C19 Implications of Valid Data Length (VDL) Slack and the Facts That It Presents

David G. Ferguson, MS, Deloitte, 1919 N Lynn Street, Arlington, VA 22102-4219*

After attending this presentation, attendees will be familiar with Valid Data Length (VDL) slack and its implications for forensic examinations. Examiners will learn what VDL slack is, how to detect it, and how to handle the two distinct hashes that these files have.

This presentation will impact the forensic science community by bringing awareness to the fact that VDL slack is not widely know by examiners, few have run into it, and it is rarely taught in examiner training. VDL slack has a number of interesting properties, one of which is that it has two distinct hashes.

Many examiners are unfamiliar with VDL slack and its potential impact on their reports or potential testimony. This presentation introduces the topics and presents some interesting facts that can be derived from files with VDL slack. After attending this presentation, attendees will understand some of unique characteristics of files that contain VDL slack (sometimes called file tail), how to detect these files, how they are created, and what they can mean to forensic examiners. One of the unique characteristics is that files that contain VDL slack have potentially two different hashes. In addition, copies of files with VDL slack can be traced back to an original file with certainty (this could be useful in child pornography distribution cases).

VDL slack is an artifact of the Microsoft's® object reuse strategy for disk space. When Microsoft® introduced New Technology (NT) and the New Technology File System (NTFS) in the 90s, they wanted to get a C2 security rating from the National Security Agency (NSA). This required that, when disk space was reused, the new user could not be allowed to see what was there before. To allow efficient reuse, Microsoft® added the VDL value in the Master File Table (MFT) entry for each file. The VDL value is in addition to the file length in the MFT as they are separate and distinct values in the MFT. When a file is created by Windows®, if the file size is known, the file is created with the file length equal to the size provided by Windows® and the VDL is set to zero. So, the VDL is always smaller or equal to the file length. As data is written to the new file, the VDL is increased to include the new data. In practice, the VDL value in the MFT is almost always the same as the file length value. When the two values are not the same, the file contains VDL slack.

VDL slack has been around for years, but it is relatively rare and only occurs on NTFS partitions. A survey of more than 10,000 partitions found that 50% of the drives had at least one file with VDL slack and on average there were ten files with VDL slack per partitions. Most of the time, the files with VDL slack are relatively large (over 1GB).

So why should an examiner learn about VDL slack? For a forensic examiner, a working knowledge of VDL slack, at a minimum, can be useful in limited cases. In some cases, a file containing VDL slack could contain data that is crucial to the case. An examiner that is ignorant of VDL slack runs the risk of appearing to be confused on the witness stand or confusing a VDL slack for an intentional attempt at hiding data. In either case, their testimony could be lacking in true understanding.

VDL, Valid Data Length, NTFS