1.Disk header format



2. Using key-files

hash - SHA256 hash

msg – first 4096 bytes of key-file

hash.Init();

hash.Update(msg);

PK=password||hash

key=PBKDF(salt, PK)