The Center for Cyber Defenders

Expanding computer security knowledge

Navigating NTFS

Marcellus Smith, Auburn University

Josh Morris, University of Missouri

Project Mentors: Victor Echeverria, 5836; Kelsey Cairns, 5852

SAND2019-8010D

Problem Statement:

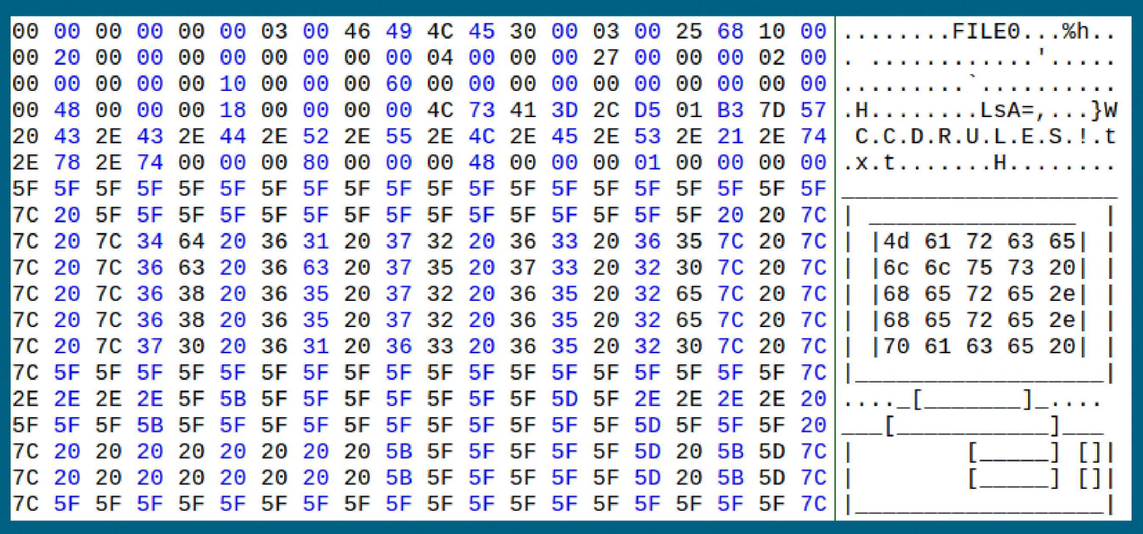
NTFS, also known as New Technology File System, was first introduced by Microsoft in 1993. Despite its long history, there is still a lot of confusion and misconceptions about NTFS. The goal of this work was to gain a better understanding of how each part of the file system is constructed and how changes at a user level affect low level parts of NTFS. This problem specifically relates to how creation or deletion of files could be obfuscated or detected at the hex level within NTFS.

Objectives and Approach:

- First, we reviewed the current research and documentation for NTFS.
- Using VMs, we then created virtual disks so that we could validate or remediate our current view of NTFS.
- Automation of this process was done by creating a parser in python. This parser should be able to identify all files within the system along with their data. It should also be able to compare changes between two different NTFS images.
- After both the parser and images were created, we identified key portions of the file system in response to changes made by users. Along side this, we gathered data to try and identify patterns in NTFS and how it responds to certain types of files.

Results:

The biggest developments from this project were a documented understanding of NTFS and a parser. The parser is the culmination of our research and manual testing of the NTFS.



Impact and Benefits:

The results of our work can be used to improve forensic investigations, especially in regards to file system changes such as file creation or deletion. Along with this, our method takes a lower level view of NTFS compared to most forensic tools. By accessing the hex data directly, there is more room for bit level comparisons to attribute changes within the NTFS.

- Reduce the amount of required manual enumeration
- Facilitate the mapping of bytes to data within NTFS
- Furthered documentation of NTFS

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.