LOGICUBE FALCON®-NEO2

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™

Monday 26th September 2023

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

A review of Logicube's last forensic imager, the Falcon®-NEO, was performed in March of 2021. That assessment, in the context of years of using forensic imagers in an operational environment, found the Falcon®-NEO to be without doubt the "Best in Class" solution among the digital forensic imagers in its tier at that time. The assessment also revealed the Falcon®-NEO to be the "premier" portable forensic imager in the marketplace at the time and a must have solution for all digital forensic, cyber security or specialist information technology practitioners.

Now, Logicube has introduced its follow-on imager to the Falcon®-NEO, and it is aptly called the Falcon®-NEO2. The Falcon®-NEO2 is advertised as taking the standards set by its predecessor to new heights by being equipped with a fully re-designed "engine" that sets new and previously unseen imaging speeds in a field imager, as well as increasing the numbers and types of ports available on the new device. This review, therefore, updates the March 2021 assessment done on the Falcon®-NEO and is designed to comprehensively evaluate the new Falcon®-NEO2 to assist organizations or individuals to streamline the quality assurance process when considering the use of the Logicube Falcon®-NEO2 without the influence of the manufacturer or other third-party competitors. The assessments and testing were performed in a controlled laboratory QA process. After proven concepts and the manufacturer claims were validated, an extensive evaluation was then performed in a live environment across real evidence.

ASSESSMENT OVERVIEW AND OBJECTIVES

Prior to using any new or updated forensic hardware or software live within any digital forensic investigations, it is standard practice to conduct a quality assurance process, independent of a manufacturer's statements of facts or claims to assess the following elements:

Relevance and Necessity

Any forensic product or its enhancements 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 a unique forensic, IT security or legal operational environment.

Using these guidelines, the Falcon®-NEO2 was vigorously tested in both a controlled and live corporate and criminal investigative environment. The level of operators using the Falcon®-NEO2 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 Falcon®-NEO2 user manual and basic hands-on instructions. They quickly grasped the basic evidence gathering concepts. The more advanced networking techniques 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®-NEO2, as well as a description of the differences between the Falcon®-NEO2 and the Falcon®-NEO, which some had used before. All investigators considered the touch screen interface of the Falcon®-NEO2 and the ease in which a keyboard, mouse and HDMI monitor can be added as a useful feature, which made the actual hands-on experience to be considerably more user friendly.

Digital Forensic Examiners

The digital forensic examiners were all familiar with the various hardware imaging solutions available in the marketplace comparable to the Falcon®-NEO2, and the fact that Falcon®-NEO2 has maintained the same form, fit, footprint, and Graphical User Interface (GUI) as its predecessor Falcon®-NEO2 was a great decision on the part of Logicube which made the introduction of the Falcon®-NEO2 and its first-use simple and streamlined. They all quickly became competent with the basic interface and navigated themselves around the Falcon®-NEO2 with ease.

The feature that the digital forensic examiners were most impressed with was the phenomenal speeds in which the forensic evidence imaging process and verification was performed. The Falcon®-NEO2 attained E01 imaging speeds reaching 120 GB/min using the fast SSD drives it was tested with. This is an industry "first" for field imagers. No forensic field imager had been able to break the 100 GB/m imaging speed barrier before. This exceptional speed (Logicube only advertises a speed of up to 115GB/m for an E01 capture) is a remarkable technological accomplishment on the part of Logicube, which until now had not been accomplished or seen by examiners with any other manufacturer's field imagers.

Forensic examiners also made note of the PCIe cloning speeds of the Falcon®-NEO2 which exceed 100 GB/m when using fast PCIe drives, and PCIe Wiping speeds of up to 115 GB/m, in comparison to PCIe capture and wipe speeds of 90GB/m on the predecessor product.

As with the previous Falcon®-NEO, the Thunderbolt, Mobile Device Capture and Network Traffic and Cloud collation were some of the key features that raised interest, and enthusiasm.

FALCON®-NEO2, "OUT OF THE BOX" USER FUNCTIONALITY

The overall look and feel of the new Falcon®-NEO2 is very much similar, and almost identical to its predecessor, the Falcon®-NEO, and the size and footprint of the product are indeed the same as the Falcon®-NEO, As stated earlier, this is of great benefit and comfort to the users of Logicube's line of Falcon family of imagers as it signifies a sense of continuity and familiarity with previous imagers. Accessories and optional modules are very impressive, particularly when comparing them to other competing and similar products in the marketplace. Falcon®-NEO2's functionality has not only exceeded the standards set by its predecessor but also 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.

The Falcon®-NEO2 host name can be customized to a user's requirements. This is useful if the unit is being used on a corporate network to acquire data during covert operations.

Appearance and Packaging

The standard carry case is made of heavy-duty luggage 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. It is strongly recommended to add the Pelican case, which is optional, and more appropriate if it is intended to be used in these types of environments. A nice aspect in the product's design is the size and weight, which conforms to the restrictions of handheld luggage if travelling by commercial air transportation. Both case options have plenty of storage area for both the cables and spare destination storage hard drives.

Physical Construction

The most striking and impressive attributes of the physical construction of the Falcon®-NEO2 are the numbers AND types of ports that have been incorporated into this new model. The number of SAS/SATA ports on the source and destination of the Falcon®-NEO2 have been increased to 4, and all are SAS-3 (12 Gb/s) ports. Furthermore, the number pf USB 3 ports on the device now stands at 6, and these ports are all USB 3.2 gen-2 ones, with maximum speeds of 10 Gbps. This level of integration and upward technology migration in a chassis that has not increased in size from the predecessor model is truly exceptional. The physical construction of the Falcon®-NEO2 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, whereas the standard Falcon®-NEO2 does not.

The availability of two DC in power ports continues to be a nice touch for extra power when fully loading the unit with multiple source and destination drives to run various tasks. It also future proofs the system if new technology requires additional power supply to maintain stability when processing them. 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 3.2 Host Ports

The 7" color LCD touch screen interface of the Falcon®-NEO2 is extremely user friendly, sensitive to the touch 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 "stealth mode" during covert operations.

The unit supports two USB 3.2 gen-2 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, and they can also be converted to SATA ports (with a use of an adapter) if additional SATA destination ports are needed. An external monitor can also be 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 used in combination with a mouse and keyboard.

Network (Dual 10GbE ports)

The Falcon®-NEO2 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 immensely powerful and allows the connection of large NAS storage devices to the unit or a combination of both NAS storage and network connectivity.

The network ports can also be utilized to capture network traffic, which can then be examined within an array of third-party software tool.

Basic users accessing the remote operation with no network experience or limited knowledge may have some difficulty, which is quickly overcome when following the remote operation instructions within the Falcon®-NEO2 User's Manual. The fully illustrated guidelines are also provided with the Falcon®-NEO2 digitally and are simple to follow and easy to use.

Source and Destination Devices

The Falcon®-NEO2 has a variety of available ports for both source and destination devices. The ability and ease to control devices externally helps the user to process them with confidence and speed. The ease and 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 breakdown of the available

Source and Destination ports on the Falcon®-NEO2 is as follows:

Source ports:
4 SAS-3 (12 Gb/s) SAS/SATA ports, through 1 SAS connector
2 USB 3.2 Gen-2 ports (10 Gbps)
1 PCIe port
2 I/O Ports for use with optional I/O cards including Thunderbolt™3/USB-C

Destination ports:
4 SAS-3 (12 Gb/s) SAS/SATA ports, through 1 SAS connector
4 USB 3.2 Gen-2 ports (10 Gbps)
1 PCIe port
1 I/O Port for use with optional I/O cards including Thunderbolt™3/USB-C

In effect, the Falcon®-NEO2 forensic imager can be viewed as a 10-source to 11-destination device, when one of the network ports is used as a source and the other as a destination, and both host USB ports are used as destinations as well.

A new and welcomed addition to the Falcon®-NEO2 design in support of the new technologies it offers (SAS-3 source and destination ports) is the inclusion of a 1-to-4 12Gbps SAS/SATA data and power cable. This new cable replaces the 4 separate SAS/SATA cables that were used on the previous Falcon®-NEO model. One end of the new 12 Gbps cable connects to Falcon®-NEO2's source and destination SAS-3 and power connectors and the cable then branches out to 4 connectors for connection to the drives. This specialized new cable is rated for 12 Gbps transfers and greatly eases the connection of source and destination drives and reduces clutter around the imager.

Additionally, with the introduction of the Falcon®-NEO2, Logicube has introduced a new 4-port USB to SATA adapter (converter). This extremely useful converter can be used to convert the 2 USB 3.2 destination and the 2 USB 3.2 host / destination ports to SATA ports, thereby increasing the total number of SAS/SATA destination ports to 8. With this added flexibility, forensic investigators can now image each of the 4 source SAS/SATA drives into 2 SAS/SATA destination drives, in effect conducting 4 simultaneous 1-to-2 captures, resulting in 2 copies of each evidence drives. This is a practice that is a requirement for many law enforcement agencies worldwide.

The accumulation of all the above resources on the Falcon®-NEO2, in terms of the numbers, types, speeds, and the ports configurations of the product make it the most powerful and integrated forensic field imager currently in the market.

Network Push Option

The Push feature allows the transfer of data from the Falcon®-NEO2 to a network location, storage drive or a repository attached to the unit. The verification option at the end of the transfer is essential when archiving old cases or creating backups to maintain data integrity.

Configuration – System Settings

The Falcon®-NEO2 is simple to set up and once they are applied, the selections become persistent, in that they are retained within the memory even if the unit is turned off and restarted.

There are eight different settings where a user can configure the Falcon®-NEO2 to their own unique operational protocols and requirements:

Setting	Overview
User Profiles	Configures a profile of the user's choice such as how the Falcon®-NEO2 boots with their imaging preferences
Passwords	Added security for system functionality and user accounts
Encryption	Advanced security and protection of destination drives
Language/Time Zone	Language and time zone settings
Display	Brightness or Stealth/Covert mode
Notifications	Extremely useful. Once a task is completed, or an error occurs a notification by sound or email/SMS/MMS, or both is sent to the user
Advanced	APFS file to file imaging can be switched on or off
Debug	Used for technical support and it is recommended that it is only used when instructed to do so by Logicube Technical Support

The user manual for the Falcon®-NEO2 is in a .pdf digital format and is written in non-technical language with simple to follow photographic illustrations that cover the various functionalities. The user manual is available online and a QR code link to the manual is included with the Falcon®-NEO2. 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 nontechnical users. A glossary of terms and definitions for commonly used abbreviations 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 the same good visual appearance of the preceding Falcon®-NEO on the Falcon®-NEO2, which continues to project a scientific approach to digital forensics when observed by the average person. The Falcon®-NEO2 is without doubt the best value for money when comparing the enhancement of the specification and the dramatic increases in speeds when processing evidence. This is particularly evidenced when running multiple processes simultaneously on one unit. The Falcon®-NEO2 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

This section covers the key features of the Falcon®-NEO2 and how it performed during the assessments conducted.

Performance and Speed

It is difficult to accurately judge the precise performance of any imaging 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 and critical consideration when gathering potential evidence to ensure it is admissible in a court of law or legal hearing.

The verification of any potential evidence is an absolute requirement to ensure continuity and integrity is maintained. However, when harvesting intelligence or in a civil matter where the law of probability is accepted, or even when time is of an issue, verification may not be viable. Therefore, having the ability to turn this feature on and off is essential. Logicube continues, in Falcon®-NEO2, the image and verification process they introduced in their previous editions of their Falcon line of imagers. 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 Falcon®-NEO2 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.

As stated earlier, the most remarkable feature of the new Falcon®-NEO2 is the phenomenal imaging speeds that it attains. Of course, to maximize the performance in speed and to reach the maximum speeds that Falcon®-NEO2 is equipped to attain, high-quality and fast SSD destination drives should be used. Even then, if the source hard drives are of an inferior brand or ageing, possess bad sectors, etc. the speeds will vary considerably. However, achieving cloning speeds of up to 115GB/m in SAS-3 SSD to SAS-3 SSD E01 imaging is a feat that is currently beyond compare.

Logicube states the Falcon®-NEO2 performs as described below:

> *"It achieves imaging speeds of up to 115 GB/min on SAS-3 SSD to SAS-3 E01 captures"*
>
> and
>
> *"Wipe PCIe drives at speeds up to 115 GB/min"*

To establish the accuracy of these statements, fast SAS-3 SSD drives (such as SanDisk Lightning Ascend Gen II 2.5" family) were used during this recent assessment together with real life experience over recent years using the preceding Falcon®-NEO. Throughout the evaluation and the years using imagers during digital investigations and an IT administrative environment, the Logicube statements were found to be accurate and reliable for both imaging and wiping processes. To further assess the Falcon®-NEO2, 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 a SHA-1 verification with no compression. The Falcon®-NEO2 surpassed the speed in acquisition and verification of all other products. Using fast SAS-3 SSD drives as source and destination, the Falcon®-NEO2 achieved 115 GB/min while no other forensic product achieved the same speed.

Wipe / Format

Sterilization of recycled storage devices between cases has always been an important and critical phase of any digital investigation to prevent cross contamination between investigations, particularly if they are of a similar nature. The Falcon®-NEO2 supports the ATA sanitize command and Secure Erase for supported nonvolatile memory express (NVMe) drives. Destination drives and repositories as the name suggest is typically where evidence files are stored to. NTFS, EXFAT, EXT2, EXT3, EXT4, FAT32 and HFS+ formats are available to enhance the flexibility of the Falcon®-NEO2.

Multiple Image Formats and Imaging Ports

The Falcon®-NEO2 complements every computer forensic analysis tool and e-Discovery platforms used in the marketplace. The evidence file formats it creates can be read using the inbuilt file browser to perform a quality assurance check. They can also be added and examined by any of the leading analytical forensic tools globally available today.

There are seven available imaging modes within the Falcon®-NEO2:

Mode	Process
Drive to File	Images the source to a DD, E01, EX01 or DMG file format. **AFF4 will be added, according to Logicube.*
File to File	Creates logical files to a LX01, L01, Zip or directory tree. An MFT report can also be generated to identify deleted files, which is extremely useful.
Partition to File	Creates a logical image in a DD, E01, EX01 file format. Bitlocker is also supported but requires the password or credentials.
Net Traffic to File	Captures network traffic and can include network, internet and VOIP activity.
Drive to Drive	Creates a bit for bit copy from source to destination drives
File to Drive	Restores a DD, E01, EX01 and DMG images providing they were originally created by the Falcon®-NEO.
***Mobile to File**	Extracts data from iOS (up to iOS 17.x) and Android (4.0 to 12) devices. **This is an additional annual subscription option.*

Logicube indicates that the AFF4 file format support will be added to the Falcon®-NEO2 in the near future, but it was not available at the time of this assessment.

The Falcon®-NEO2 can "reverse read" any bad sectors encountered. Over the years this technique has found data missed by many products that do not have this ability. Reverse read simply skips the bad sector and reads it backwards, potentially capturing data that otherwise would have been marked with zeros, which is a great feature, leaving no stone unturned.

The Falcon®-NEO2 is equipped to resume an imaging process for drive to drive, drive to file or partition to file if the power to the unit is interrupted or a task is aborted. This feature can also be set to automatically resume once power is reconnected. Again, this is something many products cannot achieve and a valuable functionality for today's digital investigations when data sets are growing exponentially.

A user can create, rename, or delete folders on a destination drive or repository using the Falcon®-NEO2, which provides much more flexibility in the data management process.

The Falcon®-NEO2 supports Apple File System (APFS) format, which can also be viewed using the inbuilt file browser. However, this option is not switched on by default and must be turned on in the system settings screen, advanced tab before commencing this process.

Destination Drive Encryption and Source Encrypted Drive Support

The Falcon®-NEO2 can encrypt the storage drives, which improves the security of harvested evidence. It can also identify any potential encrypted drives and if the password is known for some types can open the containers to expose the data within them.

Destination Storage Drives – Encryption

The Falcon®-NEO2 supports the ability to encrypt the destination drive where the evidence files are created and saved. This is particularly useful if transporting potential evidence using public courier services or protecting sensitive case information.

Source Encrypted Drives

If the source drive is encrypted with ATA security, OPAL, VeraCrypt, TrueCrypt, FileVault or BitLocker a padlock icon will appear next to its details. Selecting the padlock icon allows the password to be applied to unlock the drive. If the encryption type is not known a message will be presented warning the user, the drive or any available partitions may be potentially encrypted.

Even without the array and flexibility of additional options available for the Falcon®-NEO2, the out of the box system is adequately equipped to handle most scenarios with the diversity and broad range of technologies a digital forensic examiner will encounter. Significantly important are the availability of a variety of 12 Gb/s and 10 Gb/s ports and a robust new 4-port 12Gb/s SAS/SATA cable, which are easily accessed for speed. These can also be utilized in combination with each other.

Source Write-Protected Capability

A maximum of 7 write-protected source devices can be connected at a single time, 4 SAS/SATA, 2 USB 3.2 and 1 PCIe. Two optional write protected Thunderbolt 3/USB-C I/O cards can also be added if required.

Destination Read/Write Capability

A maximum of 9 destination devices can be connected at one time, 4 SAS/SATA, 4 USB 3.2 (2 on the destination side and 2 at the front of the unit if not used for a mouse or keyboard) and 1 PCIe. One optional write protected Thunderbolt 3/USB-C I/O cards can also be added if required.

There are also two 10GbE network ports, which can also be utilized for super-fast NAS destination storage or network imaging/storage and collection, or each as either a source or a destination port.

Source and Destination Flexibility

Using the optional new 4-port USB to SATA converter adapter available from Logicube, the destination configuration of the imager can also be increased significantly, by enabling 4 simultaneous 1-to-2 captures. Adding the Thunderbolt, FireWire, SCSI, and Fibre Chanel modules to either the source or destination sides makes the Falcon®-NEO2 the most versatile and flexible all-encompassing digital imaging solution available by any manufacturer.

Network Analysis/Capture

Logicube provides significant abilities 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 Falcon®-NEO2.
- Span the Net Traffic to File images over two or more Destination drives. The captured data is saved to a .pcapng file format, which can be examined by many third-party security and digital forensic analysis tools.

The contents of a mounted network repository can also be viewed with the inbuilt file browser.

GUI support has also been added for multiple iSCSI connections, which is important if multiple NAS units are available across a network for data to be written to.

Imaging Surface Pro 4+ / MacIntosh Systems

As technology develops and devices become more sophisticated in their architecture the ability to recover potential evidence quickly and safely from within them is equally challenging and complicated. The Falcon®-NEO2 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 computers in their native O/S environment.
- Supports Surface Pro 4+
- Supports Macintosh systems target disk mode

Multi-task

The collection of large volumes of time sensitive information is critical in modern day digital investigations. Forensic examiners are often required to quickly assess if data can be eliminated, preserved in its entirety or a selective harvest of relevant information is to be collected. 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 Falcon®-NEO2 has taken the speed and functionality of the harvesting process to a level never before seen by any forensic imagers.

Multi-task Macro Management

The Falcon®-NEO2 continues Logicube's design philosophy of minimizing both time and effort and can be configured to run a maximum of five multi-task macro processes, each of which can run nine tasks sequentially.

To validate this functionality and replicate a live scenario, the unit was configured to run a series of tasks as follows:

Macro	Task	Process	Destination / Source Port	Media
Macro 1	Task 1	Wipe Drive (Custom)	Destination Port 1 (D 1)	250 GB SSD
	Task 2	Image 1 (L01)	Network Port 1 (LAN 1)	Cloud Storage - Dropbox
Macro 2	Task 1	Wipe Drive (Custom)	Destination Port 2 (D 2)	250 GB SSD
	Task 2	Image 2 (Mobile Device Capture)	Source Port (USB 1)	iPhone 8, IOS 12.5
Macro 3	Task 1	Wipe Drive (Custom)	Destination Port 3 (D 3)	250 GB SSD
	Task 2	Image 3 (E01)	Source Port (S 1)	100 GB
Macro 4	Task 1	Wipe Drive (Custom)	Destination Port Thunderbolt Drive (TBT D 1)	2 TB SanDisk Removable Drive
	Task 2	Image 4 (EX01)	Source Port Thunderbolt Drive (TBT S 1)	1 TB SanDisk Removable Drive
	Task 3	Hash Device	Destination Port Thunderbolt Drive (TBT D 1)	1 TB SanDisk Removable Drive
Macro 5	Task 1	Wipe Drive (Custom)	Destination Port (D 4)	250 GB SSD
	Task 2	Image PCIe	Source Port (PCIe SCSI Module S 1)	100 GB SCSI

The slowest device in the configuration controls the performance of the multi-task processing. The key advantage of multi-task macro management is the significant saving in time and person hours. Large volumes and a variety of data can be processed out of normal hours, such as overnight or across a weekend.

Using the notifications in conjunction with multi-task macro processing an email or the new SMS option can be sent when the process has finished or even if an error occurs. Setting up each macro and its associated tasks was extremely simple and 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®-NEO2 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 Falcon®-NEO2, carried over from its predecessor the Falcon®-NEO, is the Targeted/Logical Imaging feature. There are four key filtering options, which not only reduces the acquisition time but also ensure quality and appropriate data is recovered.

> **Path Filter.** An investigator can navigate through a device of interest using the simple browser interface and select the files or directory structure relevant to the investigation. The preset filter option allows a more permanent automated filtering options such as, include all users' directories or exclude windows directories. A custom file path filter can also be added if required.
>
> **Date Filter.** Often in civil litigation a court will restrict the data being harvested by a date range. The Falcon®-NEO2 has a date filter option to include or exclude a date range of the information being harvested.
>
> **Signature Filter.** This is another useful feature that specifically targets categories of data sets such as, documents, audio, images, videos, or archive type data and is run after a path or date range filter.
>
> **Keyword Filter.** A list of keywords relevant to the investigation can also be run after any previous filters have been applied. This will naturally reduce the data sets being harvested and is often a requirement by the courts during many digital investigations and e-Discovery preservations.

When filters are used collectively with keyword searches only specific and relevant files are harvested. The Falcon®-NEO2 allows a very versatile output format, which can be preserved in a forensic evidence file format L01, LX01 or even a ZIP file or a directory tree structure replicating the respective storage device or targeted area. The L01 or LX01 formats now have the option to change the segment size and compress the output evidence files created. Having the ability to also generate an MFT audit log is extremely useful to quickly identify the presence of deleted files. These useful enhancements in the Falcon®-NEO2 once again demonstrate that Logicube listens to their users to enhance the ability to better manage the final output data sets.

The data sets collected can be either reviewed directly on the Falcon®-NEO2 display or managed over a network from a forensic workstation using a web interface to access the unit remotely.

Targeted and logical imaging allows investigators and organizations to perform sensitive evidence gathering over large network environments or individual devices, while maintaining an efficient, accurate and reliable evidence collection to ensure the integrity and continuity of the process.

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 Falcon®-NEO2 or via a web browser. Logs can also be exported in XML, HTML or PDF format to a destination device connected to the unit. In addition to the audit logs, S.M.A.R.T. data logs pre and post capture are generated and can be exported together with the audit log files from the LOGS screen.

Cloud Storage Acquisition

A very significant and highly useful addition to the standard and built-in features of the Falcon®-NEO2 is the cloud storage acquisition capability. This feature, which was an annual renewable software subscription solution in the preceding Falcon®-NEO (same as the mobile device capture feature) is now active and enabled out of the box on the Falcon®-NEO2. It currently supports Microsoft OneDrive, Google Drive and Dropbox. The log on credentials for the respective storage area are required to successfully perform an extraction of data from them. The data from the cloud storage can be saved locally in a forensic evidence format L01, LX01 or a Zip file or a directory tree structure replicating the respective storage area.

Using the File-to-File functionality the process to harvest the information is a simple step by step operation that even non-technical users can perform. With the growth of offsite storage being used by most users, this feature is again a must have solution to ensure a full investigative capability can be exploited leaving no data behind or unavailable for examination.

OPTIONAL FUNCTIONALITY AND ENHANCEMENTS

The Falcon®-NEO2 encompasses an array of options compared to other products available in the marketplace and although the main out of the box unit itself is more than adequate for most cases, there are often occasions when unique scenarios and drive types play an integral part of a digital investigation. Logicube's foresight and years of extensive experience in the digital extraction and preservation field have designed a wide range of additional solutions that complement and enhance the functionality of the Falcon®-NEO2. If these are not purchased at the time they can always be added as and when required. The optional functionality and equipment to compliment the Falcon®-NEO2, as listed below, were also vigorously tested as outline throughout the various sections of this assessment:

Mobile Device Capture

The mobile device capture option is an annual renewable software subscription solution. It currently supports iOS and Android v 4.0 and above devices. An iTunes backup is performed for unlocked iOS devices. A physical extraction is performed for rooted Android devices and a logical for non-rooted. The Falcon®-NEO2 does not have the ability to decrypt a device and the user's password must be known. However, this is also the case with most mobile forensic acquisition solutions. Some do have the ability to decrypt the log on credentials but often at a substantial additional cost to an already expensive solution.

There are two particularly important advantages with the mobile device capture:

- It is extremely easy to use with a simple interface that replicates the same sequence of options used when acquiring physical drives. Even non-technical operators can safely and quickly perform an extraction of an iOS or Android device using the Falcon®-NEO2.

- It is exceptionally more cost effective than other available solutions in the marketplace.

Mobile device capture extracts the key elements typically required during most digital investigations, such as messages, call logs, website history, contacts, wi-fi settings, photographs, and videos etc. Obviously much more data can be harvested if a physical extraction is performed on an Android device.

This is an exceptionally good additional option and a must have feature, particularly for small organizations or individuals with no mobile forensic capability and minimal budgets. The use of mobile device capture will extend their investigative skillset and ability when budgets do not allow the more expensive solutions. Although limited to iOS and Android devices, from a practical perspective these types of mobile phones account for the

majority that are typically encountered in a criminal enquiry or used in a corporate environment. Therefore, having this option available in a single piece of equipment, together with the variety of data capture options the Falcon®-NEO2 possesses is both an efficient and extremely cost-effective way to include a mobile device capture capability to any organization.

PCIe Adapter Kit

The PCIe adapter kit is another must-have option as drives become more compact across the variety of systems available. The PCIe adapter kit includes cards for the M.2 PCIe, M.2 SATA, M.2 NVMe, mSATA, PCIe and mini-PCIe drives. These are easy to use and attached to the PCIe slots on the Falcon®-NEO.

2.5" / 3.5" IDE, 1.8" to SATA, 1.8" ZIF adaptors, flash media reader

These adaptors and flash media reader are useful additions when encountering devices of this type. Often, it is the absence of the simplest of things such as the availability of a flash media reader that halts the investigation in its tracks.

USB 3.2 to SATA converter and power supply cable

As stated earlier, the 4-port USB 3.2 to SATA adapter is an extremely useful addition and allows much more versatility to the Falcon®-NEO2 adding additional source or destination drives to the USB ports for increased processing and efficiency. This is a must add feature for large investigations, e-Discovery type acquisition involving many physical drives to be preserved in a limited amount time. The additional power slot at the back of the unit is used to power the adapters and ultimately power the additional drives.

Thunderbolt 3/USB-C IO Card

One of the distinguishing features of the Falcon®-NEO2 (a continuation from the Falcon®-NEO) is its scalability and being future-proof. The Falcon®-NEO2 has the capability to integrate new technologies and interfaces that may appear through the deployment of IO cards, the first and current instance of which is the TBT card. The Falcon®-NEO2 is the only forensic imager in its class (high-end, portable, and field-ready) to offer support for Thunderbolt.

There are currently three available Thunderbolt 3/UCB-C IO card slots on the Falcon®-NEO2, two on the source side, which are write protected ports and one on the destination side, which is a read \ write port. These are excellent when encountering removable drives such as the Samsung and SanDisk portable external drives, which were used during the test as both a source and repository drive. The speed in processing were again consistent with Logicube's claims.

The installation of the IO card is easy and straight forward and does not require any significant technical expertise. Logicube provides a screwdriver with picture step by step guidelines to install it.

It is highly recommended that at least one Thunderbolt 3/UCB-C IO card is added to each side of the Falcon®-NEO2 to take advantage of the enhanced functionality, capability, and flexibility.

Fibre Channel / FireWire / SCSI Modules – General

The Fibre Channel, FireWire and SCSI modules can all be connected to either the source, write protected or destination read / write PCIe ports. They are exceptionally durable add on modules and the cable ribbon, which is permanently connected and held firmly in place by a unique storage mount can be quickly and simply attached to the Falcon®-NEO2 desired PCIe port.

All the features and functionality of the standard Falcon®-NEO2 are also available for the three optional modules, such as evidence file formats, drive to drive, encryption, task macro and concurrent image with verification processing etc. The speed, performance and stability were again consistent with the general functionality of the Falcon®-NEO2 and Logicube claims.

Each solution is delivered in a standard heavy duty cardboard box,13" x 9" x 4" and all three together wight approximately 9 lbs.

Fibre Channel Module

The Fibre Channel module is a hardware solution that attaches to the Falcon®-NEO2 and supports drives using a 40-pin SCA-2 connector and enclosures with a small form-factor pluggable (SFP) connector. The out of the box solution allows the creation of evidence files from or to a fibre channel drive and or enclosures. It can also capture data from a one 40-pin fibre channel drive to one SFP drive or vice versa. If the Fibre Channel module is added a must have is the optional kit (Part# F-DP-FC-KIT) which allows the cloning of a 40-pin drive to another 40-pin drive.

FireWire Module

The FireWire module is extremely useful and not only supports FireWire enclosures but also when imaging a Mac system when it is in target disk mode. It comes standard with a 6-pin FireWire 400 6ft cable and a FireWire 800 to 400 converter connector. A Mac system with a Thunderbolt port can also be connected to the module using any off-the-shelf Thunderbolt to FireWire adapter. The FireWire module was vigorously tested on several Mac systems that were booted in target disk mode and once the connection was authenticated the simple Falcon®-NEO2 processes were successfully applied even by the less experienced forensic examiners and investigators.

SCSI Module

The SCSI module provides a 68-pin SCSI port as standard and 50 and/or 80 pin adapters available if required. The adapters are a must have if adding the SCSI option to complement the Falcon®-NEO2. The SCSI module can be added to the PCIe port as either a source, write protected or a destination, read \ write device. Some forensic hardware manufacturers have ended the life for SCSI support for their digital forensic solutions, but surprisingly these types of drives are still around and often appearing in both criminal and civil investigations.

CONCLUSION

For many years Logicube forensic imaging solutions have been a leading forensic component used around the world by leading government, law enforcement, military and corporate organizations. The enhancements now available within the Falcon®-NEO2 represents a critical inflection point in the development of forensic imagers. This is evidenced with the level and amount of technology packed into the Falcon®-NEO2, and particularly the speed barriers that it now surpasses. This exceptional milestone for forensic examiners provides unprecedented efficiency during the digital preservation process. Logicube has once again demonstrated their global reputation as a leader and innovative in the field of secure digital data preservation whilst maintaining continuity and integrity of the data harvested. While nearly all the features of the preceding Falcon®-NEO are carried over to the new Falcon®-NEO2, they were nevertheless vigorously tested again as part of this assessment. With the introduction of new technologies (SAS-3 and USB 3.2 gen-2) and attainment of imaging speeds never before seen in a field imager, a review and further vigorous testing was performed.

In accordance with best practice the following is a review of the manufacturer's statements of facts and claims together with an independent physical hands-on assessment:

Relevance and Necessity

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 once again exceeded all expectations with the speed enhancements and new technologies available for the Falcon®-NEO2. They have clearly maintained pace with technology, listen to their user's requirements and always look forward to new initiatives and developments. For the first time investigators have the ability and benefit of speeds of over 100 GB/m computer media imaging, network traffic and cloud collections together with a mobile forensic capability using the same hardware.

The increased enhancements in functionality and capability of the Falcon®-NEO2 with a variety of devices supported, encryption, mobile device capture, network traffic and cloud collections, with remote operating, once again demonstrates that Logicube remains the unquestioned global leader in the field of data imaging and ahead of its competitors with the all-encompassing new features and options available in the Falcon®-NEO2.

Authentication, Reliability and Accuracy

The touch-screen interface and variety of options available continue to give the Falcon®-NEO2 a very professional and confident factor, leading the way in digital forensic imaging. Statements by any manufacturer professing speeds in processing are always ambiguous but in reality, the Falcon®-NEO2's imaging speeds against its main competitors were superior and exceeded those of all other field acquisition solutions available in the market. The speeds in acquisition of up to 115GB per minute and wiping at up to 115GB per minute as validated is simply phenomenal. The concurrent verification enhances the efficiency of data acquisitions and speed in which they can be performed to ensure the continuity and integrity of data collected. The speeds achieved both in a laboratory and field environment, not only meet the requirements when handling high volume sophisticate business systems but also the extremely large capacities of standard home computers now being encountered even in small digital investigations.

The ability to automate and selectively harvest information is critical for investigations involving privacy or e-Discovery requirements. The increased capability of date range, file type and keyword filtering further increase the efficiency and quality of data collected. Many of the features of the Falcon®-NEO2 are considered standard and are expected from such a product but the combination of the macro-task, network, cloud, and mobile device capture functionality allows greater diversity in the use of such a tool and simplifies the process for non-technical first responders.

As a user of other competitive products that are similar, Logicube have surpassed all expectations with the new technologies (SAS-3, USB 3.2 gen-2) and speeds now available for the Falcon®-NEO2. This is particularly evidenced when considering not just the unprecedented speed in which it processes but the additional advanced features, functionality and support it provides with mobile device capture, cloud storage acquisition, fibre channel, firewire, SCSI and thunderbolt options.

In comparison to other digital forensic imaging solutions in the marketplace today, from a hands-on comparison and vigorously 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 Falcon®-NEO2. The many features and functionalities of the Falcon®-NEO2 continue to exceed those of its competitors and as such the consistent advancements in functionality, processing speed and reliability is not only superior but critical for today's highly developing digital investigative and IT management world.

Complies with Global Standards and Guidelines

The simple and automated functionality, which includes remote access as required, 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. This is a must have tool in any forensic or IT security/management department, which complies with global standards and guidelines.

The Falcon®-NEO2 produces evidence files and data that are compatible with all major computer, mobile forensic, IT security and e-Discovery analysis and processing tools. The time saved with this all-in-one solution with its simple but secure data analysis and harvesting is a financial investment and will save many person hours in the long term.

Final Comments

When Logicube's last forensic imager **(**Falcon®-NEO) was released in 2018 and the massive enhancements and capabilities that it introduced to the digital forensic market, it was difficult to imagine that any new or competing products could reach, let alone surpass, its specification in the next few following years. An assessment done by me in 2021 on the Falcon®-NEO found it to be the Best-In-Class among all digital forensic imagers available to forensic examiners. While the first part of that prediction has indeed materialized and other digital forensic imagers are still a generation behind the preceding Falcon®-NEO's features, Logicube themselves have been the ones to surpass the standards set by it by the introduction and release of the Falcon®-NEO2. While maintaining the same size, footprint, GUI, and look and feel as their last product, the Falcon®-NEO2 packs such a collection of new technologies, additional ports, accessories, and unprecedented imaging speeds into its box as to make it a groundbreaking powerhouse available to discerning forensic examiners. Falcon®-NEO2 is the first field forensic imager to surpass the 100 GB/Min E01 imaging speeds. The upgrade of the SAS source and destination ports of the product to SAS-3 (12 Gb/s) and its USB ports to USB 3.2 Gen-2 (10 Gb/s) and the inclusion of the Cloud Storage Acquisition capability as a standard feature, along with a multitude of options that enable the support for practically every drive technology, make Falcon®-NEO2 the most powerful and peerless field forensic imager, bar none. In their marketing literature, Logicube refer to the Falcon®-NEO2 as the "Best Ever" forensic imager made. While it is neither the purpose nor the purview of this assessment to validate that claim, it is indeed the finding of this assessment that no other digital forensic imager has ever reached the levels set by the Falcon®-NEO2 in terms of the breadth and multiplicity of its features, functions, capabilities, technologies, and certainly its imaging speeds.