## C2 An Analysis of a Photocopier Hard Drive for Forensically Relevant Artifacts

*Trevor Bobka, BS*, Marshall University, 2950 Auburn Road, Apt A7, Huntington, WV 25704; Ian Levstein, MS, Marshall University, 1401 Forensic Science Drive, Huntington, WV 25701; Nevin Westurn, BSc, Superior Office Services, Inc, 108 Eight Avenue, Huntington, WV 25701; and Terry Fenger, PhD, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will feel more confident in their ability to analyze photocopier hard drives and will better understand what files can and cannot be recovered. Attendees will also be more confident using their own forensic tools to retrieve such information.

This presentation will impact the forensic science community by providing information regarding forensic artifacts that can be recovered from a photocopier hard drive during four stages: (1) a blank hard drive; (2) a hard drive with an Operating System (OS) installed; (3) a hard drive with data generated; and, (4) a hard drive that has been initialized or wiped by the photocopier. The goal of this project was to determine which stage yields the most data and to see how accurate the photocopier's wiping process is. It is believed that data files can be recovered due to the nature of hard drives themselves.

In the world of digital forensics, many people fail to recognize photocopiers, or Multifunction Peripherals (MFPs), as having any probative value. These machines actually contain a hard drive to aid in processing or sorting multitasking functions. Thus, the hard drive acts as a storage media and saves the documents sent to it for the various jobs the machine performs. These machines are heavily used in many offices (businesses, government, universities, etc.), and the devices can potentially be a gold mine if the data falls into the wrong hands. Contrary to popular belief, the hard drives are fairly easy to obtain if the photocopier breaks or gets replaced by a newer model. This is due in part to some offices simply tossing out the old copiers and paying no attention to the hard drive left in the machine, thus making the hard drive available to anyone who wants to take the time to remove it.

The project involved removing the hard drive from a Canon® imageRUNNER ADVANCE 4035 photocopier during the four stages of its life cycle and analyzing the content obtained. The hard drive was cloned twice at each stage using a Disk Jockey PRO Forensic Edition to provide an actual and working copy to use during analysis. The results suggest that data generated on the machines was able to be recovered using forensic software programs such as FTK® 5.6.13 and Autopsy® 4.0.0. The files that were obtained corresponded to time stamps for the various jobs performed, phone numbers for faxes, email addresses, and other log files. In one case, an exact document matching the original was found as a PDF file. After initializing the photocopier, the data was overwritten by the machine and only the files associated with the working OS remained.

**Photocopier, Hard Drive, Forensics**