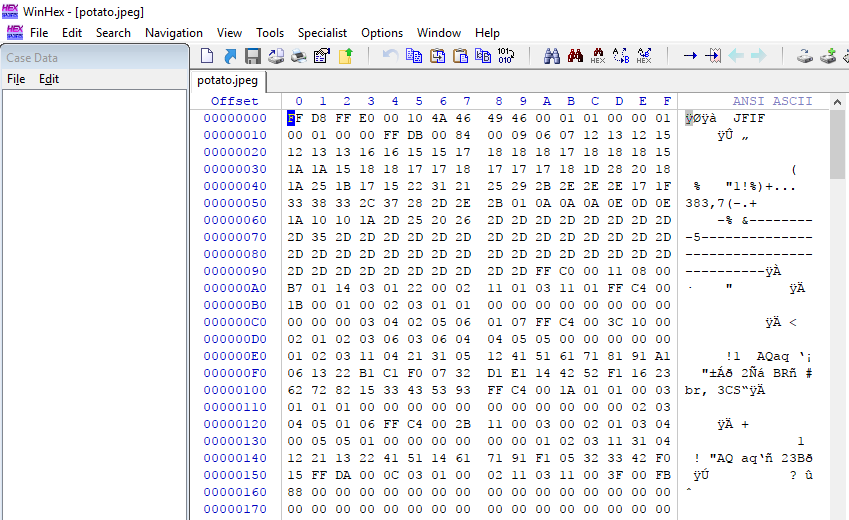
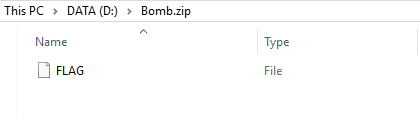
1. One Steganography Technique: PKZIP Inside JFIF

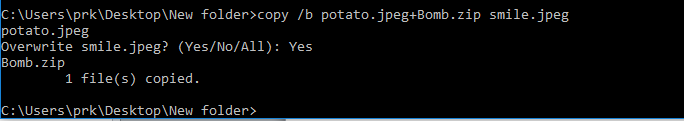
One of the most classic yet powerful Steganography techniques is to hide a file inside an image. Given a simple potato image with hex dumped like:



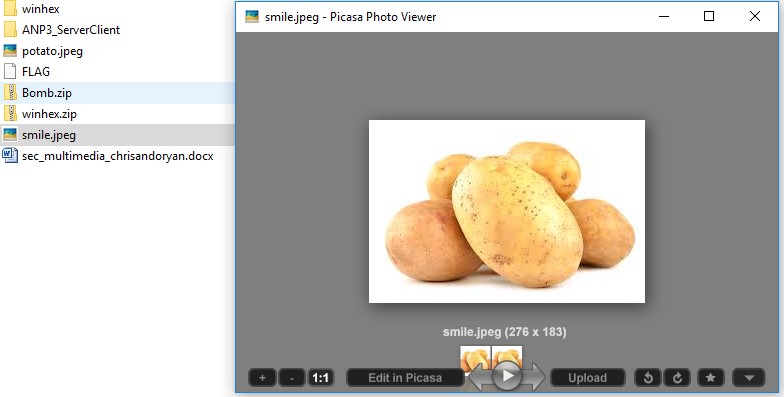
Take a look at hex number at offset 00000000, FF D8 FF E0, or string JF IF in ANSI ASCII Section. Those were called File Signature, which the computers used to identify a file, and how to open it. In this case, JF IF is a file signature for JPEG file. JPEG also have a terminating byte at the end, represented by hex FF D9.

In the picture below, I create a zip file, containing a single file named FLAG, followed by my attempt to copy all the hex structure into our potato image. Why doing this? The goal is to create an image, still can be opened and viewed by a regular photo viewer, but when we open it using compression tool (WinRAR or something else), we could see our FLAG file, which originally stored inside our zip file.

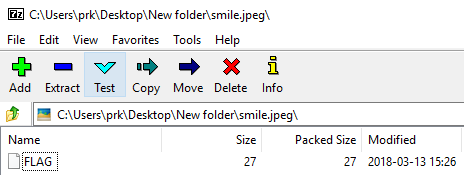




The copy /b command above treats our files as binary, and then copies them copies them byte for byte, one after another. So it simply means we append every binary inside potato.jpeg file, append them with binaries from Bomb.zip file, and then copy all the appended binaries into smile.jpeg file.



Finally, as theorized above, we could still open it with a regular photo viewer.



But still openable also using 7zip Archive Manager.

Why is this possible? In short hands, this could be happened because an image file has starting and ending bytes, dictating the size of the image (the JF IF and FF D9). Upon displaying the picture, an image viewer will look after the starting bytes, and then stop its reading process after encounter the terminating byte. It used the information between these bytes, but ignoring anything after the terminating byte, which is then, in fact, filled by our zip file binaries.

1. EXIF and Metadata

EXIF stands for Exchangeable Image File Format, which is a standard for storing metadata in image and audio file. There are so bunch of tools available online to inspect and display the metadata (including EXIF), but this time we give Picasa a go.

1. Hexdump with WinHex

WinHex is a disk and hex editor used to dump and display hex bytes of a file, along with its related ASCII, whenever they are printable. WinHex and similar tools is really useful in data recovery and digital forensics.

