ლექცია 8

შიფრაცია, ფაილების შიფრაცია, დისკების შიფრაცია. შიფრები და ალგორითმები, მეთოდები, გასაღებები. პროგრამული პაკეტები. დისკების, ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt, მისი საშუალებით სხვადასხვა კომპონენტების დაშიფვრა და გახსნა. გასაღების შექმნა.

შიფრაცია, ფაილების შიფრაცია, დისკების შიფრაცია

ზოგადად დაშიფვრა არის ინფორმაციის ან მონაცემების კოდად გადაქცევის პროცესი, რათა თავიდან იქნას აცილებული არასანქცირებული წვდომა. ეს არის უსაფრთხოების ზომა, რომელიც გამოიყენება სენსიტიური მონაცემების წაკითხვისა და მის დასაცავად. დაშიფვრა მოიცავს ალგორითმებისა და გასაღებების გამოყენებას, რათა გარდაქმნას ჩვეულებრივი ტექსტი (წაკითხვადი მონაცემი) დაშიფრულ ტექსტად და პირიქით.

ფაილის დაშიფვრა და დისკის დაშიფვრა არის უსაფრთხოების ზომები, რომლებიც შექმნილია მონაცემების არაავტორიზებული წვდომისგან დასაცავად. ისინი ჩვეულებრივ გამოიყენება სენსიტიური ინფორმაციის კონფიდენციალურობისა და მთლიანობის უზრუნველსაყოფად.

შიფრაცია

ზოგადად დაშიფვრის ალგორითმები იყენებენ გასაღებს Key პარამეტრს. გასაღები აუცილებელია შიფრული ტექსტის ხელახლა გაშიფვრისთვის უბრალო ტექსტად. გასაღებზე დაფუძნებული დაშიფვრის ორი ძირითადი ტიპი არსებობს: სიმეტრიული და ასიმეტრიული.

- **სიმეტრიული დაშიფვრა:** იყენებს ერთსა და იმავე გასაღებს როგორც დაშიფვრისთვის, ასევე გაშიფვრისთვის. ეს უფრო სწრაფია, მაგრამ მოითხოვს გასაღების გაცვლის უსაფრთხო მეთოდებს.

- **ასიმეტრიული დაშიფვრა:** მოიცავს საჯარო და კერძო გასაღებების წყვილს. საჯარო გასაღები გამოიყენება დაშიფვრისთვის, ხოლო კერძო გასაღები გამოიყენება გაშიფვრისთვის. ეს მეთოდი ხშირად გამოიყენება უსაფრთხო კომუნიკაციისა და გასაღების განაწილებისთვის.

ფაილების შიფრაცია

ფაილის დაშიფვრა უსაფრთხოების ერთ-ერთი ყველაზე ეფექტური გადაწყვეტაა. უსაფრთხოების მოწინავე კონტროლთან ერთად, ის უზრუნველყოფს თქვენს ბიზნესს მონაცემთა ყოვლისმომცველ დაცვას, რათა შემდგომ გაშიფროს მასში არსებული ინფორმაცია.

ფაილის დაშიფვრა არის ფაილების კოდირების გზა, მათ შორის მგრძნობიარე მონაცემების ჩათვლით, მათი უსაფრთხოდ გაგზავნის მიზნით. კოდირება ხელს უშლის არასანქცირებულ წვდომას და მავნე ფაქტორების ხელყოფას. ის იცავს ფაილს უცხო პირის მიერ წაკითხვისგან, გარდა იმ ადამიანებისა, თუ ვისთვისაც ის იყო განკუთვნილი.

დისკების შიფრაცია

დისკის დაშიფვრა არის ტექნოლოგია, რომელიც იცავს ინფორმაციას კოდად გარდაქმნით, რომლის გაშიფვრა შეუძლებელია არაავტორიზებული ადამიანების მიერ. დისკის დაშიფვრა იყენებს დისკის დაშიფვრის პროგრამულ უზრუნველყოფას ან აპარატურას, რათა დაშიფროს ყველა ბიტი მონაცემი, რომელიც მიდის დისკზე ან დისკის მოცულობაზე. იგი გამოიყენება მონაცემთა შენახვაზე არაავტორიზებული წვდომის თავიდან ასაცილებლად.

სრული დისკის დაშიფვრა - Full Disk Encryption (FDE) (ან მთლიანი დისკის დაშიფვრა) ნიშნავს, რომ დისკზე ყველაფერი დაშიფრულია. ზოგიერთი აპარატურაზე დაფუძნებული სრული დისკის დაშიფვრის სისტემას შეუძლია ბოლომდე დაშიფროს მთელი ჩატვირთვის დისკი, მათ შორის MBR ტიპის დისკები.

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

TrueCrypt – ეს არის ფუნქციური პროგრამული უზრუნველყოფა. მას შეუძლია შექმნას ვირტუალური და დაშიფრული დისკები, რომელიც გამოყენებული იქნება მომხმარებლის სისტემაში. TrueCrypt საშუალებას აძლევს მომხმარებლებს შექმნას უსაფრთხო დანაყოფი, მას ასევე შეუძლია მყარი დისკების დაშიფვრა, ფლეშ დრაივების, მეხსიერების ბარათების და სხვა მოწყობილობების. TrueCrypt საშუალებას იძლევა მომხმარებელმა დაშიფროს თითოეული ფაილი და თავისუფალი სივრცის გამოსაყოფად შექმნას სხვადასხვა შიფრირების ალგორითმები.

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

TrueCrypt ის ძირითადი მახასიათებლები:

- მუშაობს Windows (10/8/7 / Vista / XP), Mac და Linux ოპერაციულ სისტემაზე;
- ვირტუალური დისკის დრაივებზე მონაცემების შიფრაცია;
- მომხმარებელს შეუძლია გამოიყენოს პაროლი მეტი უსაფრთხოებისათვის;
- მხარს უჭერს AES, Serpent და Twofish დაშიფვრის ალგორითმებს
- მასში ხელმისაწვდომია გაფართოებული პარამეტრები;
- TrueCrypt-ს აქვს შესაძლებლობა გააგრძელოს დაშიფვრის პროცესი მოგვიანებით.

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

გაითვალისწინეთ, რომ TrueCrypt არასოდეს ინახავს გაშიფრულ მონაცემებს დისკზე - ის მხოლოდ დროებით ინახავს მათ RAM-ში (მეხსიერებაში). მაშინაც კი, როდესაც მოცულობა დამონტაჟებულია, ან მაშინ როდესაც ტომში შენახული მონაცემები კვლავ დაშიფრულია.

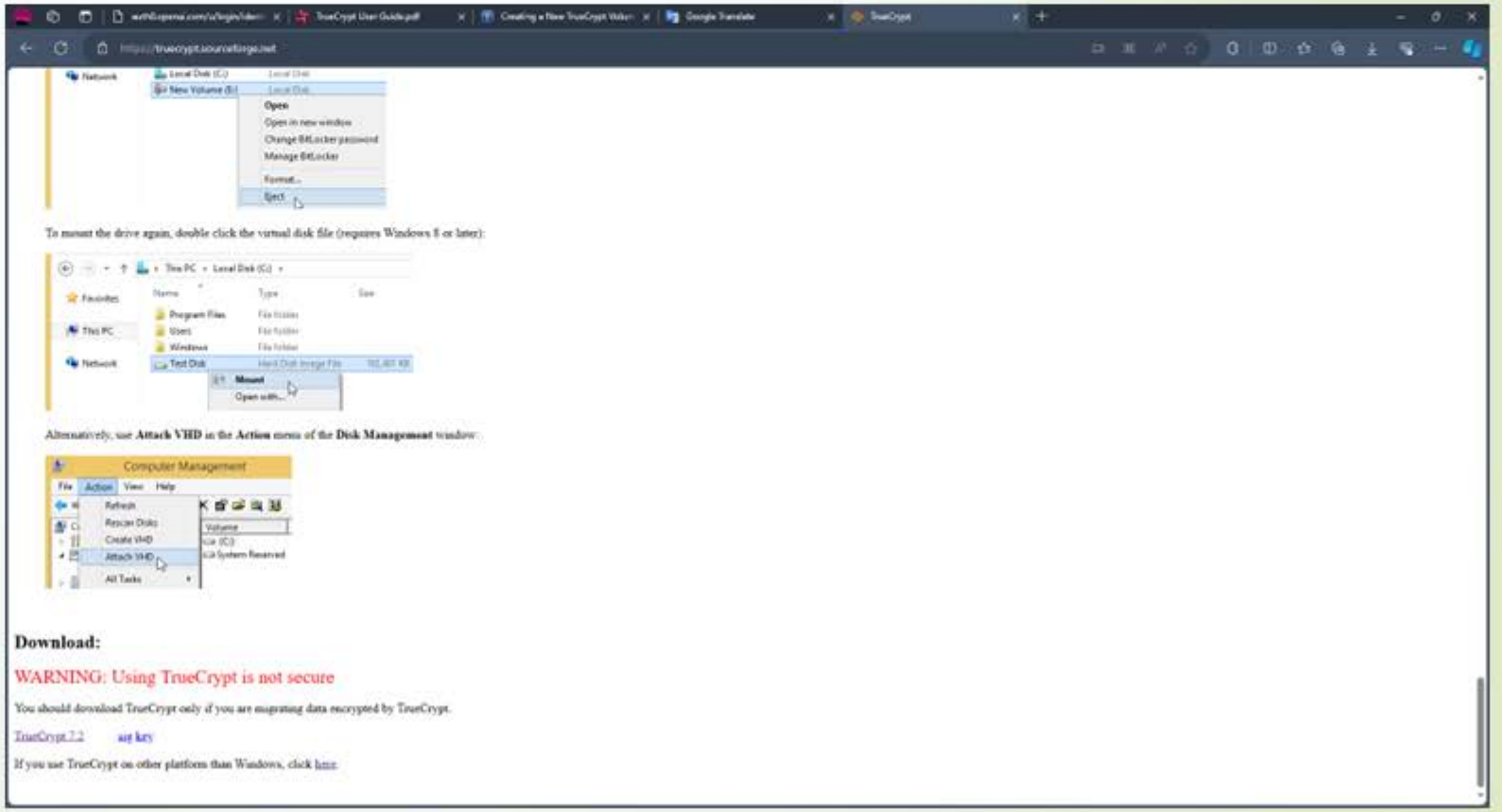
მისი გამოყენებით როდესაც მომხმარებელი გადატვირთავს Windows-ს ან გამორთავს კომპიუტერს, მოცულობა დაიშლება და მასში შენახული ფაილები მიუწვდომელი (და დაშიფრული) იქნება. მაშინაც კი, როდესაც ელექტროენერგიის მიწოდება მოულოდნელად გაწყდება (სისტემის სათანადო გამორთვის გარეშე), მოცულობაში შენახული ფაილები მიუწვდომელი გახდება. ამისათვის მომხმარებელმა უნდა დააგენერიროს გასაღები ან დააყენოს პაროლი რომლის საშუალებითაც ექნება ამ ინფორმაციაზე წვდომა.

TrueCrypt 7.2-ის გადმოწერა

TrueCrypt 7.2-ი ვერსიის გადმოწერა შესაძლებელია TrueCrypt.sourceforge.net - ვებ გვერდიდან.

ქვემოთ მოცემულია TrueCrypt-ის საბოლოო ვერსია, რომელზე დაკლიკვისას მომხმარებელი გადმოიწერს 7.2 ვერსიას. თუმცა უნდა აღინიშნოს, რომ ეს ვერსია ბოლომდე არ არის გახსნილი და ფუნქციური windows10 -ის მომხმარებლებისთვის;

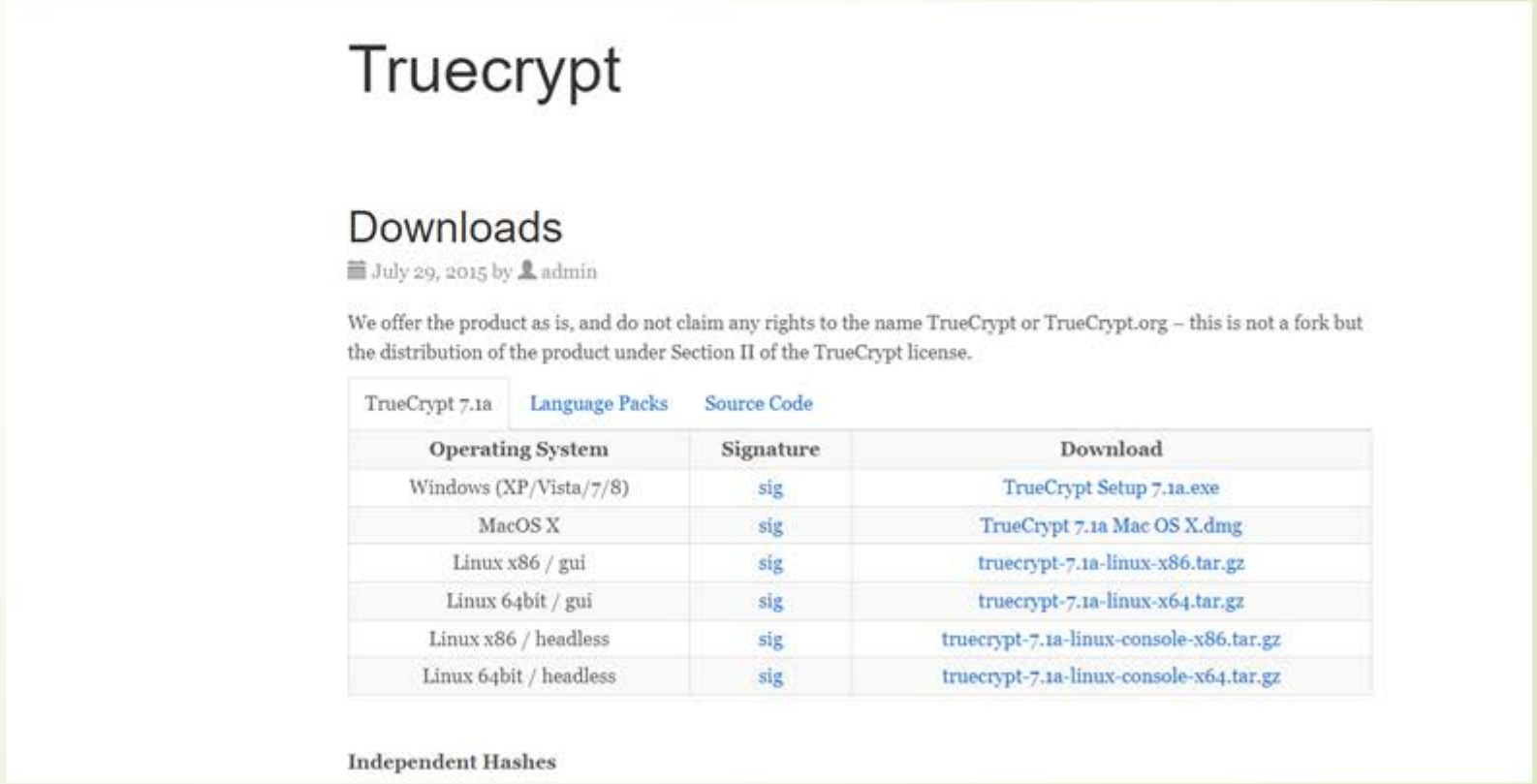
ამისათვის უმჯობესია მომხმარებელმა გადმოიწეროს მისი წინა ვერსია -TrueCrypt7.1a



TrueCrypt 7.1a-ის გადმოწერა

TrueCrypt 7.1a-ი ვერსიის გადმოწერა შესაძლებელია www.TrueCrypt71a.com - ვებ გვერდიდან.

ქვემოთ მოცემულია TrueCrypt-ის ვერსია, რომელიც მორგებულია ვინდოუსის ოპერაციულ სისტემაზე და მისი გამოყენებით მომხმარებელს შეუძლია მასში არსებული ყველა ფუნქციის გამოყენება.



Truecrypt

Downloads

July 29, 2015 by admin

We offer the product as is, and do not claim any rights to the name TrueCrypt or TrueCrypt.org – this is not a fork but the distribution of the product under Section II of the TrueCrypt license.

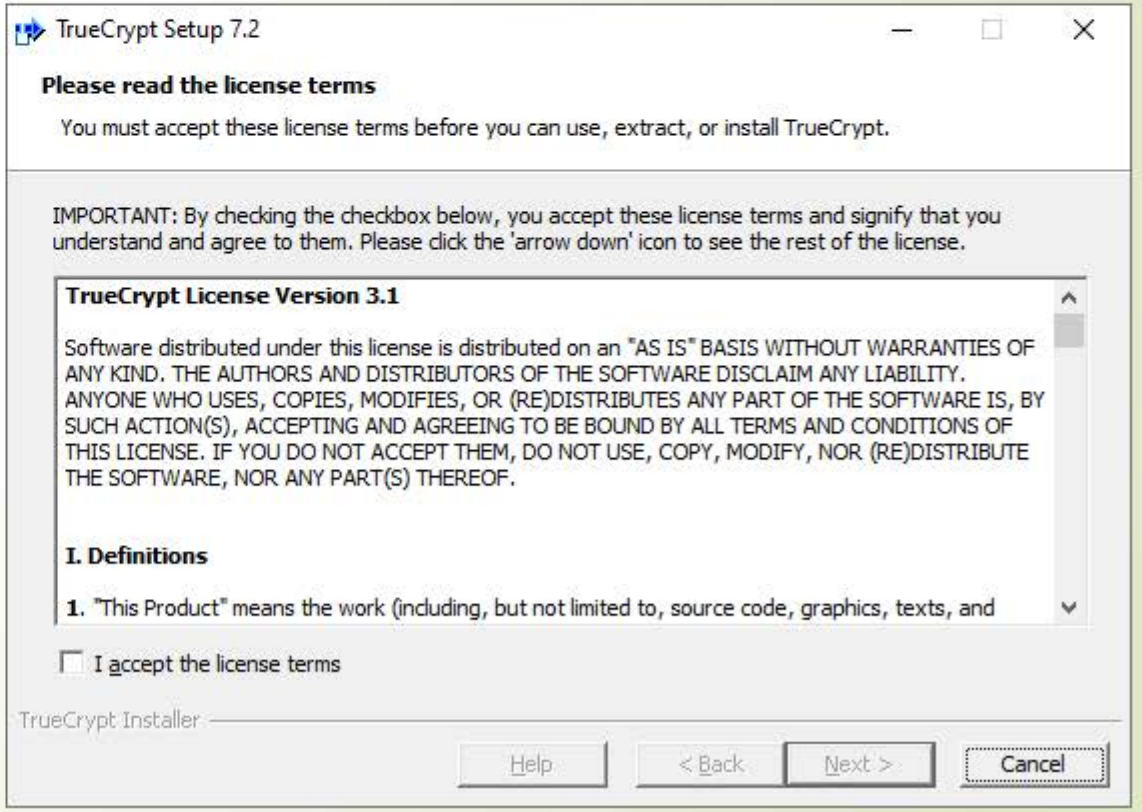
TrueCrypt 7.1a | Language Packs | Source Code

Operating System	Signature	Download
Windows (XP/Vista/7/8)	sig	TrueCrypt Setup 7.1a.exe
MacOS X	sig	TrueCrypt 7.1a Mac OS X.dmg
Linux x86 / gui	sig	truecrypt-7.1a-linux-x86.tar.gz
Linux 64bit / gui	sig	truecrypt-7.1a-linux-x64.tar.gz
Linux x86 / headless	sig	truecrypt-7.1a-linux-console-x86.tar.gz
Linux 64bit / headless	sig	truecrypt-7.1a-linux-console-x64.tar.gz

Independent Hashes

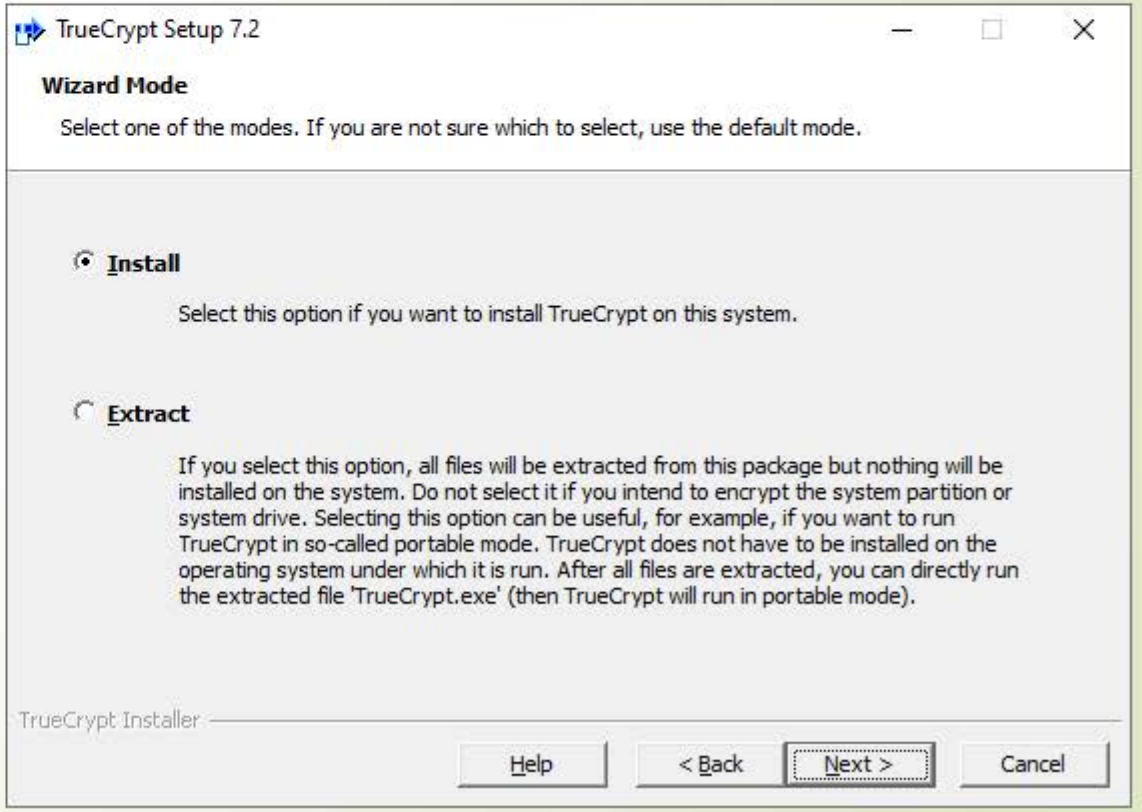
TrueCrypt-ის ინსტალაცია

პროგრამის ინსატალაციისას მომხმარებელი ეთანხმება მის წესებს და პირობებს, Next-ღილაკით კი გადადის შემდეგ ეტაპზე.



TrueCrypt-ის ინსტალაცია

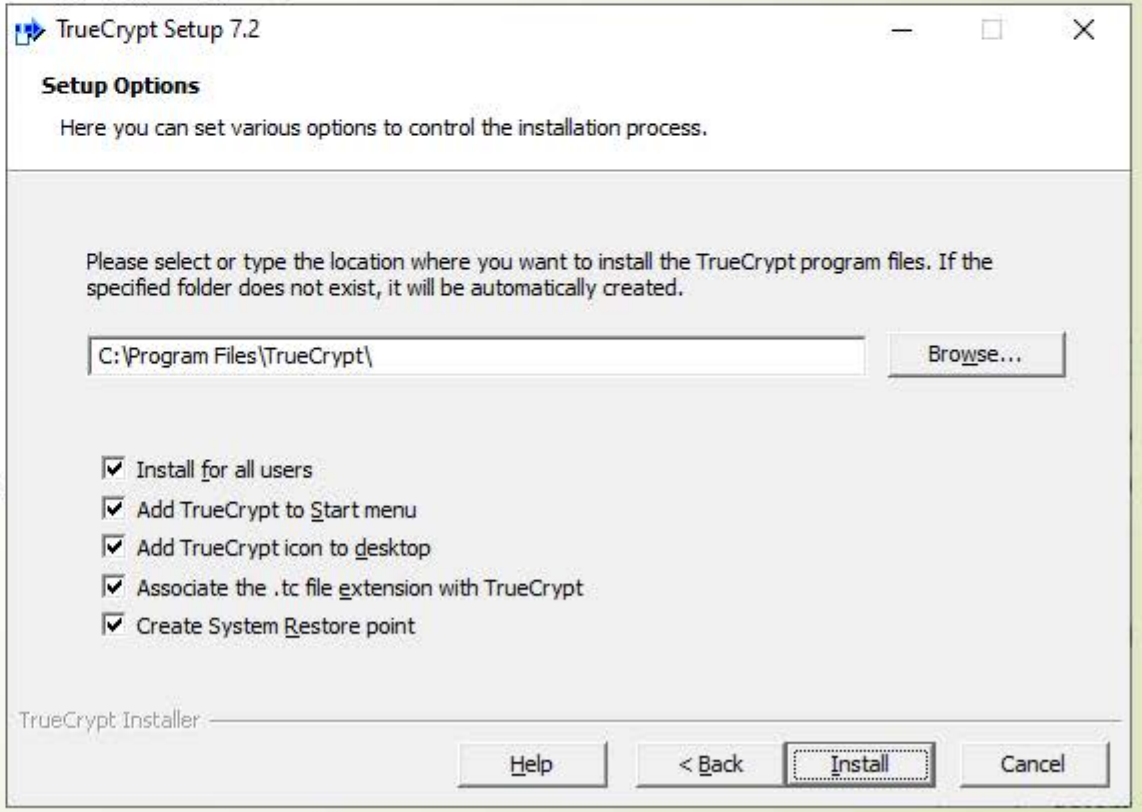
იმ შემთხვევაში თუ მომხმარებელს სურს პროგრამის ინსტალაცია მის კომპიუტერში, მან უნდა აირჩიოს Install ღილაკი. ხოლო თუ იგი მონიშნავს Extract ღილაკს, ყველა ფაილი დაექსტრაქტდება ამ პაკეტიდან თუმცა პროგრამა არ დაინსტალირდება. მისი დაინსტალირებისას პროგრამა პორტატულ რეჟიმში იმუშავებს.



TrueCrypt-ის ინსტალაცია

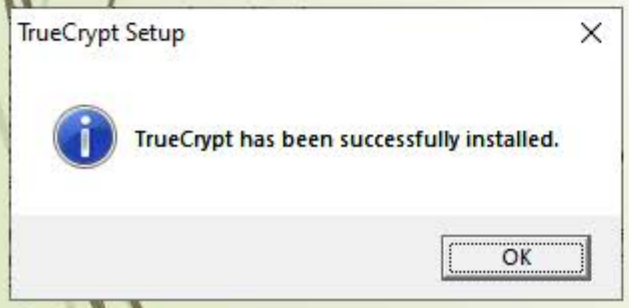
Browse-ღილაკით მომხმარებელი ირჩევს ადგილს თუ რომელ ფაილში უნდა დაამახსოვროს პროგრამა.

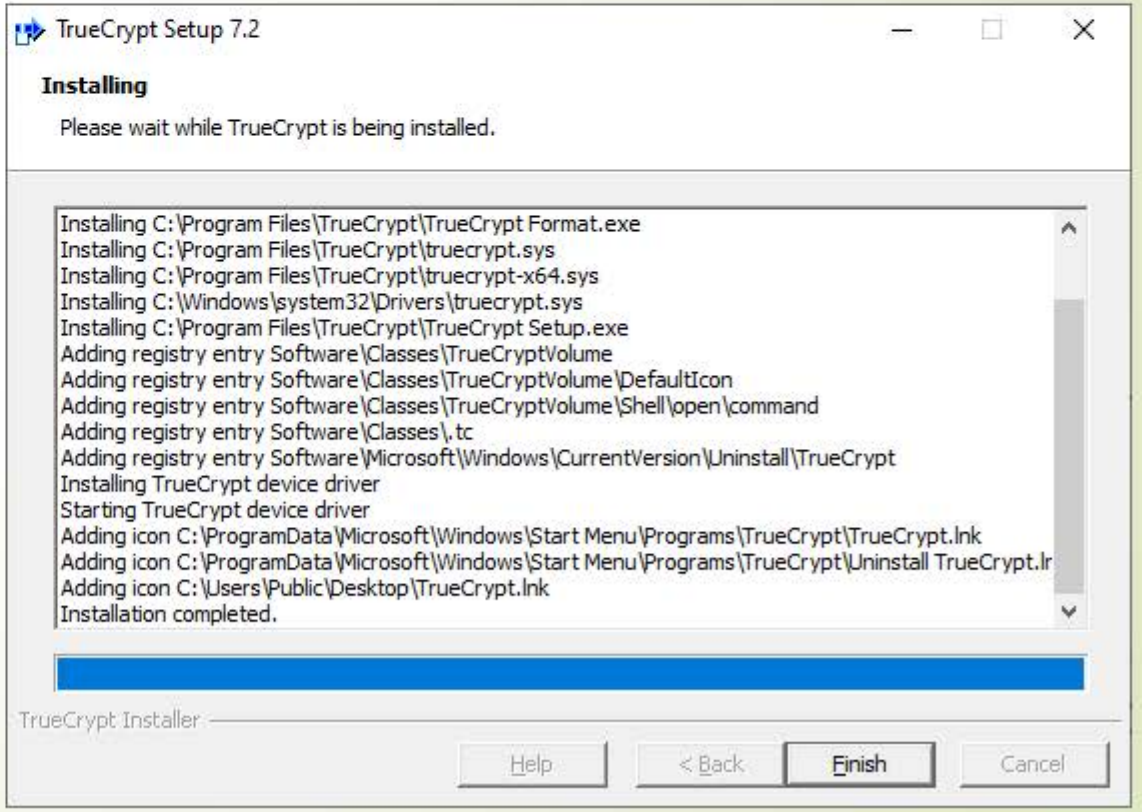
- Install for all users – ყველა მომხმარებლისთვის დაინსტალირება;
- Add TrueCrypt to Start Menu - პროგრამის სტარტ მენიუში დამატება;
- Add TrueCrypt icon to desktop - პროგრამის დესკტოპზე გამოჩენა;
- Associate the .tc file extension with TrueCrypt – .tc გაფართოების ფაილების მხარდაჭერა;
- Create System Restore Point - სისტემის აღდგენის წერტილის შექმნა.



TrueCrypt-ის ინსტალაცია

Finish ღილაკზე დაჭერით სრულდება ინსტალაცია.

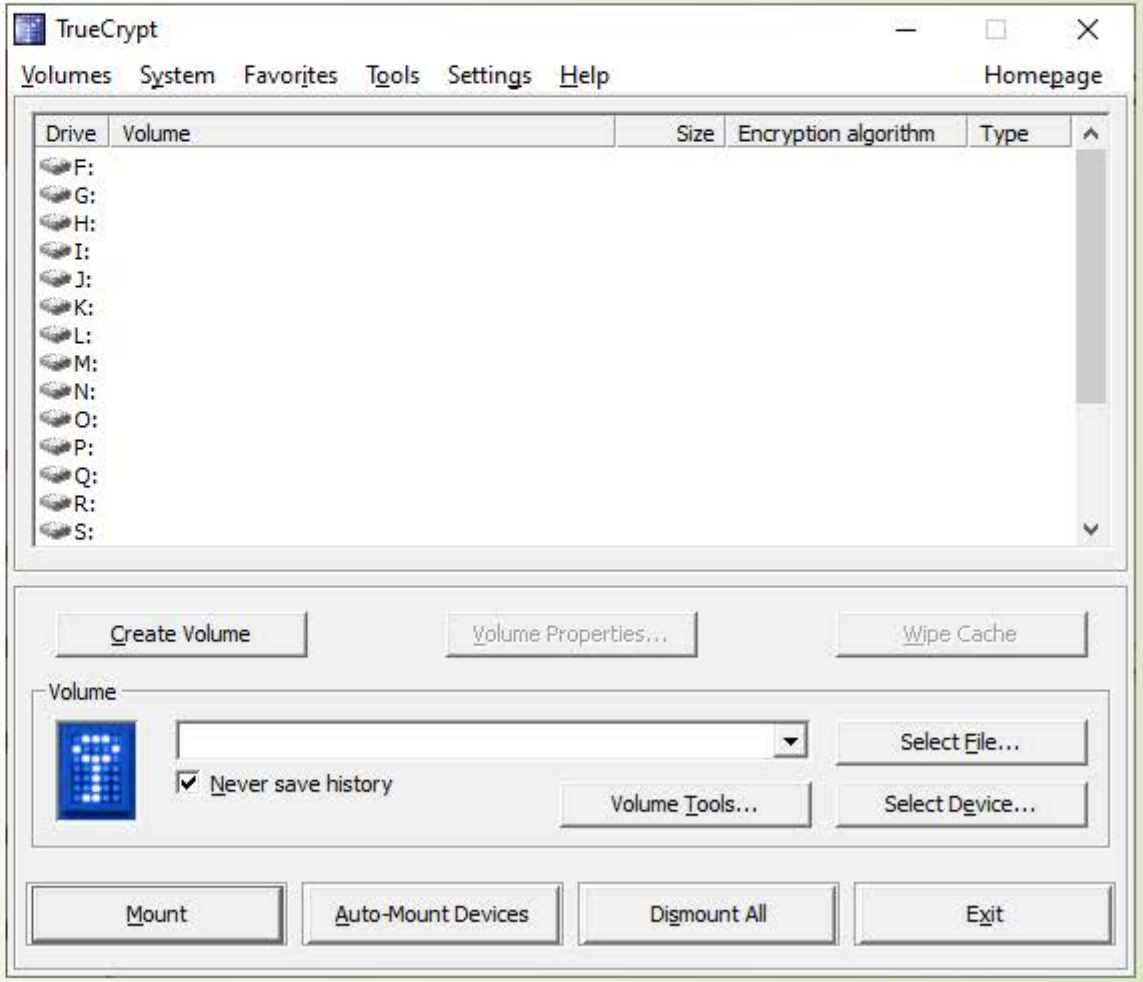




დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

მთავარ მენიუში ზემოთა მხარეს გვხვდება:

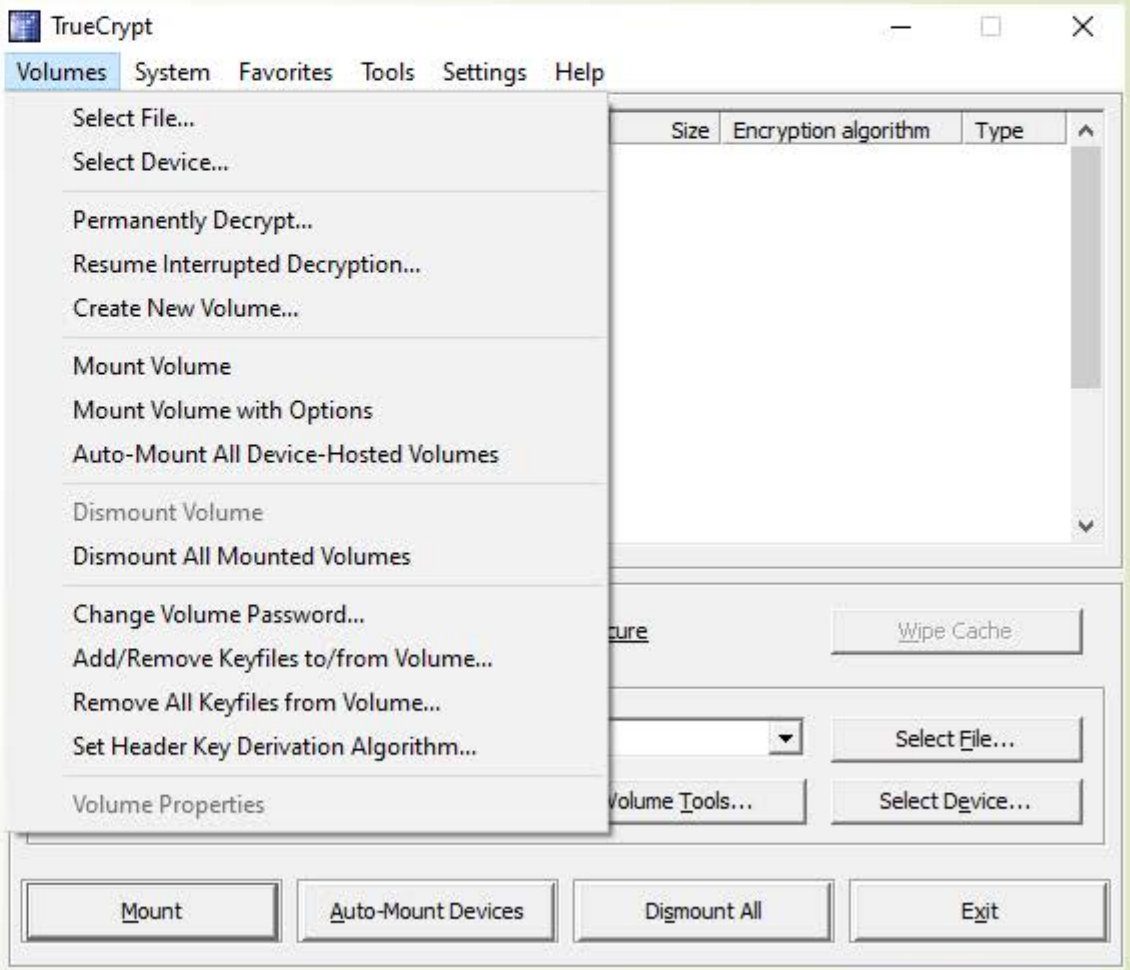
- Volumes - მეხსიერების ადგილი;
- System - სისტემა;
- Favorites - გამორჩეული მეხსიერების ადგილები;
- Tools - ხელსაწყოები;
- Settings - პარამეტრები;
- Help - დახმარება



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Volume-ს ჩამოწათვალში გვხვდება:

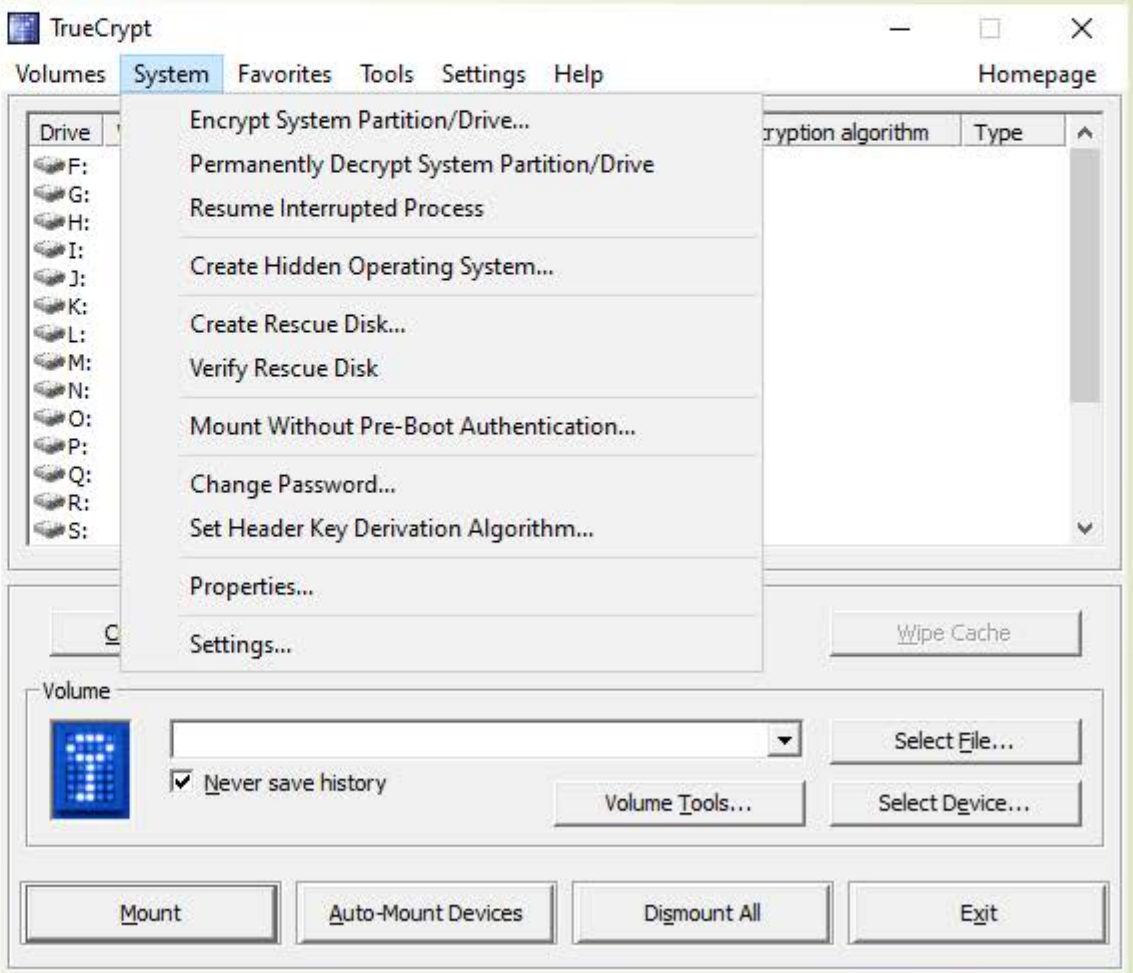
- ფაილის არჩევა;
- მოწყობილობის არჩევა;
- სამუდამოდ გაშიფვრა;
- შეწყვეტილი პროცესის გაგრძელება;
- ახალი მეხსიერების დაწაყოფის შექმნა;
- დაწაყოფის პროგრამაში მიმაგრება;
- დაწაყოფის პროგრამაში მიმაგრება სხვადასხვა პარამეტრებით;
- ყველა მოწყობილობის ავტომატურად მიმაგრება;
- მთელი მოცულობის დაშლა;
- მეხსიერების დაწაყოფის პაროლის შეცვლა;
- ყველა Keyfile-ბის წაშლა მეხსიერების დაწაყოფიდან;
- გასაღების ალგორითმის დამატება;
- დაწაყოფის მახასიათებლების დათვალიერება.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

System ჩამონათვალში გვხვდება:

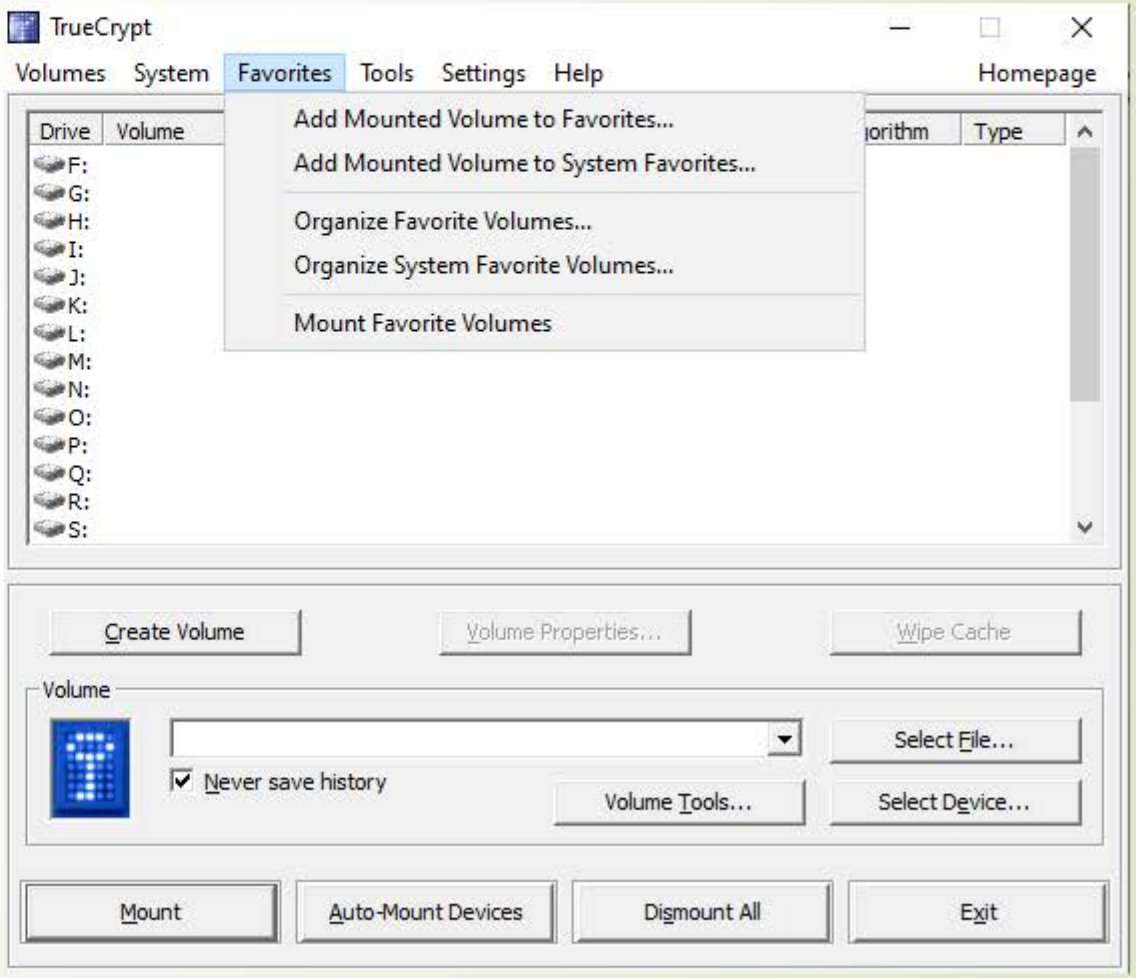
- დაწყოფის შიფრაცია;
- სისტემის დაწაყოფის სამუდამოდ გაშიფვრა;
- შეწყვეტილი პროცესის გაგრძელება;
- დამალული ოპეცაციული სისტემის შექმნა;
- სარეზერვო/სამაშველო დისკის შექმნა;
- დისკის ვერიფიკაცია;
- დამონტაჟება წინასწარ ჩატვირთვის ავთენტიფიკაციის გარეშე;
- პაროლის ცვლილება;
- გასაღების ალგორითმის დამატება;
- მახასიათებლების დათვალიერება;
- პარამეტრები.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Favorites ჩამონათვალში გვხვდება:

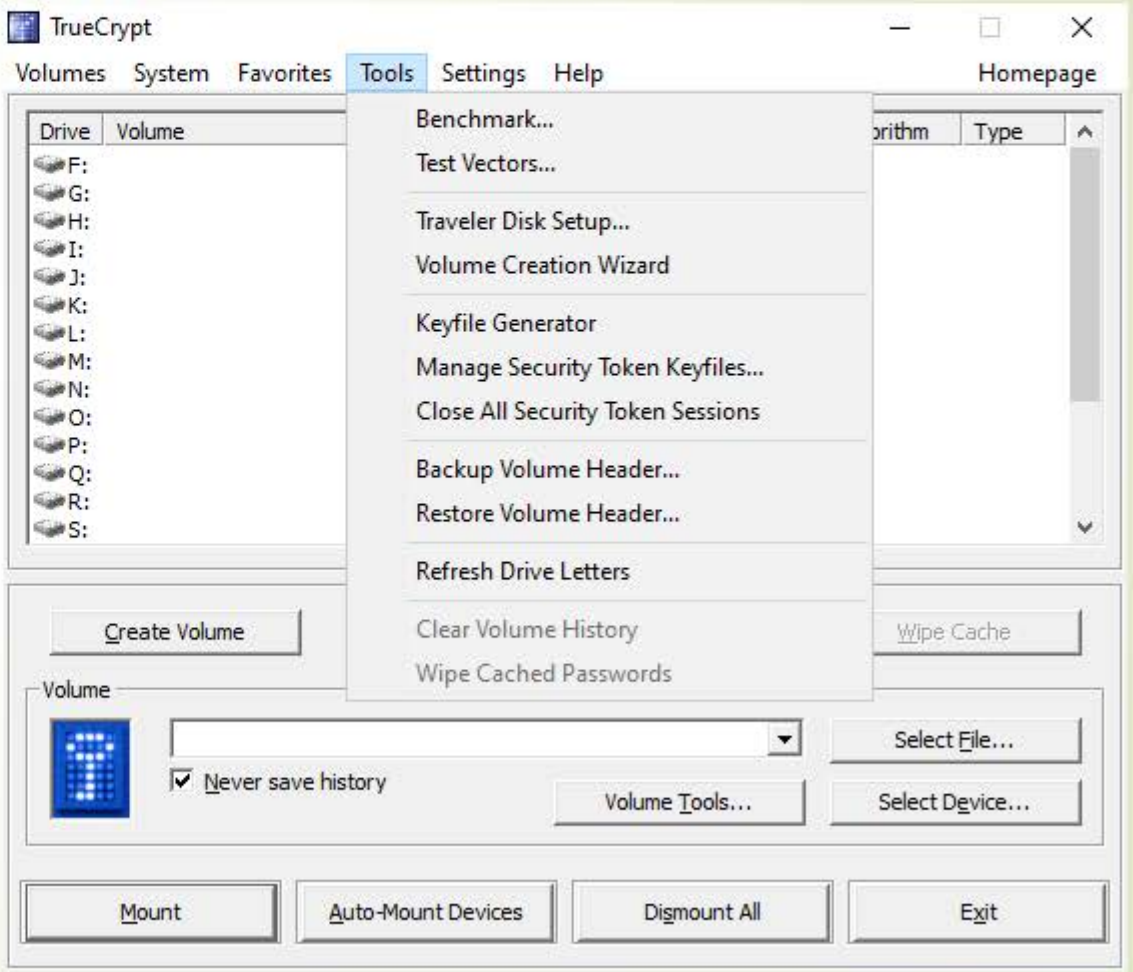
- პროგრამაში მიმაგრებული დანაყოფების ფავორიტად დამატება;
- პროგრამაში მიმაგრებული დანაყოფების სისტემურ ფავორიტად დამატება;
- ფავორიტი დანაყოფების ორგანიზება;
- ფავორიტი სისტემური დანაყოფების ორგანიზება;



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Tools ჩამოწათვალში გვხვდება:

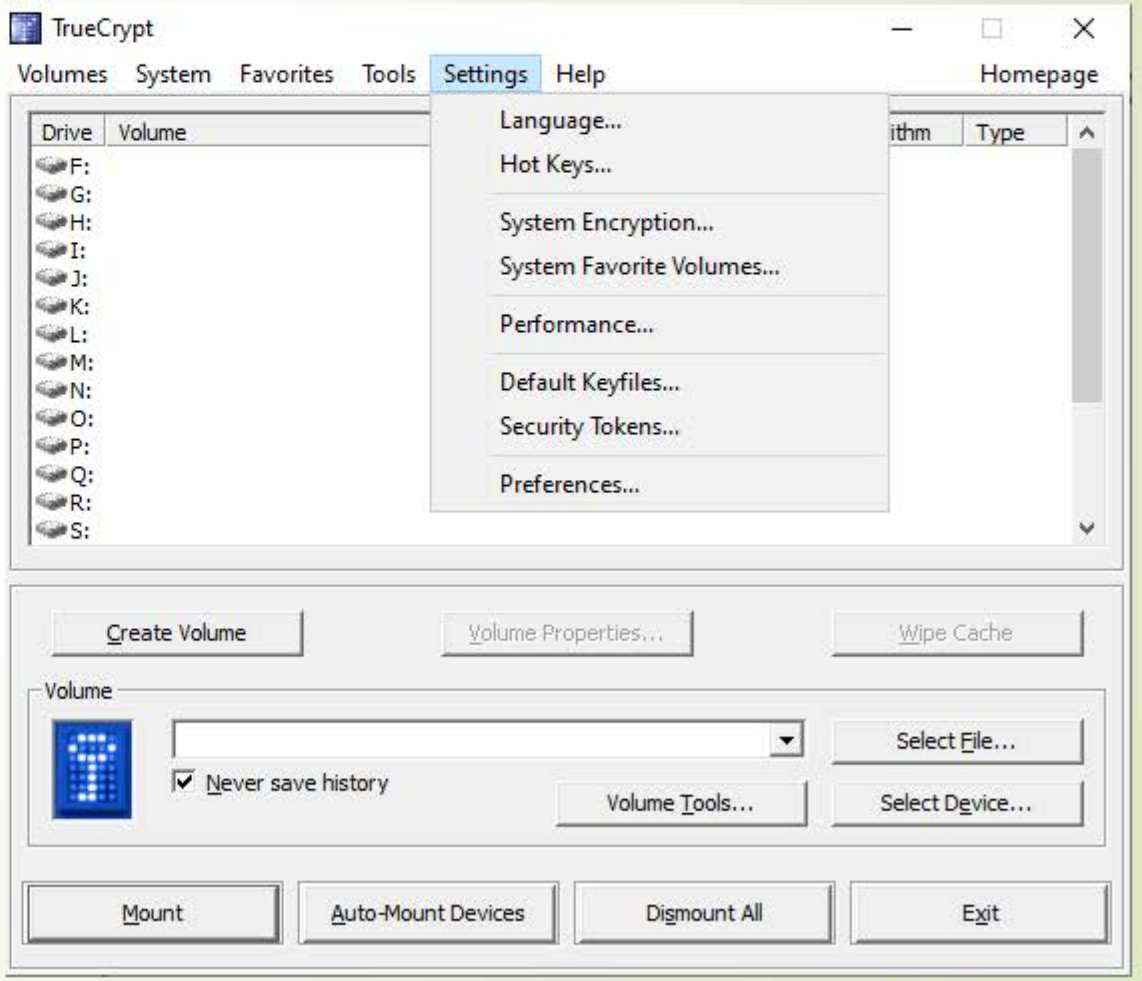
- ბენჩმარკი;
- ვექტორების ტესტირება;
- დისკის დაყენება;
- დანაყოფის შექმნა;
- გასაღების გენერირება;
- გასაღების უსაფრთხოების მენეჯმენტი;
- ყველა უსაფრთხოების ტოკენის გათიშვა;
- დანაყოფის სათაურის ბექაფის გაკეთება;
- დანაყოფის სათაურის რესთორის გაკეთება;
- დრაივის სახელების დარეფრეშება;
- დანაყოფის ისტორიის გასუფთავება;
- ქეშირებული პაროლების წაშლა;



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Settings ჩამონათვალში გვხვდება:

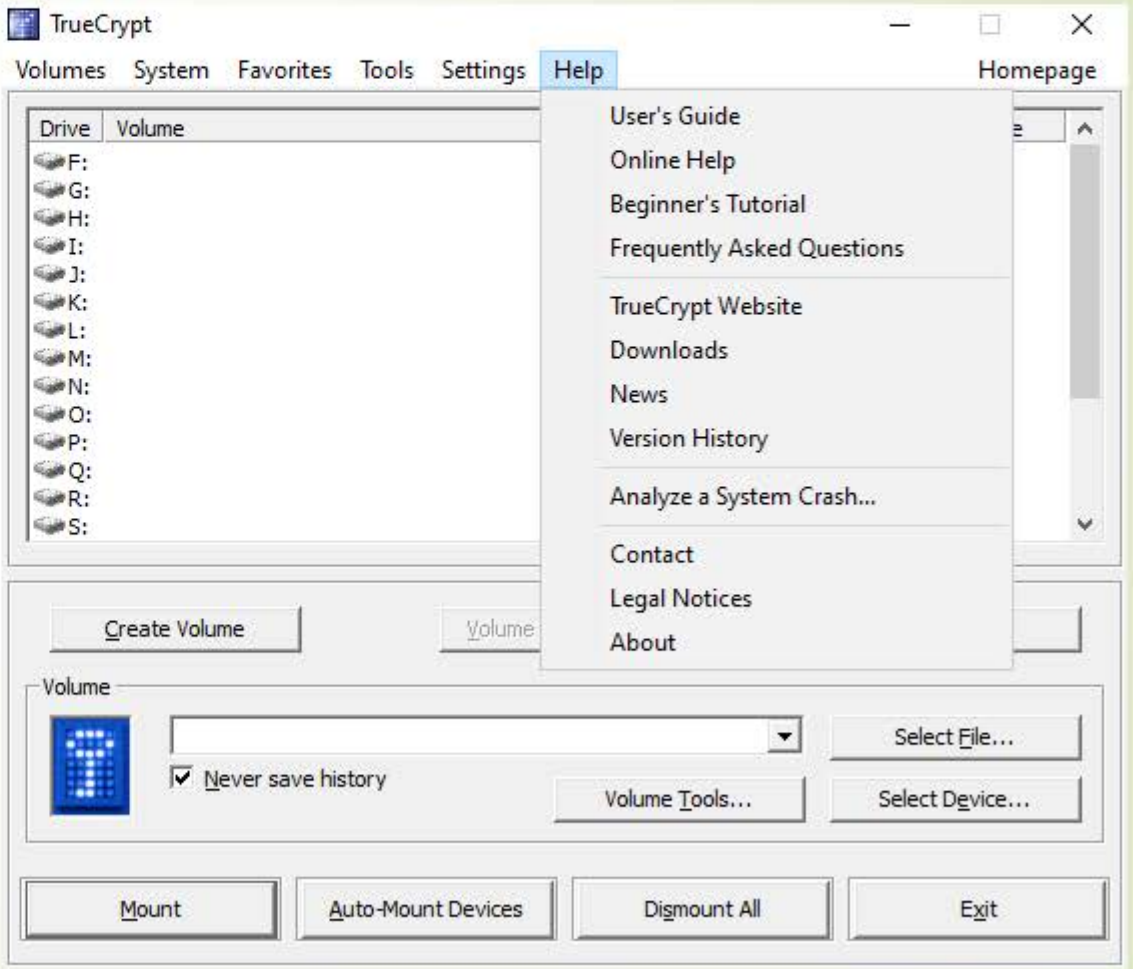
- ენის ცვლილება;
- კლავიატურის კომბინაციების დაყენება;
- სისტემის შიფრაცია;
- სისტემის ფავორიტი დანაყოფების დაყენება;
- პერფორმანსის ნახვა;
- სტანდარტული გასაღების ფაილები;
- უსაფრთხოების ტოკენები;
- პრეფერენციები;



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

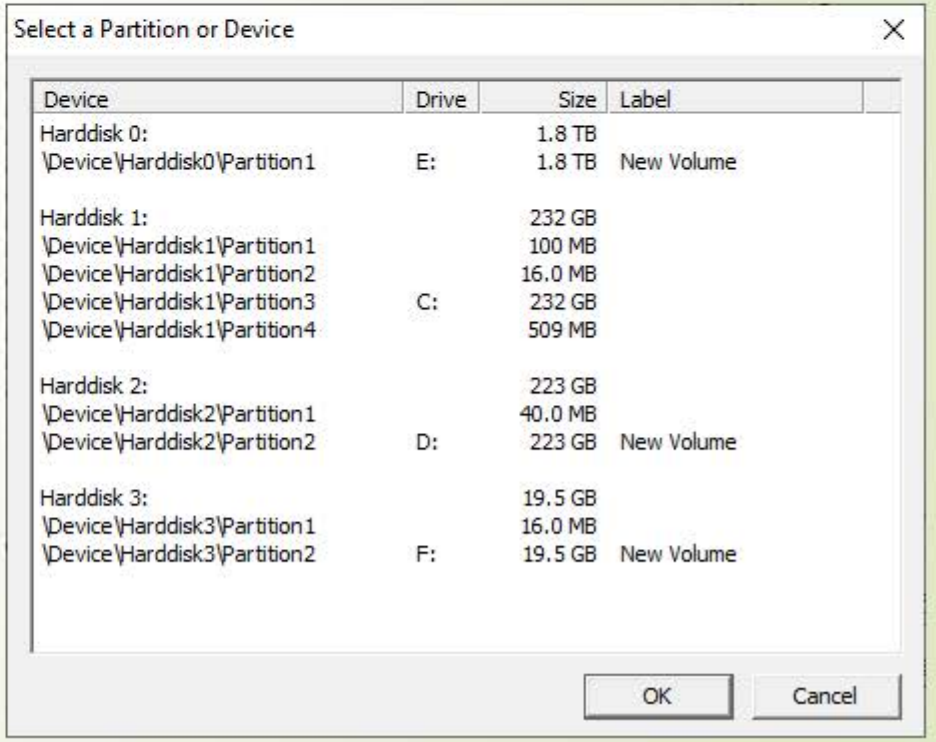
Help ჩამონათვალში გვხვდება:

- მომხმარებლების სახელმძღვანელო;
- ონლაინ დახმარება;
- დამწყები მომხმარებლის ტუტორიალების ნახვა;
- ხშირად დასმული კითხვების დათვალიერება;
- პროგრამის ვებგვერდზე გადასვლა;
- გადმოწერა;
- ახალი ამბების ნახვა;
- ვერსიის ისტორიის ნახვა;
- სისტემური ანალიზი;
- კონტაქტები;
- ლეგალური გაფრთხილებების ნახვა;
- პროგრამის შესახებ ინფორმაცია.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

მთავარ გვერდზე Select Device- ღილაკზე დაჭერისას მომხმარებელს შეუძლია აირჩიოს კონკრეტულ მყარ დისკზე განთავსებული დანაყოფი.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Volume Tools - ღილაკზე დაჭერისას მომხმარებელს შეუძლია განახორციელოს:

პაროლის ცვლილება;

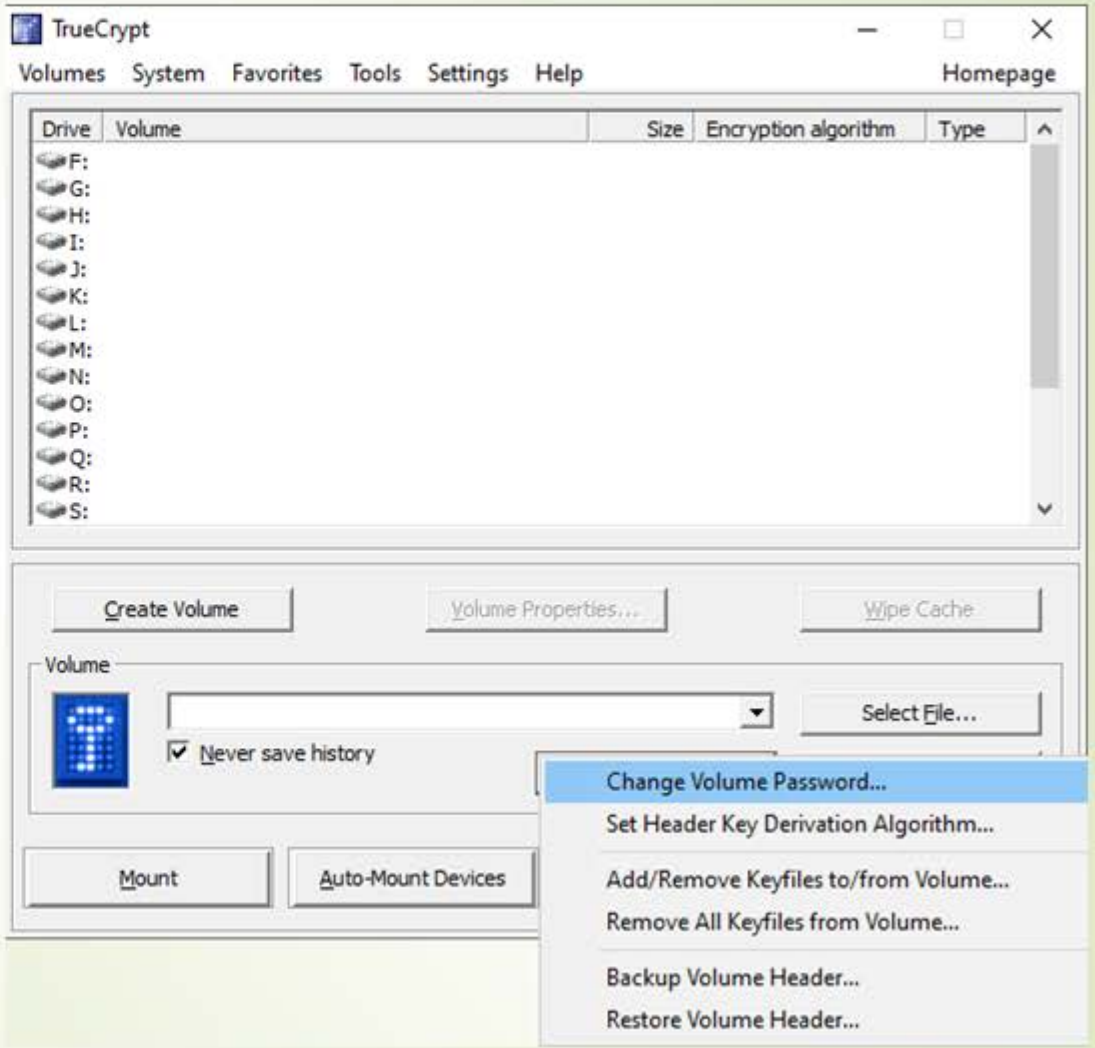
გასაღების ალგორითმის დაყენება;

გასაღები ფაილების დამატება და წაშლა;

მყისიერად დაშიფვრა;

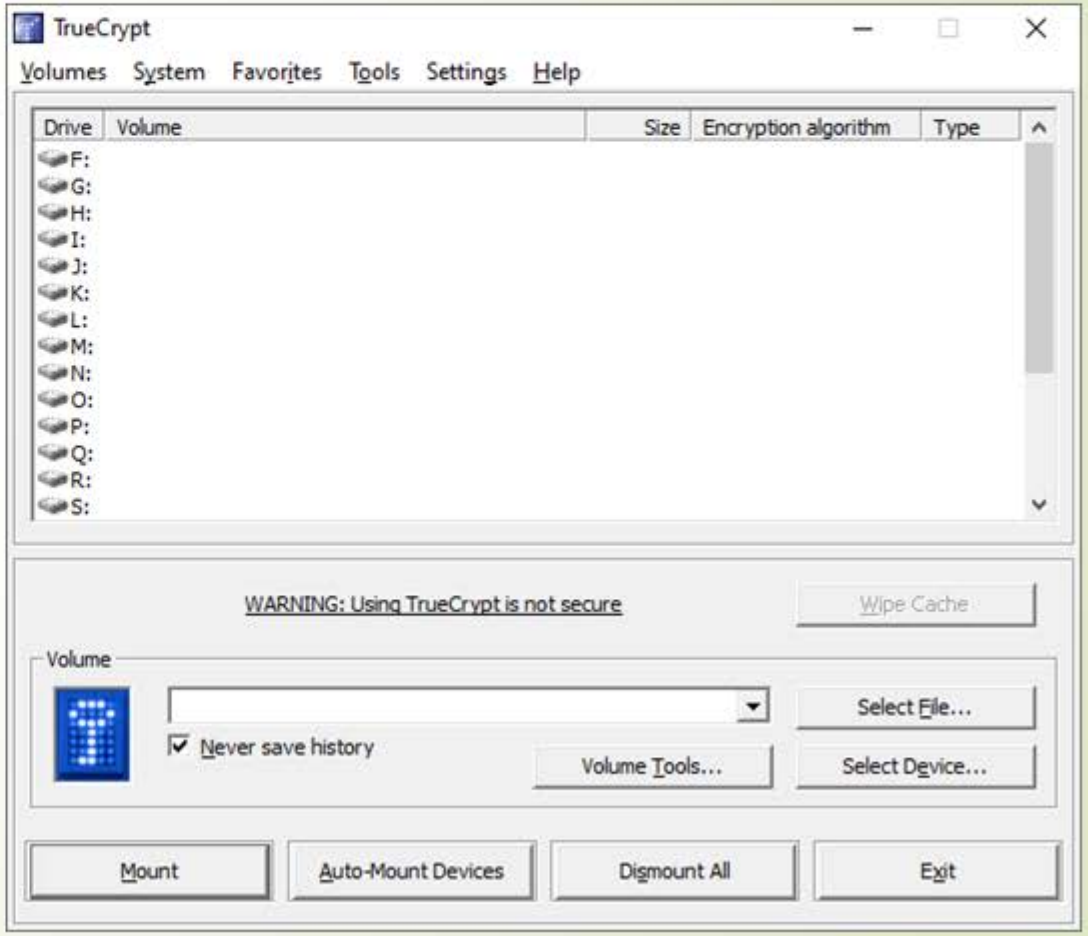
მეხსიერების ბექაფის გაკეთება;

მეხსიერების აღდგენა;



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

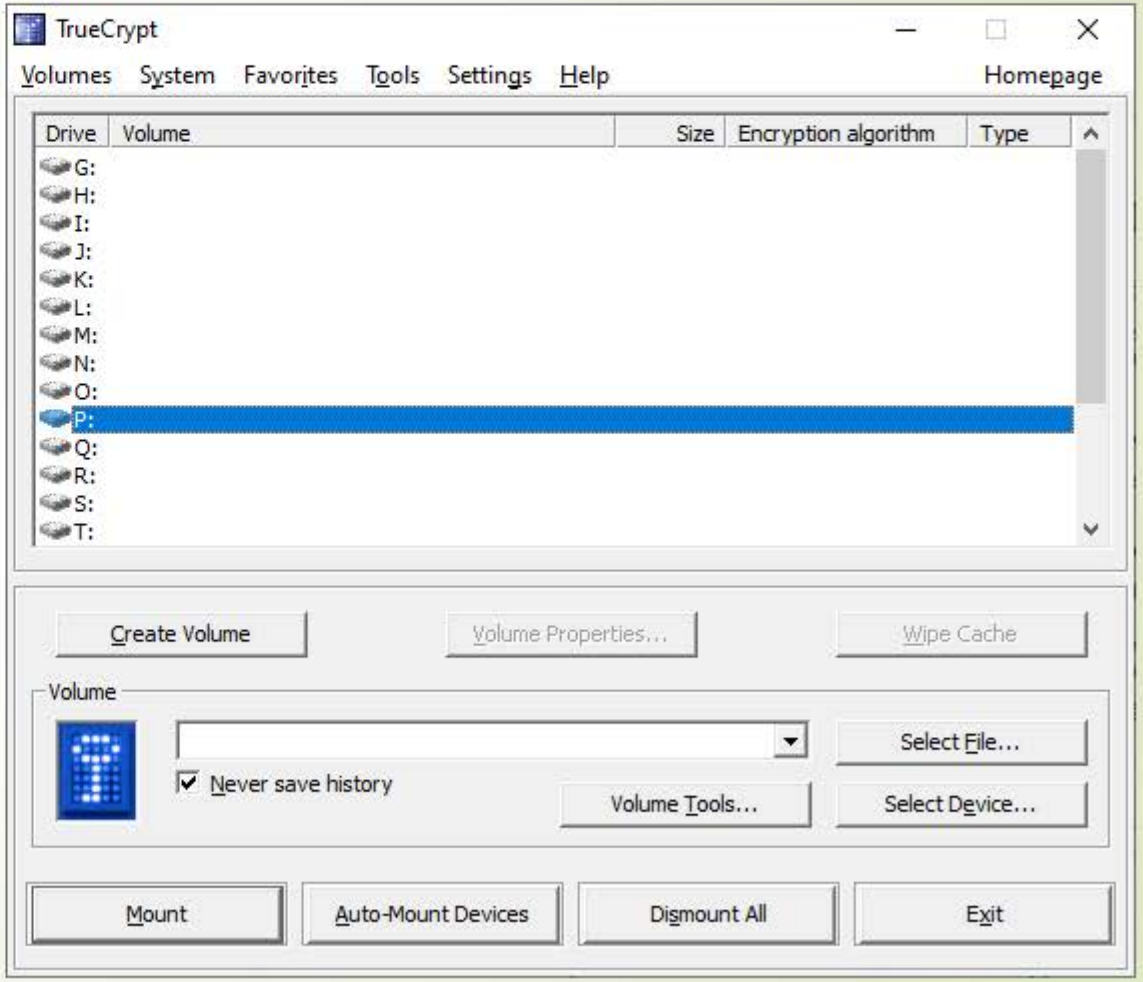
TrueCrypt 7.2- ის ოფიციალურ ვებგვერდზე წათქვამია, რომ პროგრამა აღარ არის დაცული და შესაბამისად სხვაგან უნდა გამოიყურებოდეს დისკის დაშიფვრის ხსნარში. თუმცა, ეს არ შეიძლება რეალურად იყოს 7.1a ვერსიის შემთხვევაში, რომელიც TrueCrypt- ის ვერსია საბოლოო ვერსიამდე გაათავისუფლეს. ამის შესახებ გიბსონის კვლევის კორპორაციის ვებგვერდზე დამაჯერებელი არგუმენტი შეგიძლიათ წაიკითხოთ.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

TrueCrypt 7.1a ვერსია მორგებულია Windows 10-ზე. შესაბამისად მისი გამოყენებით მასში არსებული, ყოველი ფუნქცია გახსნილია და შესაძლებელია მათი გამოყენება,

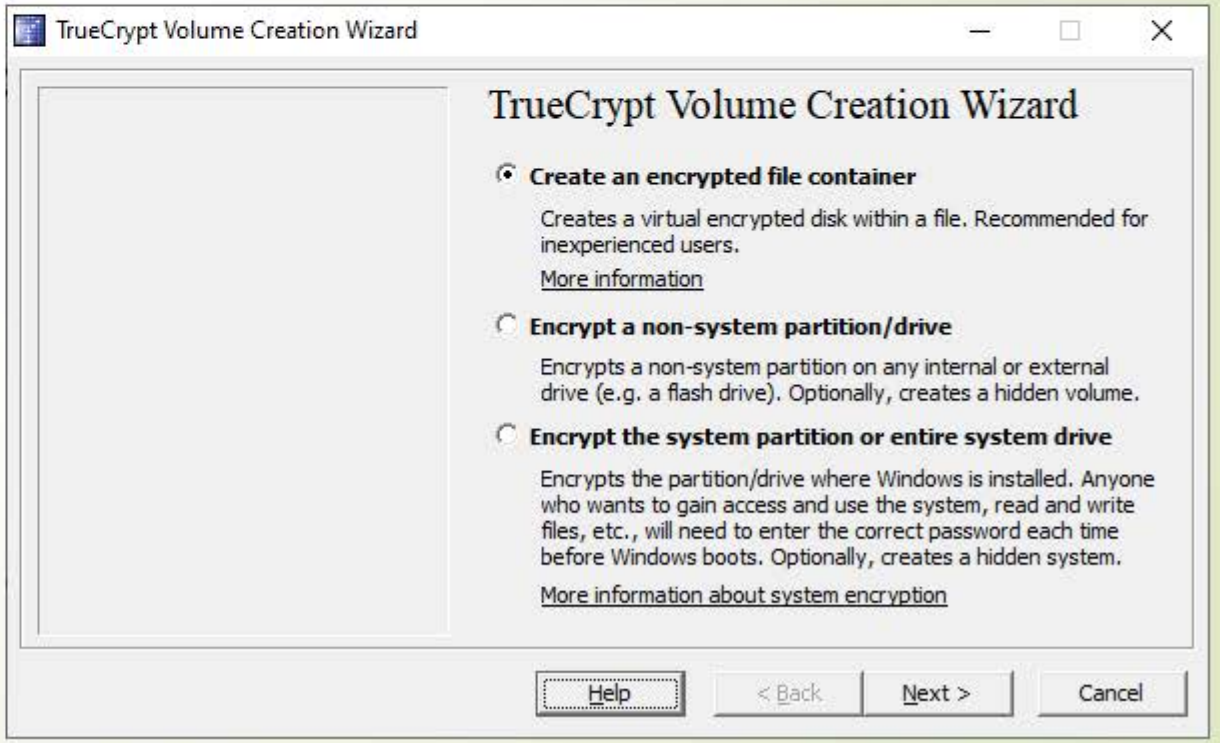
Create Volume-ზე დაკლიკვისას მომხმარებელს ფაილების შიფრაციის 3 ტიპის შექმნის შესაძლებლობა აქვს.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Create Volume ღილაკზე დაკლიკვისას გამოდის ფანჯარა რომელზეც მოცემულია 3 ოფცია, ესენია:

- Create an encrypted file container - დაშიფრული ფაილ კონტეინერის შექმნა;
- Encrypt a non-system partition/drive – არასისტემური დანაყოფის დაშიფვრა;
- Encrypt the system partition or entire system drive - დანაყოფის ან მთლიანი სისტეის შიფრაცია;



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

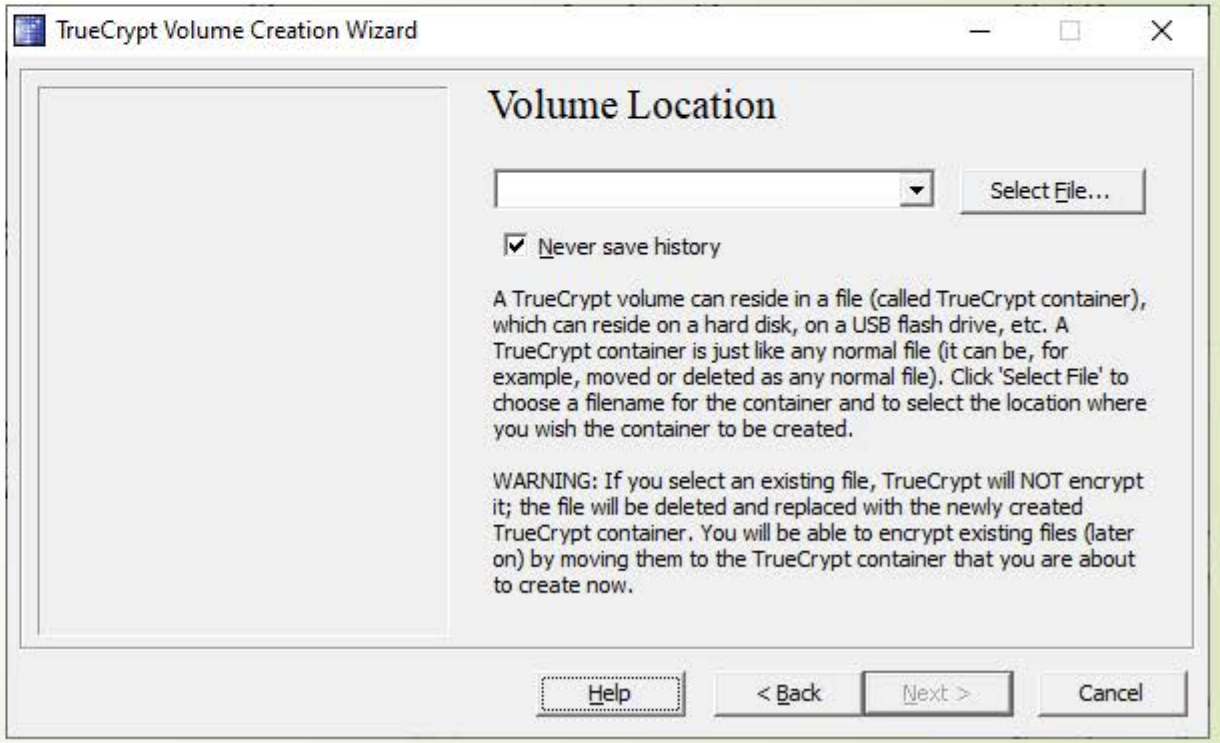
Create an encrypted file container - მონიშვნისას **Next** ღილაკით მომხმარებელი გადადის მეხსიერების ტიპის შექმნის გვერდზე, სადაც მოცემულია ორი არჩევანი:

- **Standard TrueCrypt volume –** მეხსიერების სტანდარტული მეთოდით შექმნა;
- **Hidden TrueCrypt volume –** მომხმარებელი ირჩევს, მაშინ როდესაც მომხმარებელს სურს დამალოს თავისი პაროლები ან მონაცემები.

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Next-ზე დაჭერით მომხმარებელი გადადის ლოკაციის არჩევის გვერდზე.

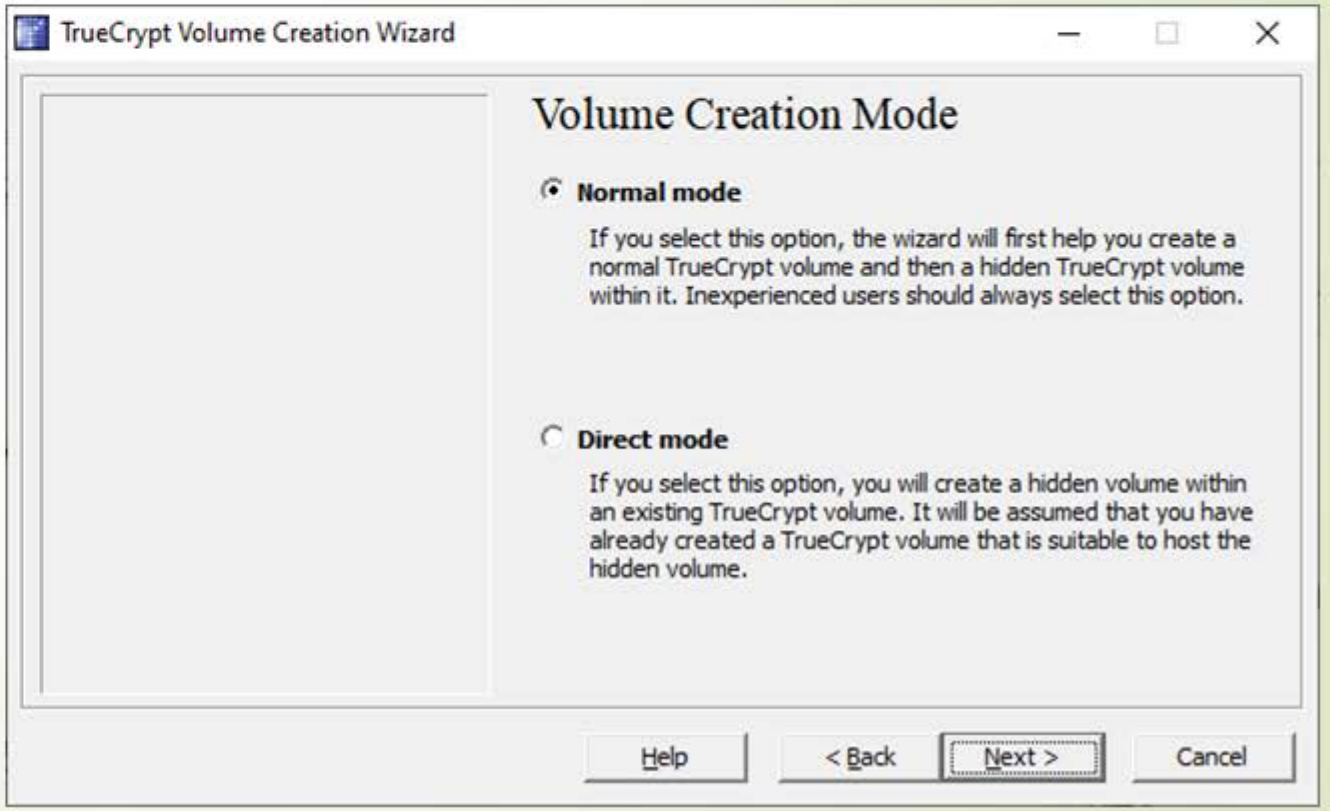
Never save history -ს მონიშვნით მომხმარებელი, პროგრამას ისტორიას აღარ დაამახსოვრებინებს, შესაბამისად პროგრამაც ნაკლებად დაიტვირთება.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Hidden TrueCrypt volume – ის არჩევისას გამოდის ორი საინსტალაციო რეჟიმი:

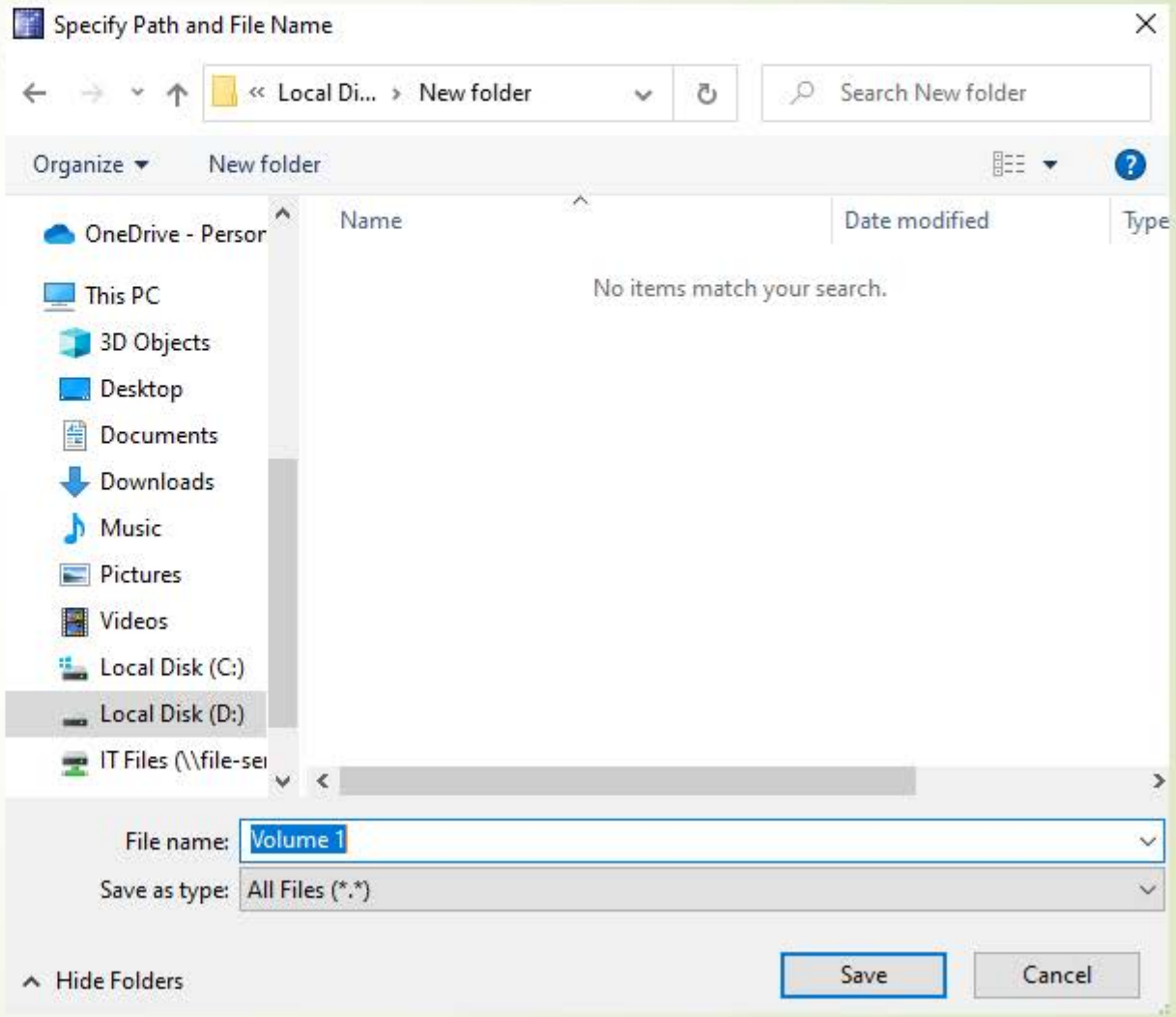
- **Normal Mode –** სტანდარტული რეჟიმი;
- **Direct Mode –** პირდაპირი რეჟიმი.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

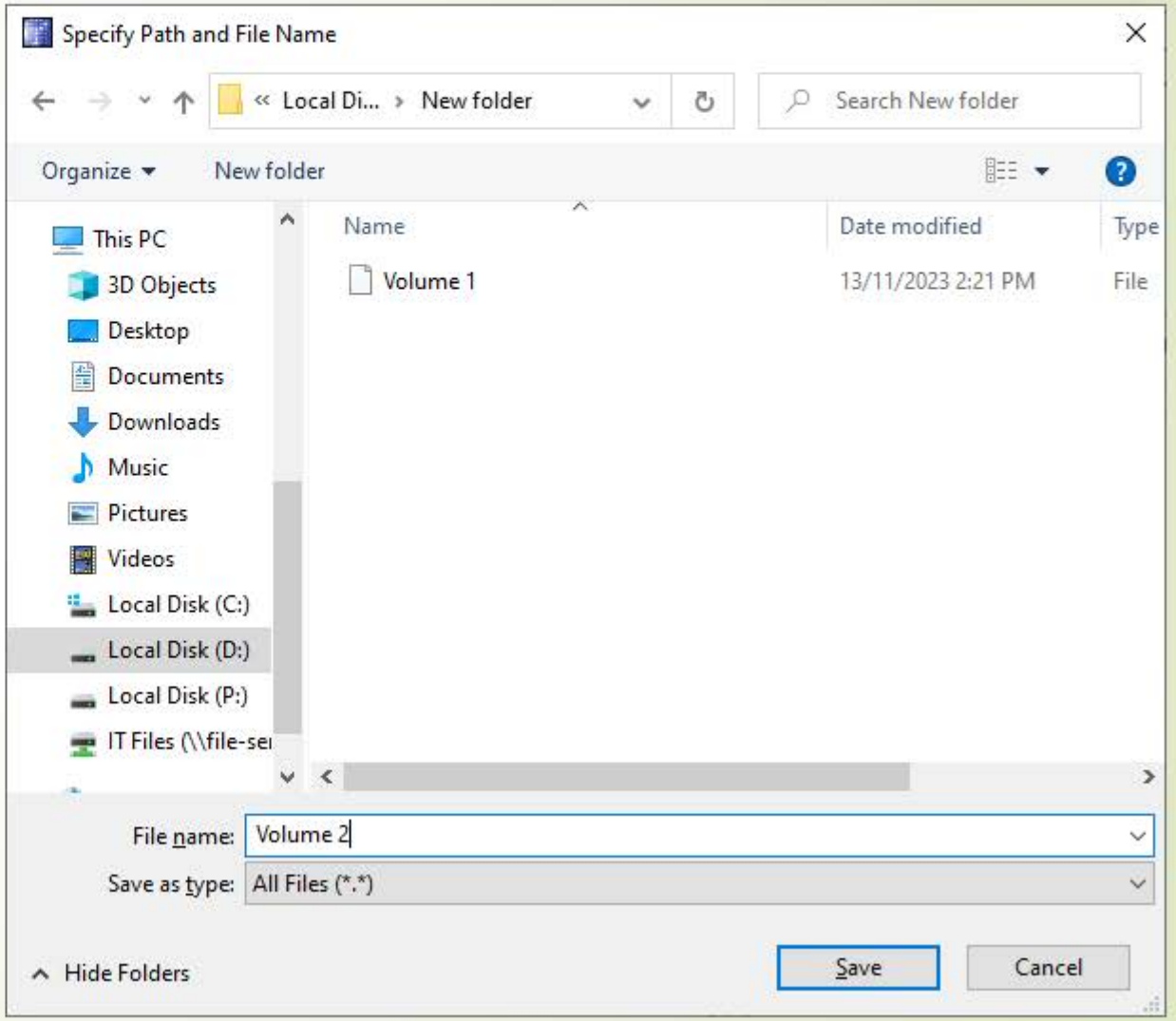
Select File- ღილაკით მომხმარებელი მყარ დისკზე ირჩევს კონკრეტულ მისამართს, რომ მასში განათავსოს ცალკე გამოყოფილი მეხსიერების დანაყოფი.

ასევე შექმნისთვის აუცილებელი დეტალია, რომ ფაილს სახელი დაერქვას **File name-** ველში.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Hidden TrueCrypt volume -ის შექმნის პროცესში, მომხმარებელი ასევე უთითებს მეხსიერების დანაყოფის სახელს, რომელიც განკუთვნილი იქნება სხვადასხვა მონაცემების დასაცავად.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

ადგილის შექმნის შემდეგ მომხმარებელმა უნდა აირჩიოს შიფრაციის მეთოდი:

AES –

Serpent –

Twofish –

AES-TwoFish –

AES-Twofish-Serpent –

Serpent-AES –

Serpent-Twofish-AES –

Twofish-Serpent –

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

ადგილის შექმნის შემდეგ მომხმარებელმა უნდა აირჩიოს შიფრაციის მეთოდი:

AES –

Serpent –

Twofish –

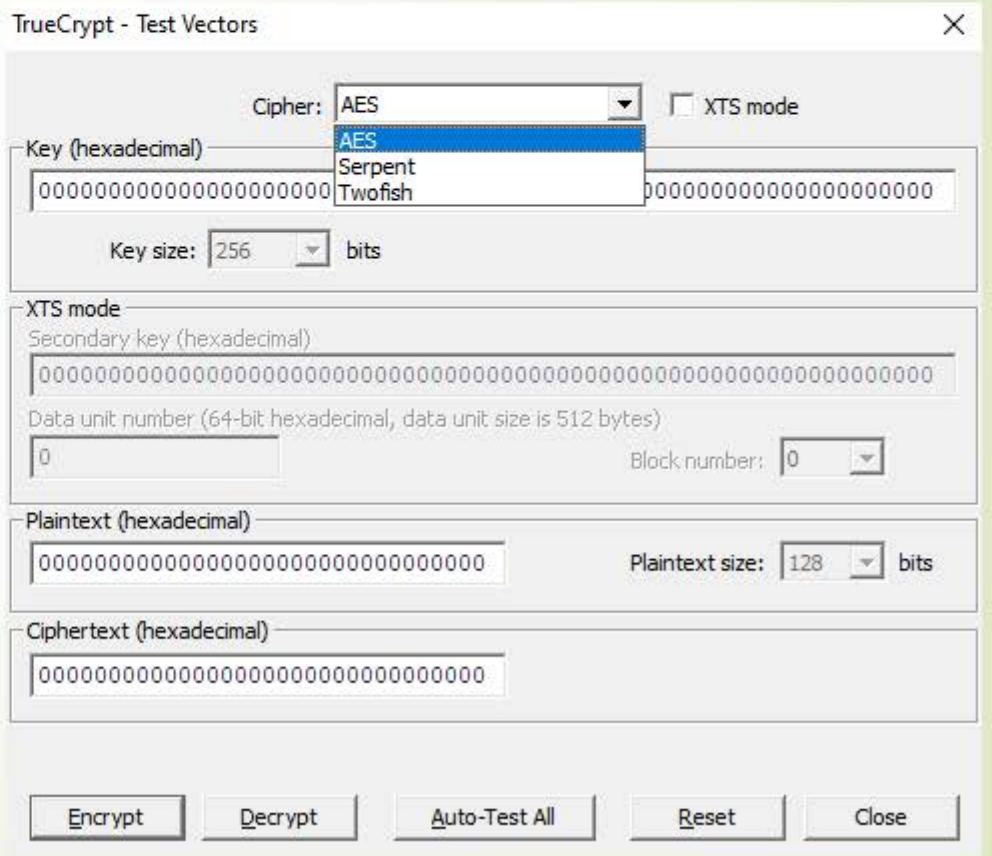
AES-TwoFish –

AES-Twofish-Serpent –

Serpent-AES –

Serpent-Twofish-AES –

Twofish-Serpent –



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

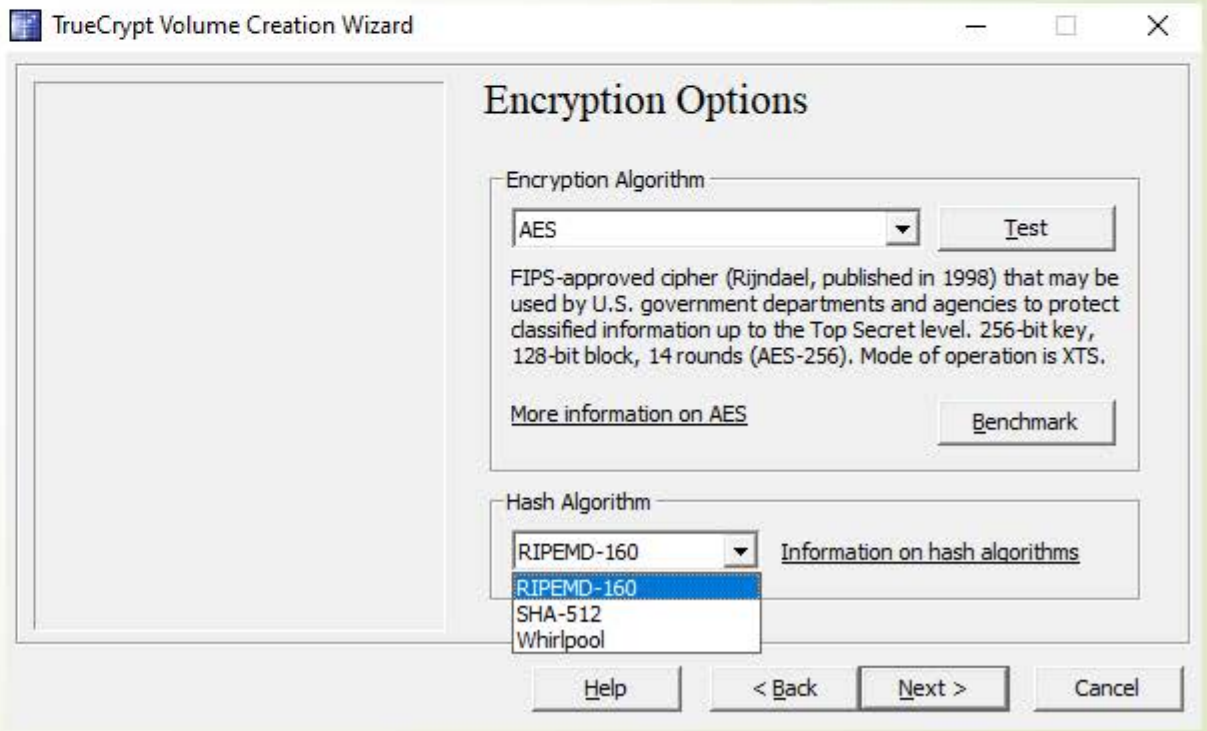
ადგილის შექმნის შემდეგ მომხმარებელმა უნდა აირჩიოს შიფრაციის მეთოდი:

ჰეშირების ალგორითმის ტიპები:

RIPEMD-160

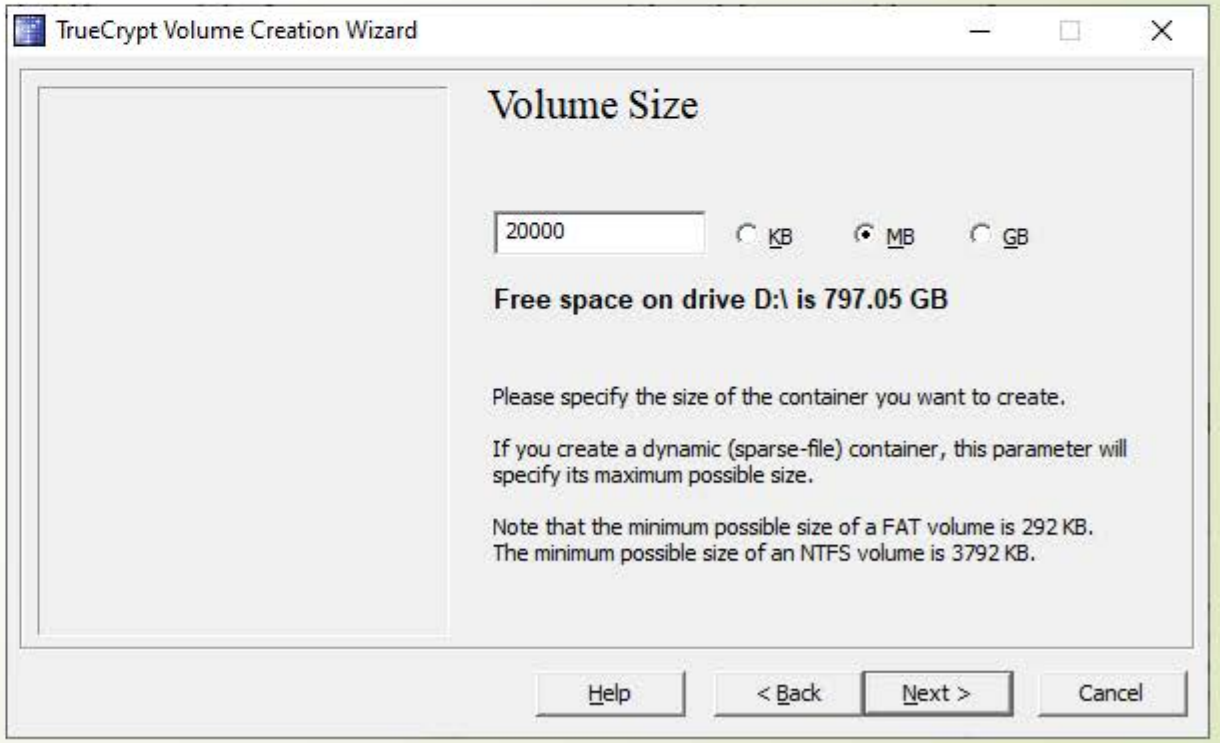
SHA-512

Whirpool



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

დანაყოფის ზომის დაყენება:



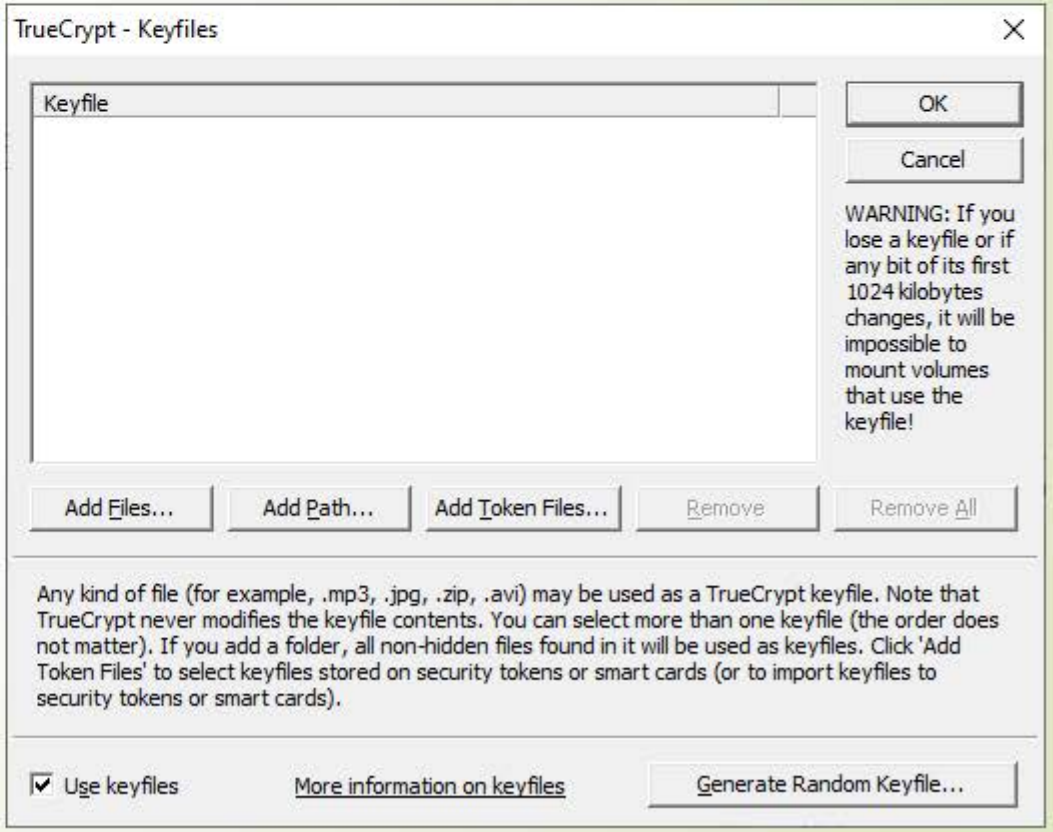
დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

დანაყოფზე პაროლის დადება:

დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

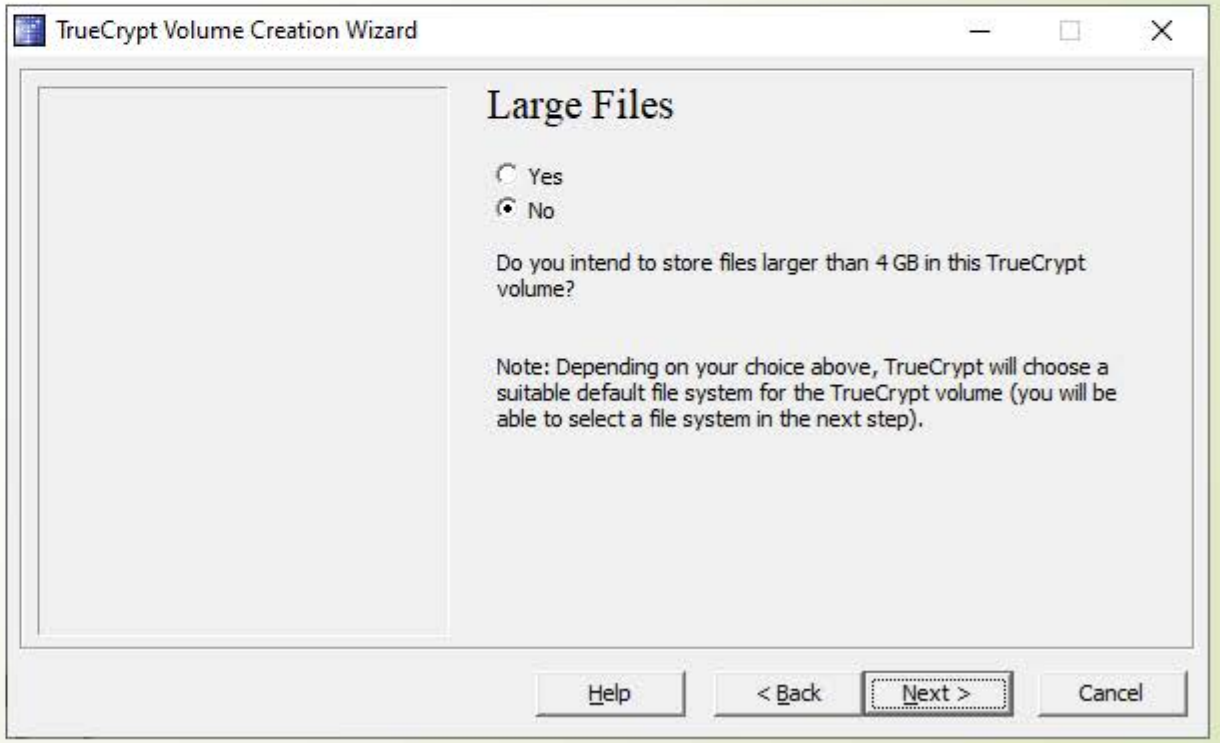
გასაღების დამატება:

Generate Random Keyfile - რენდომ პრინციპით ახალი გასაღების დაგენერირება.



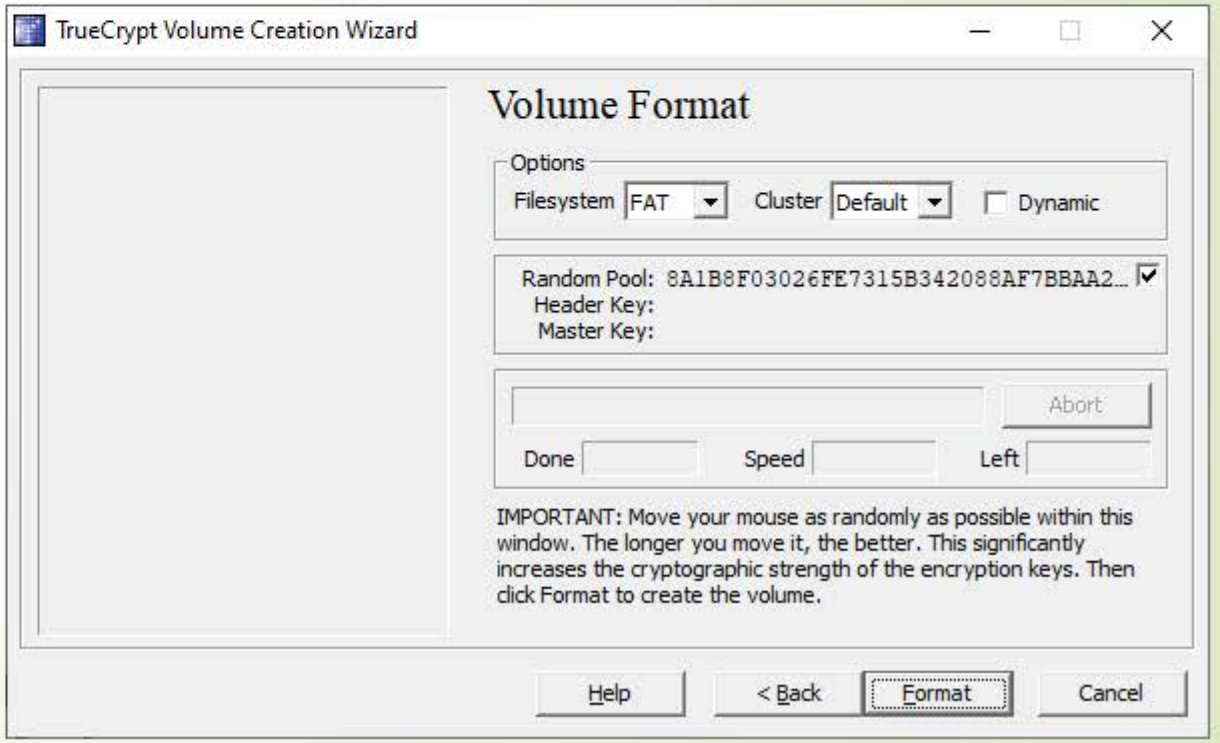
დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

იმისთვის თუ მომხმარებელი დაწაყოფში დიდი მოცულობის ფაილების შენახვას აპირებს, რომელთა ზომა 4 გიგაბაიტზე მეტია, მაშინ უნდა მოინიშნოს **Yes**, ხოლო თუ არა მაშინ **No**.



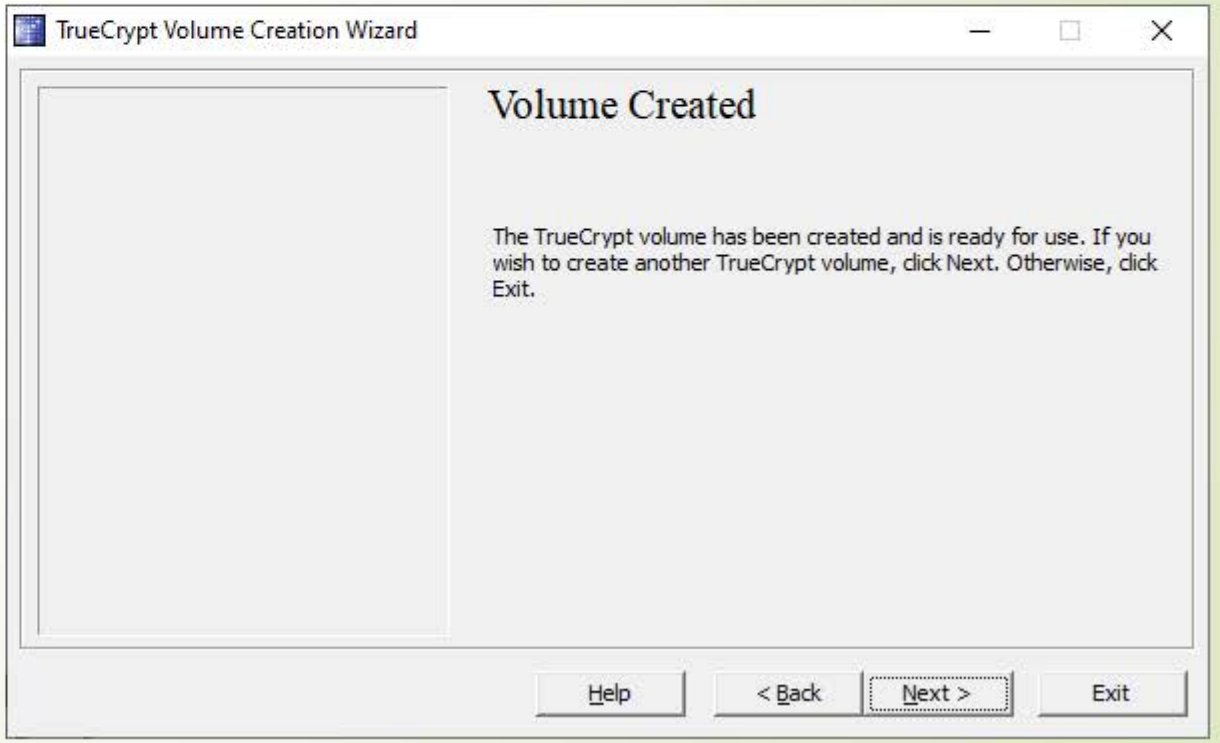
დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

დანაყოფის ფორმატი:



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

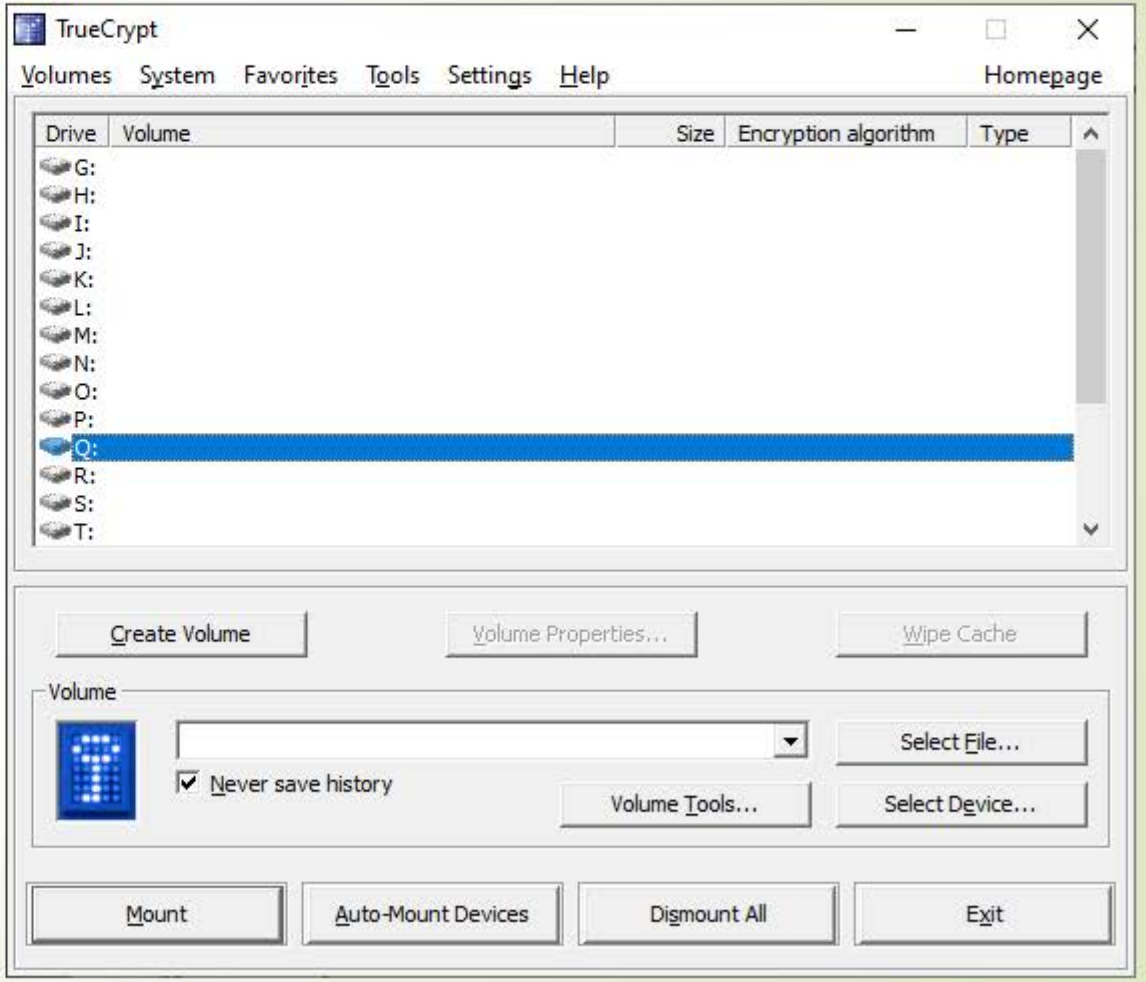
მოცემულ გვერდზე სრულდება დანაყოფის შექმნის პროცესი. იმ შემთხვევაში თუ მომხმარებელს სურს დაიწყოს ახალი დანაყოფის შექმნა **Next** ღილაკით აგრძელებს ახალი დანაყოფის ინსტალაციას, სხვა შემთხვევაში გამოდის **Exit** ღილაკით.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

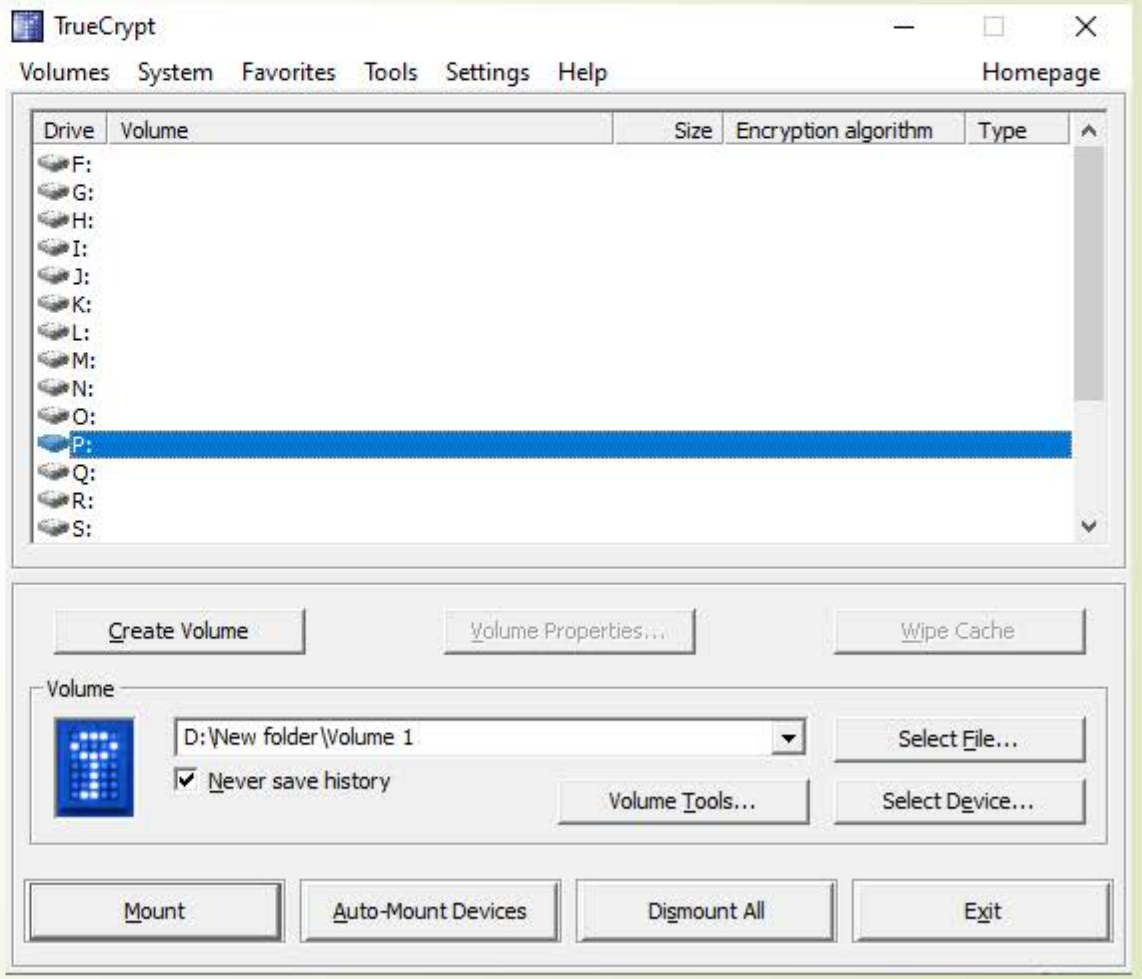
ქვემოთ განთავსებული ღილაკების მნიშვნელობები:

- Mount – დამონტაჟება;
- Auto-Mount Devices – მოწყობილობების ავტომატურად დაყენება;
- Dismount All – ყველა მონაცემის დემონტაჟი;
- Exit – გათიშვა;



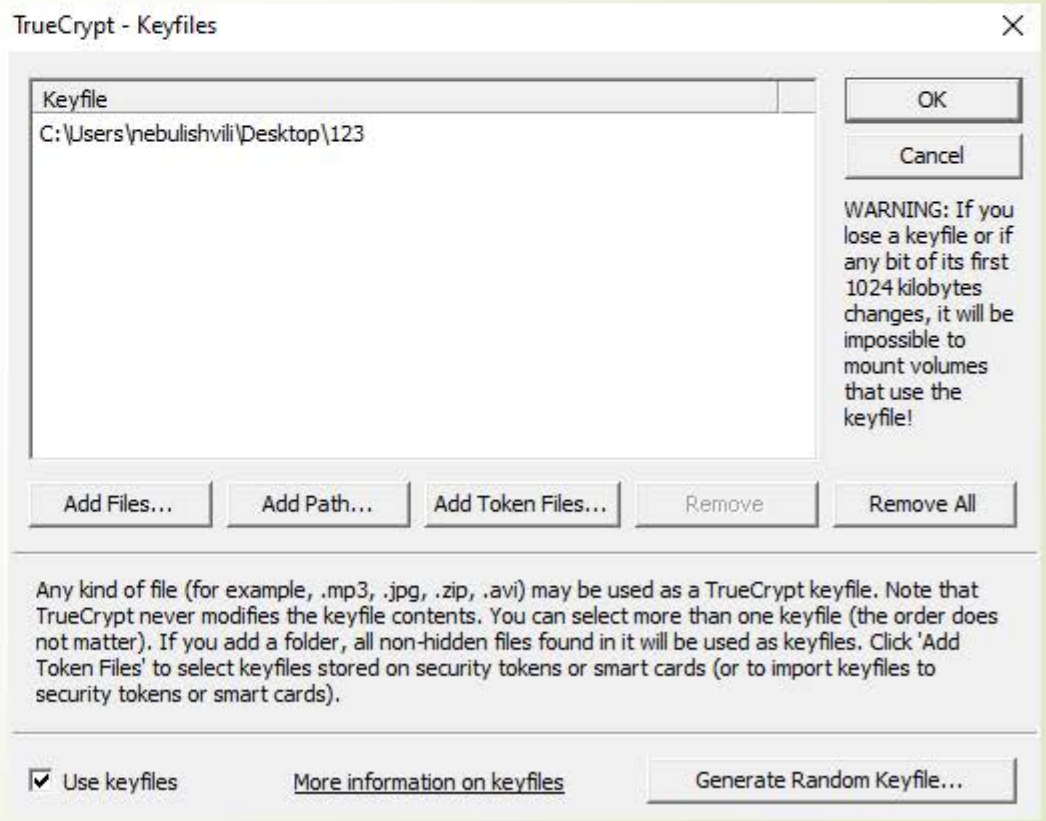
დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

იმისათვის, რომ მომხმარებელმა პროგრამაში დააფიქსიროს და გამოაჩინოს დანაყოფი, ქვემოთ განთავსებული ღილაკით Select File-ით ირჩევს, ახლად შექმნილი დანაყოფის მდებარეობას დისკზე.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

Mount ღილაკზე დაჭერის შემდეგ აუცილებელია მივუთითოთ პაროლი რომელიც დაგენერირებულია როგორც გასაღები და მისი მითითების შემდეგ ვაწვებით **OK** ღილაკს.



დისკების და ფაილების შიფრაციის პროგრამული ხელსაწყო TrueCrypt

OK ღილაკზე დაჭერის შემდეგ, პროგრამაში გამოჩნდება დანაყოფი, რომელიც შემდგომ მომხმარებელს შეუძლია გამოიყენოს ფიზიკურად და მართოს იგი სურვილისამებრ.

Dismount - ღილაკით შესაძლებელია მონიშნული დანაყოფის პროგრამიდან წაშლა.