By Steve Ragan,TheTechHerald.com
DECAF has returned, and COFEE is not the only forensic set that it will monitor. After the first version of DECAF was pulled on December 18, with a notice that it was all a “stunt” and anyone who downloaded the software discovered it wasn’t working. Now it’s back, with new features, and an explanation as to why it was really pulled. Legal fears.

First, DECAF was not fake, the tool worked. Still, the mass media ran wild, and the big focus was not on the tool, but how, “hackers are helping criminals”. The sad thing is most of the articles were written by some who never bothered to test DECAF in the first place.

One notable podcast, Cyberspeak, went so far as to ask that DECAF be taken down because “it is gaining more attention, not from law enforcement, but from the bad guys.”

A few days later, DECAF was gone. The site explained that, “We hope that as you realize this was a stunt to raise awareness for security and the need for better forensic tools that you would reconsider cutting corners on corporate security.”

Last night, DECAF was released, and in a statement the real reason for the removal of version one was made public.

“We originally pulled the app because of legal pressure. With DECAF v1 originally set out to restrict forensic extractions made by Microsoft COFEE, it raised major concerns with its ethical nature and potential hazard to the disruption of criminal investigations...,” the statement explained.

“We used the words ˝publicity stunt˝ because when we pulled DECAF v1 offline and disabled the applications, we had a lot of media attention. We decided to use that channel to raise awareness for better security and more privacy tools.”

The statement went on to add that the Cyberspeak interview had a lot to do with the application being removed. After the podcast interview, Mike, one of the DECAF developers, spent a good deal of time talking with the two former federal agents, where “…they informed me of my hazardous circumstances and gave me excellent advice; take DECAF down…”

The removal caused issues, the statement noted, including a DoS attack on the site. After that, another researcher and programmer (SoldierX) reactivated DECAF and enabled it for use. There was also talk about a phone home feature, which wasn’t at all malicious as originally speculated.

“We were going to use the phone home feature to notify private tracker admins of a seeder/node who had COFEE ran on his/her machine. This feature was not complete before release but we did have it semi-working, hence the COFEE usage reporting…We decided v2 will not report usage back. We also do not perform automated version checking,” the statement said.

The new version of DECAF will monitor for the usage of Microsoft COFEE. At the same time it will also watch for Helix, EnCase, Passware, ElcomSoft, FTK Imager Port, Forensic Toolkit, ISOBuster, and ophcrack. In addition, users can add their own custom signatures, as well as CD-Rom monitoring and the ability to execute files, to disable the device where the signatures were found, and start-up in monitor mode.

Tools like DECAF can be used by criminals, but so can tools like TrueCrypt. Does that mean TrueCrypt is something to be shunned? If not, then why shun DECAF? A tool is just a tool; the person using it determines its risk. The automation of evidence collection with tools is nice, but most experts will tell you
that those tools are only one part of the process.