LOGICUBE FALCON^{TM}

A PRACTITIONERS EXPERIENCE AND ASSESSMENT

BY

John (Zeke) Thackray, Churchill Fellow, FSS Dip

THACKRAY FORENSICS LTD
Leading the way in Computer Forensics, Data Discovery & Recovery℠

First Published Friday, 28th February 2014

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

The objective of this paper is to share an independent review of actual hands-on, in the field experiences when gathering evidence using the Logicube Falcon™**.**

The most important phase of any digital investigation is the initial preservation and verification of potential evidence. If this is not achieved in a safe and reliable manner any future analysis may be jeopardized and considered inadmissible. Choosing the right tools for the designated operational environment is exceptionally important to ensure maximum efficiency and insurance that all available information has been collected. Financial restraints of any organization are probably the most limiting element when choosing forensic tools. Organizations must compare short-term purchase costs of equipment and adequate certified training against an individual and departments long-term operational efficiency. Speed, accuracy, integrity and continuity over purchase cost increases operational efficiency and running costs.

Logicube Falcon™ - Assessment Overview and Objectives

Prior to using any new product live within a digital forensic environment, it is standard practice to conduct a quality assurance process, independent of a manufacturer's recommendation to cover the following elements:

Relevance and Necessity

Any forensic product must be relevant and necessary to complement the objectives of an organization and the environment it is designated to operate in.

Authentication, Reliability and Accuracy

Assess its reliability and accuracy. (Authenticating the manufacturer's statement of fact, ability and functionality).

Complies with Global Standards and Guidelines

Complies with global guidelines, procedures and unique local judicial regulations.

Compatibility

Compatibility with third party tools used within the unique forensic operational environment.

Using these guidelines the Falcon™ was vigorously tested in both a controlled and live corporate and criminal investigative environments. The level of operators using the Falcon™ varied between CSI (Crime Scene Investigators) and SOCO's (Scenes of Crime Officers) who are first responders with no technical background and highly trained and skilled digital forensic evidence examiners.

Field Investigators - First Responders (CSI/SOCO's)

The CSI/SOCO's were given the Falcon™ user manual and very basic hands-on instruction. The lack of their scientific technical knowledge and understanding surrounding the concepts of digital evidence was more of an obstacle than the actual use of the Falcon™. They quickly grasped the basic drive-to-drive evidence gathering concepts. However, the more advanced networking techniques were well beyond their ability and highlighted the need for more in-depth training of not only the product but the theory of digital forensics and evidence gathering.

These investigators were provided with competing products, similar in operating concepts and abilities as a comparison to the Falcon™. All investigators considered the touch screen interface of the Falcon™ and actual hands-on experience to be considerably more user friendly.

Digital Forensic Examiners

The digital forensic examiners were all very familiar with the various hardware acquisition tools available in the market place similar to the Falcon^{TM}. They all quickly became competent with the basic interface and navigated themselves around the Falcon^{TM} with ease. Some forensic examiners were less confident with the more advanced network functionality. Their understanding of the concept and need for a network functionality was limited until they were provided with specific scenarios. This once again highlighted that even highly trained digital examiners lacked basic knowledge and practical skills on the most important aspect of the forensic process, "the acquisition and preservation of data".

Falcon^{TM}, "OUT OF THE BOX" USER FUNCTIONALITY

The overall look and feel of the Falcon^{TM} is impressive. Its appearance and functionality definitely keeps pace, if not exceeds, the requirements of modern day high-tech digital investigations. Its design maintains the high quality of existing products available from Logicube and is both compact and lightweight, which is important for remote on-site examinations.

Appearance and Packaging

The carry case of the unit tested is made of heavy-duty fabric and although compact, the contents may be vulnerable to day-to-day movement in the long term. A nice aspect in the design is the size and weight; 2.5 lbs (1.09 Kg), which conforms to the restrictions of hand held luggage if travelling by commercial air transportation. The case has plenty of compartments for both the cables and spare destination storage hard drives. As standard, the cables and accessories do not come well organized and they seem to be randomly placed inside the carry case. This is a minor irritation, which can be quickly customized by the user for their unique requirements. A simple management system would ensure all relevant cables and accessories are easily identified and available when attending crime scenes away from a laboratory.

Physical Construction

The physical construction of the Falcon^{TM} is not "soldier proof"; the plastic outer case would not withstand excessive heavy handling in a battlefield or some crimes scenes. This is also true for the majority of Logicube's competitors, some of which have additional bulky hardware add-on accessories, where the Falcon^{TM} does not.

Destination and Source Hard Drives

The first significant observation of the Falcon^{TM}, is Logicube have abandoned their previous design as seen in products such as the Talon^{TM} and Dossier^{TM}, where the destination hard drive was contained within the unit. Having the destination drive for the collection of potential evidence inside an acquisition product is generally considered a fail-safe solution for first responders or less technical investigators. This does require advanced technical investigators to prepare the units for first responders prior to their use, adding additional steps, time and inconvenience to the "fail-safe" process. In reality, having the destination drive inside the unit can be restricted, confusing and awkward when dealing with high volumes of data or multiple suspect devices, which is often the case. It is common for non-technical investigators to cause damage to the connection cables and destination hard drives if they have to change them. Additionally, more serious errors occur when a suspect drive has been accidentally connected inside the unit to the destination area, causing potential evidence to be over written and destroyed beyond recovery. This feature is not necessarily a design fault of the acquisition device but the failure of organizations to educate their investigators in basic techniques and the technologies involved. Connecting both the source and destination drives on the outside of the unit, with clear markings that identify the separate connection ports, is much simpler and less confusing. It is ironic that other manufacturers are now replicating Logicube's old design by placing their destination drives inside their respective acquisition tools. Regardless of drives inside or outside the actual unit, there is still a strong requirement to educate all users in both the principles of digital evidence gathering and the functionality of the respective tool.

Touch Screen

The touch screen interface of the Falcon^{TM} is extremely user friendly and simple to navigate through. Some screen options are close together and using fingers to select or enter information can be crowded and less sensitive. Utilizing a stylus touch pen eliminates this problem completely. Unfortunately, the unit does not come standard with one. Alternatively, the unit supports two USB ports at the front of the device, which can also be used for a mouse and keyboard. The unit was not as responsive when using a Wi-Fi USB keyboard and mouse. If a USB mouse and keyboard are physically connected there is no port available to export a Falcon^{TM} generated log file. Alternative work rounds in this event are:

1. The Falcon^{TM} can also be connected to an existing network, or attached to a forensic workstation using a cross-over cable. The Falcon^{TM} can then be directly controlled through a web browser interface.

2. Connecting a mouse and keyboard through a USB hub will also provides spare ports to be used.

Configuration

The Falcon^{TM} is extremely simple to set up and use in its basic drive-to-drive operation. The user manual that accompanies the Falcon^{TM} is in a .pdf digital format and is written in non-technical language with simple to follow photographic illustrations that cover the various functionalities. For the more advanced aspects and particularly the network preview, capture and acquisition modes the user must have some sound networking technical knowledge. The only key element missing in the manual is a glossary of terminology. This would assist greatly for non-technical investigators to understand some of the basic terms used throughout the manual and also for advanced digital examiners when explaining their process in technical reports.

Non-Technical First Impression

The appearance of the Falcon^{TM} does project a "geek" factor and scientific approach for digital forensics when observed by the average person. This is emphasized further with the option to remote access the device across a network. This functionality takes the preview, discovery and acquisition phase of digital forensics into a new dimension, allowing non-technical investigators to be deployed with remote assistance or "hand holding" supervision. The deployment of the Falcon^{TM} in this way will not only increase the speed and efficiency of larger corporate and criminal investigations but also facilitate an extremely cost effective solution compared to some e-Discovery software products available.

KEY PRODUCT FEATURES

Performance and Speed

It is difficult to accurately judge the precise performance of any acquisition tool when estimating the process speed. There are far too many variables to consider such as the make, model and type of drives, the volume and type of data contained within them, their format and ultimately the age and conditions of both source and destination drives. Equally, the format of the evidence files and the use of compression and verification will affect the speed in which evidence is gathered and secured. Some manufacturers do not consider the time to verify the image files created as part of the acquisition speed. As a forensic investigator this is a major factor for consideration when gathering potential evidence. The verification of any potential evidence is an absolute requirement to ensure its integrity and continuity and its admissibility in a court of law.

It is important that the destination drives used to hold any potential evidence are fast and in good condition. Ultimately, the speed data can be read and written to a drive will determine the actual time it takes to collect any potential evidence regardless of the forensic tool performing the task.

The recommendations outlined by Logicube are consistent with the tests conducted. To maximize the performance in speed, high-quality and new destination drives were used. Even then, if the source drives were of an inferior brand or aging, the speeds varied considerably.

> *"Using fast, healthy SATA drives using mirror mode the Falcon would achieve approximately 11GB/min and when using e01 or dd format we expect speeds of 7-9GB/min. Logicube recommends that for the best performance use SHA-1 verification for all modes, and use the default compression setting when using e01 or ex01 mode".*

To accurately establish if the Falcon^{TM} performed as described by Logicube, the scenario outlined in their documentation, (provided above) was simulated. Throughout the tests, the Logicube statements were found to be accurate with very slight variables. To assess the Falcon^{TM} in reality a comparison of it was performed against the various competing forensic acquisition hardware and software tools. The exact same source and destination drives were used on each forensic product. An .e01 evidence file was created using SHA-1 verification and no compression. The Falcon^{TM} consistently equaled or bettered its competitors.

Multiple Image Formats and Imaging Ports

The Falcon^{TM} complements every computer forensic analysis tools and e-Discovery platforms in the market place. The file formats it creates can be read and examined by any of the leading analytical tools globally available today.

The Falcon^{TM} is more than adequately equipped to handle most situations that a crime scene examiner will encounter with the broad range and diversity of technology available throughout the world today. Of significant importance are the availability of ports included and the combinations in which they can be used.

Write Protected Source Devices

A maximum of four write-protected source drives can be connected at a single time, two SAS/SATA, one USB 3.0 and one Firewire device. The USB 3.0 port can be converted to a SATA using a USB to SATA adapter increasing the support to three SATA write-protected source ports as required. An IDE adapter is also provided to convert one SATA port to IDE.

Read/Write Destination Devices

A maximum of five destination drives can be connected at one time, two SAS/SATA, two USB 3.0 and one Firewire device. The two USB 3.0 ports can be converted to SATA using a USB to SATA adapter, increasing the support to four SATA destination ports. A network share (repository) can also be used to act as a destination.

Multi-task

Harvesting and processing large volumes of time sensitive information is critical in modern day digital investigations. Investigators need to know immediately in the majority of cases they conduct to either eliminate data or preserve it, to further their investigations. With the increasing high capacity of devices available to the average person, the task of harvesting and processing data from them is growing out of control.

Multi-task Macro Management

The Falcon^{TM} has been developed to eliminate both time and effort and can be configured to run a maximum of five multi-task macro functions. To validate this functionality and replicate a live scenario, the unit was configured to run a series of tasks as follows:

Task 1 Image from 80 GB SATA drive (S1) to a SATA destination drive (D1)

Task 2 Image from a 64 GB USB storage device (USB 1) to a USB 3.0 destination device (USB D1)

Task 3 Image from a 250 GB SAS drive (S2) to a network repository

Task 4 Wipe a 500 GB SATA destination drive (D2)

Task 5 Hash a destination drive 16 GB USB (USB D2)

The slowest device in the configuration controls the performance of multi-task processing. There appeared to be no significant difference in speed of each process between single or multi-task processing.

The multi-task management feature allows investigators to configure the Falcon^{TM} for a variety of scenarios and save each processing session for use at a later time. Building a library of sessions allows multiple users who do not have daily hands-on experience to confidently process and manage evidence. This also ensures that first responders and forensic examiners replicate best practice when gathering digital evidence.

Forensic Preview and Filter-Based File Copy

An extremely useful feature of the Falcon^{TM} is the preview and filter-based file copy. This feature alone allows small organizations to perform sensitive evidence gathering over large network environments.

When conducting proactive investigations in large business environments considerable delays and inconvenience can be caused. If a business has the focus or luxury of deploying expensive e-Discovery software solutions, this process is less invasive and disruptive. Unfortunately, this is not the case in the majority of incidents, particularly if local government agencies are investigating individuals in a medium-sized business environment. Deploying the Falcon^{TM} under these circumstances can be extremely beneficial. The Falcon^{TM} is simple to use and control across a network, specifically when searching for and identifying potential evidence on target computers by the file extension. All complications experienced during this type of forensic investigation were outside the control of the Falcon^{TM} and were caused by the speed of the network and its access privileges.

CONCLUSION

The most important phase of any digital investigation is the initial harvesting and preservation of potential evidence. The Falcon^{TM} achieves this and more and is, without a doubt, a breath of fresh air for the interrogation, acquisition and preservation phase of digital forensic investigations. The touch-screen interface gives the unit a feel good factor and the web browser and remote access is an excellent feature for real-time evidence identification and gathering. Its performance and speed to preview, acquire and save across a network together with the traditional drive-to-drive solutions is phenomenal for today's requirements. The automated and selective harvesting of information is an excellent feature for investigations involving privacy or e-Discovery requirements. Statements of speed are always ambiguous by any manufacturer but in reality the Falcon^{TM} performed admirably against its main competitors and exceeded any software solution available today. Many of the features of the Falcon^{TM} are considered standard and expected from such a product but the combination of the macro-task and network functionality allows greater diversity in the use of such a tool and simplifies the process for non-technical first responders. The remote access and automated functionality also provides a fail-safe solution for first responders and investigators to ensure consistency and best practice guidelines are adopted and guaranteed.

The Falcon^{TM} should not be considered as just a digital forensic acquisition tool but also as a key element by IT security consultants, system administrators and system auditors when identifying and harvesting information during routine non-criminal investigations. The Falcon^{TM} complements all forensic analysis, intelligence, e-Discovery and administrative IT software solutions.

In comparison to other digital forensic imaging solutions in the market today, that were tested, the Forensic Falcon™ is the most complete and extremely user-friendly solution for digital forensic investigations. The features of the Forensic Falcon™ are beyond those of its competitors and as such the functionality in speed, processing and reliability is superior.