

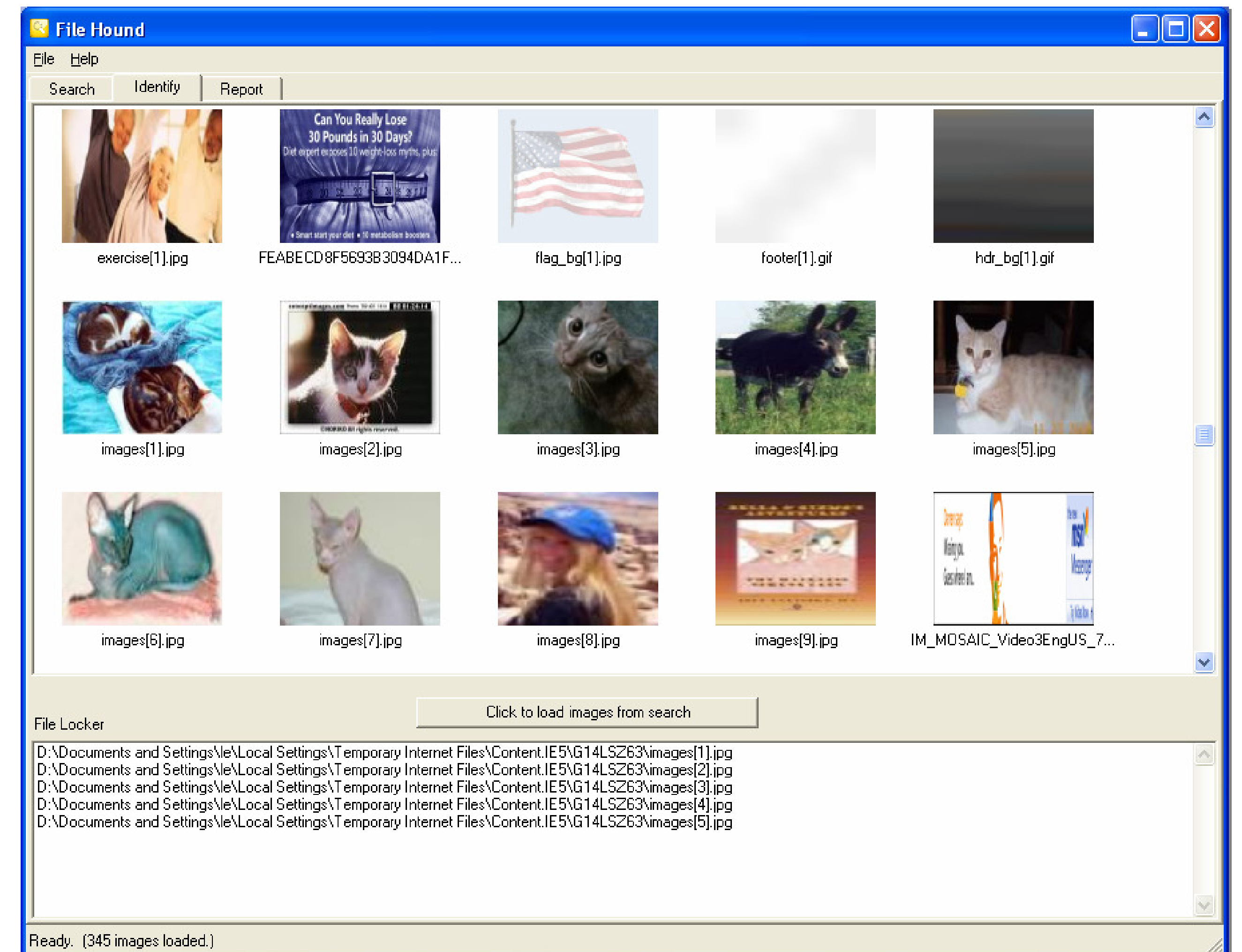
File Hound: A Forensics Tool for First Responders Wm. Blair Gillam & Marcus K. Rogers

ABSTRACT

Since the National Institute of Justice (NIJ) released their *Electronic Crime Needs Assessment for State and Local Law Enforcement* study results in 2001, several critical strides have been made in improving the tools and training that state and local law enforcement organizations have access to. One area that has not received much attention is the computer crime first responder. File Hound, a “field analysis” software program for law enforcement first responders developed at Purdue University, is currently used internationally by over 40 law enforcement agencies. It has been successfully used in several cases ranging from child pornography to fraud.

PROBLEM

A paradigm shift has occurred wherein computer forensics investigations occur out “in the field” rather than back in a lab. There is a need for software that can help investigators quickly find and identify contraband content while satisfying 4th Amendment requirements. Both commercial and open source tools have overlooked the first responder aspect of computer forensics.



Identifying contraband images

RESULTS

File Hound was originally released to the law enforcement agencies attending the August 2004 National White Collar Crime Center training conference at Purdue University—the response was overwhelmingly positive.

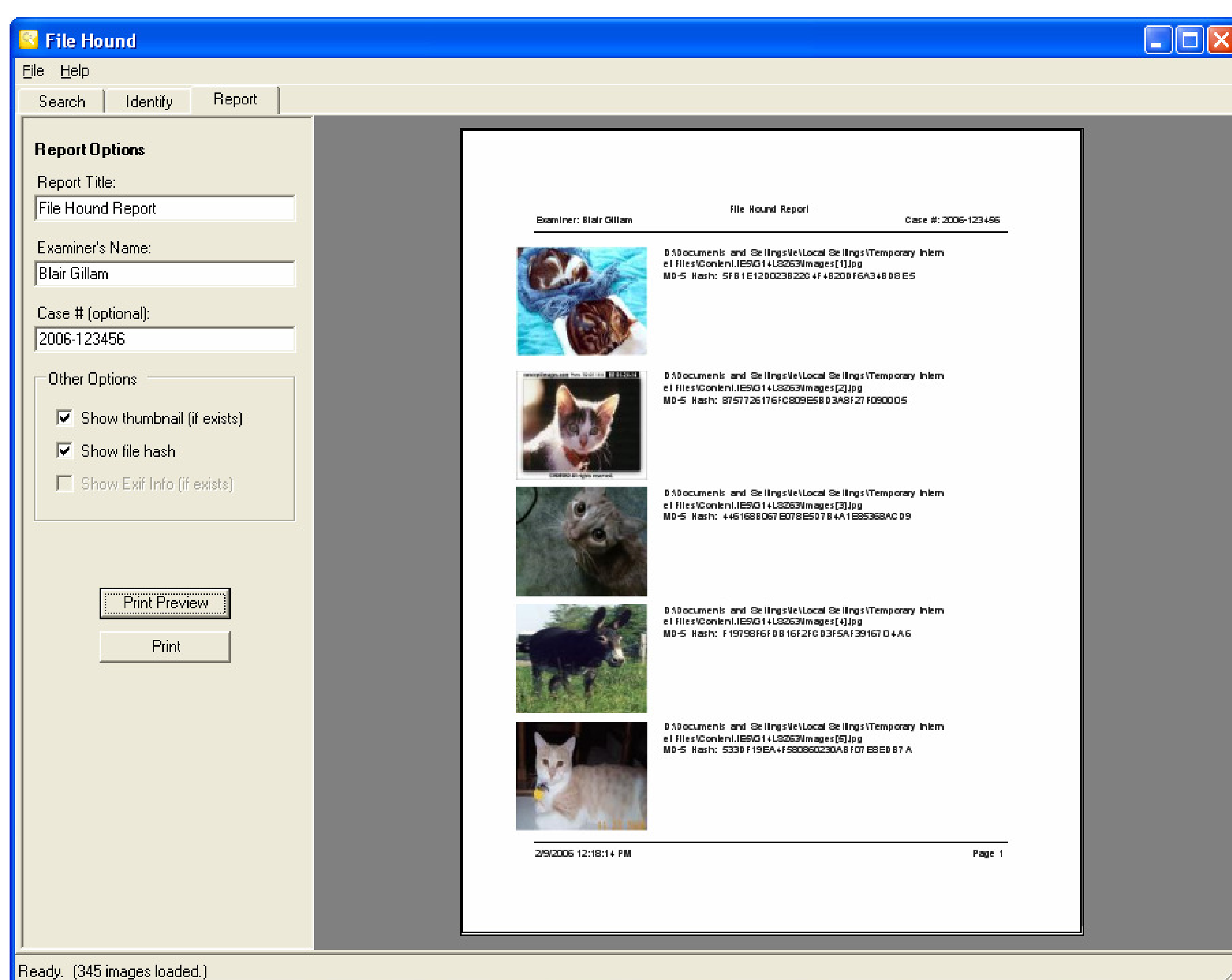
Current users include:

- Indiana State Police
- Various other Indiana agencies
- Virginia Attorney General’s Office
- Tigard Police Department (Oregon)
- Canadian Border Services Agency (Ontario)

FUTURE WORK

File Hound is continually evolving based on input from our law enforcement users. Future capabilities in development include:

- Platform independence
- Timeline viewer
- Hash comparisons
- Compatibility with different file systems



Creating the final report in File Hound