..::Nitin Kushwaha's Techportal::..
All about hAckiNg and Forensics!

# Posts Tagged With: NTFS

## Notes for Forensic Beginners' Part1

Posted on June 5, 2009 by Nitin Kushwaha
Hello All,

I still remember my days 7 years back, when I was very keen in learning and working on Computer Forensics, however there were no good resources available for understanding the concepts and practicals for the same.

I am starting this short series for all those who are still struggling to start their career into Digital / Computer Forensics.

However, I wont be covering the basic steps or Phases involved in Computer Forensics and Incident Response, as there are numerous books available for the same, and a Google search may help you all a lot.

So, Let's start with NTFS Filesystem:-

Currently it is NTFS v3.1 for XP/2000/2003/Vista

NTFS: New Technology File System

formerly known as *NTFS* is a registered tradmark of *Northern Telecom* File System, you can still find them on older version's of CD for Windows 3.5 NT and 4.0.

Going a bit deeper,

NTFS consists of records and entries of MFT,

$MFT= Master File Table

The length of the $MFT within NTFS is 1024 bytes.

Standard Sector size within NTFS is 512 bytes

Standard Cluster size within NTFS is 4096 bytes (8*512 sectors)

MFT is the primary file within NTFS file system,this file points to the locations of the other files within the NTFS formatted filesystem.

Within the MFT there are "entires", and each entry contains information about the file it points to. These entries provide a variety of information about the file it points to, and it also includes the following:

File Name, File Size, dates about the file included:-

Created=C

Entry Modified=M

Written=E

Accessed=A

ocation of the data of the file.(MACE)

Typically an MFT entry is 1024 bytes in size, or two sectors, and starts with either FILE0 OR FILE*, depending and signifying whether the given partition was formatted using Windows XP , Windows 2000 respectively.

The first 16 MFT entries within the MFT are reserved.

In Next Series of this article we will go deep into NTFS structure with reference to MFT and other records.

Need all your comments.

Thanks

Nitin Kushwaha

CHFI.CEH.SCSCA.CIW-SA.MCSE.MCSA.MCP.ITIL.CCLA.CCHA.CCSECA.CCW2K

Categories: Basics, ComputerForensics, DigitalForensics, Microsoft Windows, MyOwn | Tags: Computer Forensics, Digital Forensics, Forensics, MFT, NTFS | Leave a comment

# Recycler or Recycled Folder?

Posted on May 30, 2008 by Nitin Kushwaha
All,

Many times people ask why do i have a Recycler folder? whereas a friend of mine has Recycled folder, on the root of their OS?

Well to answer them: here is a liitle details on as to why there are such differences?

well Recycler folder will exists only and only if you are running Windows versions on NTFS formatted Partition.

whereas Recycled folder will exists only if the windows versions are running on a FAT32 formatted partition.

However, I have also seen people those who had both of these folders existing on the root of their OS.

Why so?, well these guys had converted their OS partitions from FAT32 to NTFS and thats what caused these two, to be found together.

Hope this helps.

Thanks

Nitin Kushwaha

Categories: Basics, DigitalForensics, IncidentResponse, MyOwn | Tags: Desktop.ini, FAT32, Forensics, INFO2, NTFS, RecycleBin, Recycled, Recycler | Leave a comment