TRIP-5/6 Recording & Snapshot Data Protection Manual Ver 1.2

Compilation and Publication Notice

This manual is covering the latest product descriptions and specifications.

It is our policy to constantly improve the design and specifications. Accordingly, the details represented herein cannot be regarded as final and binding. The contents of this manual and the specifications of this product are subject to change without notice.

NextVision reserves the right to make changes without notice in the specifications and materials contained herein and shall not be responsible for any damages (including consequential) caused by reliance on the materials presented, including but not limited to typographical and other errors relating to the publication.

For Further information please contact
NextVision Stabilized Systems Ltd.
info@nextvision-sys.com

Table Of Contents

1. Introduction

The following document is the recording & snapshot data protection user manual for the TRIP5 and TRIP6 systems.
The document will explain how to enable and use encryption for the local recording and snapshot that the system generates.

2. *Recording and Snapshot Data Protection*

The TRIP-5 system is able to encrypt the local recording and snapshots that it generates during its normal operation, the encrypted data will be stored in the SD Card.

The TRIP-5 system uses RSA4096 in order to encrypt a AES256 key that will be used for the encryption/decryption.

In order to make things as secure as possible the following method is used:

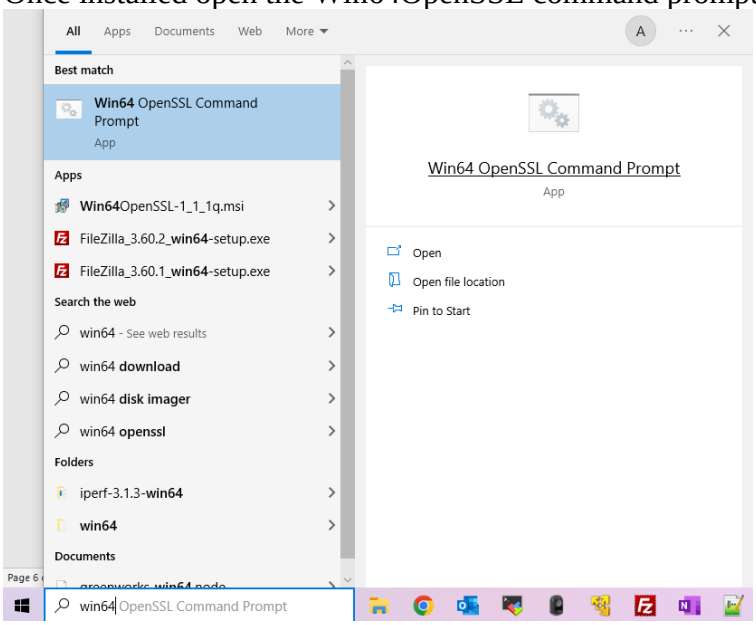
1. The user will use Win64OpenSSL in order to generate a key pair using RSA4096
2. The generated public key will be copied to the root directory of the SD Card that is inserted in to the TRIP device.
3. Using the TRIP website encryption must be enabled.
4. The TRIP will generate its own unique key and will use it to encrypt the recordings and snapshots, the encryption method is AES256-CBC.
5. The TRIP will encrypt the unique key using the public key that was copied to the SD Card and will save it to a file.
6. The user will decrypt the encryption key using the private key.
7. With the encryption key the TRIP Decryption tool will be used to decrypt the data.

The next parts explain in detail how to implement the steps from the above list

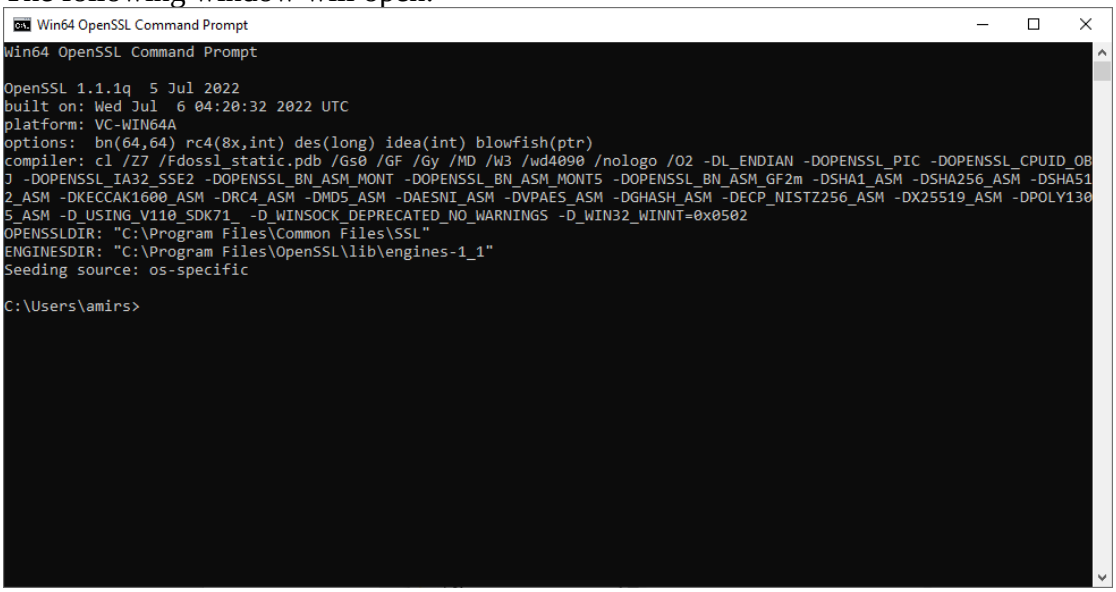
2.1. Generate an RSA4096 Keypair

Download and Install Win64OpenSSL-1_1_1q from the following link:
https://slproweb.com/download/Win64OpenSSL-1_1_1q.msi

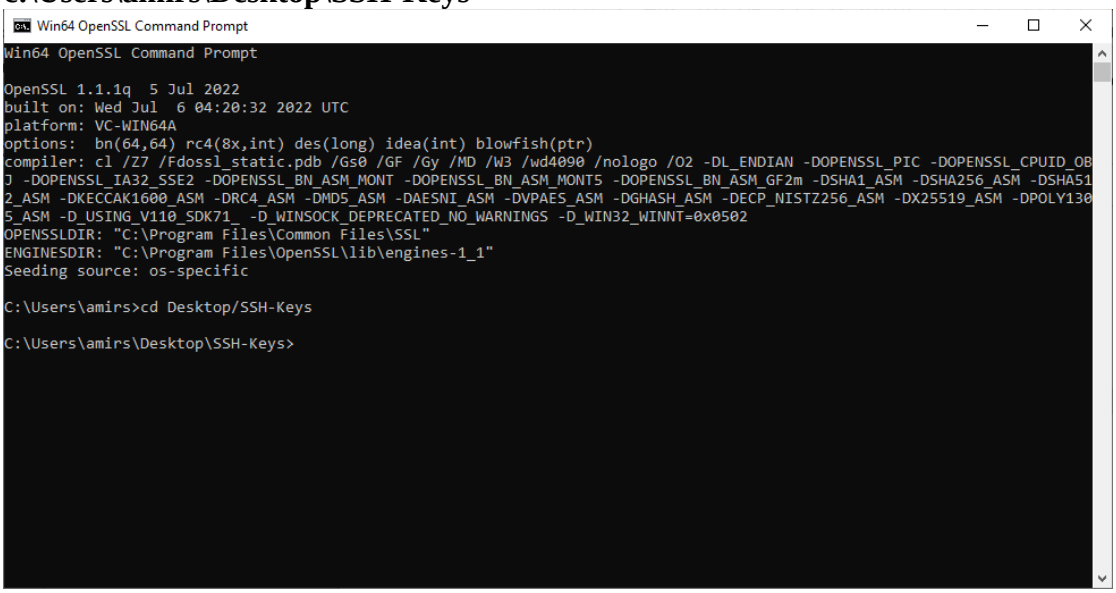
Once installed open the Win64OpenSSL command prompt



The following window will open:

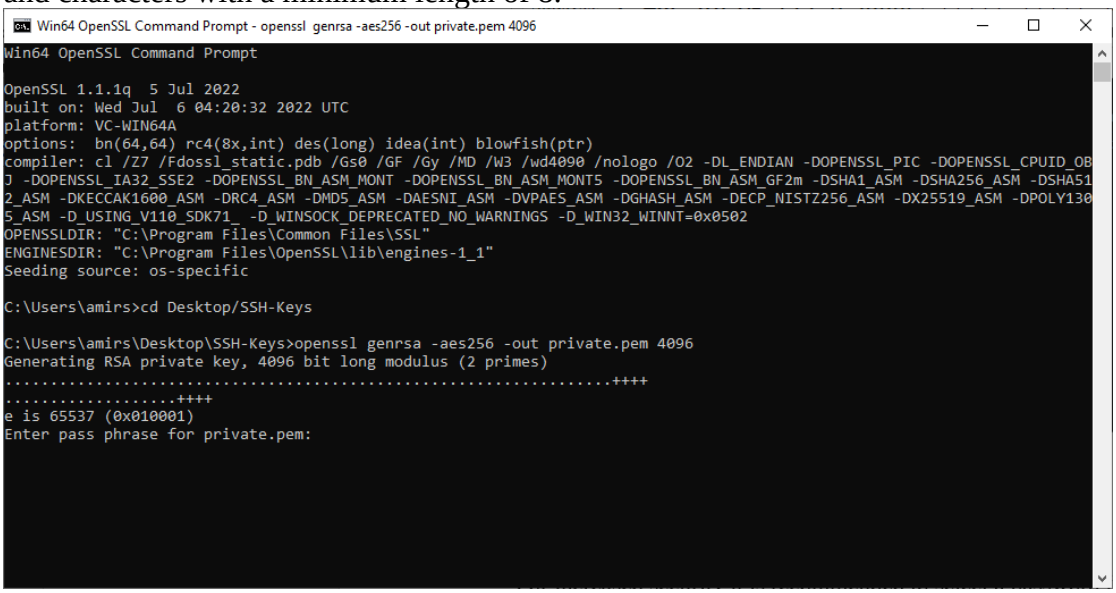


Using the cd command enter a directory of your choosing, once generated the keys will be saved there.
In the following example the keys will be saved to
c:\Users\amirs\Desktop\SSH-Keys



Use the following command in order to generate the keys:
openssl genrsa -aes256 -out private.pem 4096

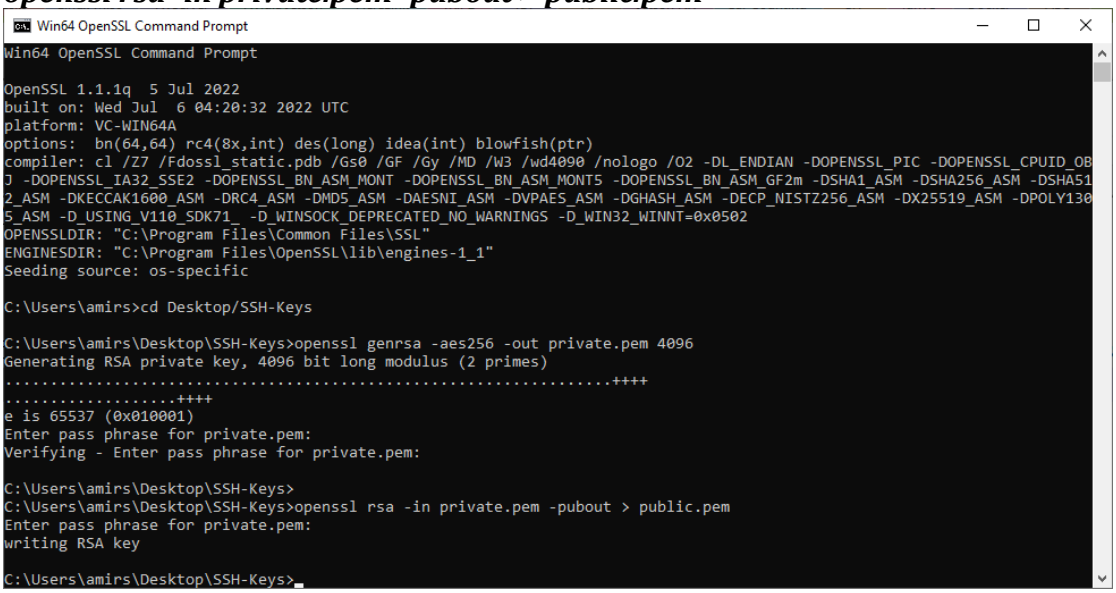
The command will prompt you to enter a password for the key,
For increased security it is recommended to select a password the has both numbers and characters with a minimum length of 8.



Enter your password in order to generate the private key.

In order to extract the public key from the private key please use the following command:

openssl rsa -in private.pem -pubout > public.pem

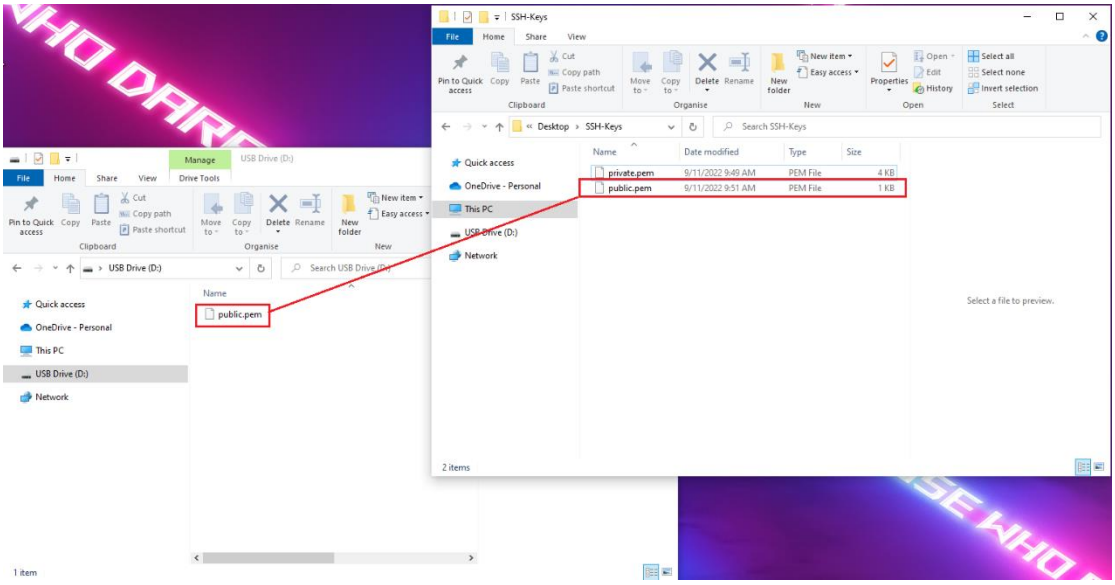


Enter your password in order to generate the public key.

Although the private key is guarded with a password, still it is recommended to keep the file in a safe location.

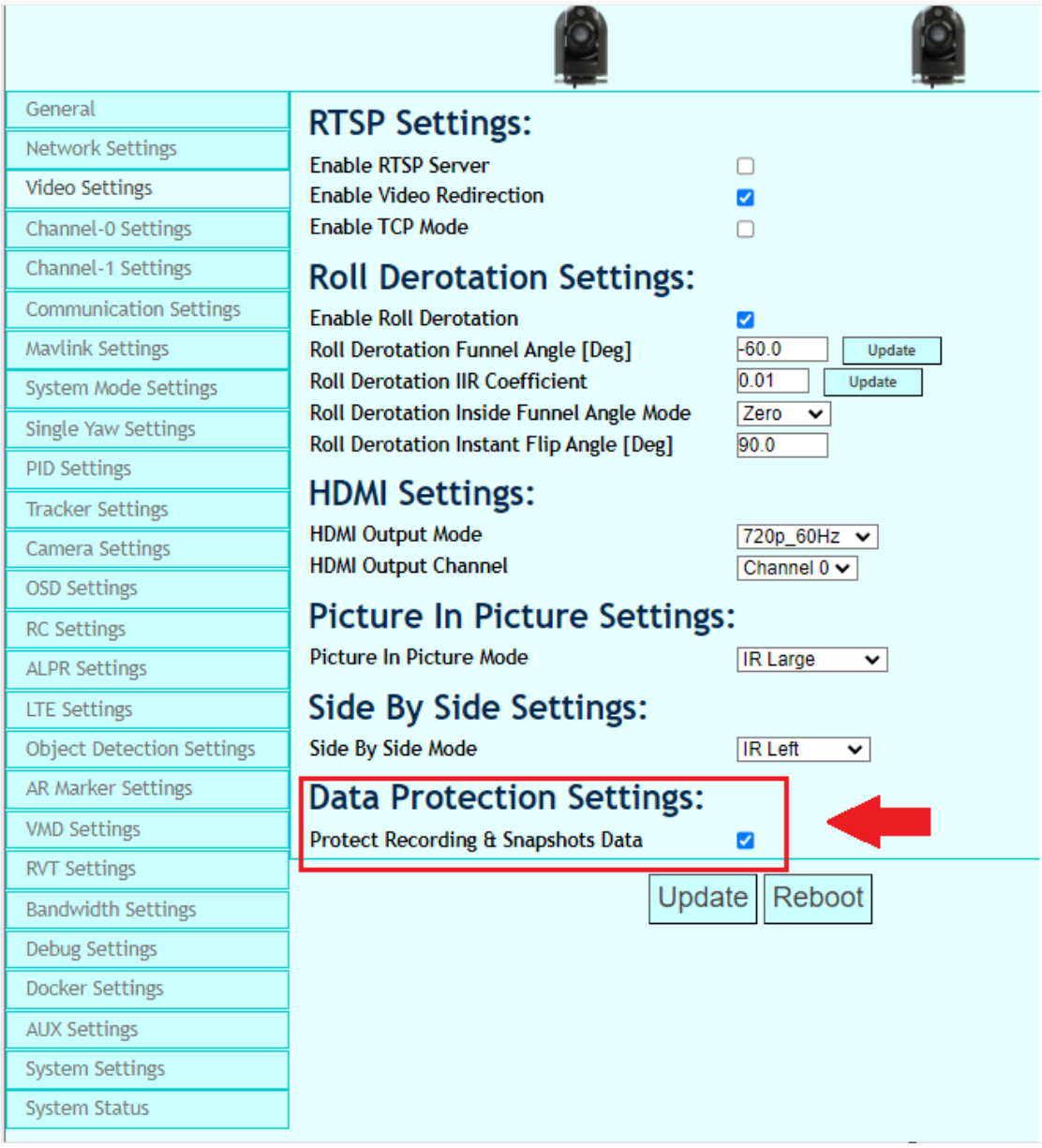
2.2. Copy the Public Key to the TRIP SD Card

Insert the SD Card to a PC using an SD Card reader.
Please make sure that you are using an SDXC card.
Please make sure that the SD Card is formatted to exfat.
Copy the public.pem file that was generated in the previous step to the root directory of the SD Card.



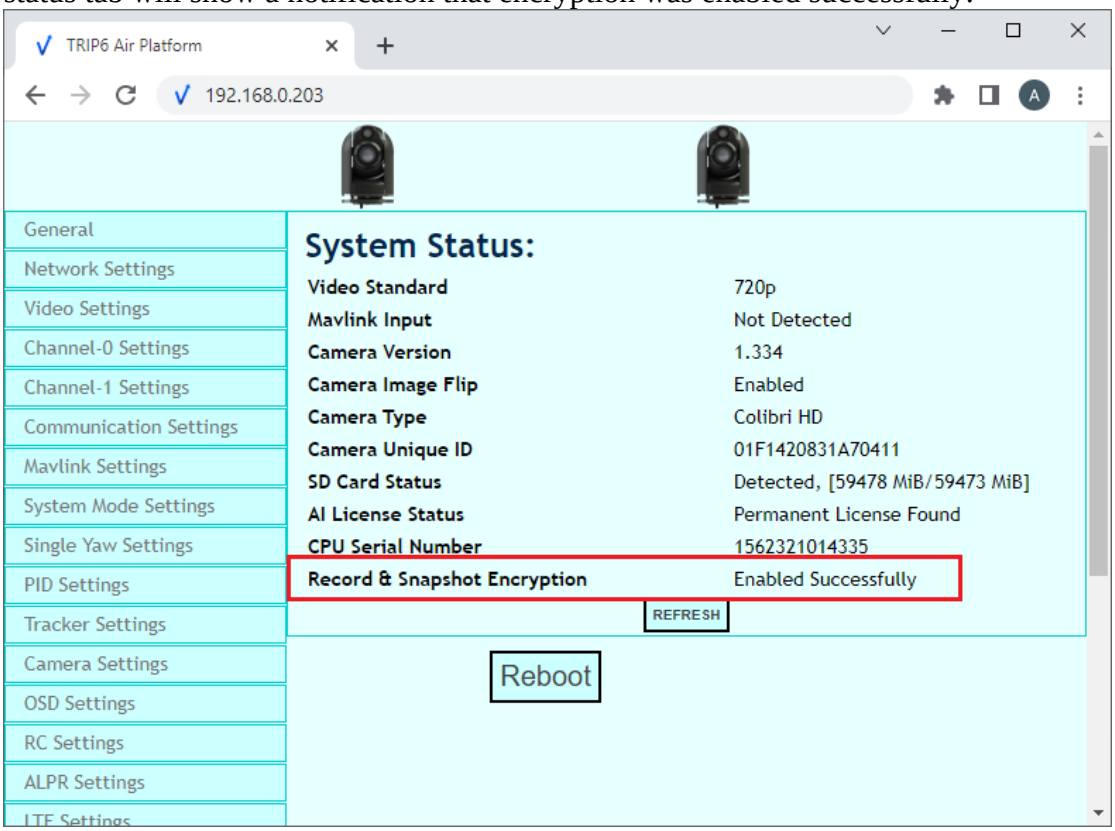
2.3. Enable Protect Recording & Snapshots Data in TRIP Website

Access the video setting tab of TRIP website and enable encryption by checking the Protect Recording & Snapshots Data checkbox:



Press on the update button

When encryption is enabled and public.pem file is placed in the SD Card the system status tab will show a notification that encryption was enabled successfully:



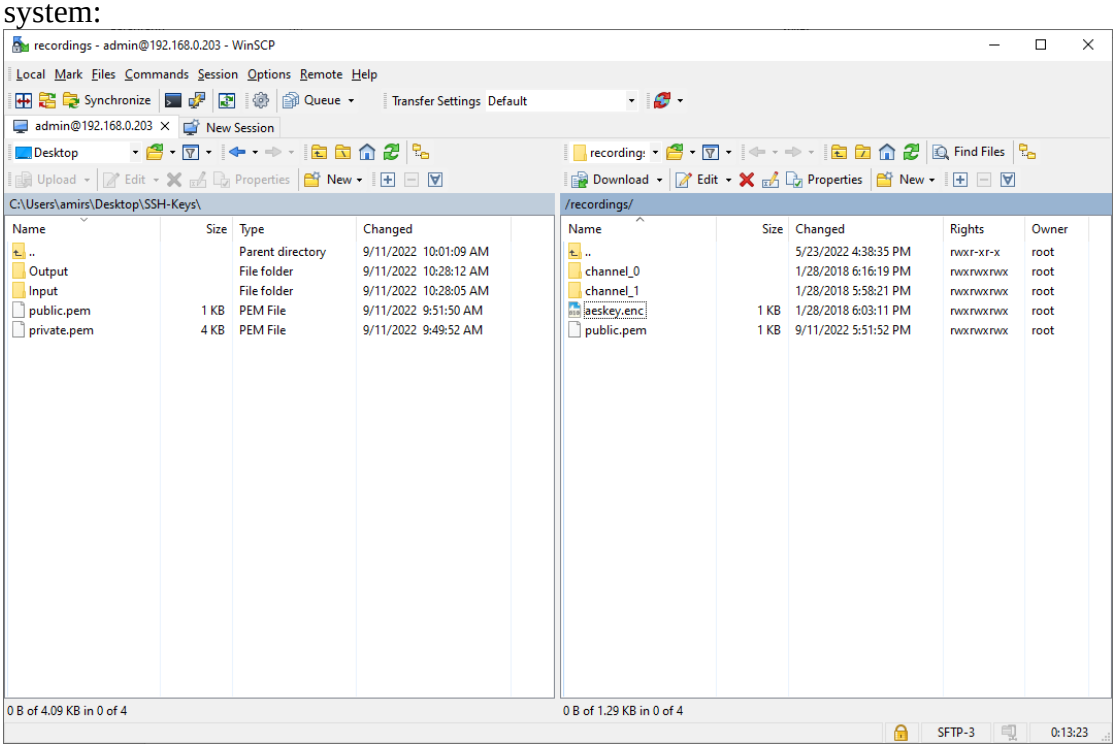
This indicates that the TRIP will encrypt the recording and snapshots

2.4. Obtaining the Decryption Key

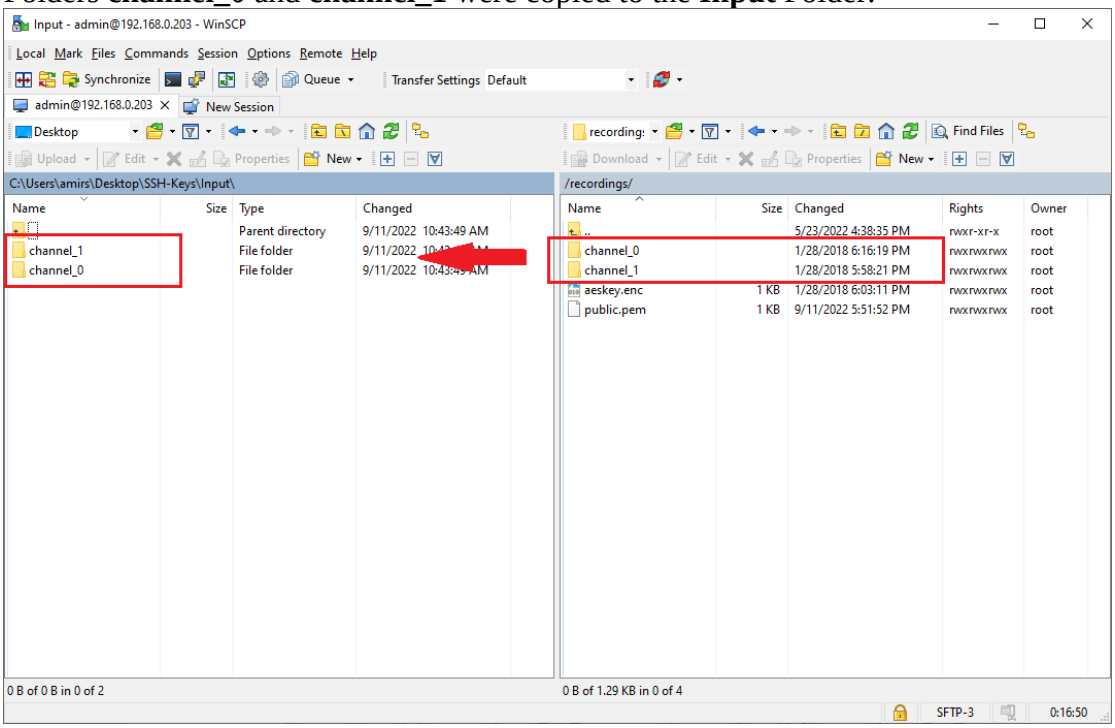
At this point the TRIP should have made some recordings and snapshots that were encrypted, in order to access them the decryption key is needed.
In order to obtain the decryption key insert the SD Card to the PC using an SD Card reader or use WinSCP to download the entire content of the SD Card to the PC.

In this example 2 folder were created: **Input** and **Output** in the same directory that we generated the keys **c:\Users\amirs\Desktop\SSH-Keys**
Please create an **Input** directory and **Output** Directory in the location that you have generated the keys.

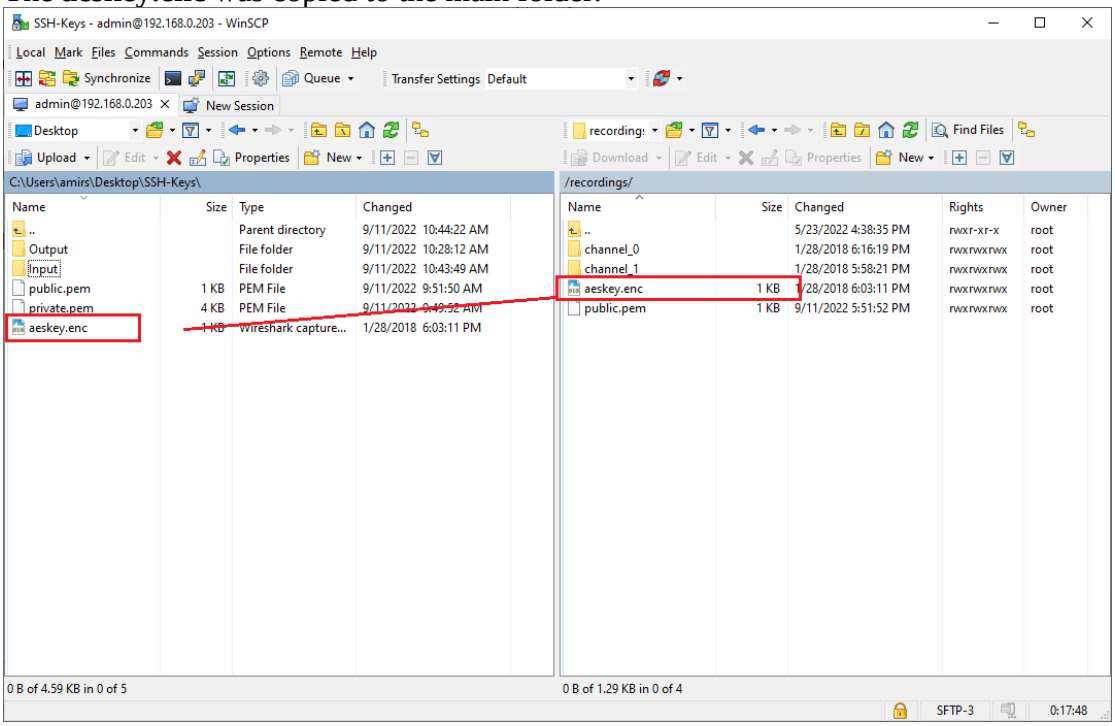
WinSCP was used to download the recording and snapshots that were taken by the system:



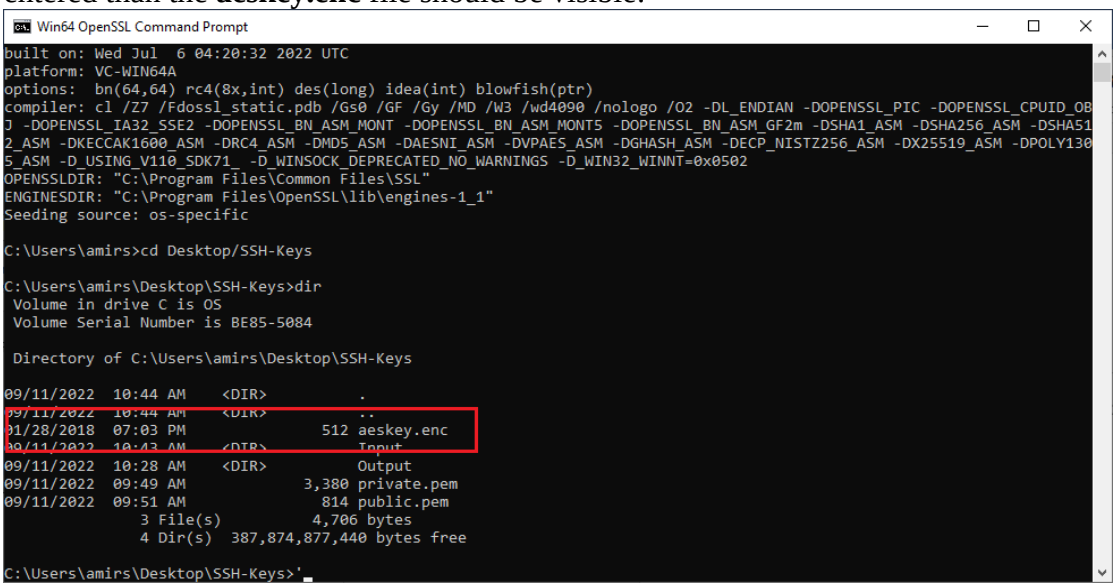
Folders **channel_0** and **channel_1** were copied to the **Input** Folder:



The **aeskey.enc** was copied to the main folder:



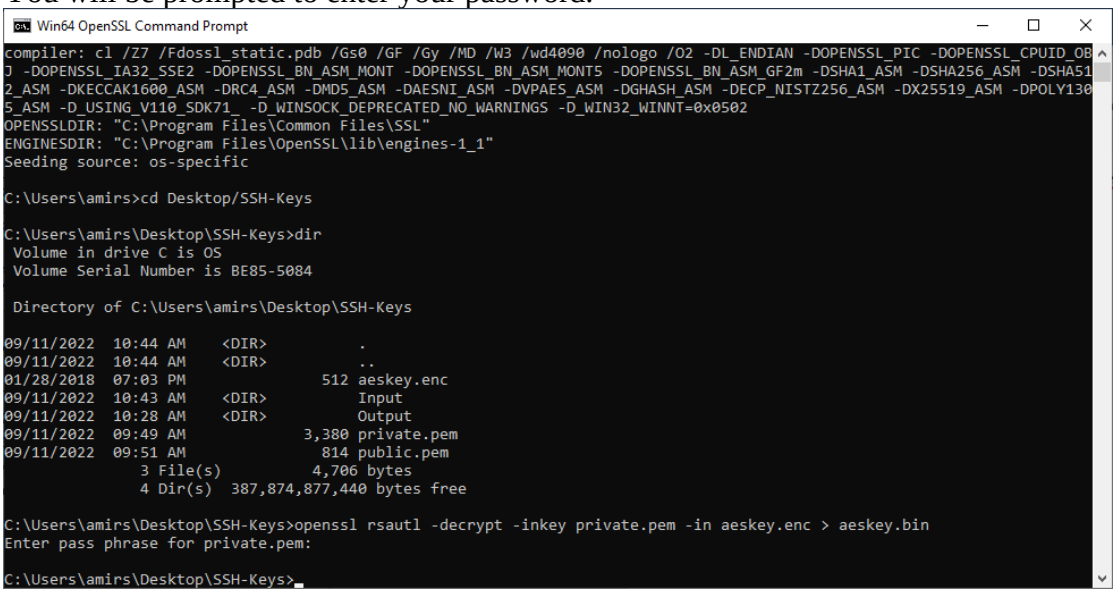
Now go back to the Win64OpenSSL command window, if the command **dir** is entered than the **aeskey.enc** file should be visible:



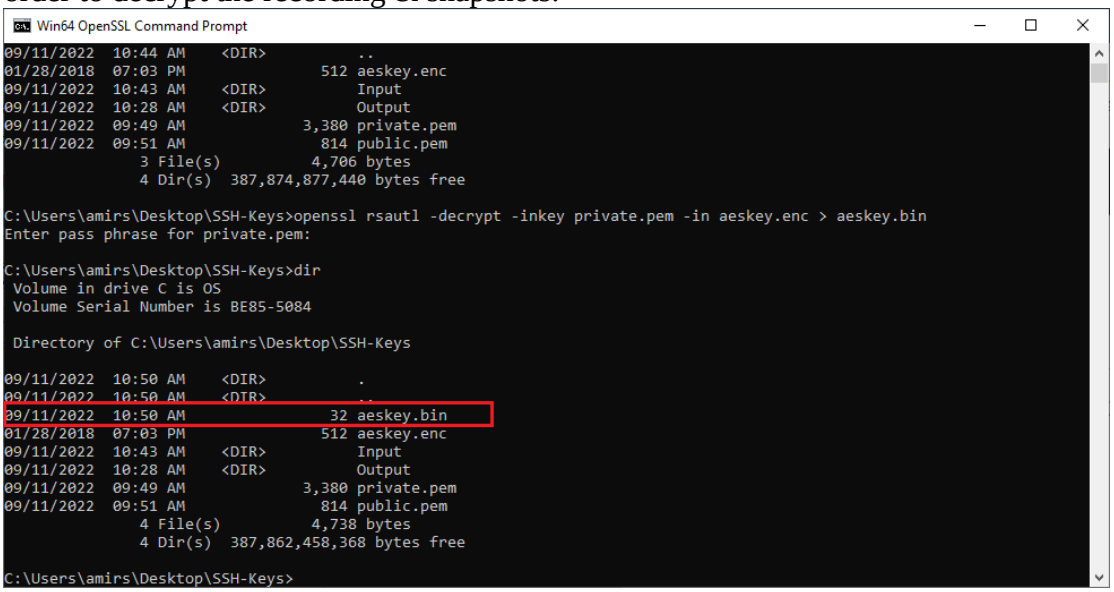
The **aeskey.enc** file hold the decryption key, please use the following command to decrypt the file:

openssl rsautl -decrypt -inkey private.pem -in aeskey.enc > aeskey.bin

You will be prompted to enter your password.



Now if the command **dir** is entered again a new file called **aeskey.bin** file should be visible, this is the decryption key that will be used by the TRIP decryption tool in order to decrypt the recording & snapshots:

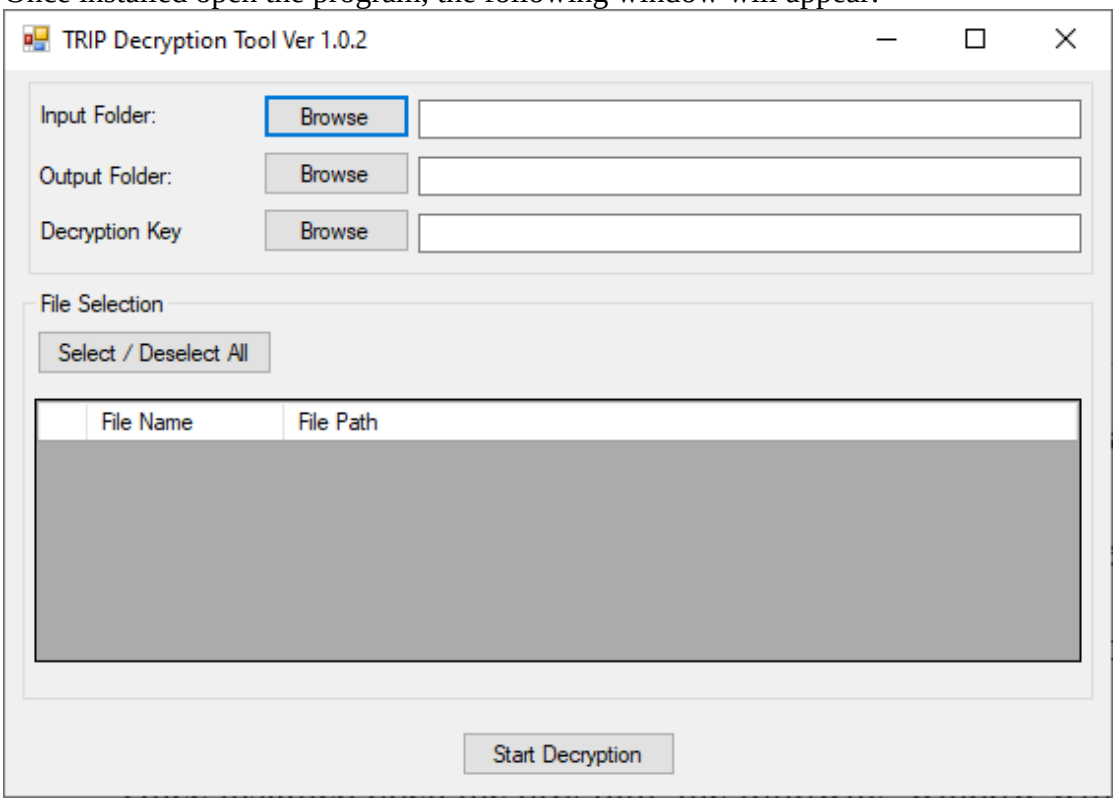


The Win64OpenSSL command prompt window can now be closed, there is no more use for it.

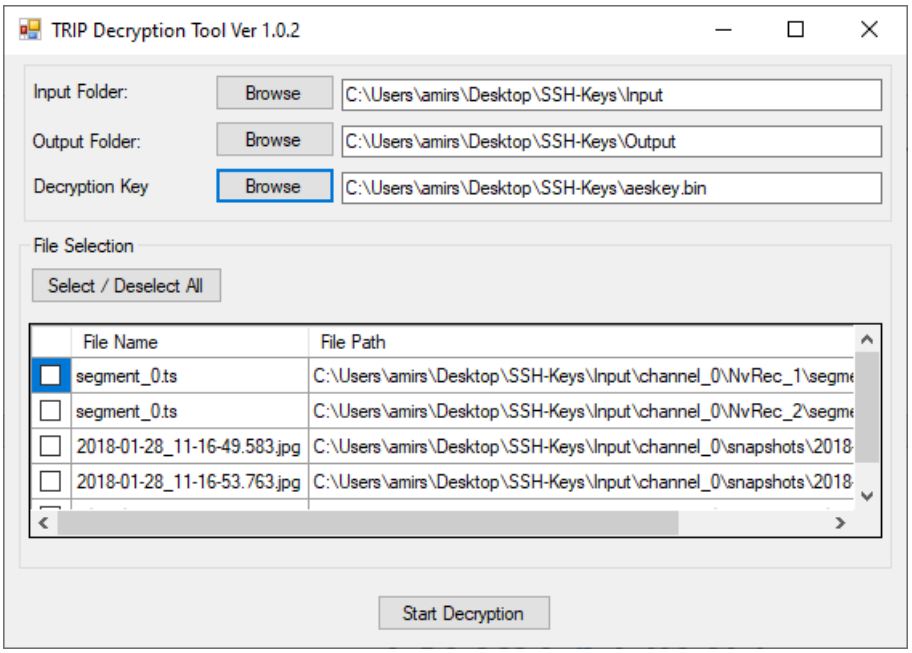
2.5. Decrypting the Recording and Snapshots

Download and install the TRIP Decryption Tool, you will be able to find it in Nextvision Google Drive under:
Applications/TRIP Decryption Tool/TRIP Decryption Tool Installer Ver x.x.x.msi

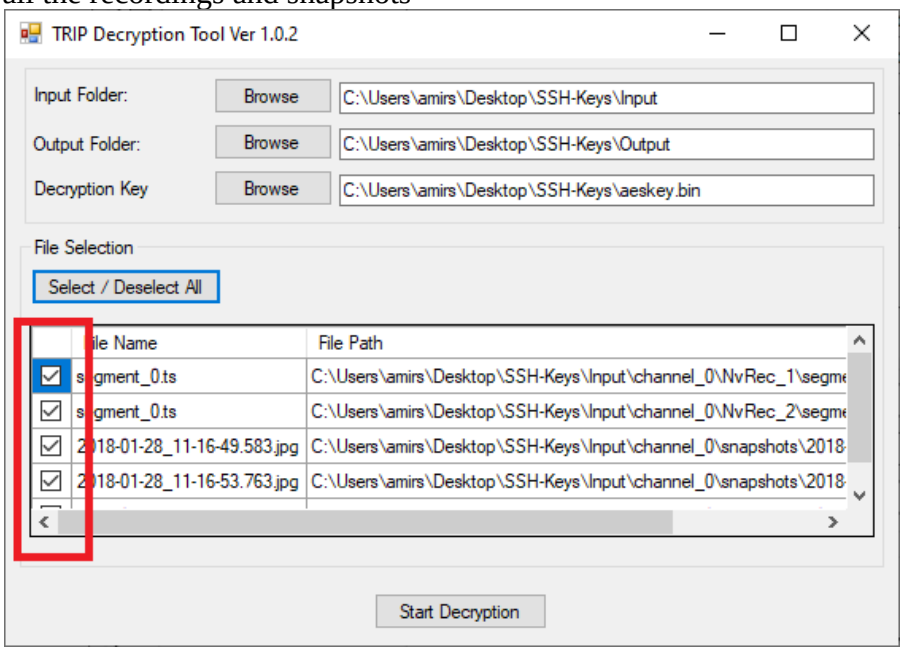
Once installed open the program, the following window will appear:



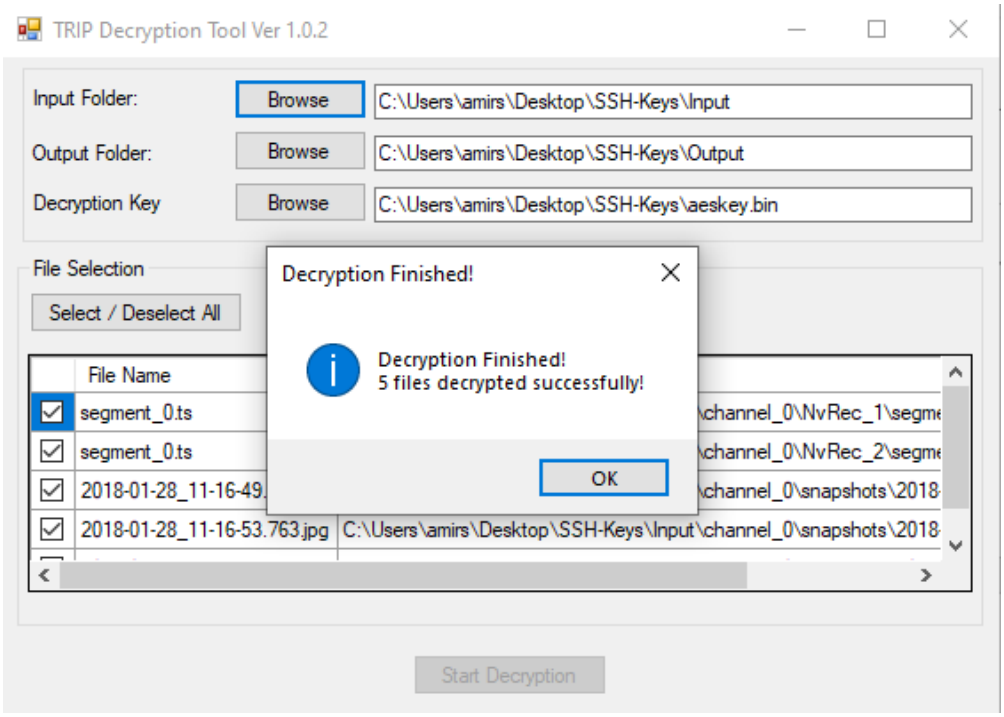
Press on the browse buttons and select the **Input** folder and **Output** folder that you have created and copied the recording and snapshots to in the previous step.
Also press on the browse button on the Decryption key and select the **aeskey.bin** file that was obtained in the previous step:



Select which recordings and snapshots to decrypt or press on the select all button to decrypt all the recordings and snapshots



Press on the Start Decryption button and wait until the decryption is done,
Once the decryption is finished a small result window will open:



The output folder will now have the exact directory structure as the input folder and within all the decrypted recording and snapshots.

For improved security it is recommend to delete the aeskey.bin file from the filesystem and clear it from the PC recycle bin

The public.pem file can remain in the SD Card in order to enable encryption using the website.
The private.pem file should be kept in a safe location.

Revision Control

Version	*Description*
1.0	Created
1.1	Update document name