



Forensic Innovations' Detects TrueCrypt and Other Encrypted Files Intentionally Hidden From Computer Forensics Tools

Forensic Innovations' File Identification Technology now identifies 3,312 File Types, including the elusive TrueCrypt. Until now, encrypted data could be hidden by appearing as random data. Computer Forensics tools might see the files, but dismiss them as unknown/unimportant data. File Investigator now reveals these files, and provides investigators with more leverage in legal cases.

Fishers, Indiana ([PRWEB](http://www.prweb.com)) April 26, 2009 -- Raising the bar in the Electronic Discovery industry, Fishers based Forensic Innovations, Inc. is now able to detect TrueCrypt, and other encryption data hiding techniques. The newly released File Investigator version 2.23 continues in their plan of supporting more file types (currently supporting 3,312) than any other product in the industry. Along with the 141 added file types, the accuracy of 78 existing file types was improved. Add to that the ability to identify more encryption file formats (including the elusive TrueCrypt) , and this version is truly a leap forward in advancing the state of the art in the analysis and filtering of Electronically Stored Information (ESI). <http://www.forensicinnovations.com>.

TrueCrypt has earned a reputation for simplifying the process of encrypting your data, as well as hiding it. On their web site, www.TrueCrypt.org they claim that "no TrueCrypt volume can be identified (volumes cannot be distinguished from random data)." That was true, until now.

Forensic Innovations engineers took this claim as a challenge, and focused their expertise on developing a method to definitively identify encrypted files that contain no identifiable header, signatures or magic numbers. The result is the ability to identify relatively any headerless encrypted file. Headerless simply means that the file header and supporting data structures are either stored elsewhere or are encrypted to blend in with the rest of the data. This is the technique that TrueCrypt, and some of their competitors, use to further secure your data and make the file unidentifiable.

When the File Investigator TOOLS product (<http://www.forensicinnovations.com/fitools.html>) finds encrypted files, it reports the type of encrypted file and, when possible, what encryption algorithm is used. While some encrypted files can't be narrowed down to a specific application, just knowing that they are encrypted can be important. In a legal case, knowing that potential evidence is encrypted and intentionally hidden can provide the leverage to entice the encryption key from the owner or show the court intent to conceal evidence. Employers can use this tool to catch employees hiding data on company computers and potentially collecting intellectual property. This technology is also available to our business partners and as a licensed API. For further details, and a discussion on this topic, visit the Innovations Blog, <http://www.forensicinnovations.com/blog>.

About Forensic Innovations, Inc.:

Founded in 1995, Forensic Innovations, Inc. provides Computer Forensics software products to customers around the world. Their software identifies and analyzes thousands of file formats, and is used in Document Management, Data Recovery, Data Security, Electronic Discovery, Government Agencies, Law Enforcement, Litigation and Research. As the number and size of hard drives increases so does the need to identify, search and organize the many types of data and files being produced.

Contact:



Beth Armstrong, Sales Associate
Forensic Innovations, Inc.
8686 Providence Drive
Fishers, Indiana 46038
P: 317-773-9717
<http://www.forensicinnovations.com>

###



Contact Information

Beth Armstrong

Forensic Innovations, Inc.

<http://www.forensicinnovations.com>

317-773-9717

Online Web 2.0 Version

You can read the online version of this press release [here](#).