Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (3) Week 6 Unit (Module) name: (Privacy & Data Protection)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Mirosław Mazurek • Paweł Dymora
Learning Activity Goals	1. Encryption of disks and partitions 2. How to use VeraCrypt Tool
Skills to be Gained	• **TS1** • **SS1** • **SS2**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • VeraCrypt program

Co-funded by the
Erasmus+ Programme
of the European Union

Brief information about the module

Description
The goal of this module is to gain knowledge and practical skills related to data protection and encryption of data on your private or corporate disk.

Content of the Learning Material

1. Encryption of disks and partitions. Theoretical basics: principle of operation, encryption algorithms. Installing the program (configuration, defining the disk, choosing parameters, generating keys).

The security of computer systems requires protection not only of resources such as the operating system itself, applications, but most of all data. Known security methods by preventing access to resources, such as a firewall, are not always effective. Therefore, multiple security methods should be combined with each other. The presented method of data encryption allows for the elimination of many threats resulting from an intruder's access to our computer.

One of the most widely used solutions is the free VeraCrypt data encryption software. It allows you to encrypt not only entire disks or partitions, but even portable USB disks and create virtual encrypted disks with a certain capacity. VeraCrypt enables encryption using the following algorithms: AES, Camellia, Kuznyechik, Serpent and Twofish; as well as multiple encryption with: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

Depending on the configuration of the computer, the speed of encryption and decryption for each of these algorithms will vary, as shown in Figure 1.

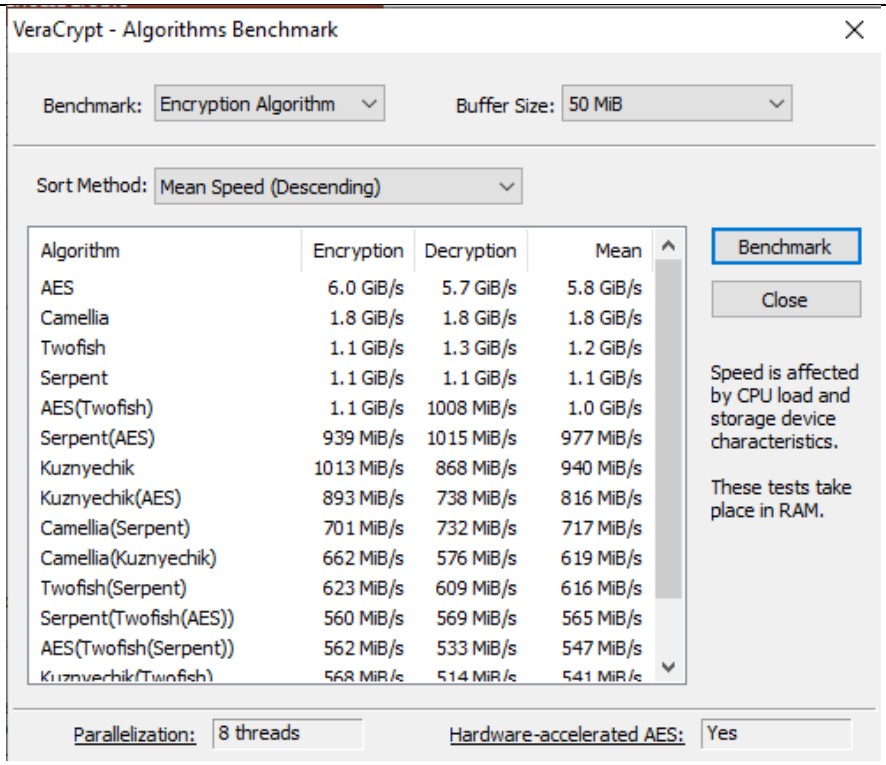

Fig. 1. Testing the speed of algorithms

The encryption process begins with the creation of the volume. You can encrypt an entire disk, partition or any volume (Fig. 2).

Fig. 2. Window of the VeraCrypt volume creation wizard

After selecting the location of the volume, you should give it a name. The VeraCrypt volume is placed in a file that can be saved on a hard disk or a USB drive. The volume behaves like a normal file, i.e. we can copy it, rename it, etc. The next step is to select the appropriate encryption

algorithm, e.g. AES, and to assign an access password in compliance with the relevant quality rules (appropriate length, upper and lower case letters, numbers, special characters). Then the volume is formatted. To increase its security, the wizard asks you to generate random mouse movements, which significantly improves the cryptographic quality of the generated keys (Fig. 3). After formatting, the volume is available for use. It only needs to be connected by entering the password (Fig. 4).

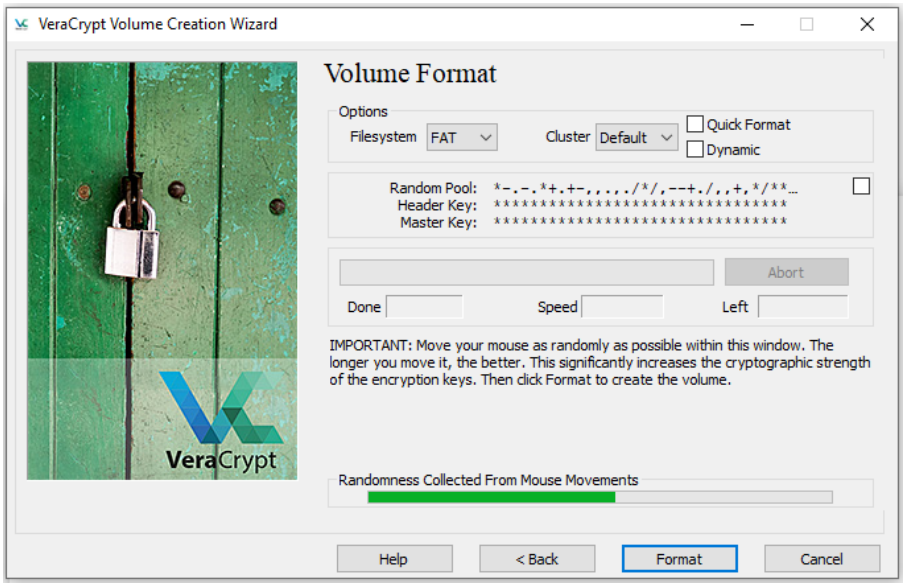

Fig. 3. The process of formatting VeraCrypt volumes

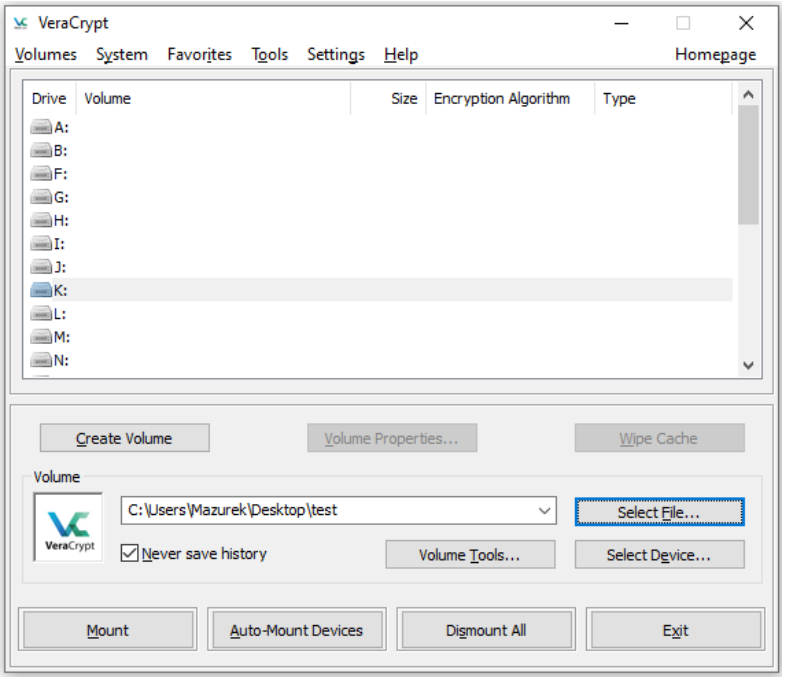

Fig. 4. VeraCrypt volumes connection window

In cases where we want a high level of protection, and we do not care about the encryption time, multiple encryption should be selected. Testing the performance during encryption for volumes of different capacities with different algorithms at the same time, one can notice that the stronger the encryption algorithm, the lower the speed of encrypting and decrypting the file. Not every algorithm responds to a change in volume size equally. Creating a volume is quick and easy, thanks to the clear instructions from the installer.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions.

1. How you can protect your data on your computer hard drive?
2. What kind of computer programs you can used in order to protect your data?

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

1. What is the safest encryption method to secure your files?

Attachments:

1. Presentation
2. Video

References:

1. https://www.veracrypt.fr/en/Home.html
2. https://github.com/veracrypt/VeraCrypt
3. https://veracrypt.eu/en/Beginner%27s%20Tutorial.html