	Competitive One on One Forensic Falcon®-NEO vs MediaClone SuperImager® Plus 8” T3		
Features	**MediaClone SuperImager® Plus 8” T3**	**Forensic Falcon®-NEO**	**Remarks**
Hardware			
Unit's Processor (CPU)	Intel i7-11700K	Embedded CPU	i7 vs Embedded: it is a big difference in performance, especial when there is a need for calculation power to calculate HASH, Encryption and Compression. Also, for running multiple session, the use of the i7 multi CORE is optimized for parallel session with very little speed degradation
Unit's Memory	32GB	unknown	
Unit's Internal Storage	1TB	unknown	
Unit's OS	Ubuntu/Win10 dual boot	Linux base	Dual OS bring the best of the 2 worlds. It allows the user to performs a fast imaging under Ubuntu, and than use the Win 10 for Forensic analysis and cellphone data extraction
Is it Open OS?	Open OS allows the user to install and use other application, which make the device very useful and versatile. Application like Encase, Nuix, Axiom, Cellebrite and more (Both Ubuntu and Win10 are open OS)	No	
Dimensions	10.6” x 7.7” x 3.15”	10. W x 6.75. D x 3.25. H (254 mm x 171 mm x 83 mm)	
Weight	5.5 lb.	3.0 lb. (1.36 kg, 48 oz.)	
Color touchscreen display	8" resistive	7" capacitive, angled	
Web-based user interface (web browser)	No	Yes	

Remote access	Using VNC protocol, the user can operate the unit from a cellphone	Using a web browser and Command Line Interface (CLI). Users can view the Falcon-NEO GUI on their PC, iPad, tablet, or smartphone (scaled to fit those devices).	
Speed	Forensic Imaging 32 GB/min with SATA SSD, 24 GB/min with E01, Image+ HASH NVMe 137GB/min, Image no HASH NVMe 187GB/min, read back from NVMe 202GB/min	Logicube is claiming that speed is Surpassing 50 GB/min (SSDs, e01) !	
Ports			
Total built-in write-protected source ports	4 (2 SAS/SATA, 2 USB3.0/3.1), but any target port can be re assigned to be source	6 (2 SAS/SATA, 1 USB 3.0, 1 PCIe 4-lane slot, 2 optional I/O ports). USB can be converted to SATA with a USB to SATA adapter.	
Total number of connected source drives that can be imaged from concurrently	4	5	
Total built-in destination ports	11 (2 SAS/SATA, 7 USB3.0/3.1, one Thunderbolt 3.0/USB3.1, one eSATA)	9 (2 SAS/SATA, 2 SATA, 3 USB 3.0, 1 PCIe 4-lane, 1 optional I/O card port). USB can be converted to SATA with a USB to SATA adapter.	
Total number of connected destination drives that can be imaged to concurrently	16 (2 SAS/SATA, 7 USB3.0/3.1, one Thunderbolt 3.0/USB3.1, one eSATA, one NVMe, 4 SAS on the expansion box)	9	
I/O card ports	Instead of optional I/O card, the user can use the supplied Thunderbolt 3.0 to PCIe Expansion Box to supports other storage interfaces.	Includes 2 source and 1 destination I/O card ports to support new interface technologies as they arrive on the market. A Thunderbolt 3/USB-C I/O card is available.	
Ethernet port	1 Gigabit Ethernet built-in and a 10GbE with use of TB3.0 to 10GbE Optional Adapter	Two 10 GbE ports. Image to a 10 GbE NAS at speeds of 30 GB/min.	

Thunderbolt 3.0 port	it is 40Gigabit/s fast port, with no degradation in performances. The port can be used for 10GbE network, Mac Acquisition, Connect Thunderbolt 3.0 to PCIE Expansion Box to support other interfaces	Thunderbolt is an option on the NEO	
Drive Interfaces supported	SATA/SAS/e-SATA/USB/IDE/1394/NVMe/Thunderbolt 3.0 built-in	SATA/SAS/USB/PCIe built-in	
	Include adapters: MSATA, MicroSATA, M.2 SATA, PATA/IDE, Flash media, NVMe M.2 ,1394A/B.	mSATA, Micro SATA, eSATA – Adapters included	
	The included Thunderbolt 3.0 to PCIe Expansion box can be used for other interfaces (SCSI, FC)	Thunderbolt 3.0 /USB-C – Optional I/O card available	
	Mini PCIE adapter is optional	M.2 NVMe/SATA/AHCI and mini-PCIe cards require an optional PCIe adapter kit	
		PATA/IDE & Flash media – Optional adapters available	
		Optional modules available for: FireWire/SCSI/Fiber Channel	
Application Features			
Image+Verify concurrently	Image with HASH and Read back Verify can run up to 132GB/min with NVMe SSD on used on the target port. If the user capture data from SATA drives (Suspect) into NVMe target SSD (Evidence), since the NVMe is fast on reading, that could make the total time of the imaging + HASH + verify much shorter	Takes advantage of fast destination drives. The duration of total image+verify processing time may be reduced by up to half.	
Multi-task. Image from multiple sources to multiple destinations. Image to one drive, wipe another concurrently	Taking the advantage of the CPU multi cores, to run simultaneously operation session with no restriction on the number of sessions!	Yes – Image simultaneously from multiple sources to multiple destinations, including a network repository. Image to one location while hashing and/or wiping a second drive. Perform up to 5 tasks concurrently. Little or no speed degradation when imaging from 2 sources to 2 destinations simultaneously.	Neo will start seeing some speed degradation when the number of running sessions will increase because of the use of embedded CPU

Targeted Imaging. Create a logical image, filter, use keyword search	Selective Imaging (Targeted Imaging) of files, folders, and partitions with file extensions filters. Keyword Search available on the Suspect drive before the capture, or during the capture.	Create a logical image by using pre-set filters, custom filters, signature filters, and keyword search. Format out to L01, LX01, ZIP, or directory tree.	
Capture Path Selection	Add folders to the destination repository and then select and image to the named folder.	Yes	
Partition Imaging	Ability to select a specific partition on the Suspect drive and save it to target drive in E01/Ex01, DD format (as long as the Suspect drive is mountable)	Select and create a logical image of specific partitions on the source drive to e01, ex01, dd, or dmg image format.	
Parallel Imaging - Image to multiple destinations with different image formats	Image to multiple destinations using a different format for each destination (native, dd, e01, ex01).	Image to multiple destinations using a different format for each destination (native, dd, e01, ex01,dmg, file).	
APFS (Apple® File System) Support	No	Supports logical imaging using File to File mode from source drives formatted APFS. Requires use of our Advanced set-up. The Falcon-NEO can also view and browse APFS files using our File Browser feature.	
Drive spanning	supported drive spanning of the source drive into many destination drives. But it is also include a parallel spanning, when the source drive is faster (read) than the target (write). The imaging spanning done suing DD format and there is not need to use any reconstruction of the image which save steps and time	Yes	
Image to/from a network repository	Use CIFS and iSCSI protocols and by using the both 1 Gigabit Ethernet port or 10GbE port with the use of optional Thunderbolt to 10GbE adapter	Using CIFS or iSCSI protocols. Two 10 GbE ports are available.	
End of task notification	Play sound by the end of a session	Email and/or sound on success and/or error.	
Cloud Storage Capture	Access Microsoft OneDrive, Google Drive, and Dropbox, by subscription to Insync Ubuntu application.	Capture from Microsoft OneDrive, Google Drive, and Dropbox. Available as a subscription option.	

Mobile Device Capture	Yes – use a 3rd Party Cellphone data extraction software like Cellebrite install on the Win10 side. Or use The MediaClone application to capture data from Android cellphones	Capture SMS, MMS, photos, videos & more from iOS and Android devices. Available as a subscription option.	
Network Traffic Capture	No, but the user can install a third party application like WireShark	Capture network traffic, internet activity, and VoIP. Sniff data on a network and store captured packets on a drive connected to Falcon-NEO.	
Network “push” feature	The application support saving DD/E01/Ex01 or files into a network location with HASH verification	Push evidence files from destination drives connected to Falcon-NEO or from a Falcon-NEO repository to a network location. Performs a hash during the push process and verifies the file transfer to ensure data integrity.	
Image from a PC/Laptop without removing the drive	Remote capture is included. It include a bootable USB stick and a cross over network cables, connecting the laptop via RJ45 the T3 unit and preforming the capture with HASH verification. Speed of the capture depends on the laptop processor. Also, the suspect laptop can be connected to the same network, and the user can capture the image over the network. The kit includes RJ45 for USB adapter in case the laptop does not have RJ45 port.	Create a forensic bootable USB flash drive to image a source drive from a computer on the same network without booting the PC’s native OS. Supports Surface PRO 4 and above.	
Image from a Mac®	Image from a Mac by using 3 interfaces (Mac with 1394, Thunderbolt 2.0, Thunderbolt 3.0) with the use of the optional Thunderbolt Kit, and the Mac is set in a Target Disk Mode	Image from a Mac® with USB-C ports using Target Disk Mode (requires a USB-C to USB-A cable) or image a source drive from a Mac on the same network and use Logicube’s USB boot device. Supports MacBook Pro®.	

Secure drive preview/triage	Using the Ubuntu: Preview the drive contents using MediaClone Virtual Emulator, or preview files using Ubuntu files manger. Using the Win10: Use Encase, FTK, Forensic Explorer to preview the Suspect data	Preview drive contents directly on the Falcon-NEO. File browser feature provides logical access to source or destination drives. View the drive's partitions and contents. View text files, jpeg, PDF, XML, HTML files. View contents of dd, e01, ex01, dmg, L01 image files created by Falcon-NEO. Other methods to preview including using the file browser feature and Falcon-NEO's web browser on a PC or preview over a network via SMB or iSCSI. 3rd party analysis tools can be used with SMB or iSCSI methods.	
Image Restore	Restore a case that was previously captured using (e01, ex01, dd) to its original format.	Restore a case that was previously captured using Falcon-NEO (e01, ex01, dd, .dmg) to its original format.	
BitLocker, Opal, VeraCrypt, and TrueCrypt decryption Support	BitLocker, Opal for SED	Decrypt BitLocker, Opal, VeraCrypt, and TrueCrypt encrypted drives (requires decryption password) then image these decrypted source drives.	
Unlock & Image ATA Security Standard	Supports unlocking od drives if the user has the passcode to unlock. In some cases the application unlock the drive automatically.	Supports unlocking of drives that are locked with ATA Security Standard (requires password).	
Image from CD/DVD/Blu-ray	No	Use a USB optical drive connected to Falcon-NEO's USB port. Supports multi-session CD/DVDs.	
Encryption/Decryption	Encryption during the capture run using AES-256 ECB protocols. Decryption at destination location done by using the T3 unit or by using the MediaClone decrypt bootable utility	Supports XTS-AES 256 Encryption. Decrypt using Falcon-NEO or open-source, VeraCrypt, TrueCrypt, or OTFE decryption software.	CPU and memory play a big role in performances of this task
Image formats	Mirror (bit by bit), Linux-DD, E01/Ex01, VHD	Native, dd, .dmg, e01, ex01	

E01/Ex01 Compression	Use up to 16 Parallel Compression engines, allows the user to select how many compression engines and the level of compression to use. Optimizing of compression parameters is a trade of saving space vs imaging time	Yes	CPU and memory play a big role in performances of this task
Hash Algorithms	The user can select to run all the 3 HASH algorithms in the same imaging session	MD5, SHA1, SHA256. Dual Hash (MD5+SHA1). SHA1+SHA256 and MD5+SHA256 available with ex01.	NEO has limited capabilities in calculating HASH
Display, print, save logs	Output to PDF and XML formats and save onto the target (Evidence) drive.	Output to PDF, HTML, and XML formats.	
Export S.M.A.R.T. data	S.M.A.R.T. data logs for Source drives used in the Drive to File and Partition to File imaging tasks are automatically exported to the Destination drive.	Yes – S.M.A.R.T. data logs for Source drives used in the Drive to File and Partition to File imaging tasks are automatically exported to the Destination drive.	
Task Macro (set tasks to be performed sequentially)	Users can set specific tasks to be performed sequentially; first, wipe or format the destination drive then hash the source drive then image the source drive. All tasks within the Macro will be performed automatically. No limitation on the numbers of macros and tasks	Users can set specific tasks to be performed sequentially; first, wipe or format the destination drive then hash the source drive then image the source drive. All tasks within the Macro will be performed automatically. Up to 5 concurrent tasks with up to 9 operations.	Here is where Neo Limitation come to play: Up to 5 concurrent tasks with up to 9 operations.
Password-protected user-profiles	Set password-protected user-profiles and save configurations/settings	Set password-protected user-profiles and save configurations/settings, e.g. “image S1 to D1” for frequently used tasks. Can set passwords for local/remote HTTP, Config lock, log file deletion.	
Image and/or wipe HPA/DCO	HPA/DCO are special area on the drive and it is important to open those area when the user run a forensic capture	Yes	

Error Handling/Error Granularity	3 options: Skip bad sector, skip a block for faster imaging, abort session when encounter a bad sector	Provides error granularity settings to improve error handling. Changing the granularity allows more sectors to be skipped. There are 3 options (512 Bytes, 4096 Bytes, 64 KiB). Reverse Read can be set.	
Resume Function	No	Can manually or automatically resume aborted imaging tasks or if power to the Falcon-NEO has been interrupted.	
Wipe feature	DoD (ECE, E), Security Erase, Enhanced Security Erase, Sanitize Erase, NVMe, and Custom User erase protocols.	Secure Erase and/or single/custom pass/DoD.	
	Custom User Erase is customizable to have many erase passes and has include one pass of verify conforming with NIST 800-88 SP1 standards. No restriction on the total numbers of passes	Secure Erase SATA/SAS/IDE/NVMe SSDs.	NEO has limitation on the number of erase passes
	Erase SSDs at speeds up to 31 GB/min, PCIe up to 137 GB/min.	Wipe SSDs at speeds up to 30 GB/min, PCIe up to 72 GB/min.	
Blank disk check	Yes	Yes	
Stealth Mode (turn off display for privacy)	No	Yes	
Firmware/Software updates	Easy software updates through any of the Unit's USB ports.	Free software and firmware updates. Update via a network connection or using a USB thumb drive.	
Bottom line	T3 unit has a greater performance, and allows the user to use the unit for many tasks, like preforming Forensic analysis on the unit while the captured data is there and complete a Forensic investigation in the field. In addition it can be use to capture cellphone, run a Triage and many other tasks and not just limited to imaging	Neo is more compact, but very limited in performance because of the hardware. Also it has limited in use for just an imager	
Main Advantage of the T3 unit	Flexibility of the hardware to adapt to a new devices and interfaces		

	Bandwidth and performance: Can not be compared the Neo or Falcon tht use embedded CPU to the T3 units with i7 11 generation CPU when running multiple capture with HASH!		
	The TB3.0 Expansion Box add more flexablity to the user and it can be use for may things, Like FC/SCSI, 4 more SAS ports, NVMe and more		
	The T3 unit also include Virtual Emulator - Great tool for preview suspect drive at its' own envriopmnet before imaging (Great for a quick Triage)		
	T3 unit configured with dual OS, both are opened. On the Windows 10 side the user can install Cellphone Data Extraction applicaion like Cellebrite, or a Forensic Anyalis applicaion like EnCase/Axiom/Nuix. Since the CPU is a desktop CPU, the user can run and complete a full analysis in the field!		