

OVERVIEW OF SIX FIELD TRIAGE TOOLS

Tools --> (Features below)	Field Search	Drive Prophet	Forensic Scan	Helix3	osTriage	ADF Triage Examiner
Cost	Free to LE	Free to LE	Free to LE (need code from ICAC)	Free download for LE	Free to LE	Cost
Website	www.justnet.org/Pages/fieldsearch.aspx	www.driveprophet.com	www.gridcop.com	www.e-fense.com	www.feeble-industries.com/forums	www.adfsolutions.com
Purpose	Field preview	Field preview	Identify images of known child pornography	Multiple	Live response and triage	Multiple
Boot of target system required?	No	No	No	Optional	No	Optional
Write block needed? Used on live system? Boot required to other OS device?	Intended for use on live system – non-forensic	Use on write-protected device or through remote connection to live system	Use write-protection during field preview	Use on live system for non-forensic or Ubuntu boot for read only	Use on live system - makes only one entry to registry	Linux Boot (Read only mount of target)
Configuration of the triage device	Simple	Simple	Simple	Simple	Simple	Comprehensive
Assess deleted files?	No	No	No	No	No	Yes
Internet browser activity extracted?	Internet Explorer (IE), Mozilla, and	IE and Chrome	No	Yes –limited with viewing of cookies	IE, Mozilla, Chrome; also recovers recent	IE, Mozilla, Chrome, Safari
Keyword searches on the running target system?	Yes	No	No	Yes	Yes	Yes
Registry – recently used or mounted	Yes	Yes – numerous registry entries	No	Yes	Yes	Yes
Recycle bin analyzed?	Yes – only files not emptied	Yes	No	Yes	Yes	Yes

<i>(Features Continued)</i>	Field Search	Drive Prophet	Forensic Scan	Helix	osTriage	ADF
Image extraction and display?	Gallery view of logical images only	Lists directories that contain images and can export them as thumbnails	Only images identified in database	Image search based on file extension	Yes	Recovers all allocated images on either ext or header analysis or both
RAM collection	No	No	No	Yes	Yes in v1.1	Yes
Volatile data collection	No	No	No	Yes	Yes	Yes
Compressed archive support?	Yes	No	No	No	Yes	Zip, gz,7z.rar,tar, squashfs, cramfs
Verify file extension to File header to detect files with renamed extensions?	Yes - optional	No	No	No	Yes	Yes
Link files – recently used files or shortcuts	Yes	Yes	No	No	No	Yes
Additional	URL history entries can be recovered	Lists all .doc/.xls/.pdf files	Requires database update upon install	Consists of several tools in one and	Contains approx. 512,000 SHA values	Collects chat log files. Also, has