**EXPERIMENT NO – 9**

**AIM:** Implementation of File System Security.

**THEORY**:

VeraCrypt is an Free and Open Source utility used for on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication. Individual ciphers supported by VeraCrypt are AES, Serpent, Twofish, Camellia, and Kuznyechik.

Additionally, ten different combinations of cascaded algorithms are available: AES–Twofish, AES–Twofish–Serpent, Camellia–Kuznyechik, Camellia–Serpent, Kuznyechik–AES, Kuznyechik–Serpent–Camellia, Kuznyechik–Twofish, Serpent–AES, Serpent–Twofish–AES, and Twofish–Serpent.

The cryptographic hash functions available for use in VeraCrypt are RIPEMD-160, SHA-256, SHA-512, Streebog and Whirlpool.

**STEPS OF PERFORMING FILE SECURITY**:

1. Open VeraCrypt tool and Click on the Create Volume.
2. Create a Standard Veracrypt volume.
3. From the select file menu, point to destination of created volume.
4. Choose the Encryption Option.
5. Create a password for said volume, be sure to use a complex password and never forget this password you set.
6. Move your mouse as randomly as possible, as tool will calculate hash based on mouse movement here, thus more random, more secure it will be once collection is complete click on the format and wait for the formatting of volume to finish.
7. Click on mount button and locate your newly create volume, once mounted it’ll show itself on the main screen.
8. Now the volume has been mounted, you can transfer your folder containing sensitive info into it like a normal drive, and once you unmount, the information in the volume created will no longer will be accessible to anyone.

**OUTPUT**:













