B10 An Odyssey Into Lesser Known Regions of Embedded Metadata in Microsoft File Formats

Eoghan Casey, MA, ONKC LLC, 3014 Abell Avenue, Baltimore, MD 21218*

After attending this presentation, attendees will understand how to find previously unknown metadata embedded in digital files that can be critical to an investigation.

This presentation will impact the forensic community by showing forensic examiners, at a practical level, how to uncover lesser-known metadata in digital files. At a higher level, this presentation demonstrates the limitations of file format documentation, existing forensic tools, and the importance of conducting methodical experiments and tests in digital forensics. Furthermore, to bring this process into the realm of science, the methodology used in all three cases is formalized to help forensic examiners repeat the process in other contexts and apply it to other file formats.

A few bytes buried in a digital file can contain crucial details in a case, like remnants of activities that contradict suspect statements, or incriminating text from prior versions of an e-mail. The main challenge for forensic examiners is that the most useful embedded metadata can be buried the deepest. Conversely, the fact that this information is difficult to locate means that it is harder to alter or destroy, and may persist despite the best efforts of the subject in an investigation.

Three cases are presented that made use of lesser known metadata in Microsoft file formats: Word, Excel, and Outlook. The embedded data used in these investigations are poorly documented. Furthermore, forensic tools are ineffective at extracting this information. This presentation guides attendees through an odyssey into Microsoft file formats, using a combination of research and experimentation to uncover important clues embedded (and in one instance encoded) within a file.

Digital Evidence, Embedded Metadata, Digital File Formats

 ** Presenting Author*