Encryption and creating decrypted copies

The U.S. Attorney's office typically sends discovery in "**encrypted**" format, whether it is on media (CD Rom, USB drive, or hard drive) or through the internet (email or USAfx). Encryption adds a layer of protection by scrambling the data so files cannot be seen unless a digital "key" (password) is provided. The goal is to protect the data while it is being shipped in case it is lost or stolen.

"**Decryption**" is the process of converting the file so it is readable. **The first step you should take when you receive encrypted files is to create a decrypted copy of the files**. The decrypted copies will allow you to search, review and work with them on your computer that the encrypted files will not, and you will not need to enter a password each time to open them.

When receiving encrypted case related materials:

1. **Look for cover letters and associated correspondence that mention password protection or encryption.** Often the sender will tell you that the files are encrypted and provide instructions on how to obtain the key (password). If the media contains encrypted files you cannot work with them unless you have that password.

2. **Use a Windows computer.** Most decryption programs included on the media are designed to work with Windows computers. Sometimes decryption can be done on Mac computers, but often it requires additional software not included with the media.

3. **Insert the media and look for either a "password" prompt or a decryption program.** Certain encryption programs (like Microsoft "Bitlocker") will automatically prompt for a password when the media is inserted. Other times the media will include Windows-based software programs that needs to be run.

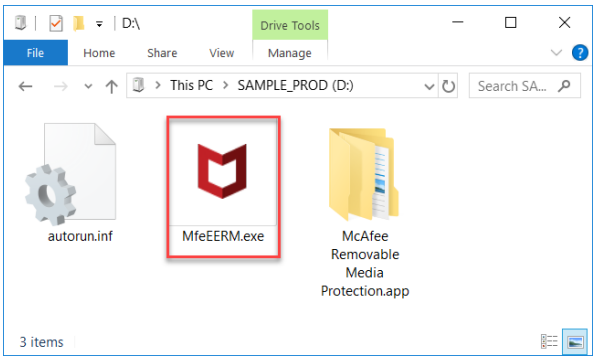
4. **Create decrypted copies of the files.** When you open a file that is encrypted a computer will typically only temporarily decrypt it. The file may be in a "read-only" mode that will not work well with most software programs, and will continue to need a password when reopening. Making a decrypted copy of the file will allow it to be correctly recognized by the programs on your computer and will no longer need a password when opening the copy.

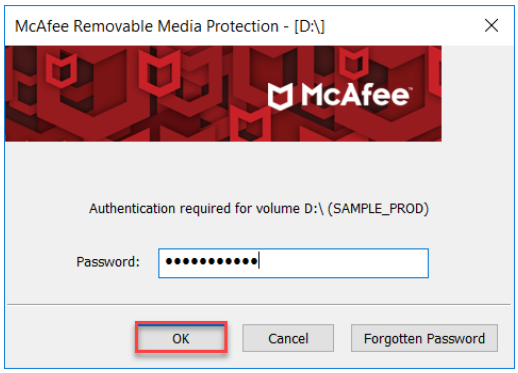
McAfee Removable Media Protection

"**McAfee Removable Media Protection**" is a common encryption program used by the USA's when delivering discovery on thumb drives and CD/DVD discs. The media usually includes an executable file that when run will allow users to make decrypted copies of the files. To create decrypted copies:

A. Create a destination. Open File Explorer (the file browser on your computer) and navigate to a destination on your computer (or external drive) with enough room to hold a copy of the files. Create a folder that will keep the unencrypted copy of the files.

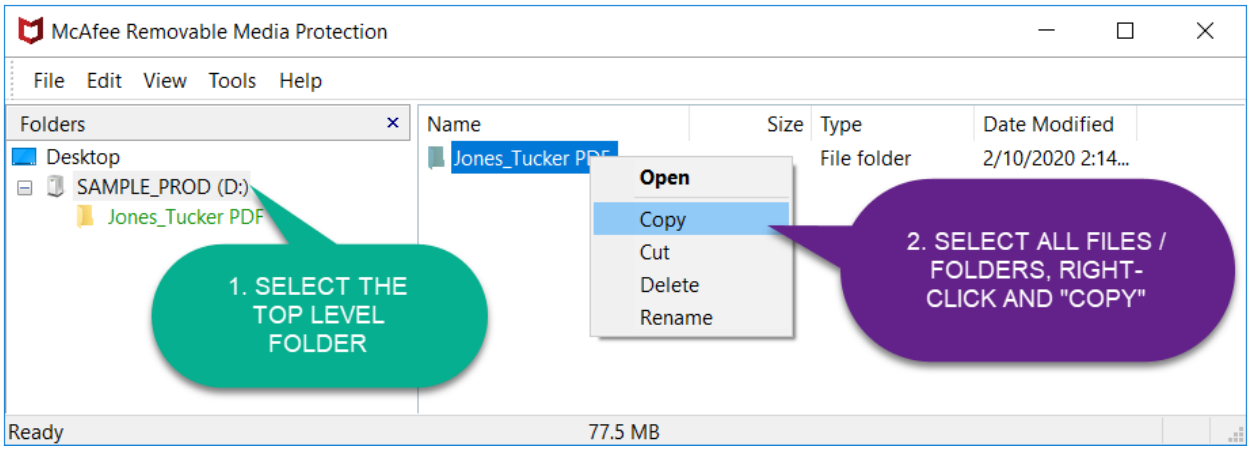
B. Open McAfee. Insert the media and look for an executable file called "**MfeEERM.exe**". Run the executable and look for a dialog window prompting for a password. Enter the password and click "OK".





C. Copy the files or folders. From within McAfee:

1. Select the "Top Level" folder from the left-hand navigation pane.
2. From the main window (on the right side), select all of the files and folders listed, right-click on them and choose "**Copy**".



D. Paste the copies into the destination. Switch back to File Explorer. Right-click on an empty space within the destination location and choose "**Paste**". For larger sets of data (over 10,000 files/folders), try dividing the copy process into smaller batches of about 1,000 files / folders each. Verify the copied files can be opened by closing McAfee and opening a few of the copied files.