

Lab-2: Hard Disk Drive Forensics & EnCase

Digital Forensics
Spring 2004

Posted: February 12th
Due: February 19th

This is a week long assignment to get yourself familiar with the internals of hard disk drives. In this assignment you will also learn to use one of the state of the art tools for hard drive forensics, EnCase. Every student in the class is provided with a copy of EnCase. If you do not have a copy please contact Kulesh (kulesh@isis).

1 Hard Disk Drive Geometry

Before getting into the forensics of hard disk drives refresh your knowledge of hard disk geometry and file systems by answering *all* of the following questions.

1. Please describe the following terms:
 - (a) Head, cylinder, tracks, spindle
 - (b) Sector, cluster, blocks
 - (c) Partition table
 - (d) Master Boot Record (MBR)
 - (e) File system
2. What is the difference between a sector and a cluster? What is the difference between a sector and a block? How would you find out the size of clusters/blocks/sectors of a hard disk drive?
3. What are the contents of a partition table? What is a logical partition?
4. How is a file deleted in FAT32? How would one “undelete” a file in FAT32? Is it always possible to “undelete” a file? (Explain why, why not.)
5. What is an inode? Name some file systems that use inodes.
6. What is an Alternate Data Stream? How would you create one? How would you detect the presence of an ADS?
7. What is RAID? How is RAID different from SCSI? What file systems use RAID?
8. Name some advantages and disadvantages of doing forensics on a RAID system (over a non-RAID system)?

2 Using EnCase for Hard Drive Forensics

Everyone enrolled in the course should have a copy of EnCase software CD. If you don't have one, please contact Kulesh (kulesh@isis) to obtain your copy. Answer the following questions based on the disk image **Quantum**. *Please attach enough proof so the graders can understand why you reached the conclusions.*

1. What is the file system type installed in the disk images in Quantum?
2. What are the operating systems installed in this particular machine? Give version numbers and date of installation.
3. List some recently used files by the users of this computer?
4. What is a GUID? What is the GUID of the machine in question?
5. Make a query to identify deleted JPEG files in this computer? Recover the file “_OG5.JPG”
6. List some web sites visited by the users of this computer?
7. Was there a printer connected to this computer? If so, who is the manufacturer and what model is it?
8. What kind of storage media were attached to this computer? (Floppy, CDROM etc.)