**PART 1**

**Lab 2.1 Securely Wiping a USB Drive**

1. **Which statement about deleted files is true?**

A - Deleted files can be built from remnants that haven’t been overwritten.

1. **When a file is deleted from a storage device, only the pointer to the file location is removed. True or False**

True

1. **According to NIST standards, how many wipes should be done to erase data completely?**

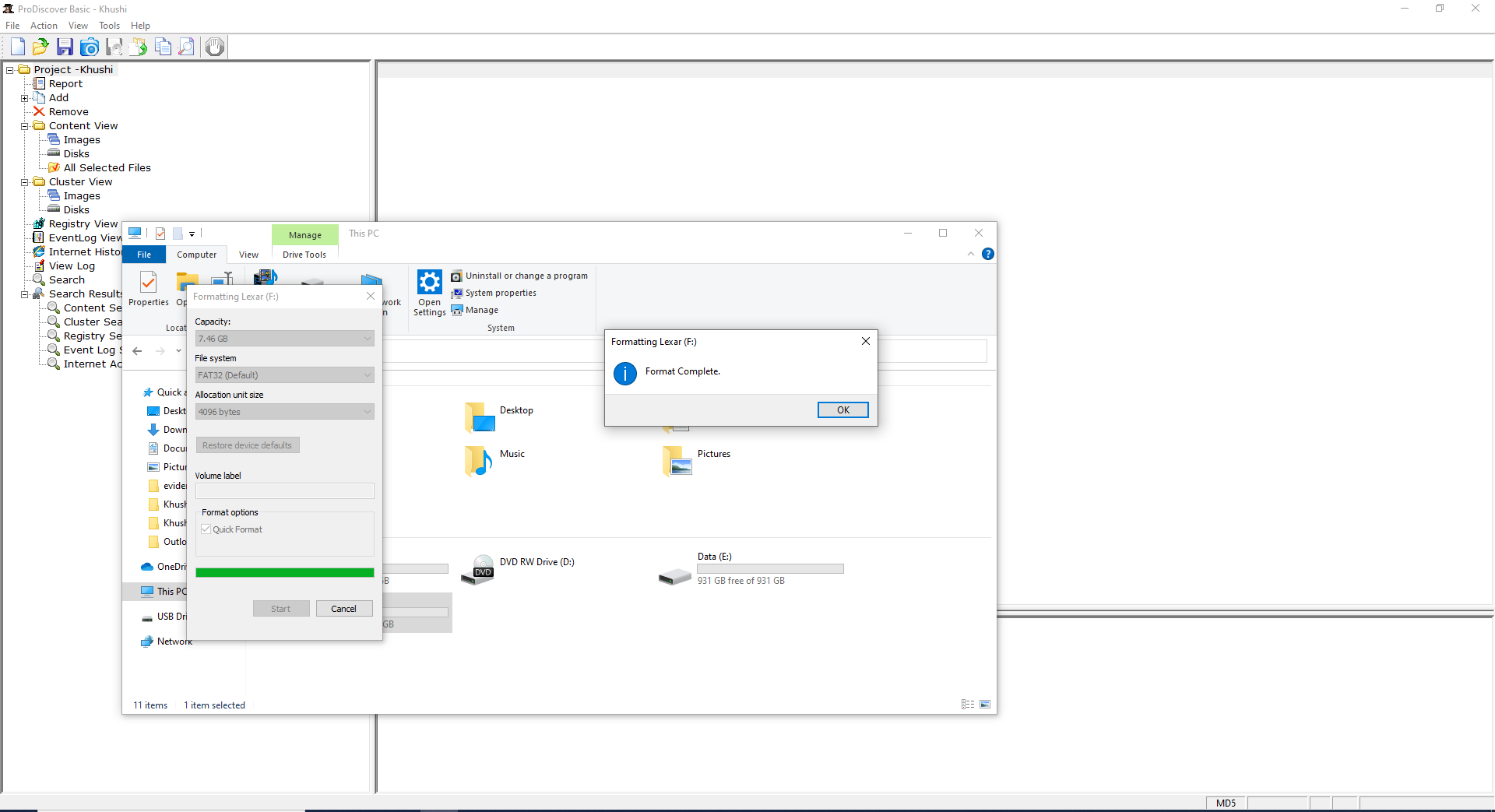
7

1. **Which of the following statements about the MFT is true?**

B - The MFT is updated to indicate free space when files are deleted.

1. **Secure destruction of digital data requires doing which of the following?**

B - Writing 0s and 1s to the storage device to overwrite file remnants.



**Lab 2.2: Using ProDiscover Basic to Image a USB Drive**

1. **ProDiscover Basic supports all the following image formats except**

C - .pdg

1. **Disk images don’t include the MFT. True or False?**

False

1. **Which statement about a ProDiscover Basic image is true?**

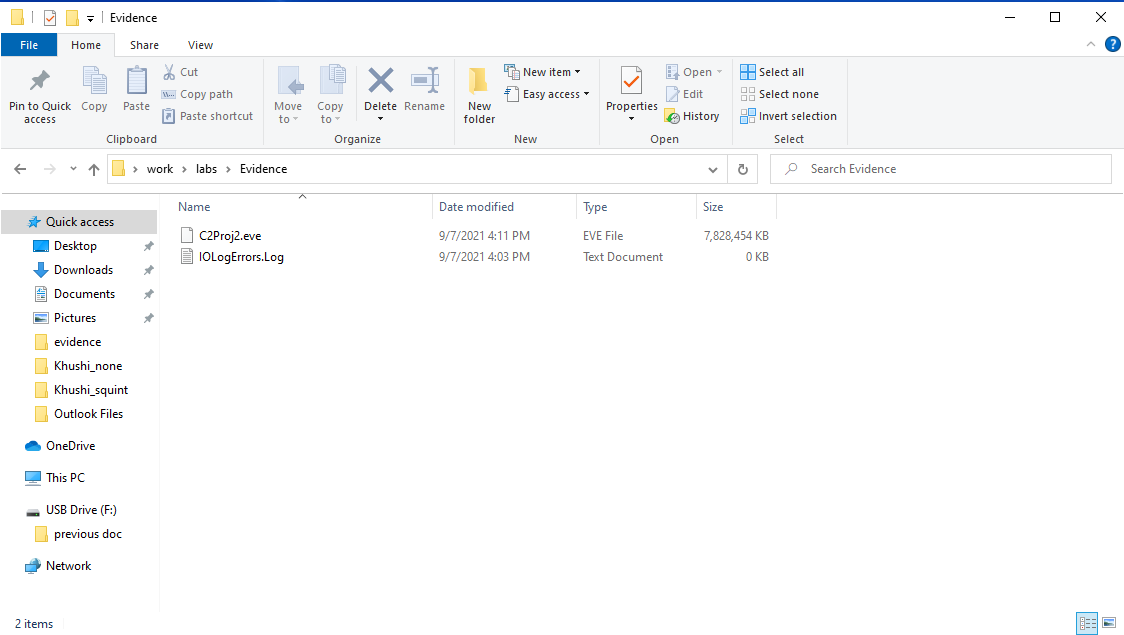
B - It copies the MFT and any unallocated free space from the original storage device.

1. **What’s the purpose of a write-blocker?**

A - Preventing any data on the original storage device from being overwritten, which would violate the chain of custody.

1. **What’s the purpose of disk imaging?**

B, D



**Lab 2.3: Converting a ProDiscover Basic Image to a .dd Image**

1. **Which image format can be read by Windows, Linux, UNIX, and Mac OS X?**

A - .dd

1. **An ISO image is stored as which of the following?**

C - Uncompressed format

1. **ProDiscover Basic can perform which of the following image conversions?**

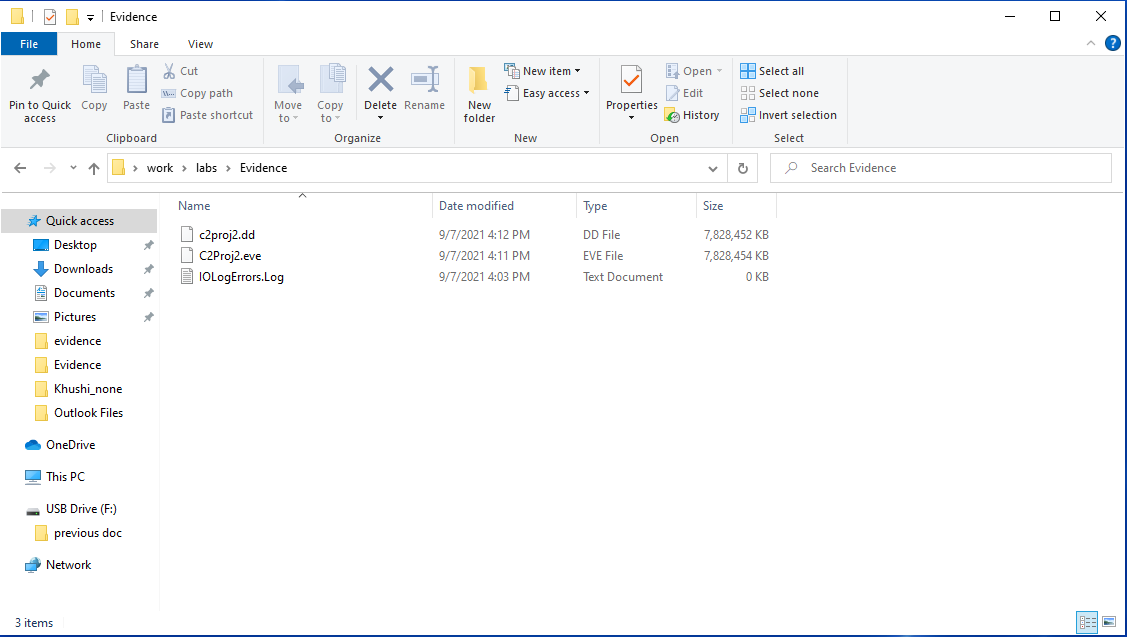
C - .eve to ISO

1. **ProDiscover images are the same size as the total size of all evidence files on the original source. True or False?**

False

1. **Forensics investigators should be familiar with more than one forensics analysis tool so that they can maintain the chain of custody. True or False?**

False



**Lab 2.4 Imaging Evidence with FTK Imager**

1. **FTK Imager can produce all the following image formats except ----------**

C

1. **Which of the following features isn’t available in FTK Imager?**

B, C - Being optimized to search large volumes of data, Creating .eve image files

1. **FTK Imager Lite is designed to be portable. True or False?**

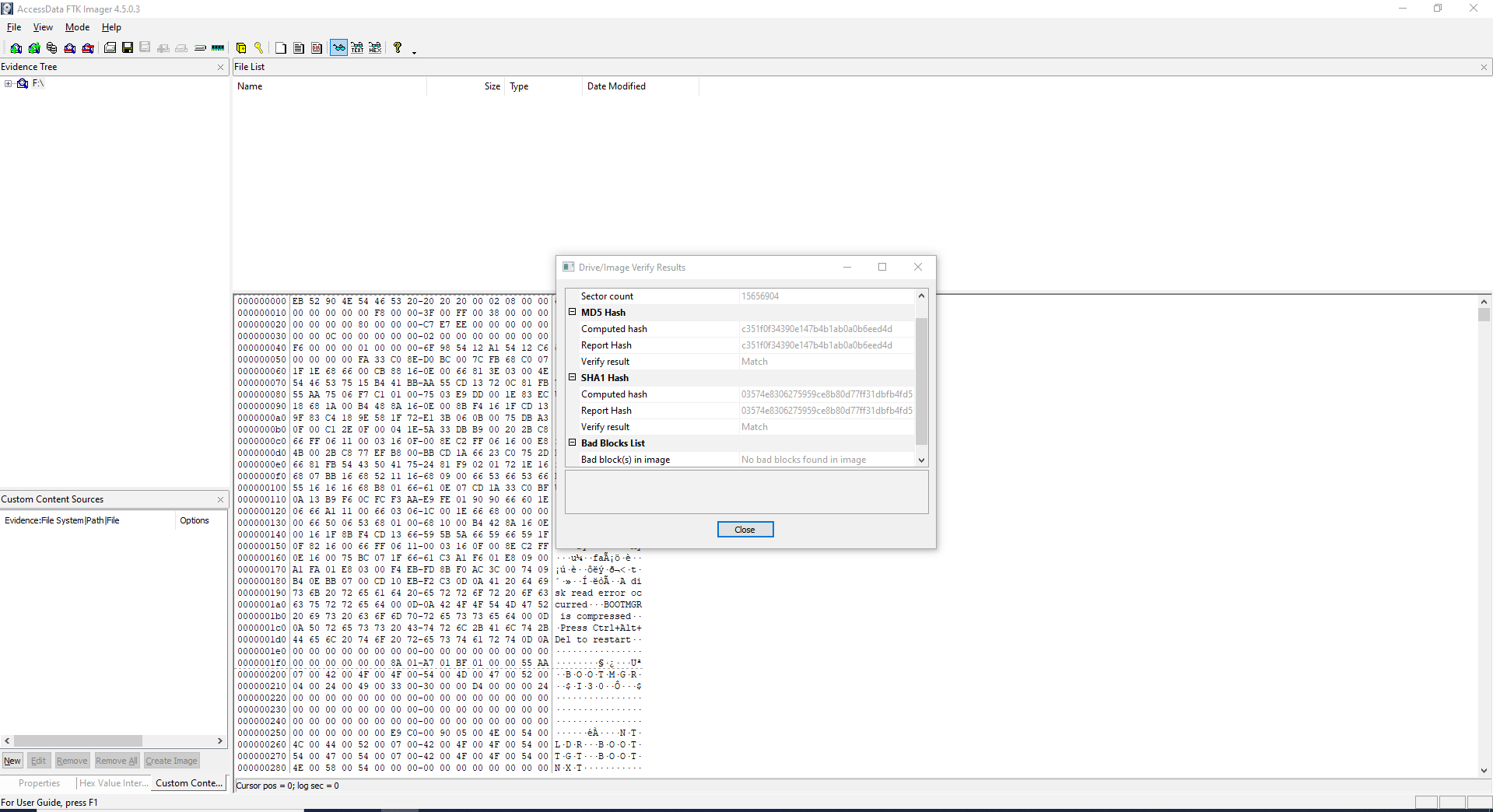
True

1. **FTK Imager calculates which hash values during file imaging?**

A - MD5

1. **Why does FTK Imager calculate two hash values?**

B - To provide redundant verification that files haven't been altered during imaging



**Lab 2.5: Viewing Images in FTK Imager**

1. **How many excel files were covered in the C2Proj4.E01 image?**

B - 7

1. **How many deleted files were recovered in the C2Proj4. E01 image?**

A - 2

1. **What’s the filename of the deleted Excel file in the C2Proj.E01 image?**

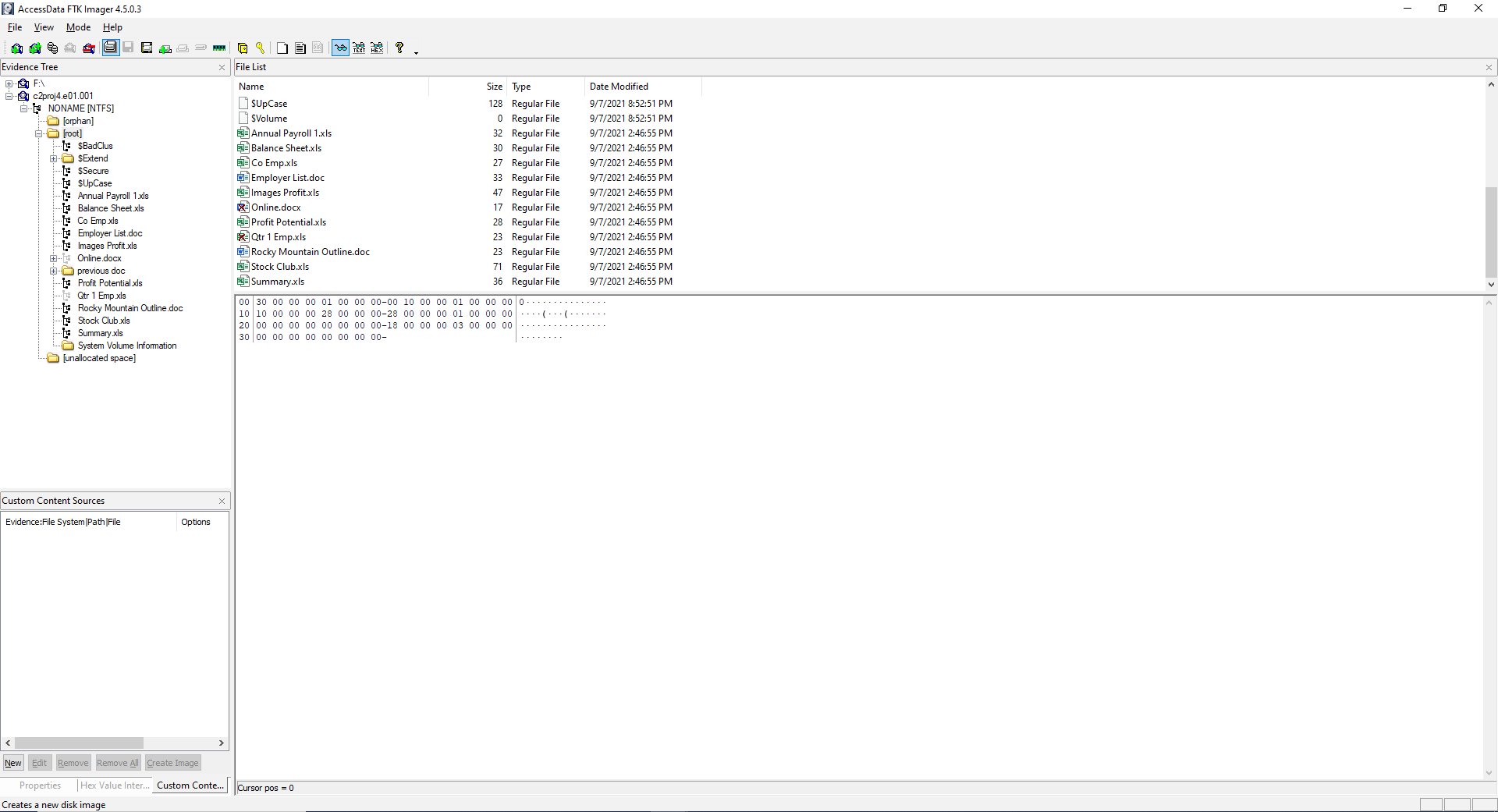
C - Qtr 1 Emp.xls

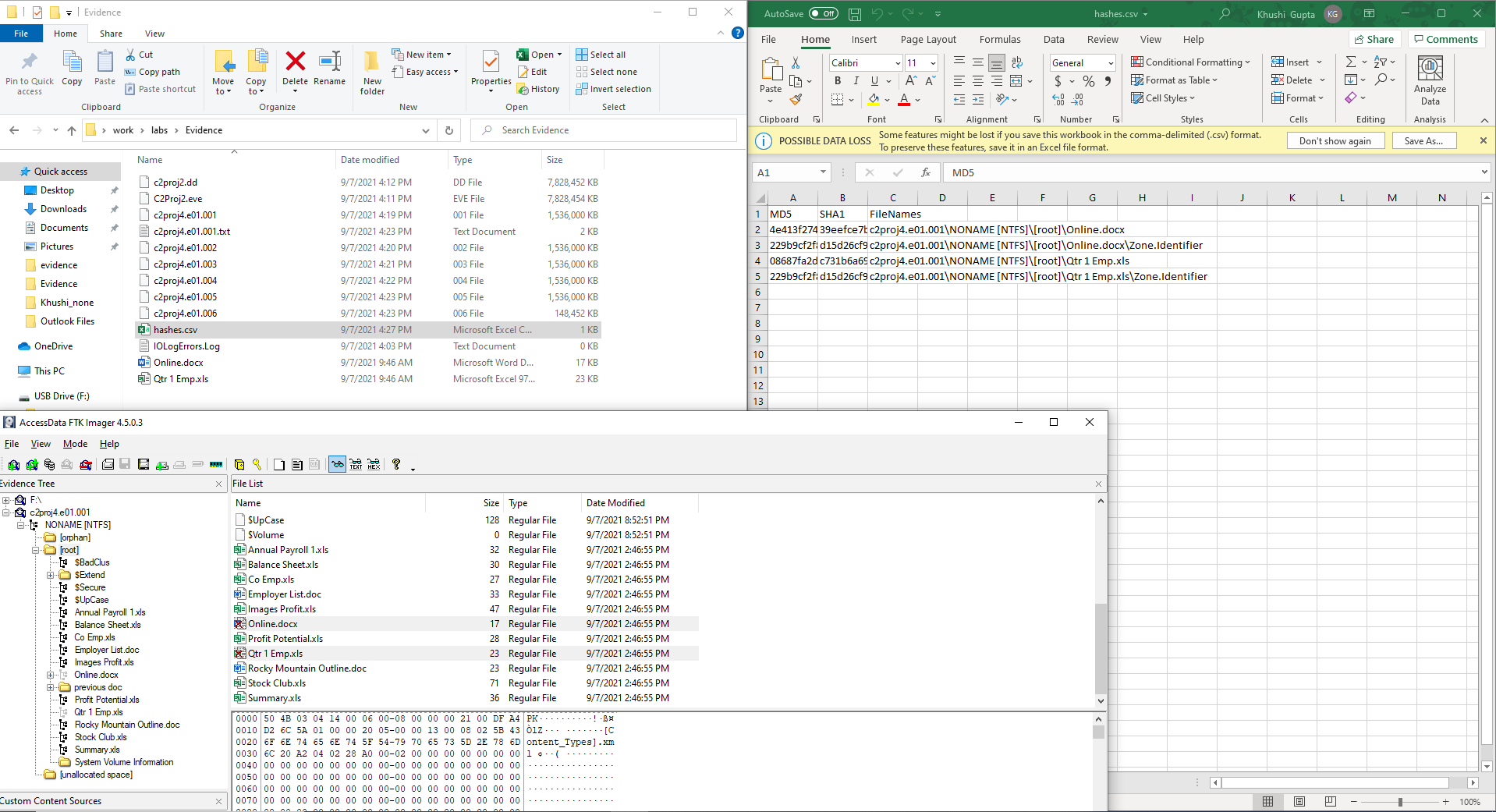
1. **What’s the name of the deleted Word file in the C2Proj.EO1 image?**

B - Online.docx

1. **How many SHA-1 hash files were exported to the C2Proj4 deleted file hashes .csv file?**

B - 2





**Lab 3.2 Examining a FAT32 Image**

1. **How many clusters are in the FAT32 image?**

B

1. **How many files (existing and deleted) are in the FAT32 image?**

C - 16

1. **How many Excel files are in the FAT32 image?**

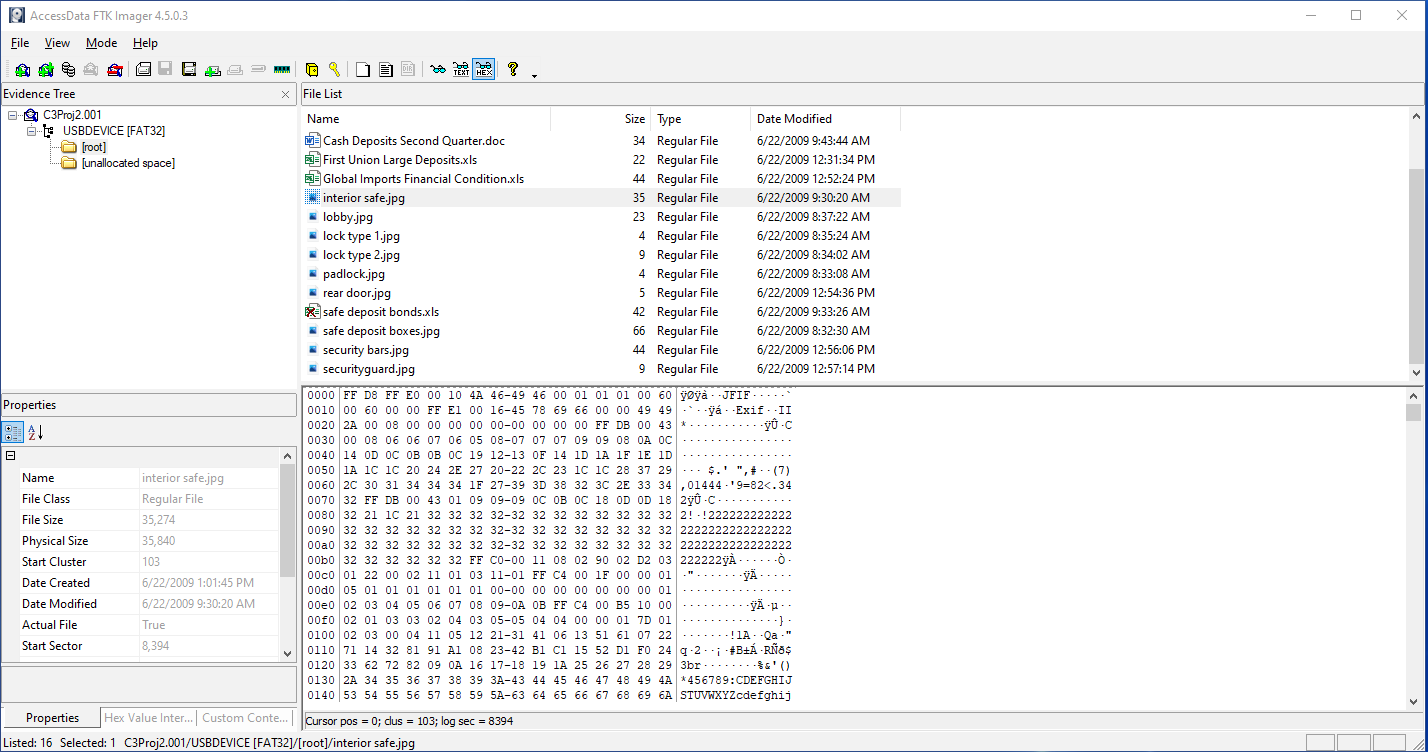
A - 3

1. **What’s the start sector of the deleted Excel file?**

B - 8616

1. **What’s the FAT32 drive’s volume serial number?**

A



**Lab 3.3 Examining an NTFS Image**

1. **What’s the cluster size in the NTFS file system?**

D

1. **What’s the volume serial number of the NTFS image?**

B

1. **What time was the .jpg file deleted?**

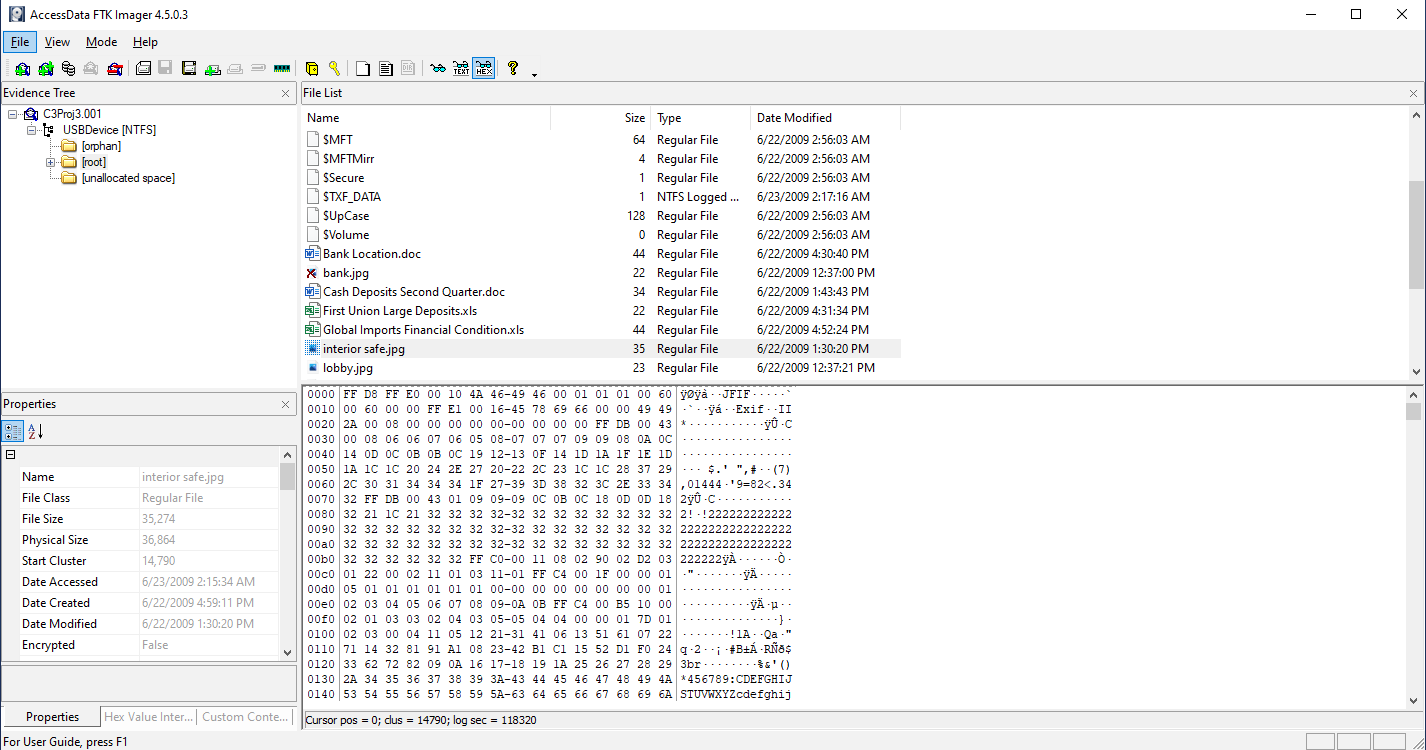
C

1. **What’s the physical size of the deleted mark .doc file?**

B

1. **What folder in the NTFS images isn’t in the FAT32 image?**

A



**Lab 3.4 Examining an HFS+ Image**

1. **What’s the cluster size in the HFS+ image?**

C

1. **How many clusters are in the HFS+ image?**

A

1. **What date was the HFS+ partition created?**

C

1. **What folder doesn’t exist in HFS+ but is found in FAT32 and NTFS?**

D

1. **In what folder are deleted files stored?**

A

