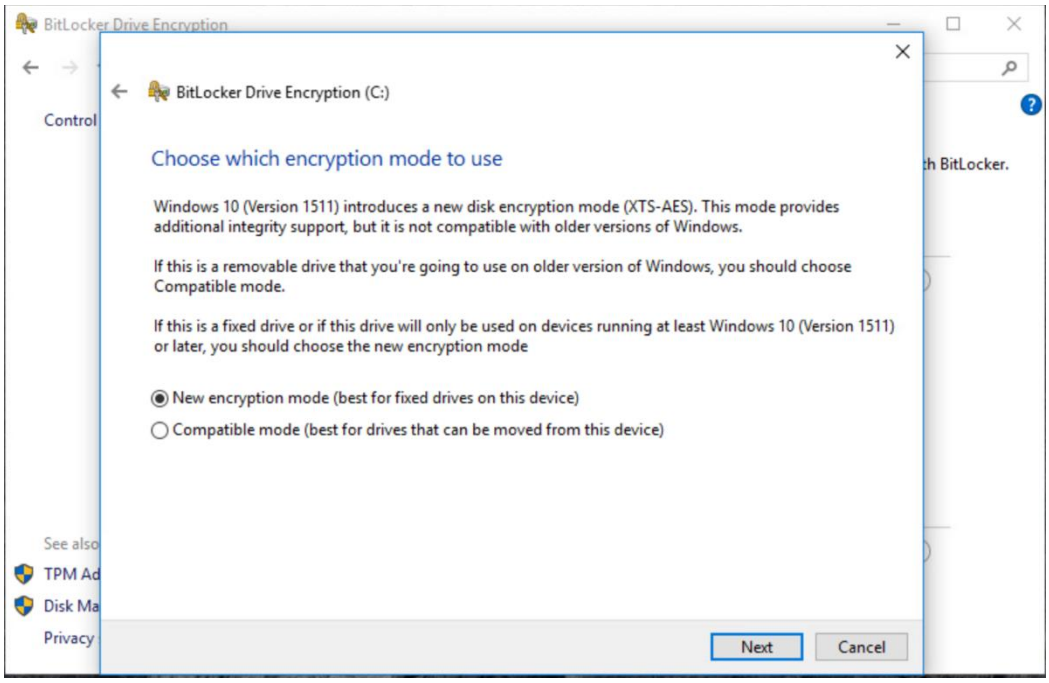
Korak 5:

Potrebno je odabrati kako sigurno spremiti ključ za oporavak. Taj ključ omogućuje pristup disku ako dođe do problema s glavnom metodom otključavanja (USB medij ili lozinka). Ako se i USB medij odnosno lozinka i taj ključ izgube **neće više biti moguće pristupiti podacima**.



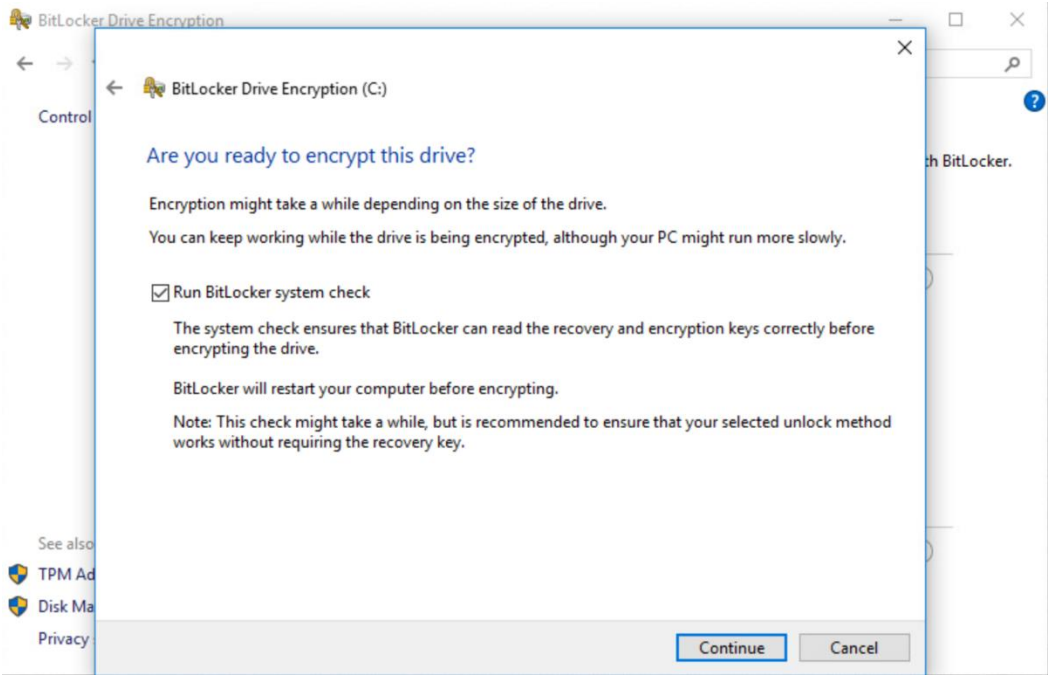
Korak 6:

Odabir šifriranja cijelog diska ili samo korištenog dijela (tj. naknadno šifriranje „praznog“ prostora kada se popuni). Preporuča se šifriranje cijelog diska kako bi prethodno izbrisane podatke bilo nemoguće rekonstruirati. Naime, prilikom uobičajenog brisanja datoteka, njihov se sadržaj zapravo ne briše, već ostaje na disku. Bit će prepisan novim podacima tek kad za njih zatreba prostor na disku.



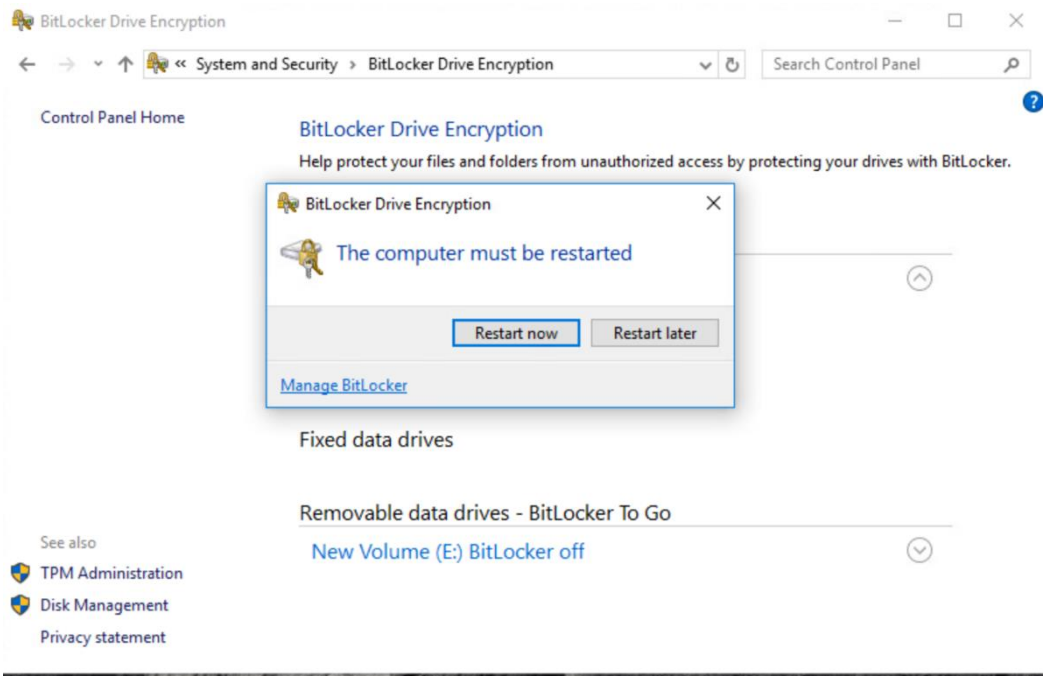
Korak 7:

Odabir načina šifriranja, preporuča se sigurniji XTS-AES način.



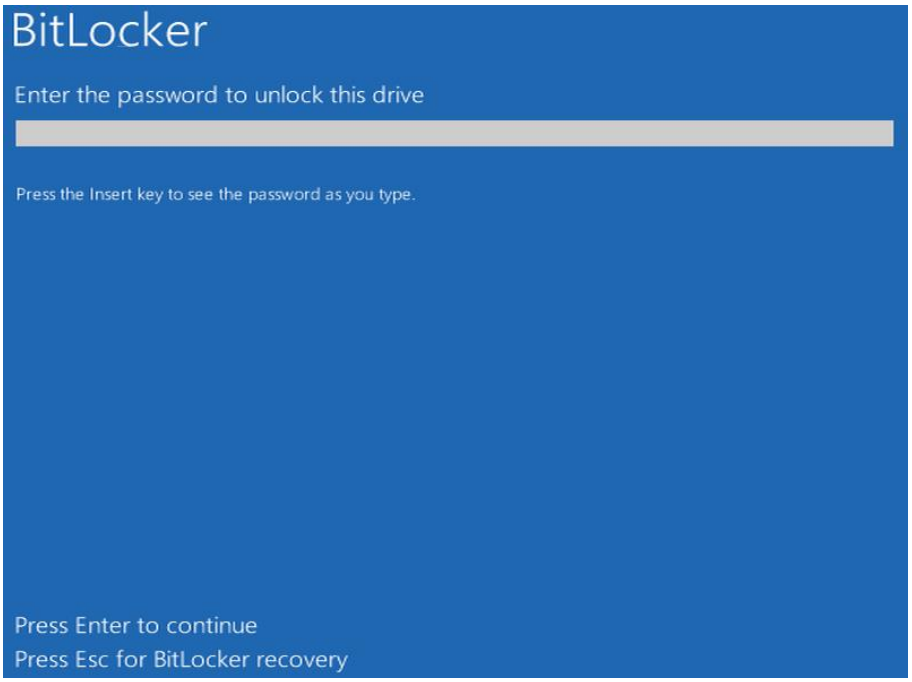
Korak 8:

Preporuča se odabrati pokretanje BitLocker provjere sustava (*BitLocker system check*). To je dodatna provjera da će sve funkcionirati prije samog šifriranja diska.



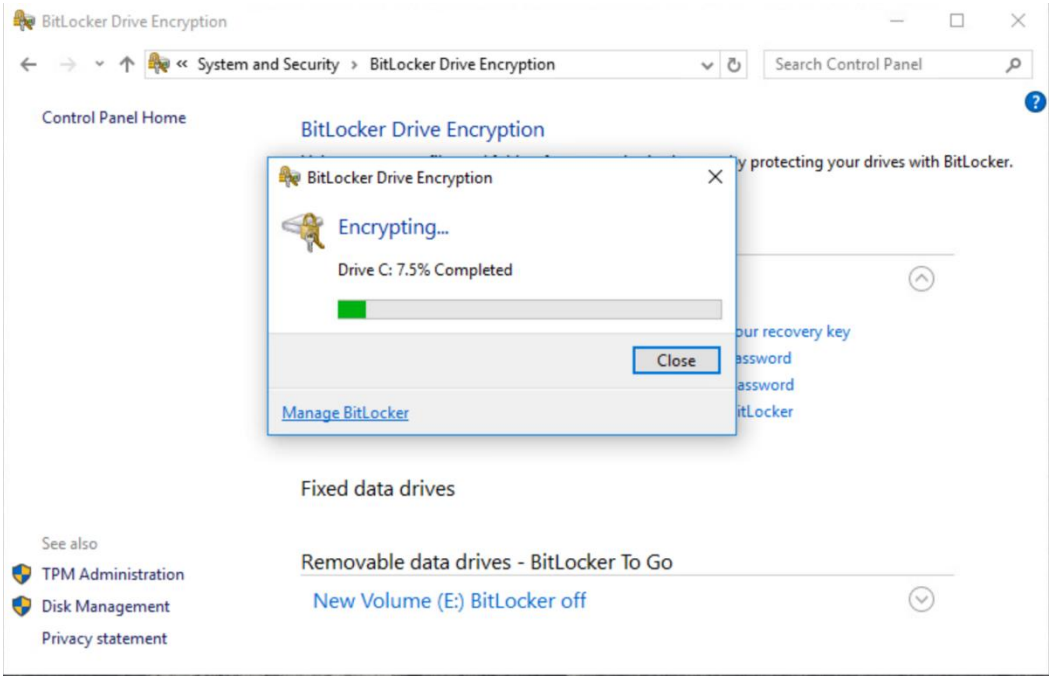
Korak 9:

Potrebno je ponovno pokrenuti računalo kako bi šifriranje započelo.



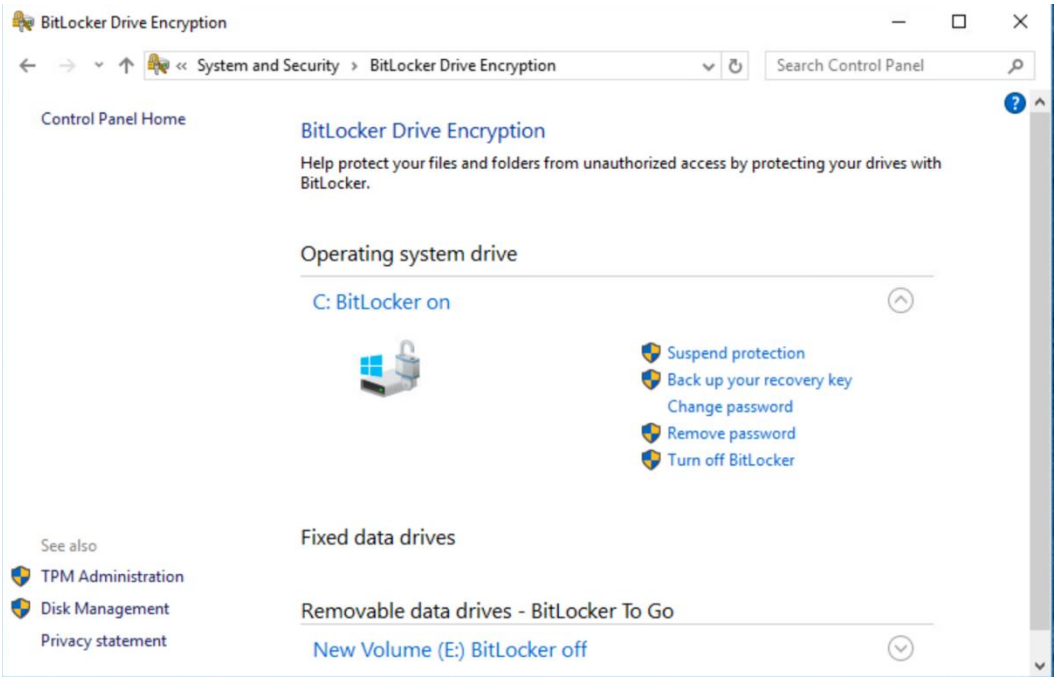
Korak 10:

Od sada je potrebno unijeti lozinku kako bi se otključao disk i nastavilo pokretanje operacijskog sustava.



Korak 11:

Nakon što je pokrenut operacijski sustav moguće je provjeriti napredak šifriranja diska (*Control Panel* – System & Security – BitLocker)



Korak 12.

BitLocker je uspješno uključen i disk je šifriran.

6.2 FileVault

FileVault je softver za šifriranje diska ugrađen u Mac OS X operacijski sustav. Prvi puta se pojavljuje u inačici Mac OS X 10.3 Panther. U prvotnom izdanju mogao je šifrirati samo korisnikov osobni (eng. *home*) direktorij upotrebom CBC (eng. *cipher-block chaining*) načina operacije šifre (eng. *block cipher mode of operation*). U kasnije verzijama Mac OSX-a integrirana je naprednija verzija programa koja može šifrirati cijeli disk koristeći sigurniji XTS-AES način operacije šifre.

U nastavku je opisan postupak šifriranja cijelog diska alatom FileVault.

Korak 1:

Kao što je rečeno, FileVault je integriran u Mac OS X operacijski sustav i nije ga potrebno instalirati već samo aktivirati. Programu se pristupa otvaranjem *System Preferences* prozora (pritiskom na ikonu u gornjem lijevom kutu ekrana, tj. na *Apple* simbol i u padajućem izborniku odabir *System preferences*) i odabirom *Security & Privacy* ikone.

Korak 2:

U *Security & Privacy* izborniku potrebno je odabrati FileVault podizbornik pa zatim simbol lokota u donjem lijevom kutu podizbornika. Sustav tada pita korisnika za administratorsku lozinku te nakon uspješnog unosa moguće je uključiti FileVault pritiskom na do tada sivu tipku *Turn On FileVault...*.

Korak 3:

Nakon uključivanja FileVault-a generira se sigurnosni ključ. Pomoću njega moguće je otključati disk u slučaju zaborava lozinke. Preporuka je napraviti kopiju sigurnosnog ključa i pohraniti ju na sigurnu lokaciju. Ako se ključ i lozinka izgube biti će nemoguće otključati disk i **svi podaci na njemu će biti izgubljeni**.

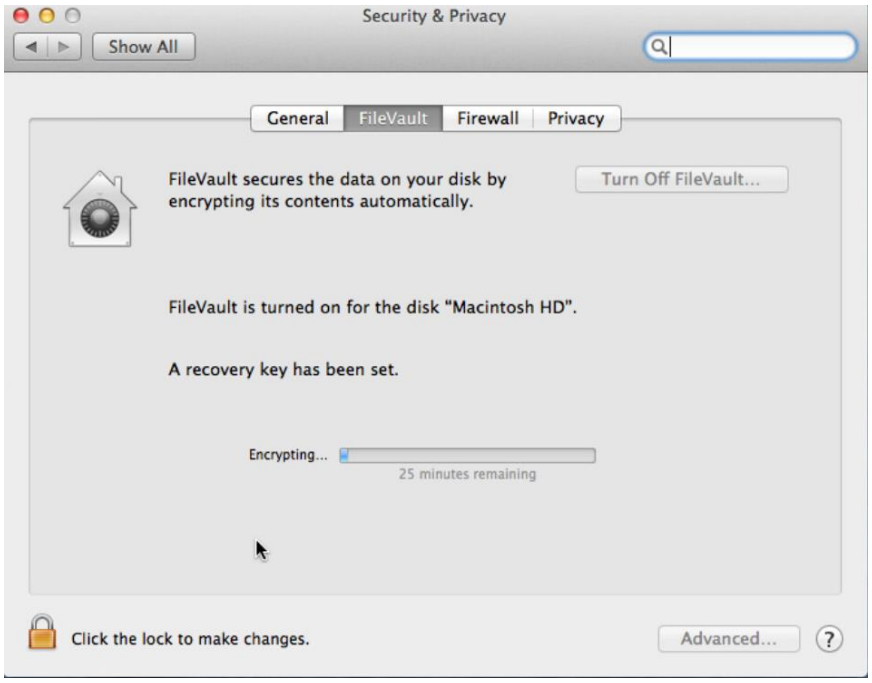
Korak 4:

Apple nudi mogućnost čuvanja sigurnosnog ključa kako ne bi došlo do situacije da korisnik izgubi svoje podatke.

Korak 5:

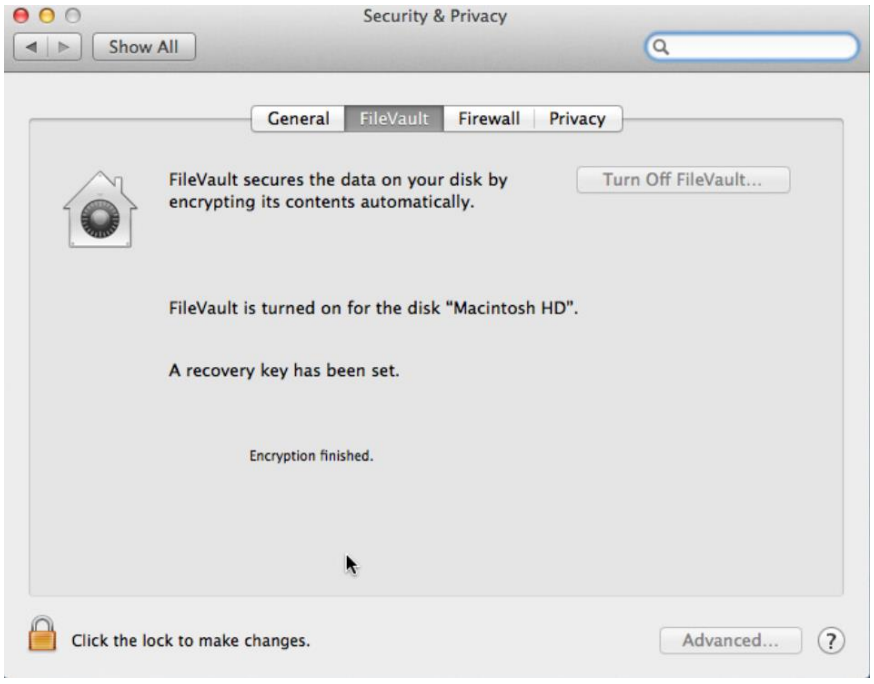
Zadnji korak je ponovno pokretanje računala. Nakon što se sustav podigne započinje šifriranje diska.

Napomena: FileVault ni u jednom trenutku ne traži korisnika da eksplicitno upiše lozinku za otključavanje diska, već pri sljedećoj korisničkoj prijavi automatski koristi upisanu lozinku. Svaki korisnik dešifrira disk istom lozinkom kojom se prijavljuje na sustav i ne treba ništa posebno pamtiti.



Korak 6:

Prikaz napretka šifriranja.



Korak 7:

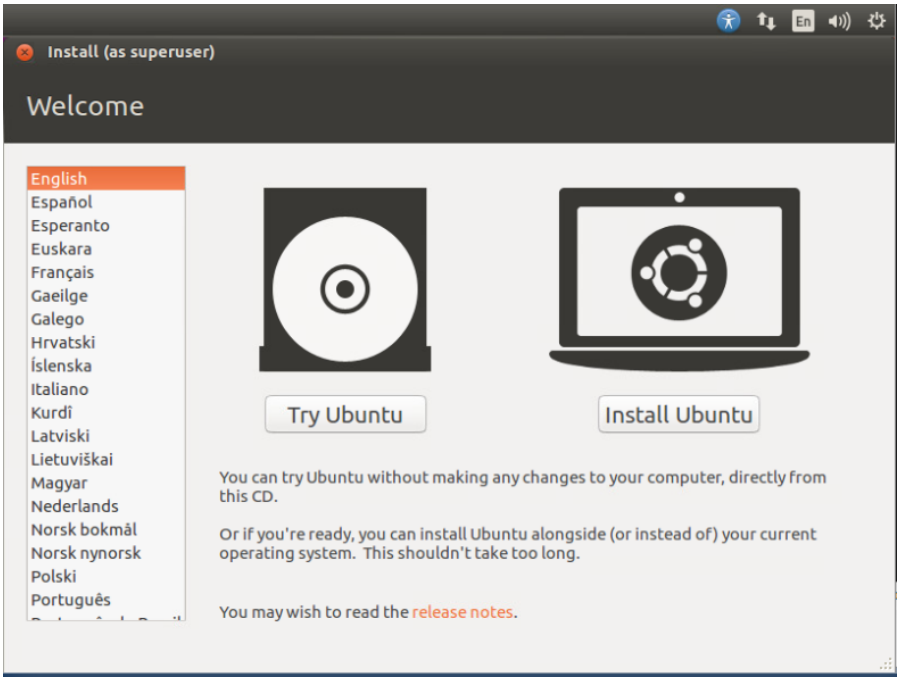
Šifriranje diska je gotovo i podaci su zaštićeni.

6.3 *Linux Unified Key Setup* (*cryptsetup*, *dm-crypt*)

Linux Unified Key Setup (LUKS) je specifikacija za šifriranje diskova, originalno stvorena za Linux operacijske sustave. LUKS propisuje standardni format za zapisivanje podataka potrebnih za šifriranje diska. On je neovisan o platformi te ga mogu koristiti različiti alati. Takav pristup omogućava kompatibilnost između različitih programa i, što je još važnije, osigurava da svi oni implementiraju šifriranje diska na siguran i dokumentiran način.

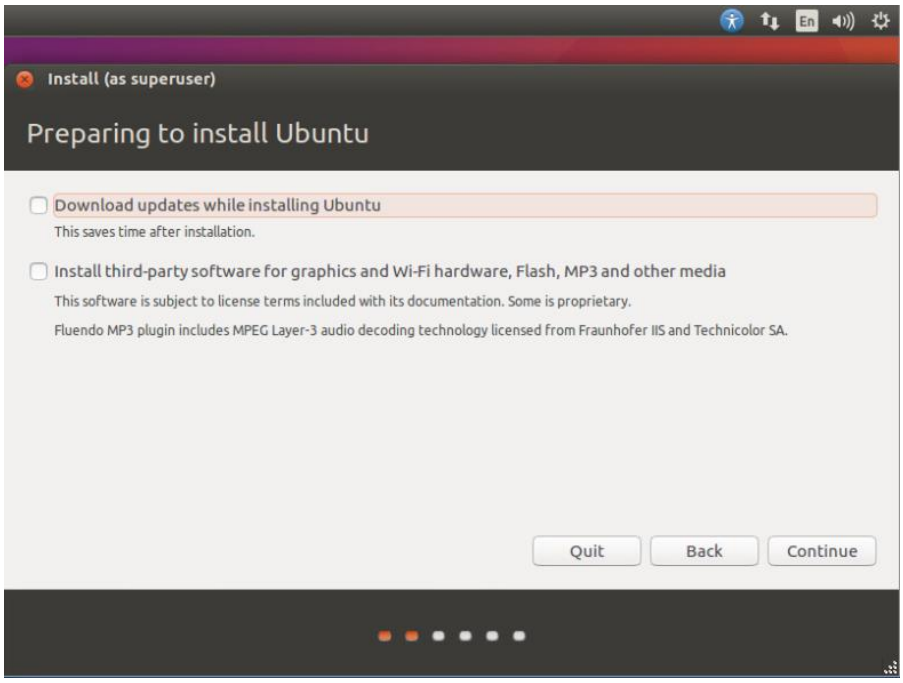
Implementacija LUKS standarda za Linux temelji se na softveru *cryptsetup* i *dm-crypt*. Također postoji i LibreCrypt, implementacija LUKS-a za Microsoft Windows.

U nastavku će biti prikazan najčešći postupak šifriranja diska na Linux operacijskim sustavima koji se sastoji od uključivanja šifriranja prilikom same instalacije operacijskog sustava. Prikazan je konkretan postupak za operacijski sustav Ubuntu Linux 16.04, no koraci se u pravilu ne razlikuju značajno za ostale distribucije.



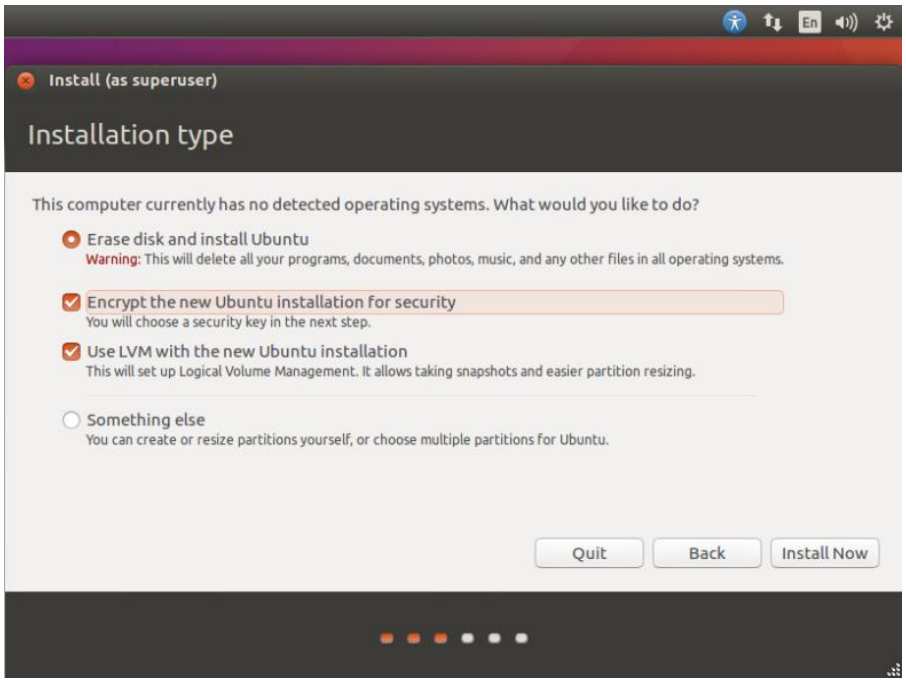
Korak 1:

Kao što je spomenuto, šifriranje se uključuje prilikom instalacije operacijskog sustava – za instalaciju je potrebno odabrati *Install Ubuntu*.



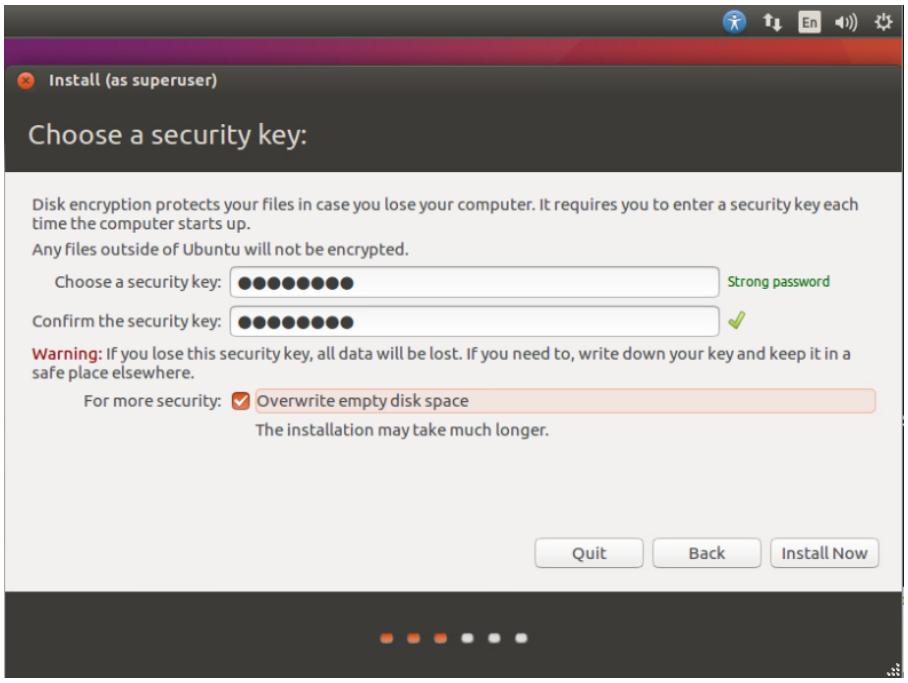
Korak 2:

Prikazan je odabir opcija za nadogradnju softvera tokom instalacije te instalacije dodatnog softvera. Te opcije ne utječu na šifriranje diska.



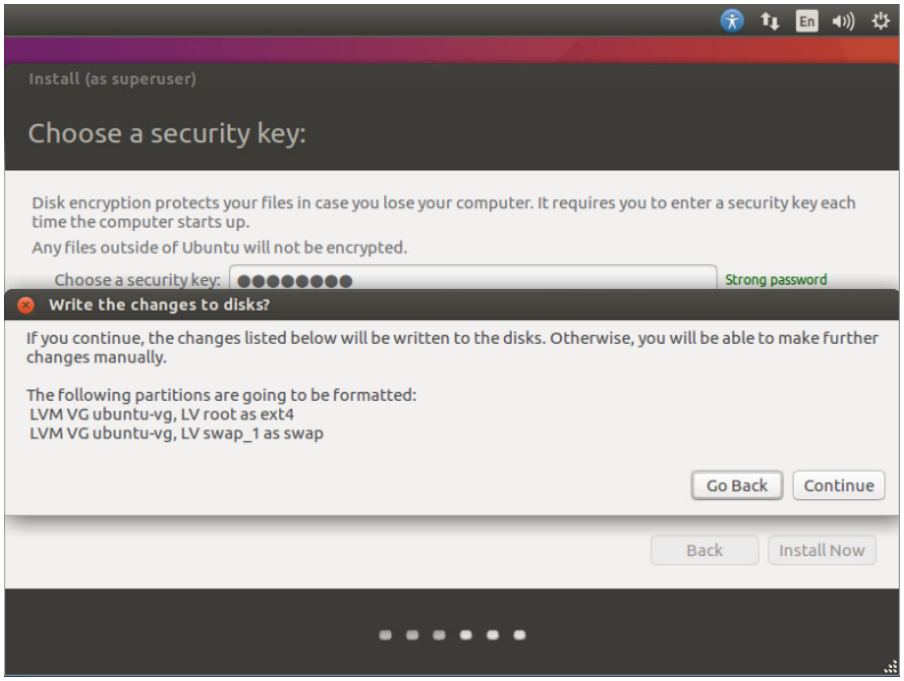
Korak 3:

Ovo je prvi korak koji se odnosi na samo šifriranje, potrebno je odabrati da nova Ubuntu instalacija bude šifrirana (*Encrypt the new Ubuntu installation for security*).



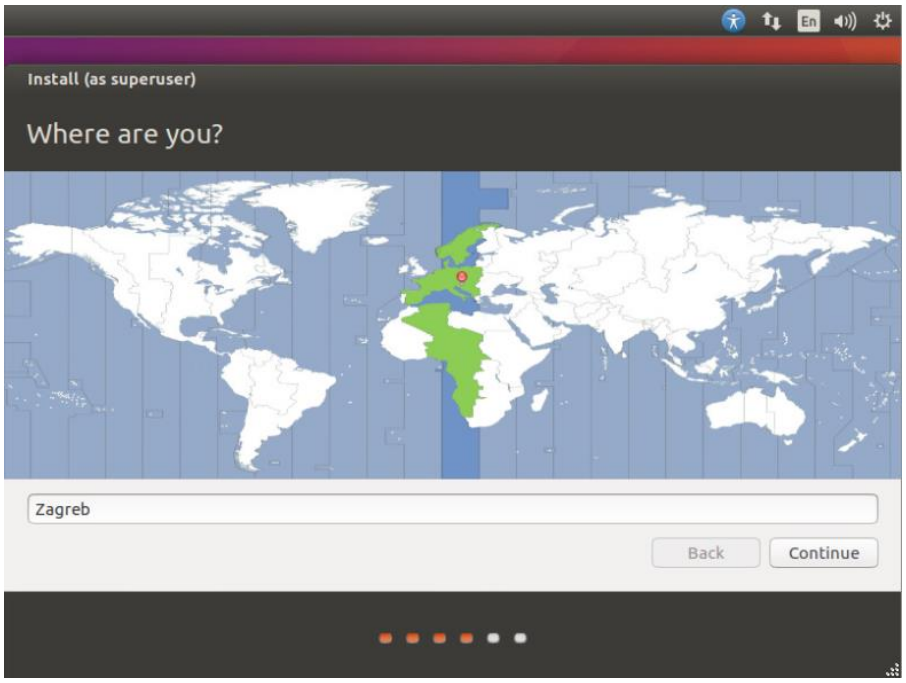
Korak 4:

Potrebno je odabrati lozinku za otključavanje diska. Također je korisno uključiti opciju „prepiši slobodan prostor na disku“ (*Overwrite empty disk space*) kako bi se prethodno zapisani podaci na disku prepisali što onemogućuje njihovu rekonstrukciju.



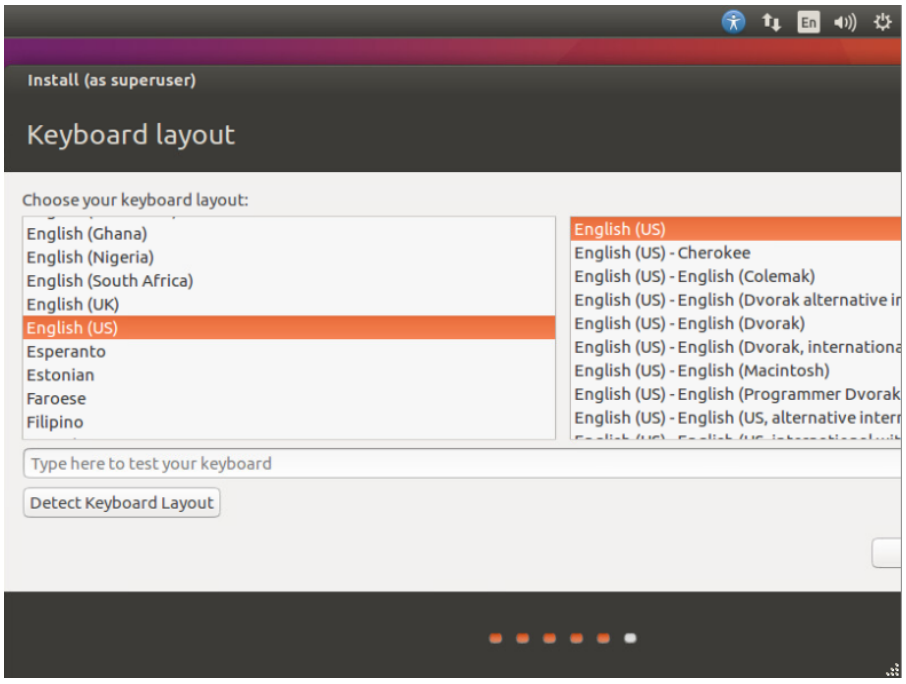
Korak 5:

Ako korisnik nije siguran u opcije koje je odabrao ili želi nešto promijeniti to je još uvijek moguće pritiskom na „povratak“ (Go Back)



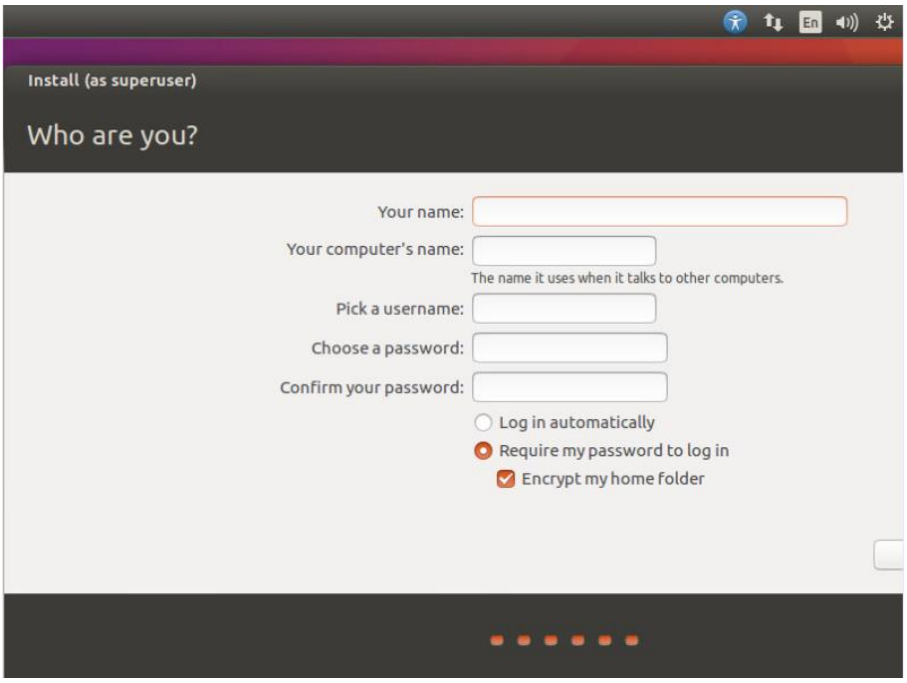
Korak 6:

Odabir lokacije (nije vezano uz šifriranje diska).



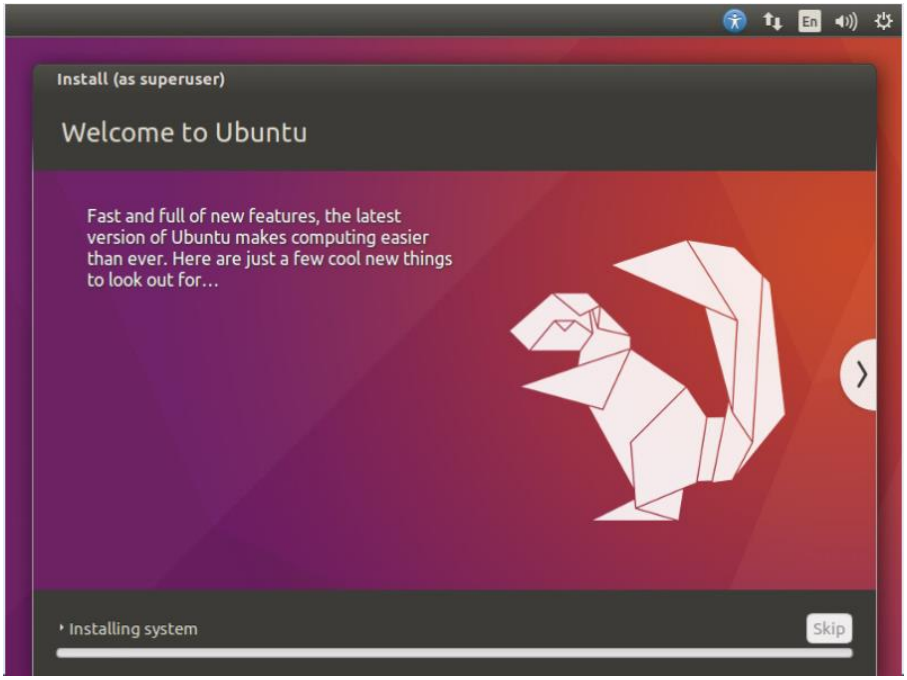
Korak 7:

Odabir rasporeda tipkovnice (nije vezano uz šifriranje diska).



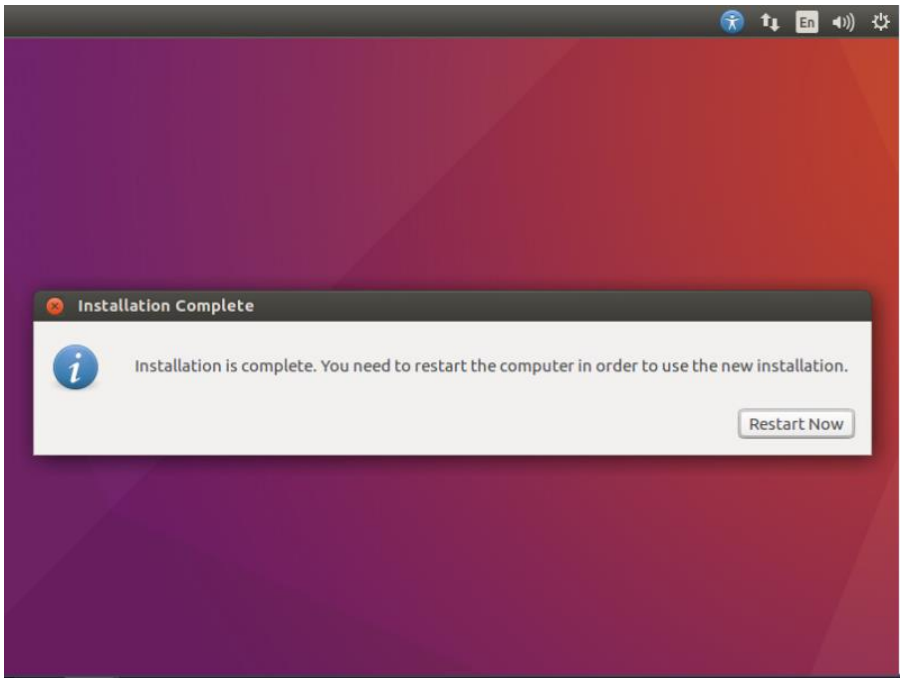
Korak 8:

Kreiranje korisnika – također nije vezano uz šifriranje diska jer se disk otključava posebnom lozinkom koja je neovisna o lozinci korisnika.



Korak 9:

Tijekom instalacije se i disk šifrira.



Korak 10:

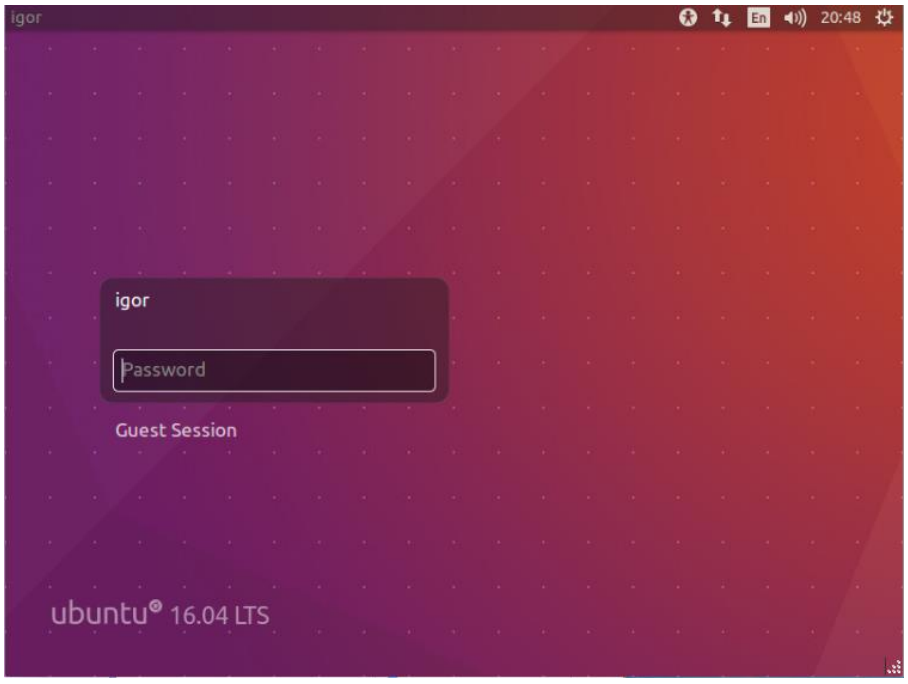
Po završetku instalacije disk je šifriran te je potrebno ponovno pokrenuti računalo.

Korak 11:

Pri pokretanju računala potrebno je unijeti lozinku odabranu u koraku 4 kako bi se disk „otključao“ (dešifrirao) te se nastavilo podizanje sustava.

Korak 12:

Uspješan unos sigurnosnog ključa.



Korak 13:

Računalo je uspješno pokrenuto kada se pojavi ekran za prijavu korisnika.

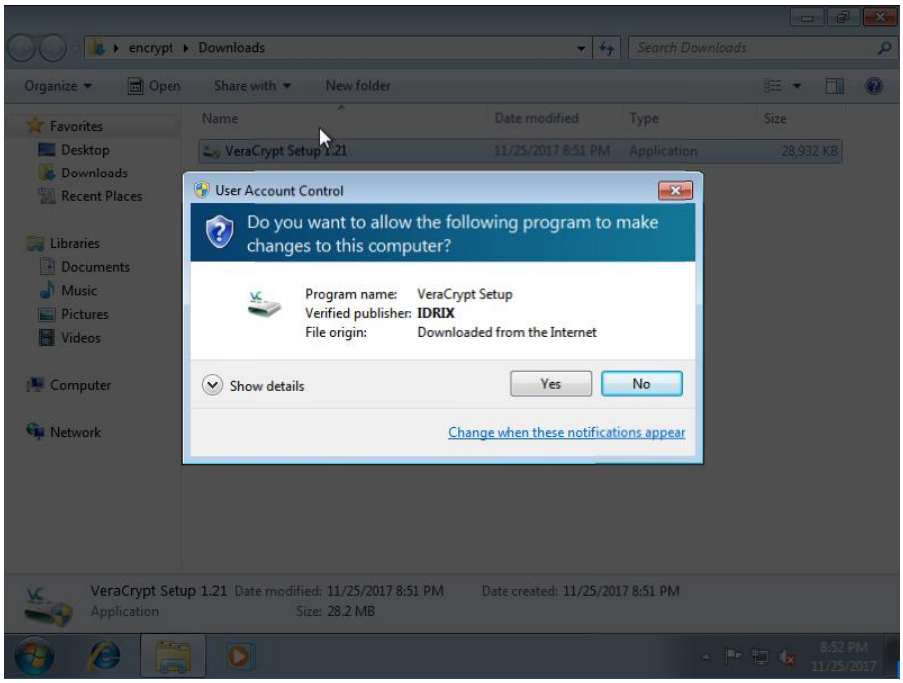
6.4 VeraCrypt

VeraCrypt je softver za šifriranje diska nastao na temelju popularnog ukinutog softvera za istu svrhu TrueCrypt 7.1a. Kao i TrueCrypt, VeraCrypt je softver otvorenog koda što mu daje veliku vjerodostojnost u usporedbi sa zatvorenim rješenjima.

Po pitanju funkcionalnosti, može se reći da je VeraCrypt jednostavno nadograđena inačica TrueCrypt-a. U usporedbi s prethodno opisanim alatima, VeraCrypt ima podršku za najveći broj operacijskih sustava – podržava Microsoft Windows, Mac OS X, Linux i FreeBSD.

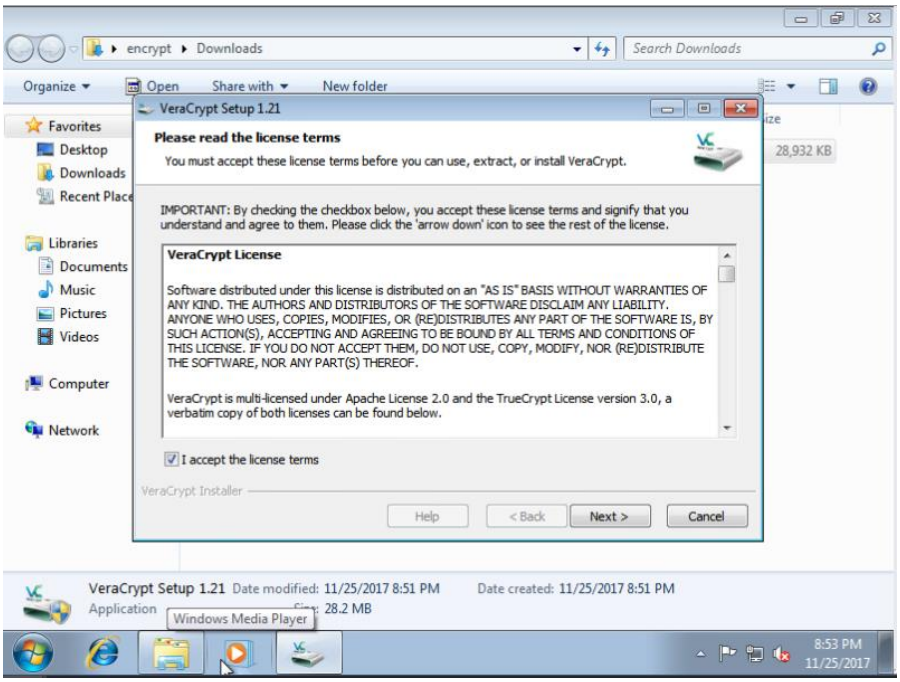
U nastavku je opisan postupak šifriranja cijelog diska pomoću VeraCrypt-a na Microsoft Windows operacijskom sustavu. S obzirom na to da VeraCrypt za razliku od prethodno opisanih alata ne dolazi integriran s operacijskim sustavom, opisani postupak je podijeljen u dva dijela: instalaciju i korištenje.

6.4.1 Instalacija



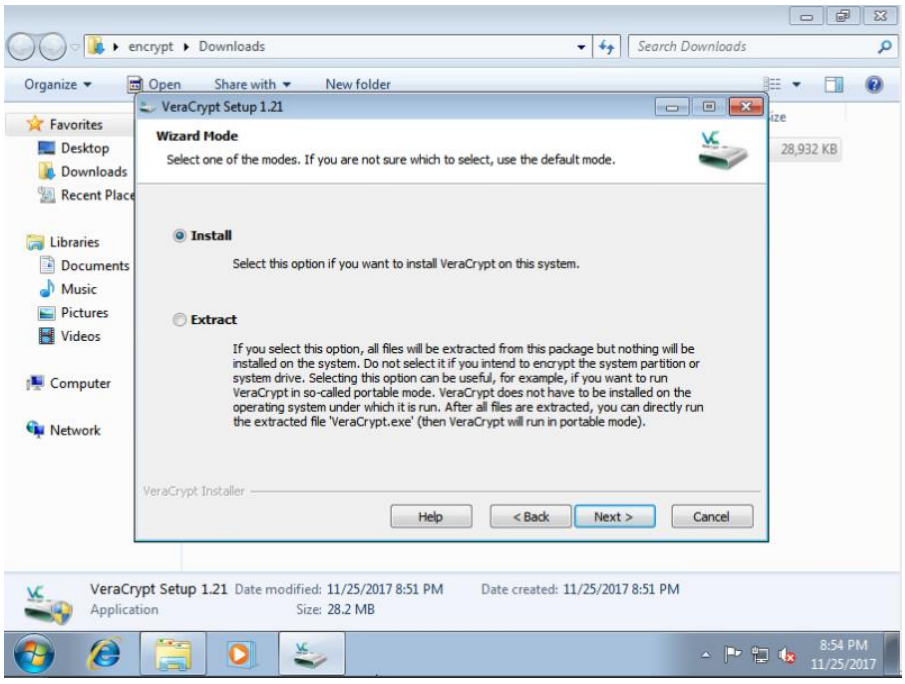
Korak 1:

Prvo je potrebno preuzeti VeraCrypt sa službene Web stranice te pokrenuti ga.



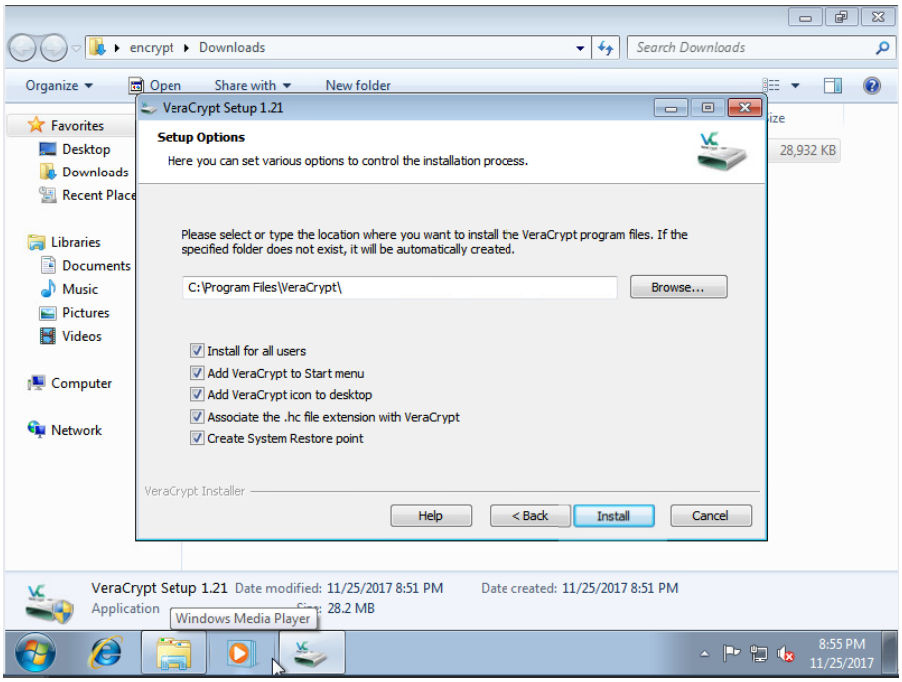
Korak 2:

Prilikom pokretanja potrebno je prihvatiti uvjete korištenja.



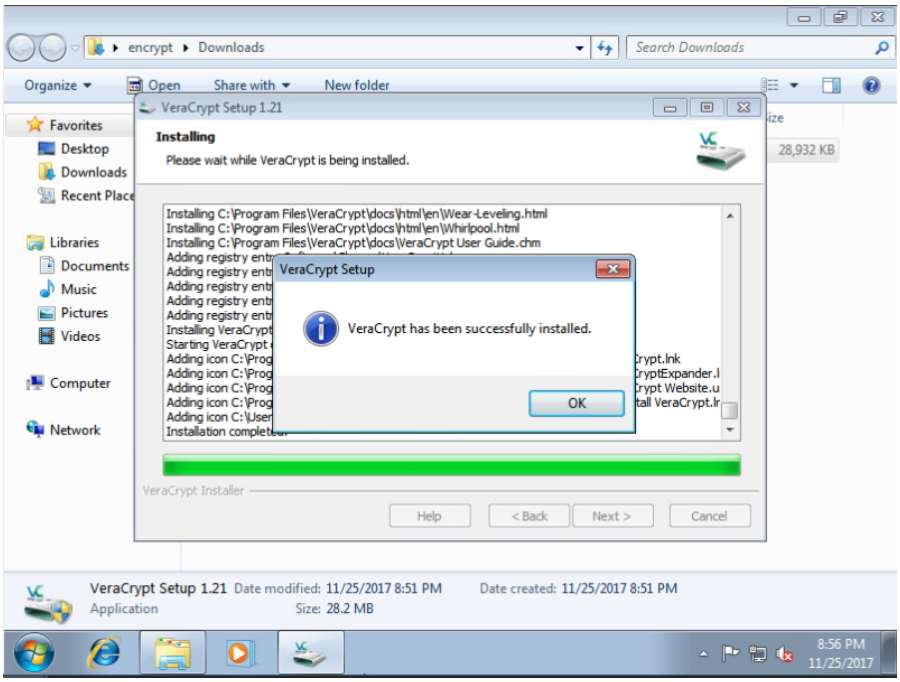
Korak 3:

Potrebno je odabrati *Install*.



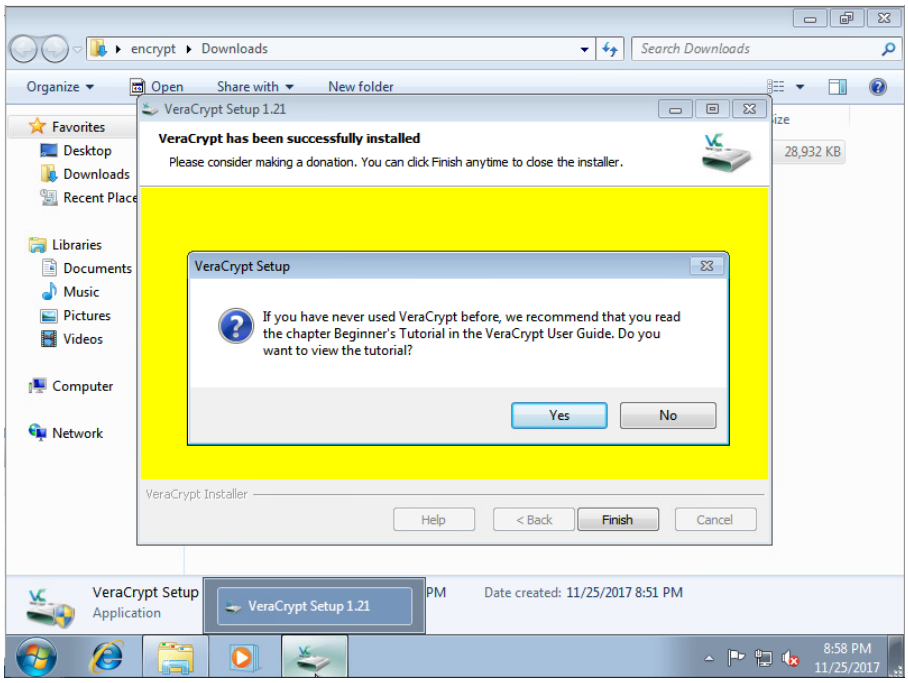
Korak 4:

Potrebno je odabrati gdje će VeraCrypt biti instaliran uz još par opcija koje ne utječu na šifriranje.



Korak 5:

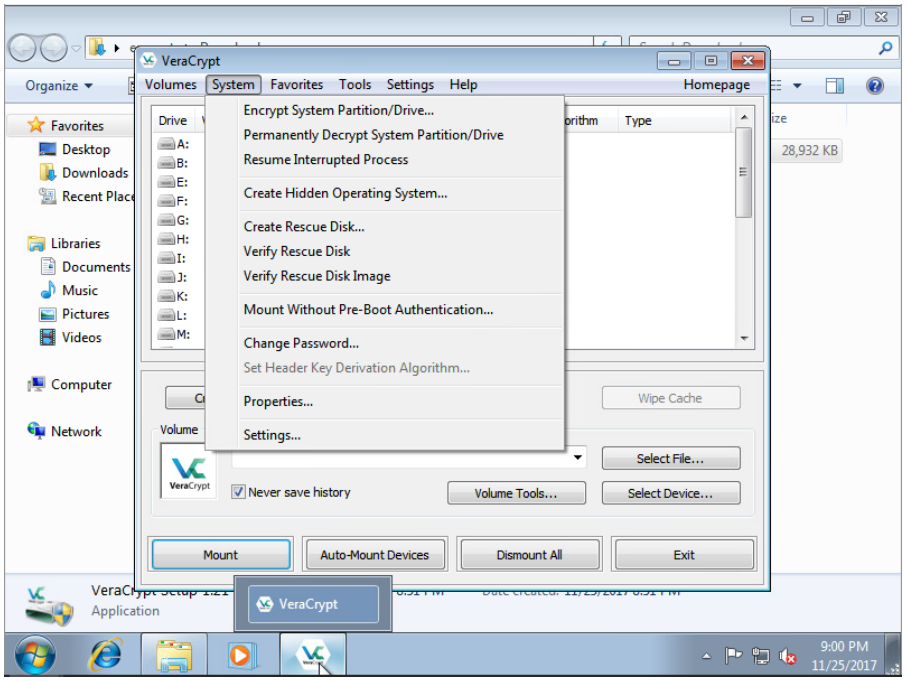
U konačnici, VeraCrypt je uspješno instaliran.



Korak 6:

Korisno je pročitati upute za početnike za bolje upoznavanje sa softverom.

6.4.2 Korištenje

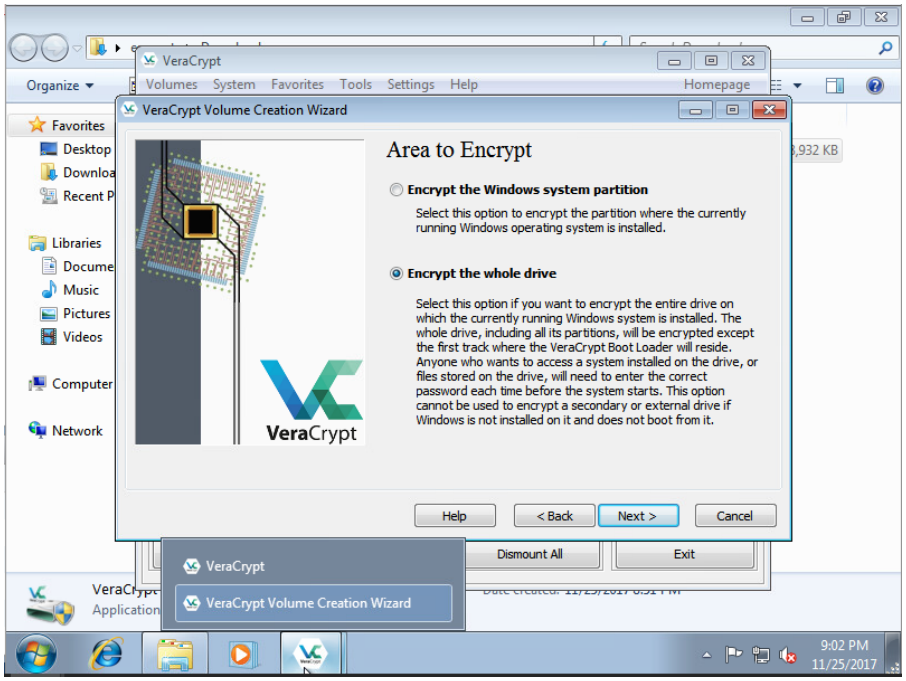


Korak 7:

Nakon otvaranja VeraCrypt-a, za šifriranje cijelog diska potrebno je odabrati *System – Encrypt System Partition/Drive*.

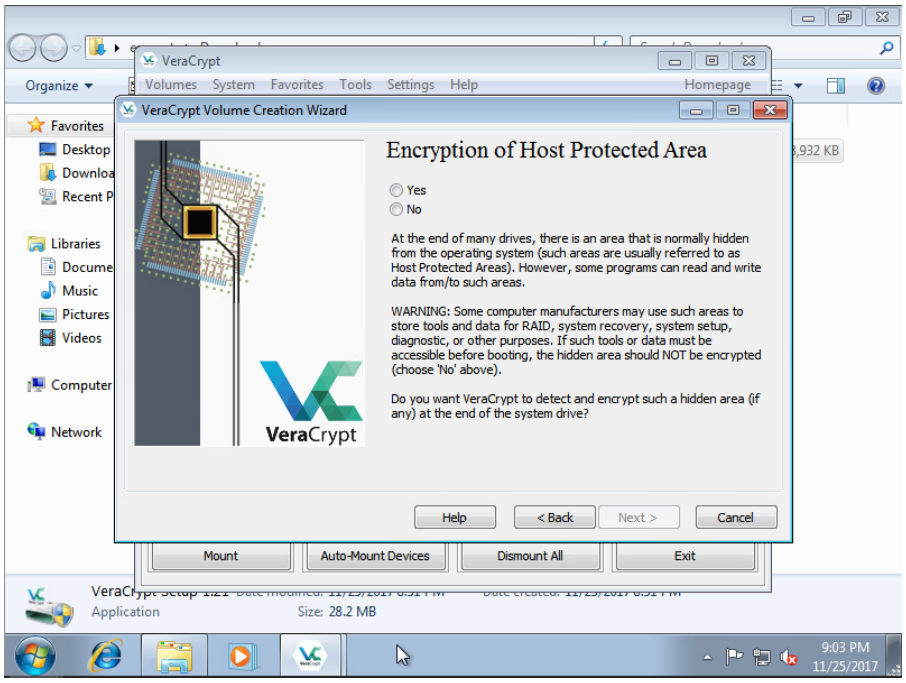
Korak 8:

Preporuča se odabir tipa šifriranja *Normal*. Za napredne korisnike moguće je odabrati *Hidden* kako bi se sakrila činjenica da je disk šifriran.



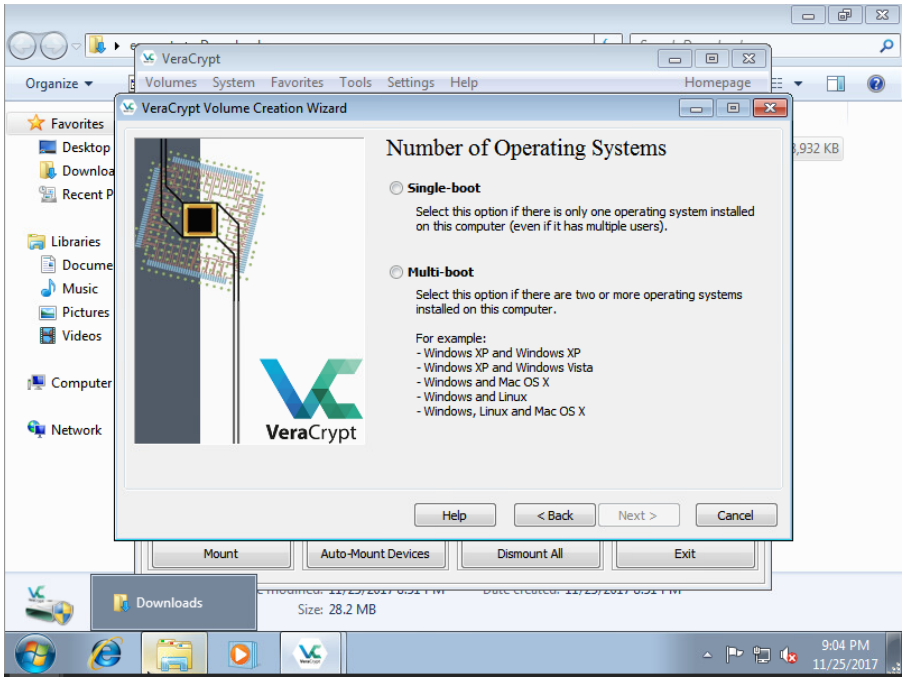
Korak 9:

Kako bi se šifrirao cijeli disk, potrebno je odabrati *Encrypt the whole drive*.



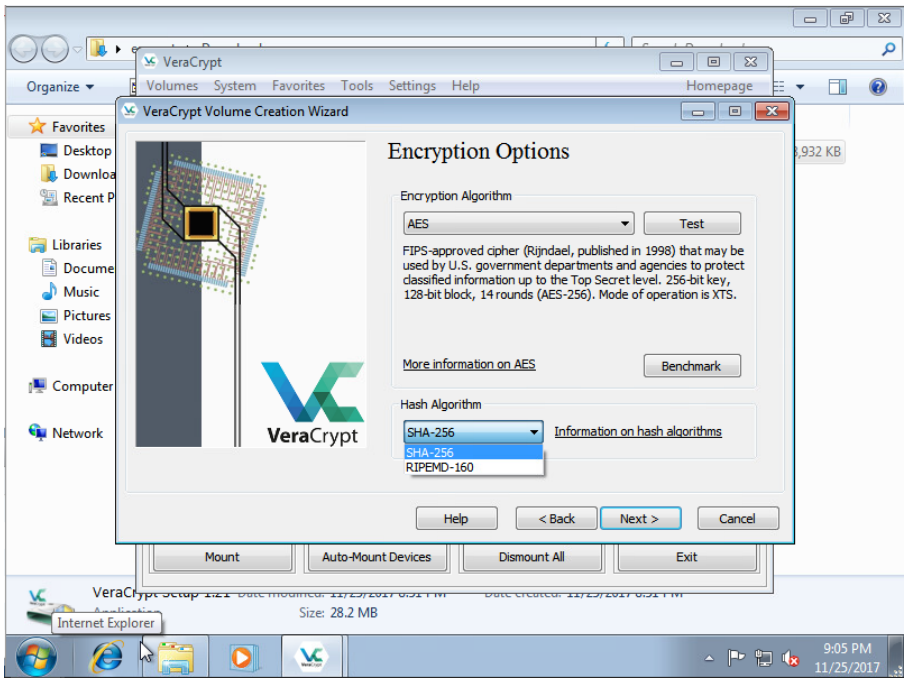
Korak 10:

Ovdje je potrebno odabrati *No* kako bi se izbjegao rizik kvarenja posebno prilagođenih instalacija.



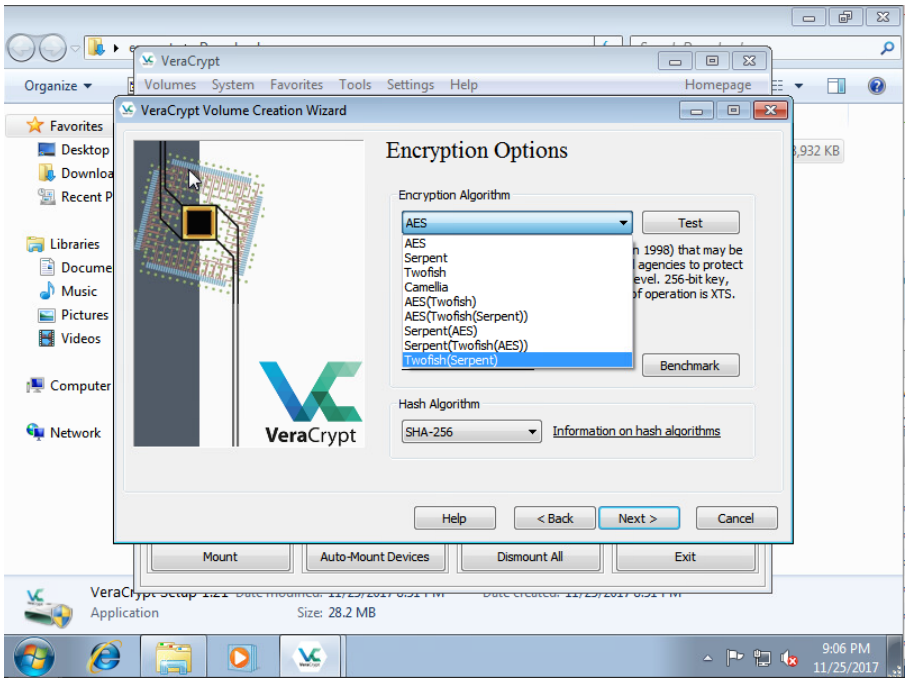
Korak 11:

Ovdje je u pravilu potrebno odabrati *Single-boot* osim ako korisnik nije instalirao više operacijskih sustava.



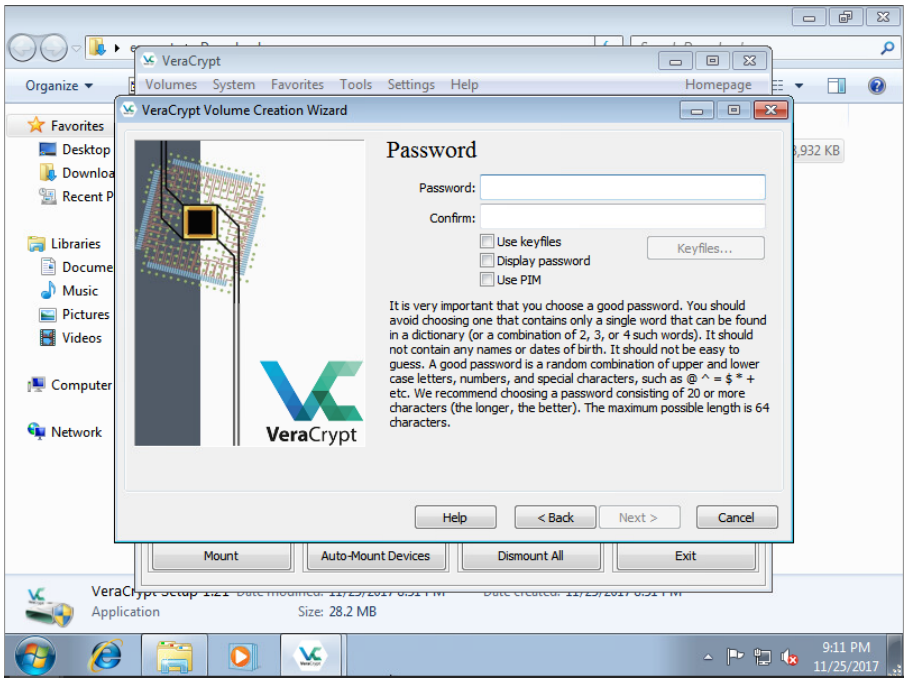
Korak 12:

Ovdje je moguće odabrati algoritam kriptografskog sažetka (eng. *cryptographic hash algorithm*). Preporuča se SHA-256 kao siguran algoritam.



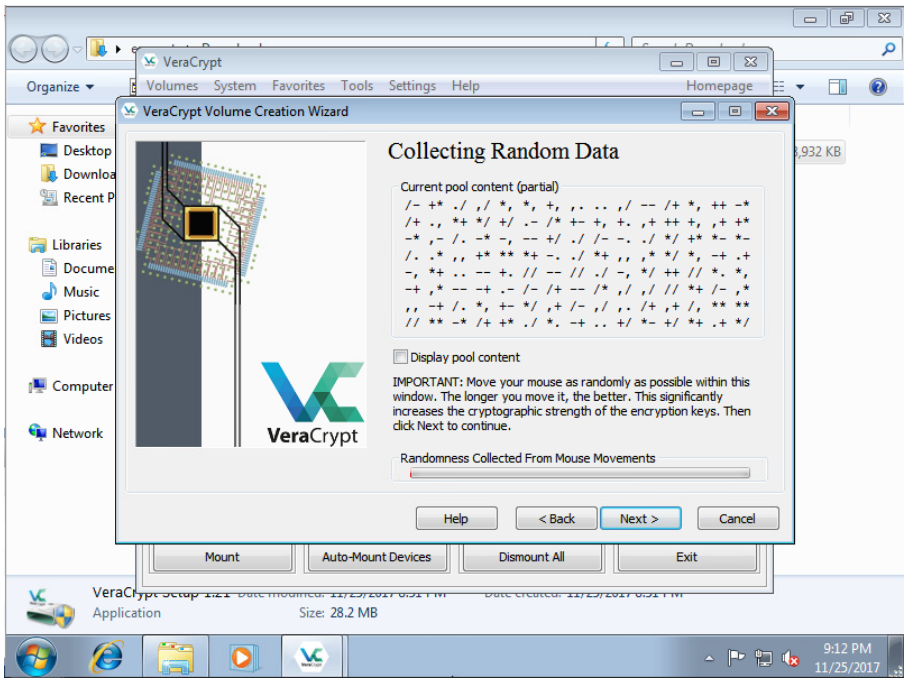
Korak 13:

Ovdje je moguće odabrati algoritam šifriranja. Preporuča se AES kao dobar kompromis sigurnosti i brzine.



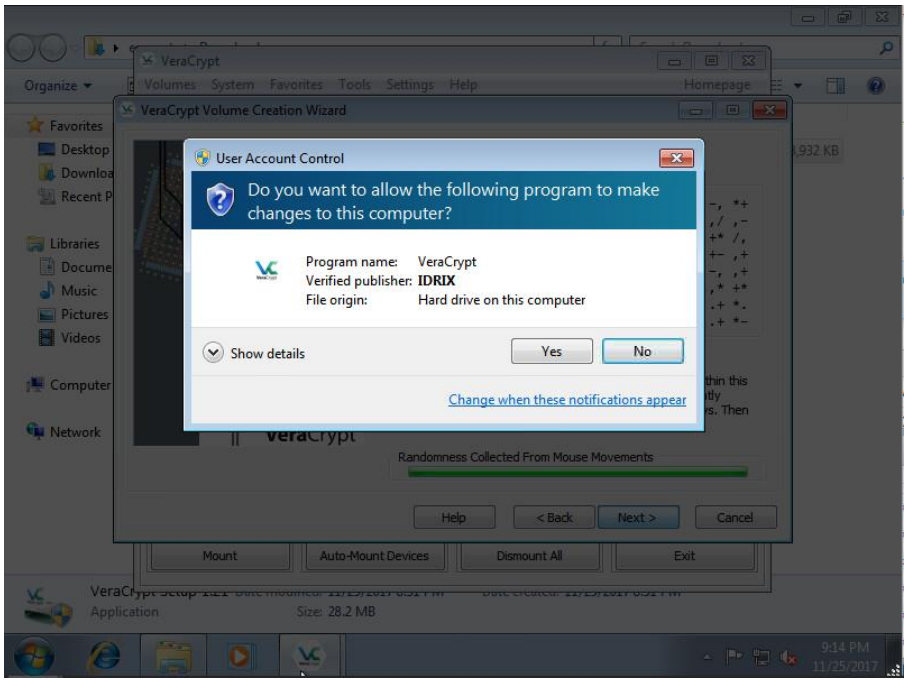
Korak 14:

Potrebno je upisati lozinku za otključavanje diska.



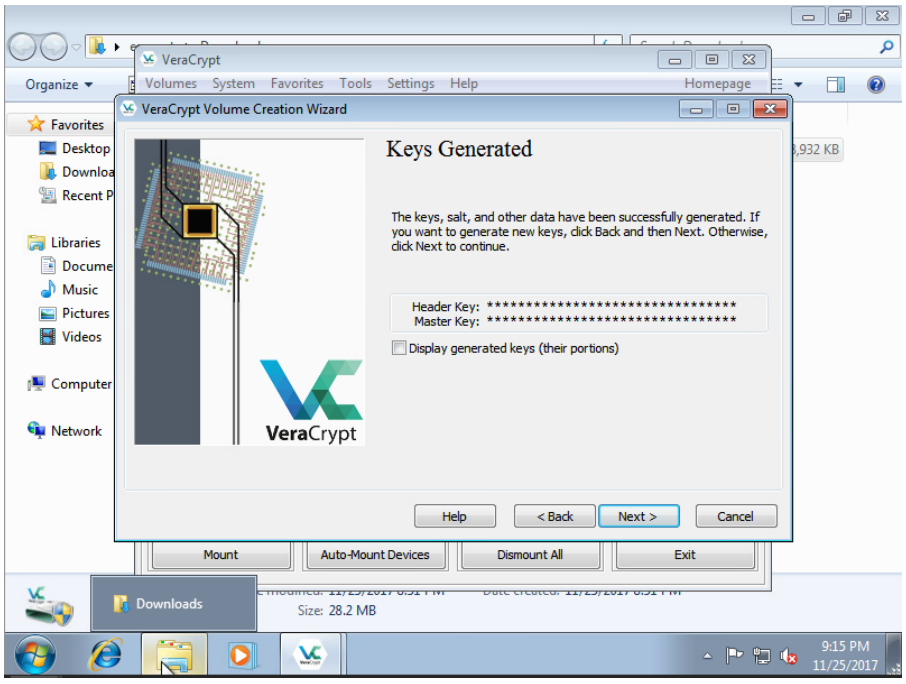
Korak 15:

U ovom koraku VeraCrypt generira kriptografske ključeve. Korisnik može nasumično pomicati pokazivač unutar prozora kako bi osigurao nasumično (pa tako i sigurno) generiranje ključeva.



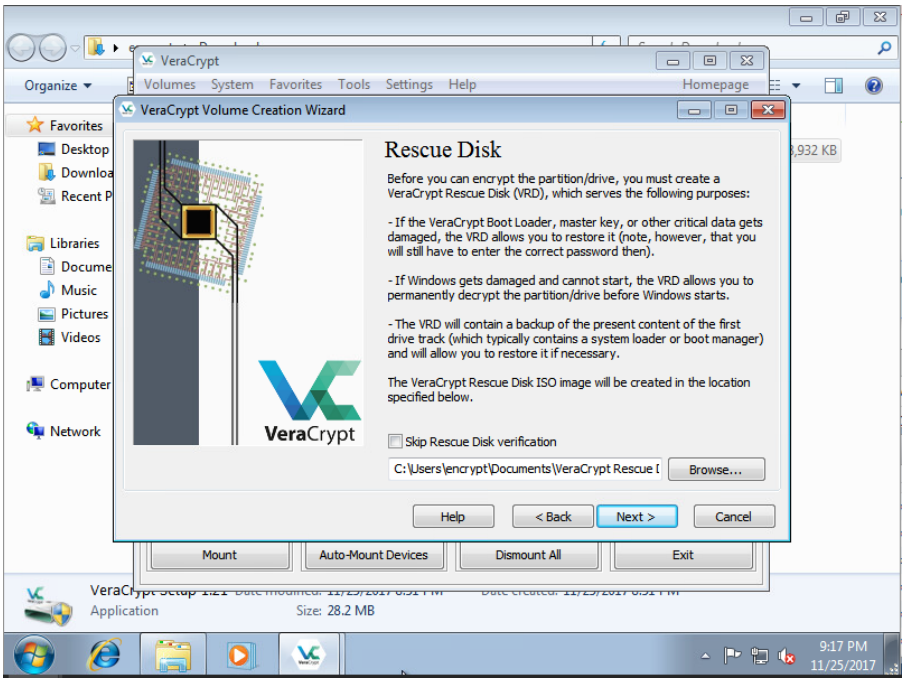
Korak 16:

Potrebno je dopustiti VeraCrypt-u da radi promjene na računalu.



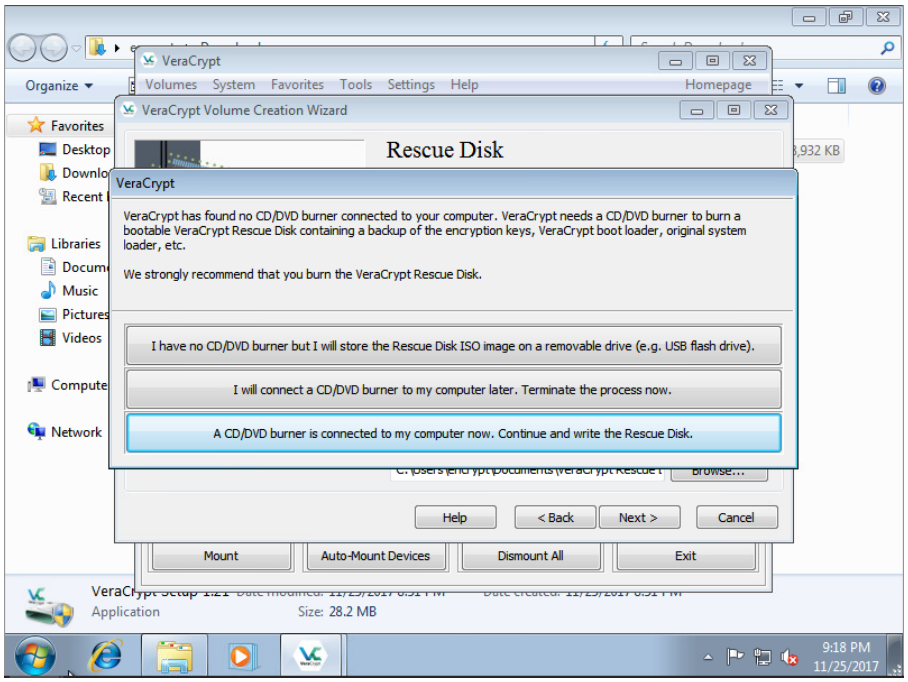
Korak 17:

Moguće je vidjeti dio generiranih ključeva, no to nema značajnu praktičnu vrijednost.



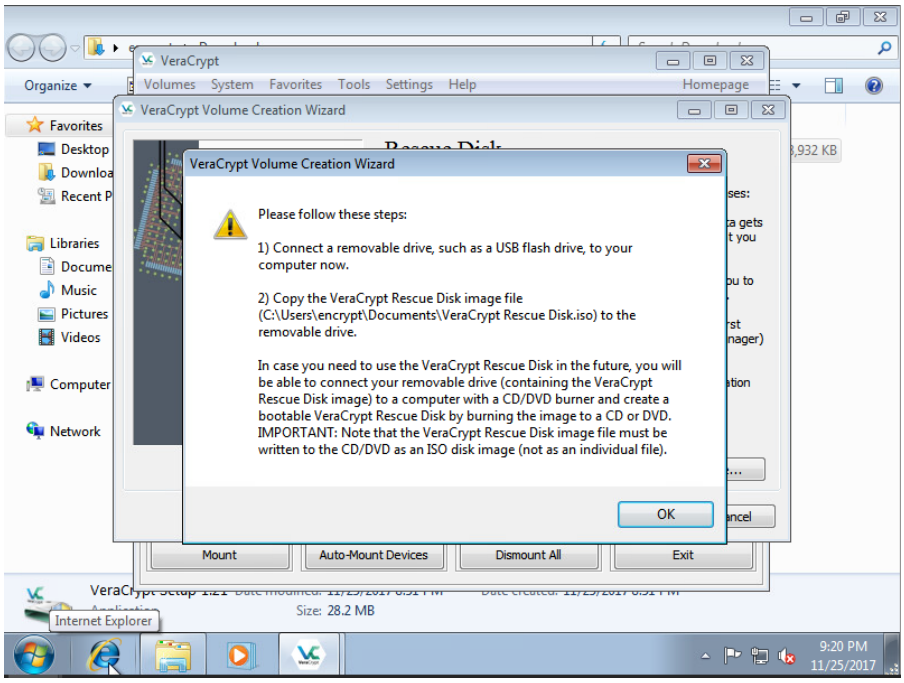
Korak 18:

Potrebno je negdje pohraniti VeraCrypt disk za obnovu podataka. Ako se određeni dio podataka na disku ošteti, ovaj disk će biti potreban za obnovu podataka.



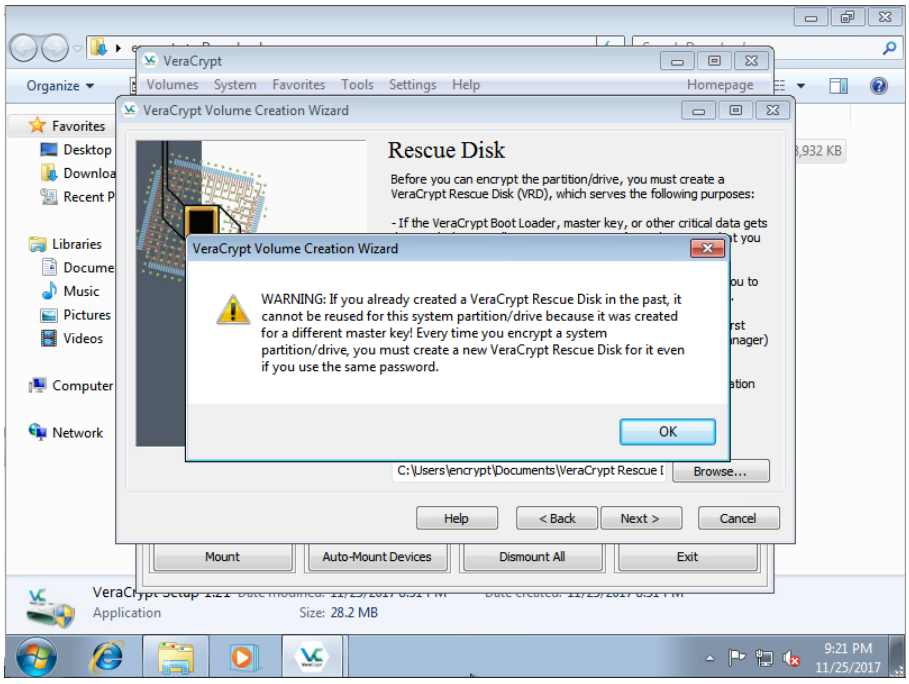
Korak 19:

Moguće je odmah generirati CD ili pohraniti sliku za kasniju upotrebu.



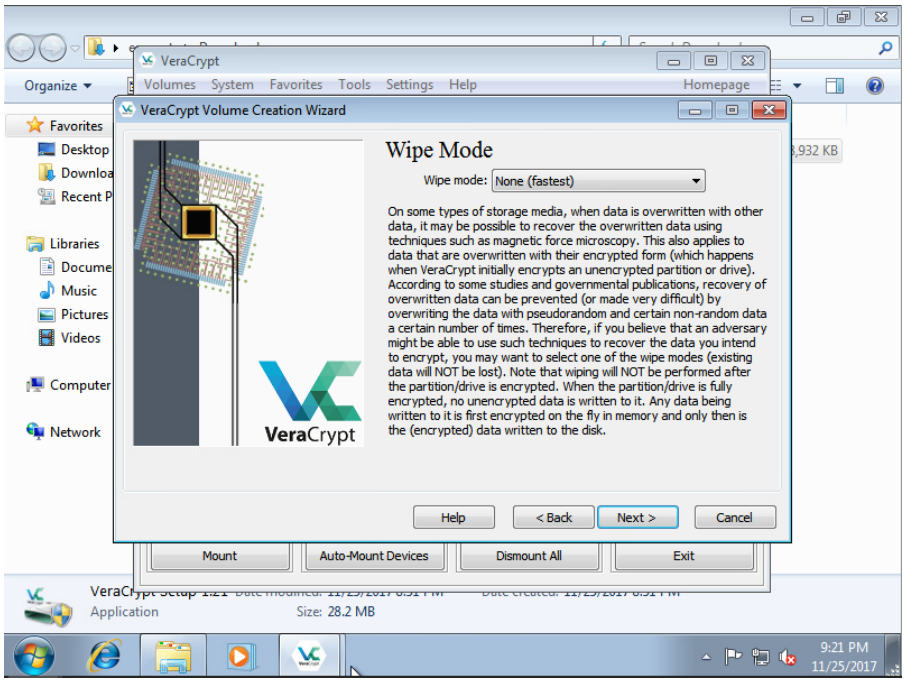
Korak 20:

Ispisan je dio uputa za korištenje diska za obnovu podataka.



Korak 21:

Za svaki šifrirani disk potrebno je napraviti novi disk za obnovu podataka.

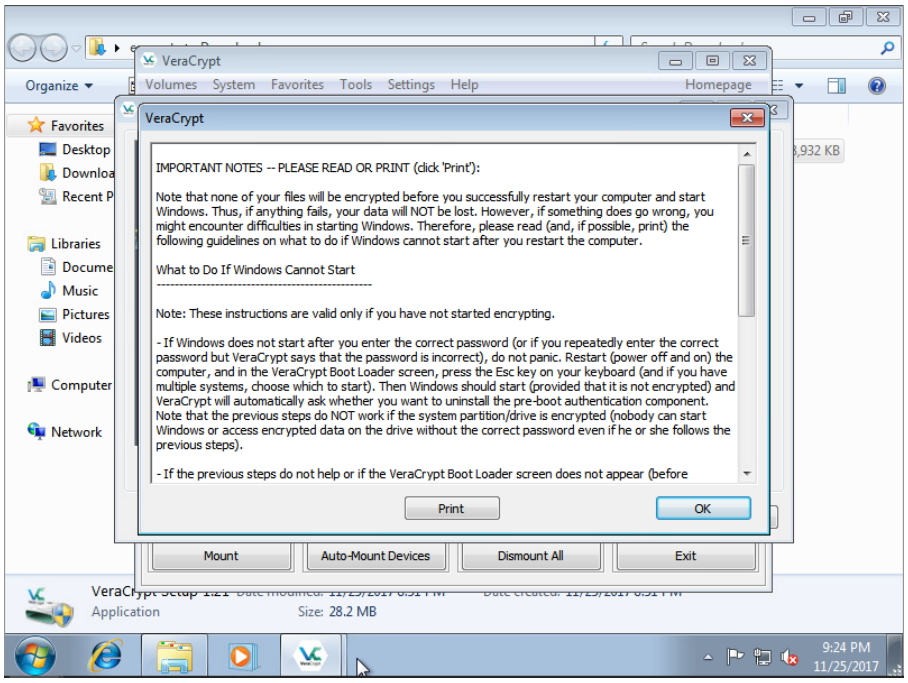


Korak 22:

Moguće je prepisati podatke prije šifriranja kako bi se otežala njihova rekonstrukcija. To u pravilu nije potrebno i većina korisnika će biti zadovoljna s opcijom *None (fastest)*.

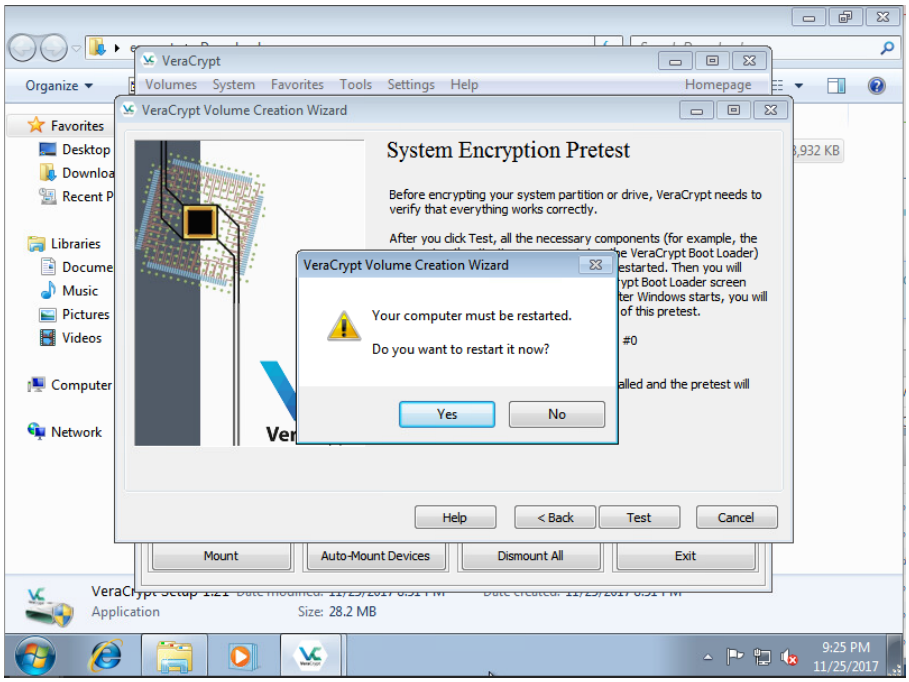
Korak 23:

U ovom trenutku će se obaviti test komponenti za šifriranje sustava.



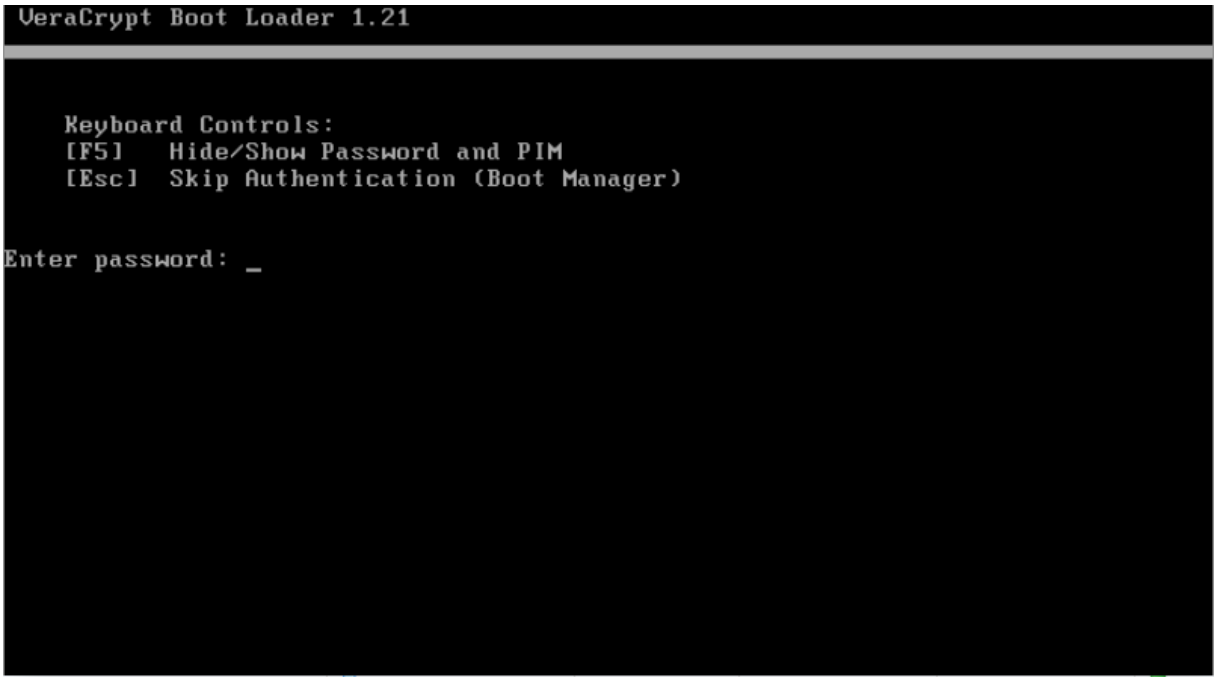
Korak 24:

Ispisane su upute koje je korisno pročitati za slučaj da test bude neuspješan i ne bude moguće uspješno pokrenuti računalo.



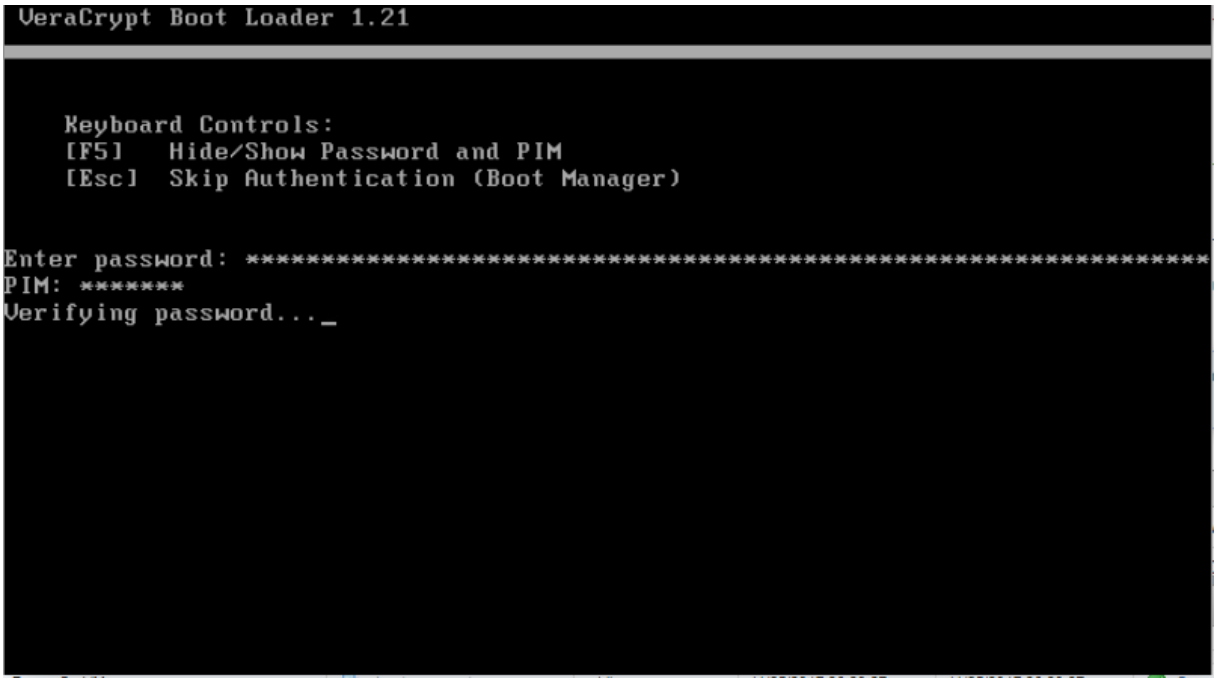
Korak 25:

Potrebno je odabrati *Yes* nakon čega se računalo ponovno pokreće čime započinje test.



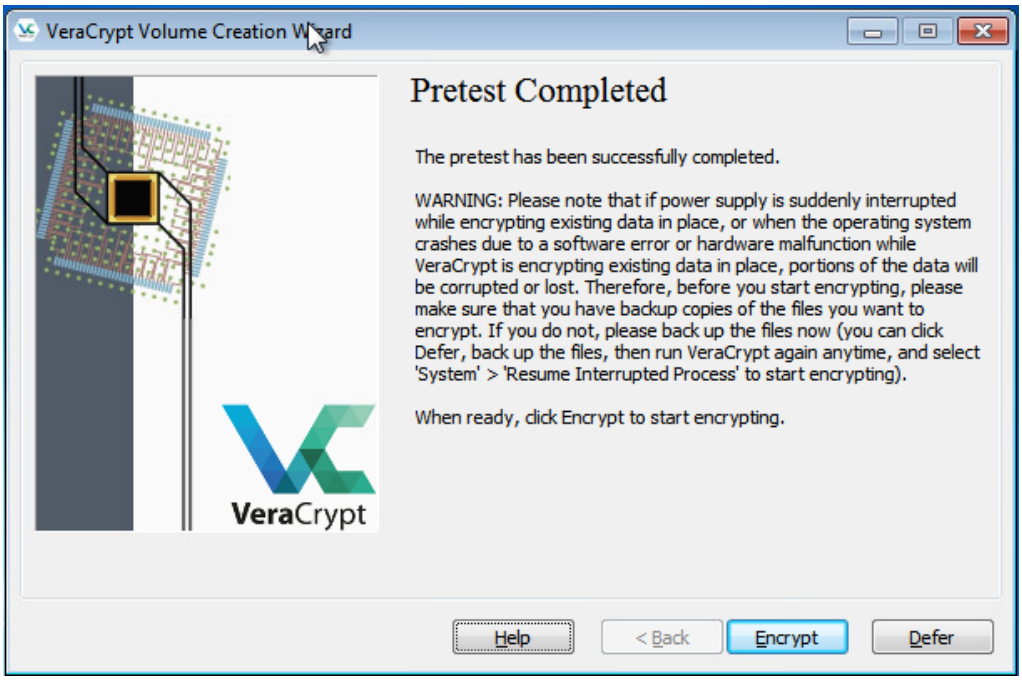
Korak 26:

Potrebno je upisati lozinku za otključavanje diska. Ukoliko je tražen i *PIM*, potrebno ga je ostaviti praznim (samo stisnuti tipku *Enter*).



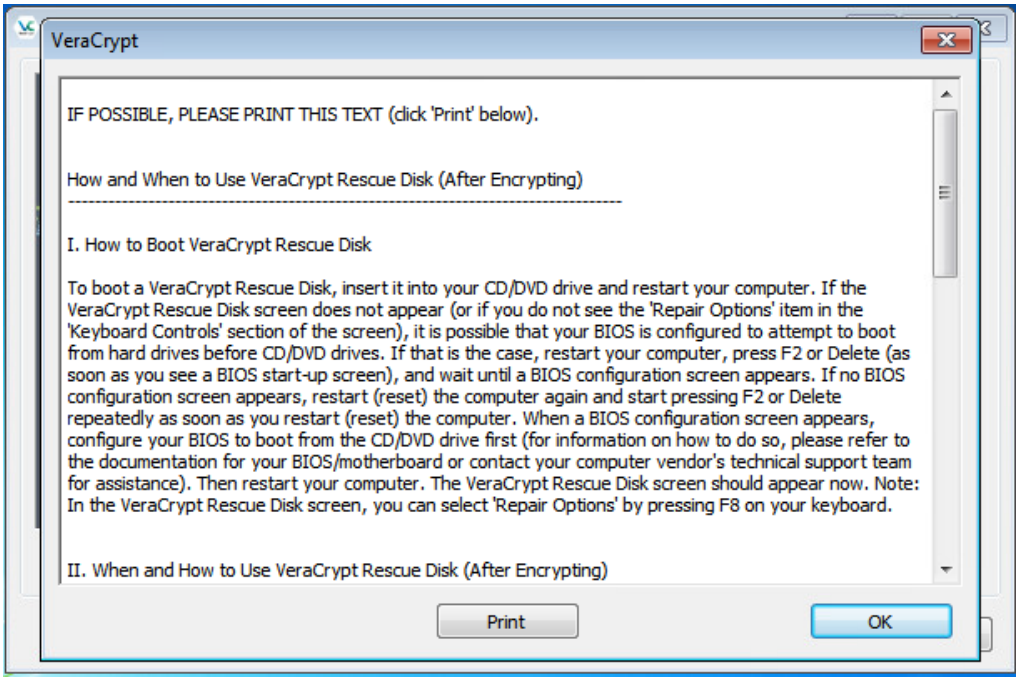
Korak 27:

U ovom koraku izvodi se ključ za šifriranje ključa (KEK) iz upisane lozinke te na sporijim računalima može potrajati dulje (do par minuta). Taj postupak će se izvoditi i prilikom svakog budućeg pokretanja računala, no on omogućava višu razinu sigurnosti od najčešćeg napada na šifrirani disk – napada grubom silom.



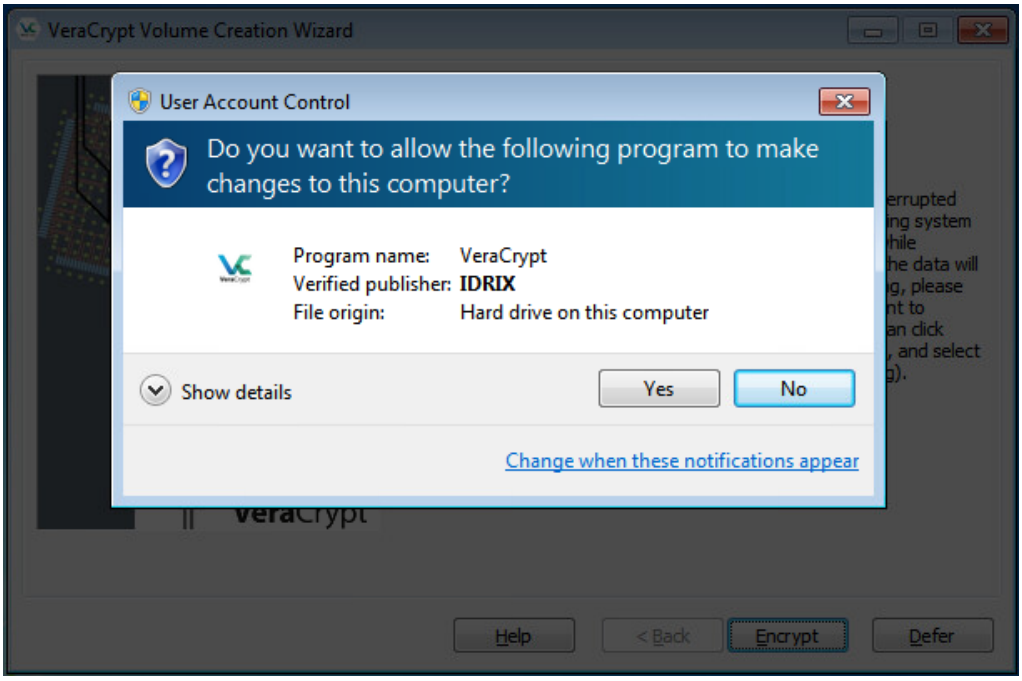
Korak 28:

Test je uspješan, pojavljuje se upozorenje koje preporuča stvaranje sigurnosne kopije podataka.



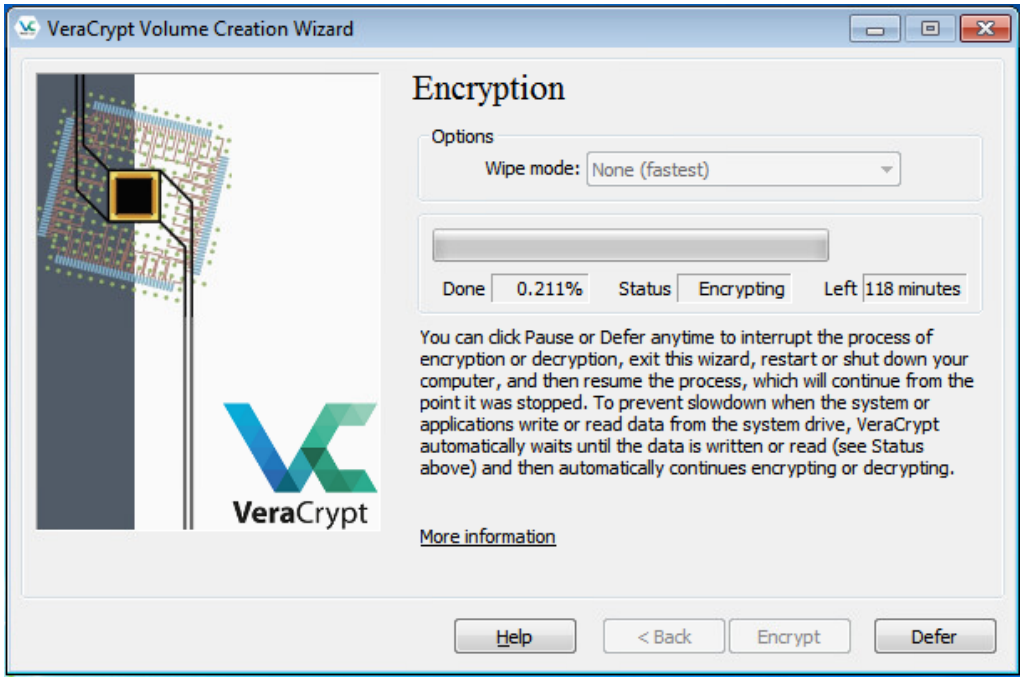
Korak 29:

Pojavljuju se i upute za korištenje diska za obnovu podataka koje je korisno imati ispisano.



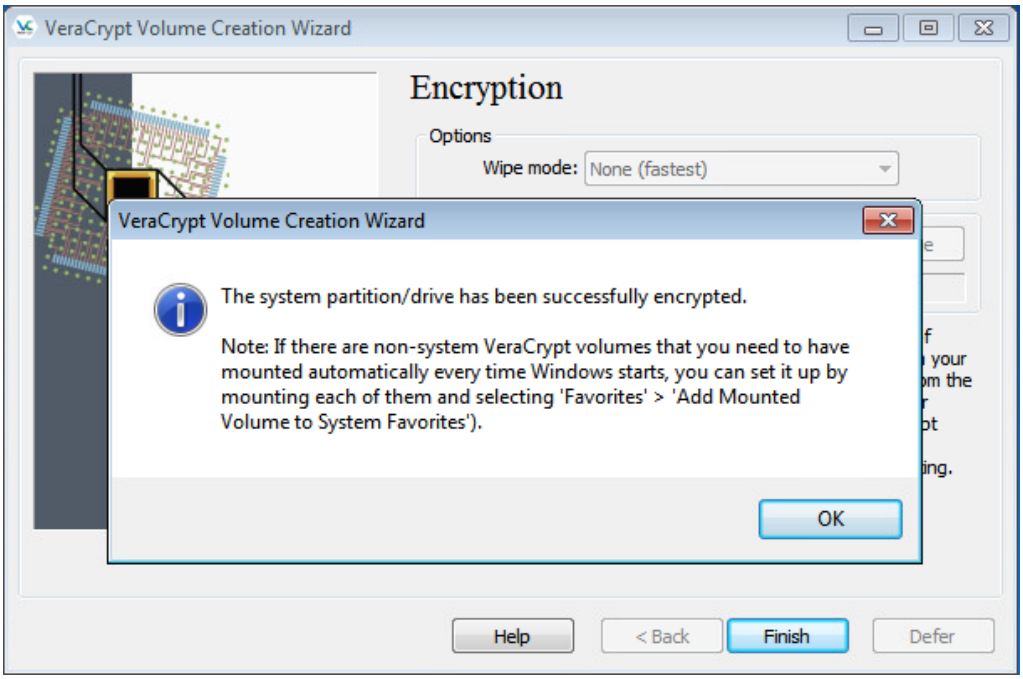
Korak 30:

Prije samog šifriranja, potrebno je VeraCrypt-u dopustiti da radi izmjene na računalu.



Korak 31:

Zatim počinje samo šifriranje diska.



Korak 32:

U konačnici pokazuje se sljedeći prozor i šifriranje je gotovo.