Forensic Implications of Apple's New Fusion Drive

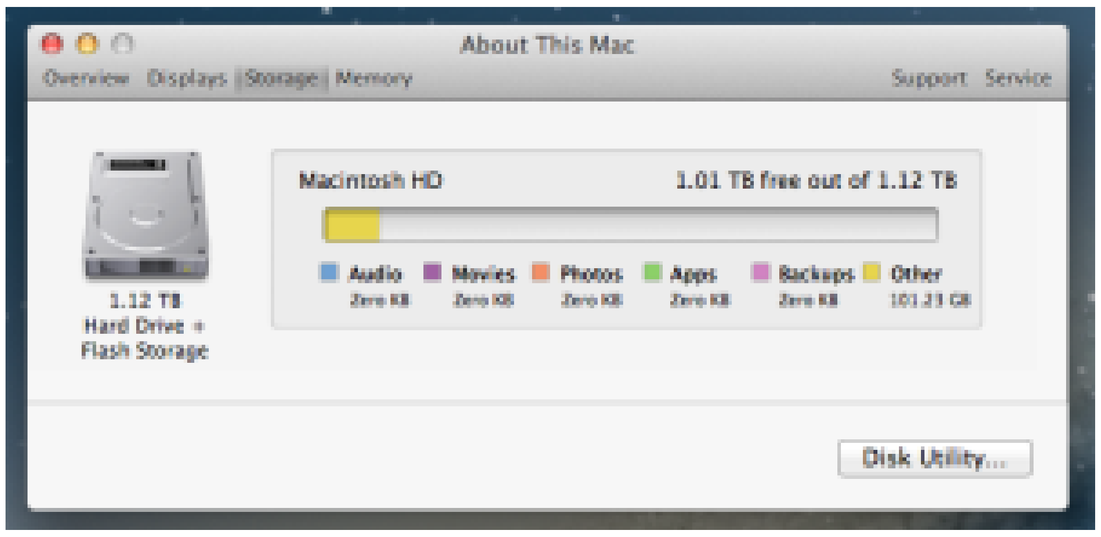
Shruti Gupta

Background

In 2012, Apple introduced the new Fusion Drive technology. The Fusion Drive is not the same as existing hybrid drives. In typical hybrid drives (like the Seagate Momentus XT), a solid state drive is used as a cache where frequently accessed files are *copied.* Thus, the flash memory is used for faster performance but the magnetic drive is used for storage. However, in the Fusion Drive, data that is frequently accessed is *moved* into the flash memory, so both drives are used for storage.

Also, unlike combinations of flash and magnetic storage, data is moved at the block level and not at the file level. Thus, it is possible that parts of the same file might exist on different blocks.

This new approach in data storage requires some analysis into the ramifications that it produces for forensic investigators.



Significance

- Mac computers are the 3rd largest manufactured personal computers (2012)
- The Mac OS X operating system has 7% global market share and 10% domestic market share in the United States (2013).
- There is a need to be able to forensically analyze any system that may be encountered in an investigation.

Methodology

The aim of the research study is to analyze whether there are any forensic implications of this new technology, and if any, to understand what they are. Steps in the methodology would include:

- Understand existing procedures for forensic analysis of Mac computers and check if these procedures still apply to the fusion drive.
- Populate the magnetic drive with certain files and predict the movement of the files based on the usage.
- Propose changes in the existing forensic methodology to accommodate changes brought about by using the fusion drive technology.