

TRACK: IT Security
SESSION #: IT#5
DATE: Tuesday April 20, 2010
TIME: 8:30-9:45am
SESSION TITLE: "Demystifying the Microsoft Extended File System (exFAT)"
SPEAKER(S): Robert Shullich, CPP, CISA, CISM, CGEIT, CISSP, GSEC, GCIH, GCFA, CEH – Sr. Security
Technology Advisor, Corporate Information Security Office
ORGANIZATION: Bowne & Co. Inc.

ABSTRACT: "Demystifying the Microsoft Extended File System (exFAT)"

In January 2008 the SD Card Association, makers of the removable SD memory cards used in cameras, cell phones, and many other consumer electronics, announced a new SDXC specification for SD cards starting at 32GB and reaching a maximum capacity of 2TB. These memory cards will exclusively use a new Microsoft file system called exFAT which is the extended file system, and has been nicknamed by some as FAT64. Because this file system is patent pending, and propriety to Microsoft, implementation of the specification requires a license from Microsoft. Although this file system has been available on desktop systems since 2008 with Vista SP1 and Windows XP since 2009, there is very little open source support available today and some tools that can process this file system are beginning to surface. As of the end of 2009 major commercial forensics tools do not support this file system. However, in early 2010 when the consumer devices that use this new technology come to market, there will be a wealth of potential digital evidence stored on removable media formatted with exFAT. This is not limited to SD cards, as USB flash drives and other removable media may be formatted using exFAT. There is not much available about the internals of exFAT and the purpose of this session is to show the forensics examiner what is under the "exFAT" hood.

exFAT topics to be covered in the session:

- History
- Features
- File System Limits
- Advantages/Disadvantages
- Relevance to forensics computing and digital investigation
- Internals of the Volume Boot Record
- Internals of the Directory
- Hiding places to look out for – where criminals can hide things

SPEAKER BIO(S): Robert Shullich CPP, CISM, CISSP, GCFA, GCIH, is an information security officer for a service provider to major financial firms and a current graduate student in the Computing Forensics program at John Jay College of Criminal Justice/CUNY. With 35+ years of IT professional experience, that includes over 15 years of security experience, he holds many industry security certifications and master degrees from The College of Staten Island/CUNY, Baruch College/CUNY and Brooklyn Polytech University.