Mactime GUI for Mac OSX
by Adam Luvshis and Dan Artinger

Table of Contents

Executive Summary
Current Condition Overview
Tool Selection
Tool development
Conclusion
References

Executive Summary

Mactime is an insurmountably useful tool in a forensic investigation. When forensically analyzing a machine, date and times of every file are crucial in order to provide a timeline analysis. This is where mactime comes in. Mactime is a program that runs in a command line interface and outputs a file's last modified, accessed, and changed times, as well as its permissions and size. Some people prefer not to use the command line, so a graphical user interface for Mac systems was created in order to welcome these people into the forensic community.

Current Condition Overview

Currently in the forensics community, there are few graphical front-ends for mactime. The ones that do provide a front-end, however, are not very inviting, especially for Mac users. Most require the user to have some experience with a command line interface and have a working knowledge of Unix systems. While Mac OSX is based on Unix, many Mac users stick to using the GUI and do not want to delve into the environment using a terminal. Because of this, there needs to be simple GUI alternatives of useful forensic tools that the common user can play around with.

Tool Selection

Mactime will be the base program for this tool. Mactime outputs a timeline in ASCII of the specified file or folder's activity. In order to do this, it requires a body file, which is gathered from a tool such as *fls* (Carrier).

Tool development

For the development of this tool, we had to install some third party applications. These applications were necessary to get Sleuth Kit installed. Once Sleuth Kit was installed we had access to utilize fls and mactime. The third party applications required was MacPorts which can be obtained at http://www.macports.org. Once we had MacPorts installed we used it to install the latest version of The Sleuth Kit.

Additionally, we had to install the latest version of Xcode (4.32) so we can utilize Objective-C and the GUI creation. We developed the GUI to bring in specific pieces of information. It was designed for users that aren't used to most of the features that mactime comes with.

The code used to develop the GUI is all Objective-C. The code will make calls out to various Mac tools and applications to obtain the necessary information. Once the information is obtained, the text boxes will be populated with the information.

Some issues that we ran into while developing the tool was originally getting The Sleuth Kit installed. Additionally, there was a feature that we wanted to implement but was unsure how to do so. The feature we wanted to implement was auto-scrolling for the other sections. So if one section gets scrolled the rest get scrolled as well. We found a feature for iPhone's but not for Mac OSX. A post has been made on StackOverFlow looking for assistance but as of now no response. If a response is made the tool can be updated even after this has been submitted.

Conclusion

The MacTime tool we developed is supposed to make “newbies” lives easier to bring in information about files and folders using mactime. Hopefully the tool is seen as useful for those first using mactime. If it manages to receive a decent to significant response from the forensic community, we may look into continuing our updates in regards to adding features and support.

References

Carrier, Brian. "Mactime." *Sleuth Kit*. N.p., n.d. Web. 29 Apr. 2013. <http://www.sleuthkit.org/sleuthkit/man/mactime.html>.