LOGICUBE FORENSIC FALCON®-NEO

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, 12th July 2018

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

The objective of this paper is to share an independent review and actual hands-on, in the field experience when gathering evidence using the Logicube Forensic Falcon®- NEO.

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.

This independent review is designed to assist organizations or individuals to streamline that process when considering the use of the Logicube Forensic Falcon®- NEO without the influence of the manufacturer or other third-party competitors. Initially the testing conducted was performed in a controlled laboratory QA process. After proven concepts and manufacturer claims were validated, an extensive evaluation in a live environment with real evidence was made.

Forensic Falcon®-NEO - 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 Forensic Falcon®-NEO was vigorously tested in both a controlled and live corporate and criminal investigative environment. The level of operators using the Forensic Falcon®-NEO varied between highly trained digital forensic examiners, case investigators and first responders with little or no in-depth technical background.

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

The CSI/SOCO's were given the Forensic Falcon®-NEO 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 Forensic Falcon®-NEO. 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 Forensic Falcon®-NEO. All investigators considered the touch screen interface of the Forensic Falcon®-NEO 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 comparable to the Forensic Falcon®-NEO. They all quickly became competent with the basic interface and navigated themselves around the Forensic Falcon®-NEO 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".

One feature that was embraced by the digital forensic examiners was the multi-tasking feature and the versatility of combining different processes to run simultaneous. They were also impressed with the exceptional speed in which the forensic evidence imaging process and verification was performed.

Forensic Falcon®-NEO, "OUT OF THE BOX" USER FUNCTIONALITY

The overall look and feel of the newly improved Falcon NEO™ is very impressive, particularly when comparing it to other competing and similar products in the market place. Its appearance and functionality has not only improved but exceeds the expectations for modern day high-tech digital investigations compared to other products. Its design maintains the high quality of a product associated with Logicube.

Appearance and Packaging

The standard carry case is made of heavy-duty fabric and although compact, the contents may be vulnerable if used in some adverse environments such as a military field environment or criminal crime scene. For adverse environments it is also available in a Pelican case, which is more appropriate for these types of operations. A nice aspect in the design is the size and weight; 3 lbs (1.36 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.

Physical Construction

The physical construction of the Forensic Falcon®-NEO 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 Forensic Falcon®-NEO does not.

The availability of two DC in power ports is a nice touch for extra power when fully loading the unit with multiple source and destination drives running various tasks. It will also future proof the system if some drives require higher power supply to get them running. Only one power supply is provided out of the box. During the evaluation, every port was utilized, and a variety of simultaneous processes were executed. Only one power supply was used during the evaluation and there was no hint of any degradation to the power requirements.

Touch Screen – HDMI – USB 3.0 Host Ports

The 7" color LCD touch screen interface of the Forensic Falcon®-NEO is extremely user friendly and simple to navigate through the various on-screen options. The brightness of the screen can be modified as desired and even turned off for in stealth mode for covert operations.
The unit supports two USB 3.0 host ports at the front, which can be used for a mouse and keyboard. **These two USB ports can also be utilized as Destination storage ports if required to save evidence to.** An external monitor can be also added for better viewing using the HDMI port at the rear of the unit. This is extremely useful when working within a laboratory environment, particularly when adding a mouse and keyboard to the unit.

Network (Duel 10GbE ports)

The Forensic Falcon®-NEO can be connected to an existing network and controlled through a web browser interface. It has two 10GbE ports at the rear of the unit. This is also very powerful and allows the connection of large NAS storage devices to the unit or a combination of both NAS storage and network connectivity.

Basic users accessing the remote operation with no network experience or limited knowledge had some difficulty, which was quickly overcome when following the remote operation instructions within the Logicube Falcon®-NEO User's Manual. The fully illustrated guidelines were simple to follow and easy to use.

Source and Destination Devices/Network Push Option

The Forensic Falcon®-NEO has increased the variety of available ports for both source and destination devices. The ability and ease to control devices externally helps the user to process most devices with confidence and speed. The ease of access to connect both source and destination devices keeps the acquisition phase of the investigation simple and efficient, while maintaining integrity and continuity to the process.

The only negative comment that could be said about the unit is, some investigators did become confused which side was the write protective source and the unprotected destination. Although it is clearly marked on each side, which function is used for each specific purpose, it would be less confusing if that was physically labeled on the top of the unit as well as the side. Regardless of the markings, once the desired software processes are selected there are on screen warnings to prevent any human errors connecting devices to the wrong area.

The Push feature also allows the transfer of data from the Forensic Falcon®-NEO to a network or storage repository attached to the unit. The user can also select a verification option at the end of the transfer, essential when archiving old cases or creating backups.

Configuration – System Settings

The Forensic Falcon®-NEO is simple to set up and utilizes six different settings:

User Profiles
Passwords for added security
Encryption for advanced security and protection of destination drive
Language/Time Zone
Display – Brightness or Stealth/Covert mode
Notifications when a process is completed, or an error occurs

The user manual that accompanies the Forensic Falcon®-NEO 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 technical networking knowledge. The frequently asked questions and index at the end of the User's Manual is most useful for none technical users. A glossary of terms would be a useful addition for field operators who are not familiar with technical computer or forensic jargon.

Non-Technical First Impression

Logicube have maintained a good visual appearance of the Forensic Falcon®-NEO, which continues to project a "geek" factor and scientific approach to digital forensics when observed by the average person. The Forensic Falcon®-NEO is without doubt good value for money when comparing the enhancement of features and the dramatic increases in speeds when processing evidence. This is particularly evidenced when running multiple

processes simultaneously on one unit. The Forensic Falcon®-NEO is compact and packaged in a very professional way, which enhances the expert appearance of a forensic examiner to those not familiar with digital investigations or the process.

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. However, when harvesting intelligence and time is of an issue, verification may not be required and having the ability to turn this feature on and off is valuable. Logicube have taken the image and verification process to another level and reduced the entire process dramatically. This is achieved by running the verification process concurrently, which commences shortly after imaging starts. This is a very efficient feature compared to traditional processes, used by many acquisition tools, which run sequentially, after the imaging phase has completed. If quality destination drives are utilized the Forensic Falcon®-NEO can reduce the image and verify process significantly.

It is important that the destination drives used to hold any potential evidence are fast and in good condition without any bad sectors etc. 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.

To maximize the performance in speed, high-quality and new destination drives should be used. Even then, if the source drives are of an inferior brand or aging, possess bad sectors, etc. the speeds will vary considerably.

A variety of different type hard drives and media both old and new were used during the evaluation to accurately establish if the Forensic Falcon®-NEO performed as described by Logicube:

> *"It achieves imaging speeds surpassing 50GB/min and can clone PCIe to PCIe at speeds of 90GB/min"*

Throughout the evaluation the Logicube statement was found to be accurate and reliable. To further assess the Forensic Falcon®-NEO, a comparison of it was performed against various competing forensic acquisition hardware and software tools with like for like functionality. 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 Forensic Falcon®-NEO consistently exceeded the speed in acquisition and verification of all other products.

Forensic Falcon®-NEO was particularly impressive in speed when running the Wipe/Format feature using all available destination ports. The only disappointment experienced in this feature is the default naming convention of the drives to the title "Repository" when formatting. It would be nice to uniquely customize the drive title at the time it is formatted.

Multiple Image Formats and Imaging Ports

The Forensic Falcon®-NEO 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. Forensic Falcon®-NEO also supports the ability to encrypt the destination drive where the evidence files are created and saved. If the source drive is using BitLocker encryption, it can be decrypted if the password/phrase or recovery key is known.

The Forensic Falcon®-NEO is adequately equipped to handle most scenarios with the diversity and broad range of technologies a digital forensic examiner will encounter. Of significant importance are the availability of ports and robust cables, which are easily accessed for speed and can utilized in combination with each other.

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, one PCIe.

Read/Write Destination Devices

A maximum of eight destination drives can be connected at one time, two SAS/SATA, two SATA, three USB 3.0 (one on the destination side and two at the front of the unit if not used for a mouse or keyboard) and one PCIe Two 10GbE network ports can also be utilized for NAS destination or super-fast network imaging.

Network Analysis/Capture

Logicube have significantly improved the ability to perform network analysis and capture in the following areas:

- Capture network traffic, internet activity and VOIP.
- Sniff data on a network and store captured packets on a destination drive connected to the Forensic Falcon®-NEO.
- Span the Net Traffic to File images over two or more Destination drives. Captured data is saved to a .pcapng file format.

Imaging Surface Pro 4+ / MacIntosh Systems

As technology develops and devices become more sophisticated in their architecture the ability to quickly and safely recover potential evidence from within them is equally challenging and complicated. The Forensic Falcon®-NEO.meets these challenges head on and can acquire data from such devices as a Surface Pro 4+, and MacIntosh systems in the following ways:

- The ability to image a laptop without removing the internal hard drive.
- Create a forensic bootable USB flash drive to image a source drive from a computer on the same network without booting the computer's in their native O/S environment.
- Supports Surface Pro 4+ and Macintosh systems.

Multi-task

Harvesting and processing large volumes of time sensitive information is critical in modern day digital investigations. Investigators need to know almost immediately in most cases to either eliminate data or preserve its entirety of specific elements, 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.

The Forensic Falcon®-NEO has taken the speed and functionality of the harvesting process to a completely new level.

Multi-task Macro Management

The Forensic Falcon®-NEO 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 Forensic Falcon®-NEO for a variety of scenarios and save each processing session for use later. 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.

Targeted and Logical Imaging

An extremely useful feature of the Forensic Falcon®-NEO is the Targeted/Logical Imaging feature. This functionality not only reduces the acquisition time but also ensure quality and appropriate data is recovered. Investigators can create a logical image by using a variety of filters that are pre-set, custom and/or file signature based. When filters are used collectively with keyword searches only specific and relevant files are harvested. Another nice feature is the ability to generate an MFT report, which may identify a list of potentially deleted files. The output format can be either L01, LX01, ZIP or directory tree structure. The data collected can be reviewed directly on the Falcon-NEO display, or manage over a network from a forensic workstation using a web interface to access the unit remotely.

This feature allows investigators and organizations to perform sensitive evidence gathering over large network environments or individual devices, while maintaining an efficient, accurate and reliable evidence gathering process that ensures its integrity and continuity.

Audit Trial / Log Files

The audit trail/log files provide detailed information on each operation conducted. The log file can be reviewed directly on the display of the Forensic Falcon®-NEO or via a web browser. Logs can also be exported in an XML, HTML or PDF format.to a destination device connected to the unit.

CONCLUSION

It is globally accepted that the most important phase of any digital investigation is the initial harvesting and preservation of potential evidence, while maintaining the continuity and integrity of it. The average size of data now encountered on even basic digital investigations can be measured in high volume terabytes. Logicube have not only met the need to increase the speed in which data can be securely harvested but have enhanced the functionality and capability of the Forensic Falcon®-NEO with devices supported, encryption, network collection and remote operating to name but a few. The enhanced touch-screen interface and options continues to give the Forensic Falcon®-NEO a very professional and feel good factor, leading the way in digital forensics. The speeds in acquisition of between 50GB to 90GB per minutes, as validated is simply phenomenal. These speeds not only meet the requirement of high volume sophisticate business systems but also the extremely large capacities of standard home computers. The concurrent verification also enhances the efficiency of data acquisitions and speed in which they are now achieved.

The ability to automate and selectively harvest information is critical for investigations involving privacy or e-Discovery requirements. Statements by any manufacturer professing speeds in processing are always ambiguous but again in reality, the Forensic Falcon®-NEO performed admirably against its main competitors and always exceeded any software solution we tested with today's technology available. Many of the features of the Forensic Falcon®-NEO 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 not only adopted but adhered to and guaranteed.

The Forensic Falcon®-NEO should not be considered just as a forensic, criminal or civil ligation solution. It should also be considered by IT security consultants, system administrators and system auditors when identifying and harvesting information during routine non-criminal investigations. It also has many features that are necessary for generic IT maintenance and management, such as the wiping functionality that will remove information beyond recovery when recycling systems within an organization or releasing them for sale to a third party.

As a user of the Falcon and other competitive products that are like for like, Logicube have surpassed all expectations with the new Forensic Falcon®-NEO. This is particularly evidenced when considering not just the speed in which it now processes but the additional advanced features, functionalities and support it now provides.

In comparison to other digital forensic imaging solutions in the market place today, from a hands-on comparison and vigorous tested, Logicube has once again produced the most complete state of the art extremely user-friendly solution for digital forensic investigations and IT management with the Forensic Falcon®-NEO. The many features and functionality of the Forensic Falcon®-NEO continue to exceed those of its competitors and as such the consistent advancements in speed, processing and reliability is not only superior but critical for today's highly developing digital investigative and IT management world. This is a must have tool in any forensic or IT security/management department. The time saved in simple but secure data analysis and harvesting is a financial investment and will save many person hours in the long term.