Detego® Field ‘Triage’ Product Overview

The complete portable digital forensic solution for the field
Military, intelligence agencies and Law Enforcement are battling their biggest digital investigation challenges to date. Frontline and lab based investigators are consistently faced with an uphill struggle against the exponential growth in the number of devices seized in investigations/operations, causing lengthy backlogs and expensive outsourcing.

We have listened to our clients and developed Detego® Field ‘Triage’; a powerful yet simple-to-use solution, that will expedite any criminal investigation or military operation. We created Detego® Field ‘Triage’ to enable end users to quickly identify the relevance of a digital device (computers, USB’s, memory cards, tablets, external hard drives etc.) during an investigation/operation. This streamlined process reduces investigation times, training burdens and costs, allowing for significantly faster charging and conviction of criminals, while Military commanders gain access to high value, critical information at the touch of a button. For some crime types, such Indecent Images of Children and Internet Crimes Against Children (IIOC/ICAC) - a court report can be produced within minutes from acquiring data.

**EASY-TO-USE USB DEPLOYMENT**

Detego® Field ‘Triage’ is licenced to removable USB devices, providing frontline investigators with a lightweight forensic tool, convenient in challenging environments. Within Detego® Analyse, the ‘Field Devices’ functionality allows the investigator to manage the licences which permit Detego® being run from removable USB devices and to import acquisitions from utilised devices. The feature also allows the investigator to revoke licences and reinstall them.

**HIGHLY CONFIGURABLE SEARCH PROFILES**

Detego® Field Triage’s simple-to-use, user interface, allows the end user to run a full digital acquisition at the click of a button. Acquisition options include:

- **Quick Config** - has been designed for frontline investigators in time-pressured environments such as Counter Terror, maximising quick ‘win’ potential with rapid access to potentially critical evidence and intelligence

- **Advanced Config** - provides the investigator complete flexibility and customisation of required search criteria. This includes ability to limit collateral digital intrusion assisting with compliance and any warranty issues as well as covering all crime types

- **Last Run** – re-run the last acquisition profile a removable device performed

- **Select Profile** - pre-configure your device to suit the objectives of your investigations and use multiple profiles for different operations and crime types. This also means that non-technical investigators can simply insert the USB stick into the target computer and perform a forensically sound digital acquisition and investigation without detailed technical knowledge
Detego® Field ‘Triage’ is a world leading complete digital media exploitation tool. As a brief overview, end users can acquire and analyse:

- Complete forensic ‘image’ of a target device be it a Windows computer, MAC or Linux system (for the world’s fastest imaging tool please ask about Detego® Ballistic Imager)
- System Profile – network profile, application profile etc.
- Internet history scan, including all browsers and applications such as Skype
- Common directories and folders (logical acquisition)
- Entire disk (logical acquisition)
- Physical acquisition (bit-for-bit copy) – Detego® Ballistic acquisition recovering deleted data and forensic image or unallocated areas (deleted) files
- Ram acquisition and or page/hibernation files

NO CONSTRAINTS

Detego® Field Triage allows complete customisation and flexibility for acquisition location(s). Investigators can customise their acquisition parameters to acquire files from internal/specifed drives, removable drives, network drives and user profiles. Acquire all files regardless of date/time and file-size, or set parameters in each of these for a tailored acquisition against specific times, regardless if the computer clock is set wrong on the target’s device. Custom file type enables investigators to target specific file types of interest by extension and header.

Detego® Field ‘Triage’s rapid acquisitions capture the entire file and can be targeted at (over 1,000) specific file types and sub groups, including, but not limited to:-

WATCH THE LIGHTS PATENT APPLICATION NUMBER 1309436.0

Detego® Field ‘Triage’s traffic light colour indicator instantly alerts ‘amber’ for suspicious content or activity, such as encryption and if pre-defined keywords, IP addresses, MAC address or other values in any languages are matched. The indicator will turn ‘red’ when known (illegal/suspicious) files are detected, such as user defined MD5s and SHA1 hashes, for example IIOC, counter terror files or organic investigation hashes.

Finally, at the end of the acquisition, if no amber or red criteria has been met, then the indicator will turn ‘green’ if the target computer is clear of a specific search type. This feature is perfect for non-technical frontline users tasked with identifying if certain hardware should be seized for further investigation. For intelligence or covert operations, the user does not need to know what is being searched, just that it has gone red/amber/green.
The colour indicators provide instant feedback, aids investigation speeds and thus reduces digital forensic backlogs and operation times. Other benefits include:

**Complimenting Digital Evidence Guidelines**

- Only electronic evidence that will potentially assist an inquiry are submitted
- An improved service delivery and efficiency in turn-around times
- Effective financial control and management
- Best value through effective and efficient use of resources
- The provision of quality products and services

**NEED TO GO COVERT?**

Detego® Covert offers the investigator the ability to capture data discreetly. Please contact us for more details on this tool.

**FORENSIC INTEGRITY**

Detego® Field ‘Triage’ is forensically sound and is fully compliant with forensic techniques. The same system supports Windows computers, Apple Mac and Linux systems all using the same interface, thus reducing training burdens, eliminating human error.

**THE 4 STEPS OF DETEGO® FIELD TRIAGE**

**POWERFUL, FAST AND FREE ANALYTICS**

Detego® Analyse® is the hub for all the products within the Detego® Suite of tools. It has a simple-to-use single interface, where all Detego® acquisitions can be analysed and reported on. Detego® Analyse is a free tool and its intuitive configuration seamlessly integrates with other Detego® products. The tool includes rapid import, acquisition processing, detailed analysis capabilities and licence management.

*please see Detego® Analyse full brochure

**TYPICALLY DEPLOYED IN**

First responder Police investigations, front line and covert operations, border security, sensitive site and tactical media exploitation and corporate investigations.
For more information from our Canadian Partner on the Detego® Suite.

Please contact: info@teeltechcanada.com
(250) 893-6125
www.teeltechcanada.com