



Triage-G2[®] Field Kit

*Tactical Site Exploitation Kit for
Defense & Intelligence Operators*

Technical Data Sheet



Contact:

J.J. Wallia

Phone: (301) 312-6578 ext. 111

7910 Woodmont Avenue • Suite 260 • Bethesda, MD 20814

Phone: (301) 312-6578 • Fax: (240) 396-1987

www.adfsolutions.com

This document contains Proprietary Information that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal.

This restriction does not limit the Government's right to use this information if the data is obtained from another source without restriction or contained in the proposal in its entirety.

Triage-G2® Field Kit

Brief Description

Triage-G2 is the most powerful tactical site exploitation tool available today for extracting intelligence from computers. The tool is primarily designed to be deployed by non-technical operators.

Triage-G2 is deployed on a simple USB key only - no computer or other equipment is required. The tool is executed directly on the suspect computer with minimal user interaction.

Triage-G2 can be run on computers that are OFF (“dead”) or ON (“live”). The USB key is inserted into the computer if ON, or booted up from the USB key if OFF. The software runs automatically, identifies critical intelligence quickly, and copies it onto the USB key. Users can pause and review intelligence directly on the target computer at any time.

More than a simple data collection tool, Triage-G2 integrates advanced search capabilities that surpass those provided by forensic programs today. In addition, the tool’s powerful search capabilities can be setup and controlled by technical users.

Key Operational Features

- Ease of use for non-technical operators;
- Lightweight deployment on a USB key - no computer or other equipment required;
- Immediate intelligence extraction that can be reviewed on target;
- Comes with multiple “Search Profiles” out of the box that can be customized by technical users;
- Software runs in stealth mode and is forensically sound.

Data Captures from Target System

The software performs a series of system captures (CapturePaks™) which are stored on the USB key. CapturePaks include:

- General OS information
- User profiling (accounts, most used apps, recent documents)
- Internet browsing history
- Internet search history
- Internet cookies information
- Google map search history
- State of drive encryption
- Networking information
- USB devices history
- Installed applications
- RAM dump (live)
- Screenshot of all applications (live)
- Clipboard dump (live)

Forensic Search Capabilities

- Immediately scans areas of recent activity on target computer;
- Identify files using search terms, hash values, image analysis and regular expressions;
- Collect file types based on file properties (extension, dates, file size, header analysis);
- Full Unicode capabilities;
- Forensic intelligence is deployed using the patented SearchPak® technology.

Intelligence Dissemination & Security

- SearchPaks® and Search Profiles act as a secure containers that can easily be disseminated over the network or via physical media;
- All data generated is fully encrypted (Search Profiles, SearchPaks and reports);
- Guaranteed integrity of extract files from target computer;
- Permission-based usage and modification of SearchPaks®;
- Encryption keys can be created by agency for advanced security.

Standard Components

Component	Dimensions (inches)	Weight (lbs/oz.)
1 x Portable Travel Case	7.25"L x 6.5"W and 1.5" H	0.25 lbs/4.0 oz.
1 x 32GB Hi-Speed USB key (*)	4"L x 1.5"W x 0.67"H*	0.08 lbs/1.3 oz*
1 x Software CD	4.72" (diameter)	0.03 lbs/0.52 oz.
1 x USB extension cable	6.0" (length)	0.04 lbs/0.64 oz.
1 x Teasing Needle	5.5" (length)	0.01 lbs/0.16 oz.
1 x Portable flashlight	3.50" L x 0.75" W	0.04 lbs/0.64 oz.

(*) Note: Dimensions and weight will vary depending on final key selection.

USB Memory Keys

The default USB memory key provided is a 32 GB Hi-Speed memory key. Alternatively the client can select larger capacity keys or other brands (additional charges will apply). ADF can also accommodate high capacity USB hard drives instead of USB flash drives.

<p>This document contains Proprietary Information that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal.</p>

Triage-G2® Field Kit Pictures



Closed view



Opened view



All components

This document contains Proprietary Information that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal.

Users

- The Triage-G2[®] software is primarily designed for nontechnical users
- The software can also be setup and controlled by technical users

Usage Scenarios

- *Scenario 1:* The Triage-G2[®] software is designed to run on computers that are turned off. Note: hard drive removal is not required.
 - The Triage-G2 USB key is inserted in the suspect computer,
 - If a CD/DVD drive is present, the Triage-G2[®] Boot CD is also inserted,
 - The computer is then booted up in a custom Linux operating system that is part of the Triage-G2[®] software.
- *Scenario 2:* The Triage-G2[®] software is designed to run on computers that are turned on (live).
 - The Triage-G2[®] USB key is inserted into the suspect computer,
 - The user starts the Triage-G2[®] application from the USB key.

Data Acquisition & Forensic Integrity

- In Scenario 1 the software is forensically sound and does not leave any trace on the hard drive.
- In Scenario 2, the software removes all traces of the inserted USB key on the live system, as well as traces of the application saved by the target OS.
- Under both scenarios, Triage-G2[®]:
 - Creates a logical copy of the suspect files that are identified during the search process. These files are stored on the USB key that collects the evidence. To ensure that the file copied is identical to the original file from the target computer, the software computes the MD5 hash value of the original file, copies the file onto the USB key, and then computes the MD5 hash value of the copied file. The report contains both hash values;
 - Does not change any timestamps of files on the target computer.

Storage Conditions

Component	Min. Temp. (°C/°F)	Max. Temp. (°C/°F)	Humidity Range (%)
Portable Travel Case ¹	-40°C/-40°F	85°C/185°F	0% – 80%
32GB High-Speed USB key	-40°C/-40°F	85°C/185°F	0% – 80%
Software CD	5°C/41°F	55°C/131°F	0% – 80%
USB extension cable	-40°C/-40°F	85°C/185°F	0% – 80%
Teasing Needle ¹	-40°C/-40°F	85°C/185°F	0% – 80%
Portable flashlight ²	10°C/50°F	25°C/77°F	0% – 80%

Operational Conditions

Component	Min. Temp. (°C/°F)	Max. Temp. (°C/°F)	Humidity Range (%)
Portable Travel Case ¹	-40°C/-40°F	85°C/185°F	0% – 100%
32GB High-Speed USB key	0°C/32°F	70°C/158°F	0% – 95%
Software CD	5°C/41°F	55°C/131°F	0% – 95%
USB extension cable	0°C/32°F	70°C/158°F	0% – 95%
Teasing Needle ¹	-40°C/-40°F	85°C/185°F	0% – 100%
Portable flashlight ²	-20°C/-4°F	54°C/130°F	0% – 95%

Notes:

1. Non-electrical component
2. Data is based on standard Alkaline Manganese batteries supplied

© 2010 ADF Solutions. All rights reserved. Triage-G2 and SearchPak are registered trademarks of ADF Solutions. CapturePak is a trademark of ADF Solutions. All other trademarks referenced herein are the property of their respective owners.

This document contains Proprietary Information that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the proposal.