Windows drive encryption detection

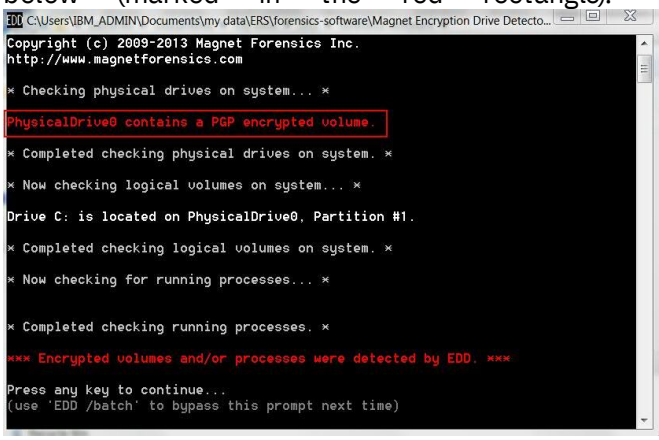
1 Preparation (on standalone machine)

1. Download Magnet Encryption Drive Detector. It is free to use and can be obtained from Vendor website: www.magnetforensics.com. It is necessary to provide contact details to download software, but the download starts after submitting the form.
2. Find removable storage media: it will be formatted, and data may be irrecoverably lost!
3. Prepare removable media:
   a. Format the media (quick format is sufficient) using NTFS or ExFAT filesystem.
   b. Copy above software onto the media.

2 Information capture (on target machine)

It is required is to have administrative rights on the machine.

1. Connect prepared previously removable media.
2. Launch Magnet Encryption Drive Detector
3. Accept "End User License"
4. Following window will be show. Let the tool run until "Press any key to continue..." will be presented.
5. Do not close the window. Take a physical note about type of encryption present in the system, by checking message "PhysicalDriveX contains a <ENCRYPTION_TYPE> encrypted volume." Example of such message is show in the image below (marked in the red rectangle):



6. In case of no encryption, following message will be shown: "No (...) encrypted volumes detectable by EDD were found."
7. When completed, close application and safely disconnect media from the system.
8. Send information about encryption to the designated IBM Security X-Force IR Consultant.