LAYER 2 FILE SECURITY (L2FS)

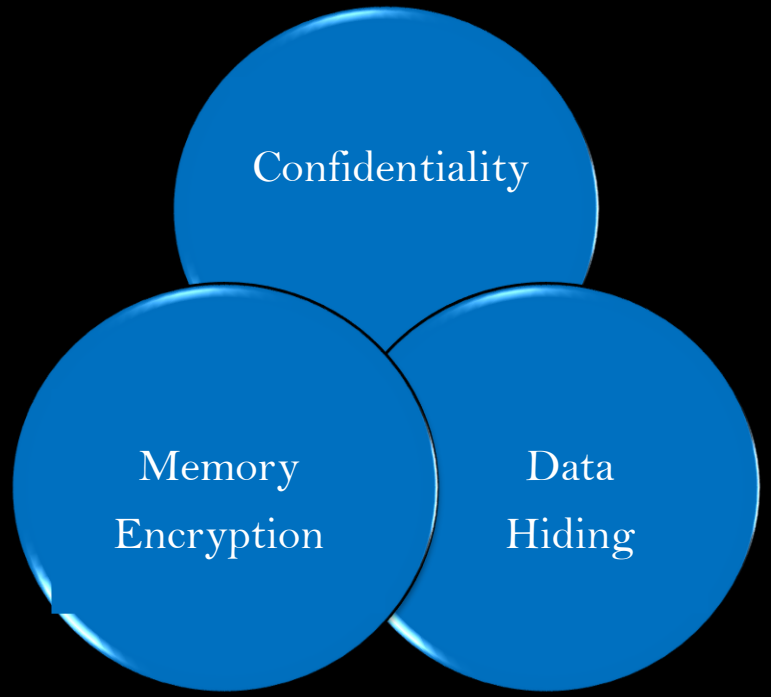
(PHYSICAL FILE HIDING)

An innovative technologies

Protecting confidential data

Against unauthorized access

تقنية مبتكرة في حفظ البيانات
السرية والهامة



Highly Confidential Document Protection

QuanTum
Smart information technology

TRUSTED SECURITY SOLUTIONS (TSS)

L2FS

Layer 2 File Security

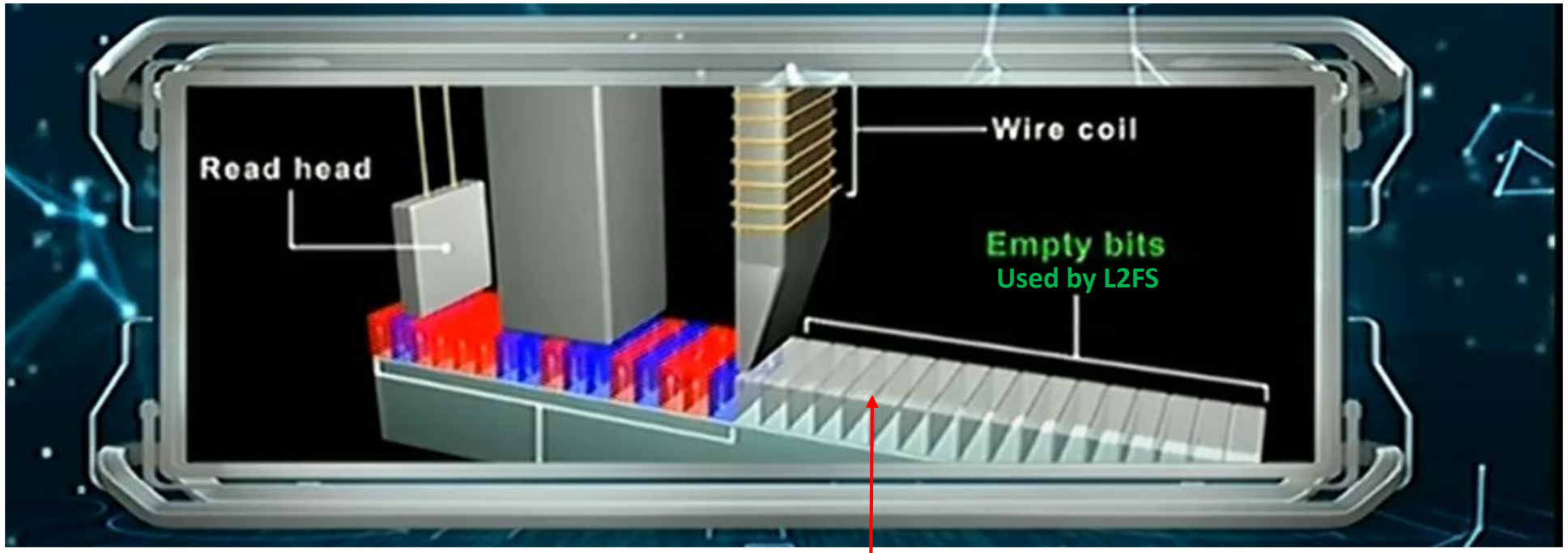
What is L2FS

The difference between
Being Secured & Feeling Secure

L2FS is sophisticated Software that enables you to build up an ironclad security strategy to protect your confidential documents from any type of attack, Users can work in an open and unprotected working environment without worries about any pertinent attacks from outside, whereas L2FS keeps your documents protected and hidden in a safe place, and this place is inaccessible and isolated from Windows Operating System environment, neither Windows nor any other utility has the power to access your hidden data in that place.

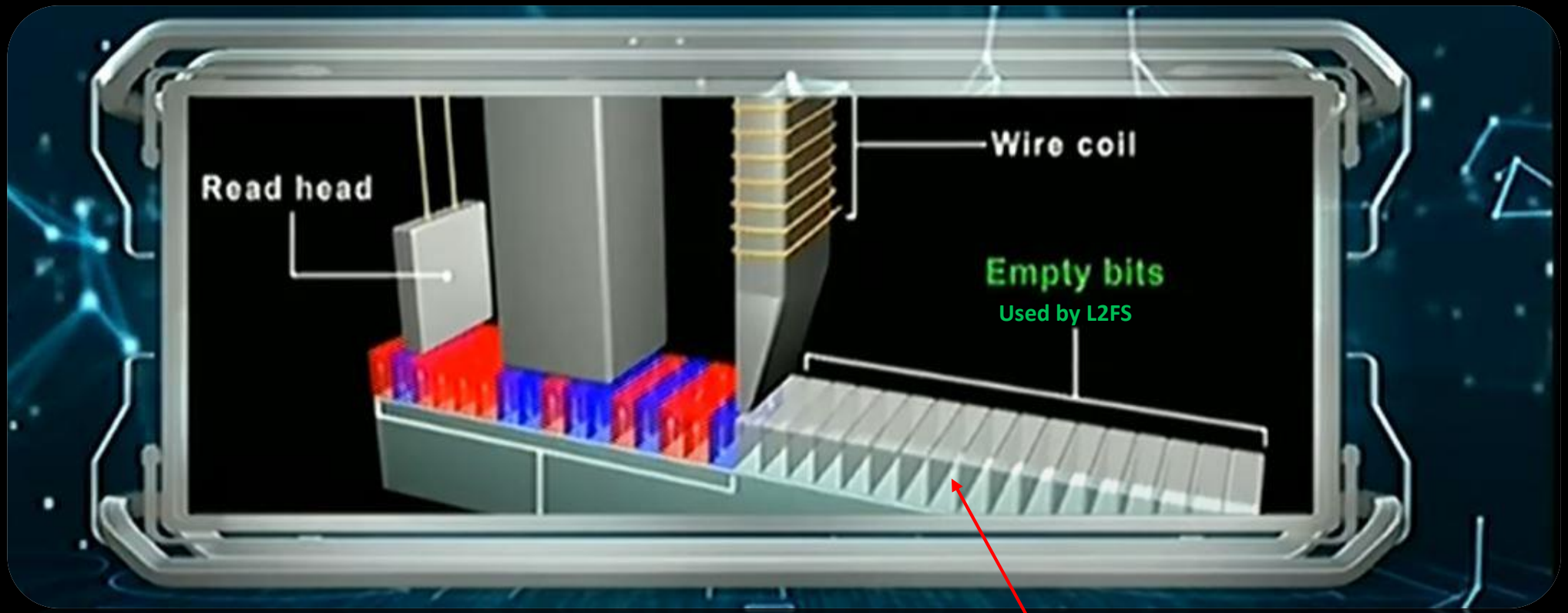
L2FS Methodology

MFT (Master File Table) is the heart of NTFS. Every file or directory has at least one entry in MFT, Microsoft calls each entry in MFT as File Record and its default size is 1024 bytes.



L2FS Application is storing Files outside MFT which is the **Non Magnetic area and unusable Space** of the Hard Disk. Only L2FS application has the power to explore the unusable area of the Hard Disk. Windows Explorer has no capability to do it.

L2FS Methodology



L2FS Application is storing Files outside MFT which is the **Non Magnetic Area** and unusable Space of the Hard Disk. Only L2FS application has the power to explore the unusable/unformatted area of the Hard Disk. Windows Explorer has no capability to do it.

L2FS Methodology

Why a Hard Drive has less Storage Space than expected?

A manufacturer considers 1Megabyte to be 1000 Kilobytes, 1Gigabyte to be 1000 Megabytes, 1Terabyte to be 1000 Gigabytes and so on. On the other hand, computers calculate on base 1MB is actually 1024 kilobytes, 1GB is 1024MB and 1TB is 1024GB and so on. This difference in the method of computation is responsible for creating unstructured/unusable area space on Hard Drive used by L2FS.

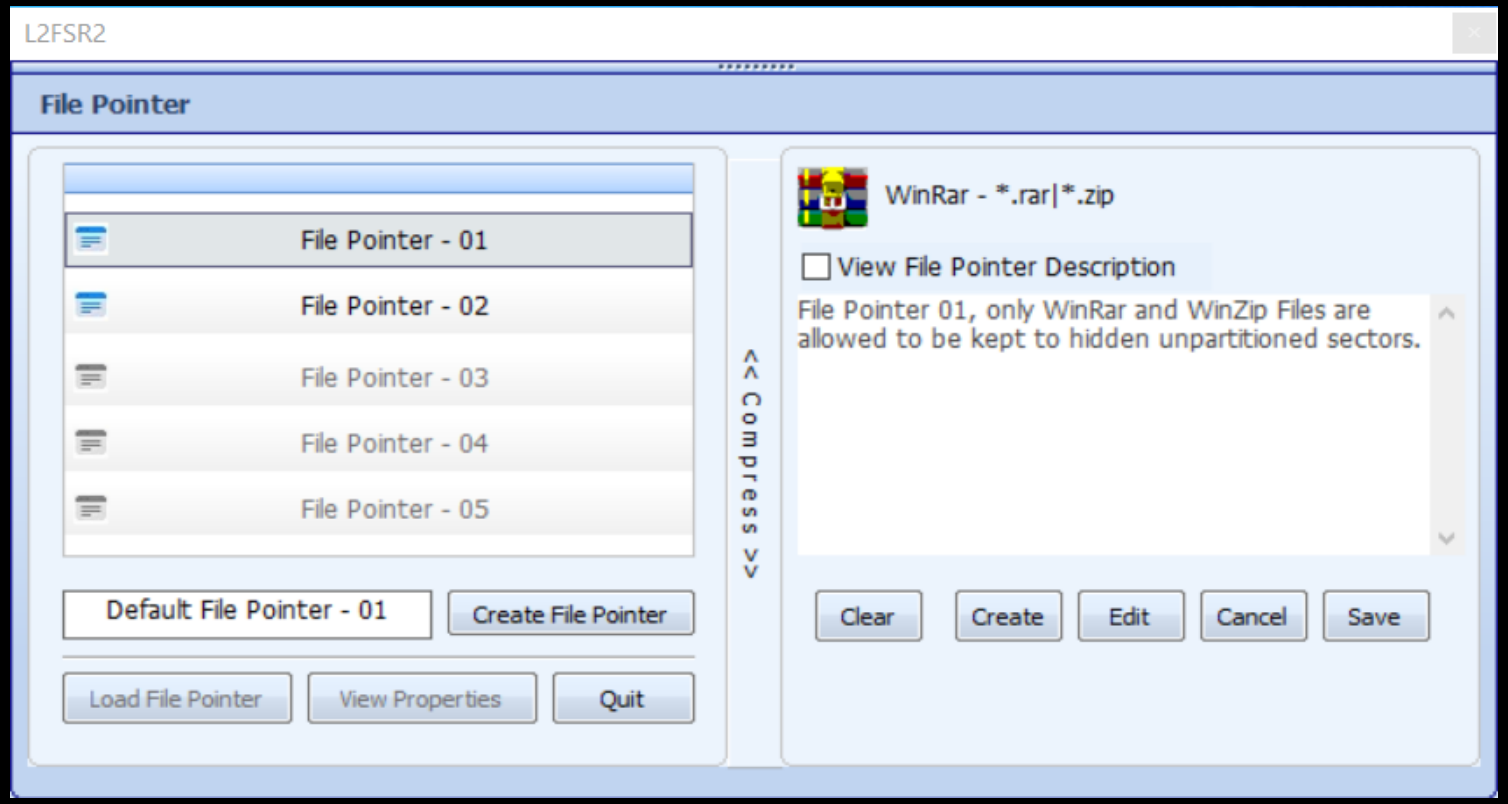
Expected Space	Displayed on PC	Space Difference
250GB	232.83GB	17.17GB
500GB	465.66GB	34.34GB
1TB	931.32GB	92.68GB
2TB	1862.64GB	185.36GB

Virtual Login Panel

Preventing key loggers from Password Detecting/Tracing

To Log in, just point to the Assigned Character Key (Not-Click)
then Point OK The keypad rotates after each point

L2FSR2 Main menu

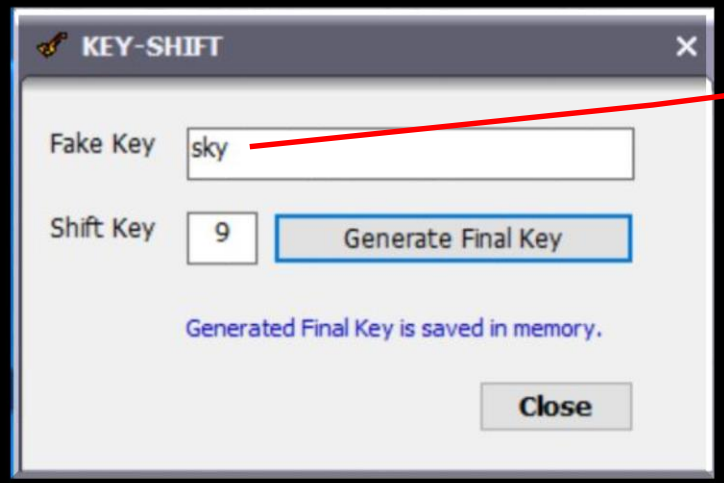


Each File Pointer can hide and store up to 2GB Compressed data of any type at Virtual list

KEY-SHIFT

Key-Shift is a new technique that enables a user to create a disguised or fake Key and transforms it into a Strong and complex Password combination, and this Key can be sent through the an unsecured internet public connection without worries.

When plugging the Fake Key and Shift Key, Press ”Gen. Final Key” the system will generate an additional layer of security and expand the key to 3072 bit during the encryption process



This is a Fake Key and a User open key. Open Key is a Key to be used on Public Communication Channels such as Facebook, WhatsApp, Messenger, and Emails. This is a key to be sent to remote Users. The Final Key is hidden while L2FS / SDC is active.

KEY-SHIFT

SDC has a unique feature for sending a password or key to remote users without affecting the integrity of the password or the key of the encrypted file.

Key-Shift is a new technique that enables a user to create a disguised or fake Key and transforms it into a Strong and complex password combination, and this Key can be sent through the unsecured internet public connection without worries.

Key-Shift password utility is used to transmit the password without compromising the password or the Key due to its disguise and fake key technique in transmission.

SDC will generate an additional layer of security and expand the key to 3072 bit during the encryption process. In other words, the User is sending the disguised and fake key to remote users then the fake key will be converted by Key-Shift to the original Key or password by the remote user in order the remote user is able to decrypt the encrypted file sent by another user. This is the safest and secure way of sending passwords on unsecured public internet communication channels such as Facebook, Messenger, WhatsApp, and Skype and so on.

KEY-SHIFT

Advantages of using Key-Shift

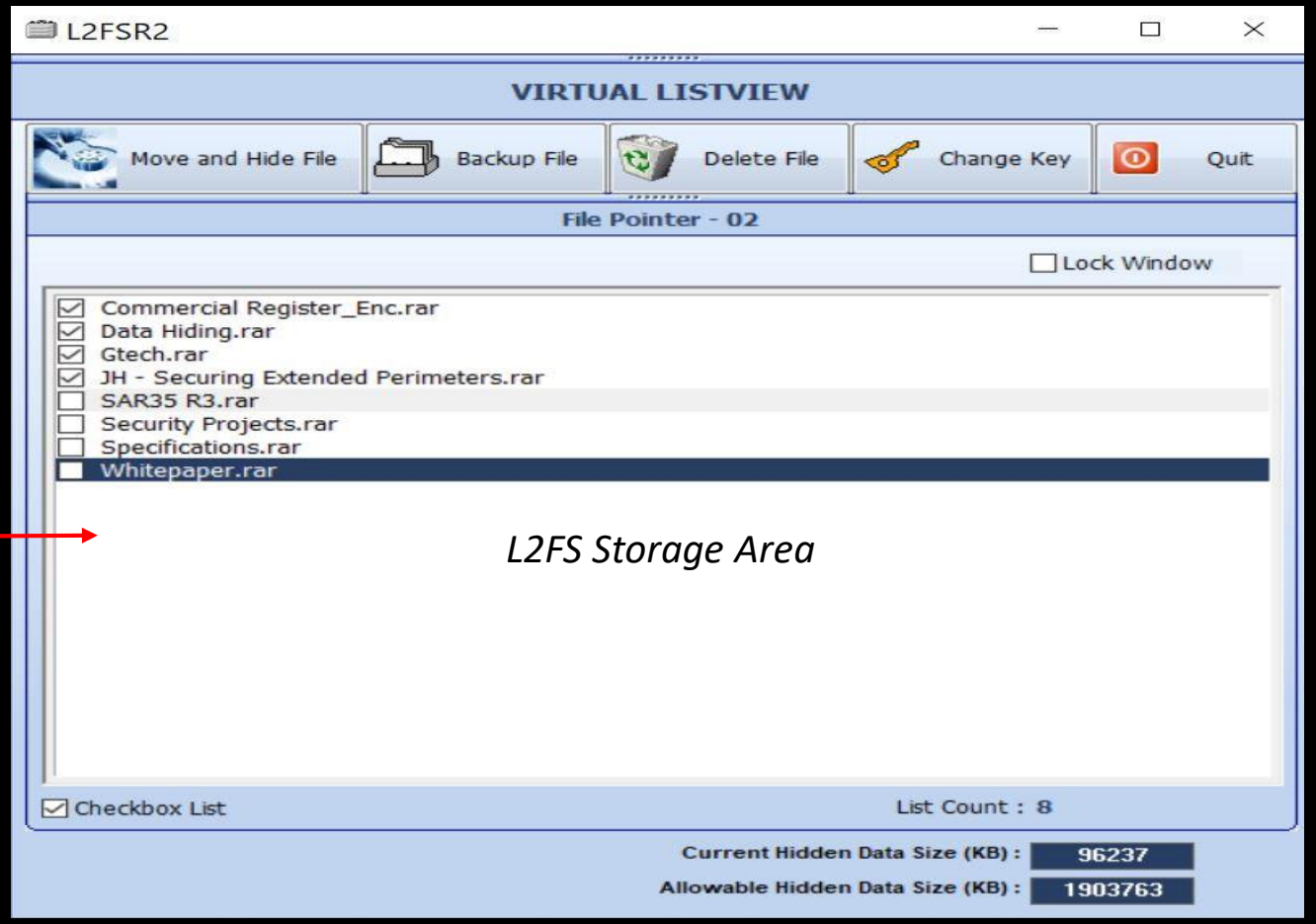
1. Easy Key or easy Password memorization
2. Easy usage in the password entry
3. Cannot be compromised on open and unsecured communication channels
4. Tricky Key
5. Forget the Final Key, Only the Fake Key to memorize
6. Key Format is flexible and reversible
7. Key length is very long
8. The Key combination is unpredictable and cannot be compromised

Encryption Process in Hiding Files

- L2FS Software is creating and preparing a Secure Virtual Working Environment in a Low-Level location of the Windows Operating System for Data manipulation.
- L2FS has a powerful technique in the encryption process, it divides the Data into 8 Blocks each block is encrypted with different keys, then it encrypts again the whole Data with the user key before applying the dissociation process. In short, the data is very secure even before storing Files in the Second Layer of the Master File Table (MFT) and GUI Partition Table (GPT).

Virtual list menu

A virtual list is a list of hidden Files stored in an unstructured area of the HD



Quantum
Smart information technology

TRUSTED SECURITY SOLUTIONS (TSS)

L2FSR2

Designed to Prevent:

- ❑ *Opening*
- ❑ *Deletion*
- ❑ *Copying*
- ❑ *Searching*
- ❑ *Infection*

FEATURES

Unauthorized access is not allowed

- **384-byte key** encryption
- Unique Encryption & Hiding technologies
- Memory Encryption
- Files secure from Malware and Ransomware attacks
- Flexible Key Usage & Secure Key Management
- Key-Shift is Secure
- PNP - Plug and Play Key in Key-Shift
- All Data Security Functions are non-repudiation
- Hiding and storing 10GB total file size at Virtual List
- Unlimited Backup storage of hidden data
- Backup of hidden files highly secure and protected
- Hiding File Outside Master File Table (MFT) and GUI Partition Table (GPT) (Beyond Windows Operating System Control)

No

- Data Memory Dump *- Reverse engineering*	*Fingerprint or trace of Data in the Hard Drive*	Weak login password is allowed

L2FSR2 Sophisticated Technique in Data Protection

Can Malware Attack

The Main L2FSR2 Executable?

The answer is Yes, but L2FSR2 has its built-in module protection to analyze its integrity. This is called ***Cyclic Redundancy Integrity Check (CRC)***. This means when Malware attacks L2FSR2 executable, L2FSR2 will not execute in order to prevent spreading of the infection, instead will prompt a message to reinstall L2FSR2 to overwrite the infected executable.

L2FSR2 is protecting data independently without third-party software conflict. If the Hard Disk is encrypted by a third-party software, the protected data by L2FSR2 are still intact and not affected.

L2FSR1 – Layer 2 File Security

Has Meet Security Software Standard

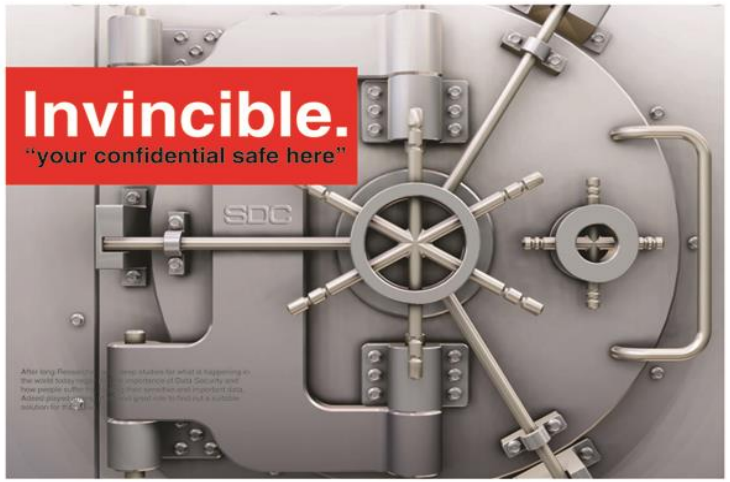
- **ISO/IEC 27045** - *Information technology - Security Techniques – Big Data Security and Privacy Processes.*
- **ISO/IEC 27034-4** - *Information technology - Security Techniques – Application Security and Application Security Validation.*

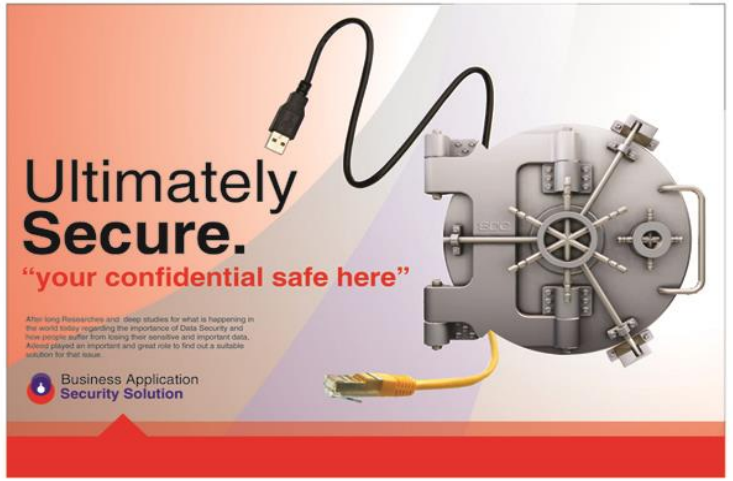
SECURE DATA ACCESS CONCEPT

Please always remember that any File/Document that is visible to the eyes of the attacker is vulnerable to attack and the vulnerabilities can be exploited at any point in time, just time matters.

Files in the Hidden Unpartitioned
Sectors of the Hard Drive unreachable

TRUSTED SECURITY SOLUTIONS (TSS)





thank you