

CERIAS

the center for education and research in information assurance and security

Digital Forensic Toolbox

<http://dftoolbox.cerias.purdue.edu>

Kelly Cole, Justin Tolman, George Kiruthu & Marc Rogers

What is the Digital Forensic Toolbox?

The Digital Forensic Toolbox website reviews and rates the various digital forensic tools in the market. The ratings come from within the digital forensic communities (Industry, Law Enforcement, Academia and Military). Thus, the communities are able to submit ratings for the tools they have used and also find the best rated tool for their needs.

DIGITAL FORENSIC TOOLBOX

STEP 1: BACKGROUND ?

COMMUNITY

LEVEL OF EXPERTISE

STEP 2: TOOL INFORMATION AND RATING ?

TOOL NAME VERSION

HARDWARE SOURCE

FUNCTION 1 OS

FUNCTION 2

GOOD 5 4 3 2 1 POOR

USER INTERFACE: ○○○○○

PERFORMANCE: ○○○○○

RELIABILITY: ○○○○○

COST: ○○○○○

PURPOSE

ACQUISITION

ANALYSIS

PRESENT/REPORT

TRIAGE

STEP 3: COMMENTS ?

PRO

CON

MISC

Why Do We Need Digital Forensic Toolbox?

The US Supreme Court in the Daubert vs Merrell decision provided specific criteria for the lower courts to rule on the admissibility of scientific evidence. One criterion is that the potential error rates of tools used be known, while another criterion requires the tool to be generally accepted by the scientific community. Currently, the error rates of digital forensic (DF) tools have yet to be published, posing a significant problem with meeting the criteria of Daubert vs Merrell. This website will serve as a reference to members of the DF community, bringing to light the errors and strengths in the tools that are in use, while also presenting which tools have been accepted by the DF community and the Courts.