FORENSIC EXPLORER

FEX Imager

User Guide

Published: 14-Jul-20 at 15:37:58

GetData

1.1 CONTENTS

1. INTRODUCTION

FEX Imager is a software program by GetData Forensics (getdataforensics.com) that will acquire a bit-level forensic image with full MD5, SHA1, SHA256 hash authentication. FEX Imager can acquire a physical drive, logical drive, folders and files, remote devices (using servlet), or re-acquire a forensic image. It can write forensic image files in:

- DD/RAW (Linux "Disk Dump")
- E01
- L01

A forensic image is a key element in the field of computer forensics. It is an exact copy of data that is used to gather and preserve evidence in a manner suitable for presentation in a court of law. A forensic image includes all data, including parts not normally displayed by the operating system, including deleted files, file slack, and unallocated clusters.

1.1 HOST PROTECTED AREA (HPA) AND DEVICE CONFIGURATION OVERLAY (DCO)

The HPA and DCO are two areas of a hard drive that are not normally visible to an operating system or an end user. The HPA is most used by boot and diagnostic utilities. For example, some computer manufacturer's use the area to contain a preloaded OS for install and recovery purposes. The DCO "allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. An example of this would be using DCO to make an 80 Gigabyte HDD appear as a 60 Gigabyte HDD to both the OS and the BIOS" (1)

Whilst the HPA and DCO are hidden, it is technically possible for a user to access these areas and store/hide data. FEX Imager does not currently support the acquisition of HPA or DCO areas.

2. DOWNLOAD

FEX Imager is available for **download from:** https://getdataforensics.com/product/fex-imager. It is downloaded as a setup executable.

3. SYSTEM REQUIREMENTS

The following minimum system specifications are recommended:

- Windows 7 or above.
- 64-bit.

- I7 processor.
- 8 GB RAM.
- Launch as local administrator user.

4. INSTALLATION

To **install FEX Imager**:

1. Launch the downloaded setup file and follow the on-screen instructions.
2. FEX Imager is a 64-bit application. By default, FEX Imager will be installed to:

   C:\Program Files\GetData\FEX Imager\FEX Imager.exe

FEX Imager is a **free program**. It does not require activation.

5. RUNNING FEX IMAGER

FEX Imager should be run as **local administrator user** to ensure that sufficient access rights are available for access to devices.

5.1 WRITE BLOCKING

An accepted principal of computer forensics is that, wherever possible, source data in an investigation should not be altered by the investigator.

If physical media such as a hard drive, USB drive, camera card etc. is a potential source of evidence, it is recommended that when the storage media is connected to a forensics workstation it is done so using a forensic write block device (write blocker).

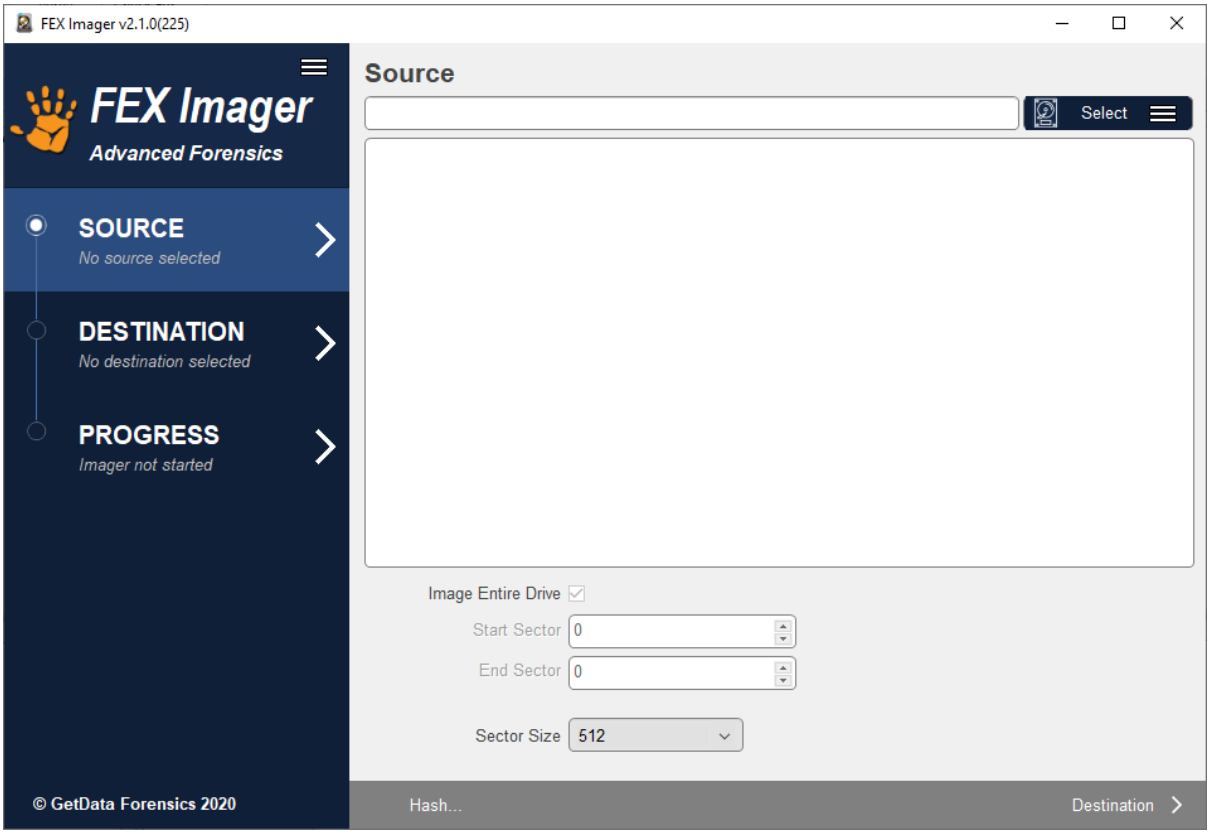
A write blocker is usually a physical hardware device which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined device. It permits read-only access to target devices without compromising the integrity of the data. There are a wide variety of forensic write blocking devices commercially available. Investigators are encouraged to become familiar with their selected device, its capabilities, and its limitations.

5.2 SOURCE WINDOW

FEX Imager is launched by running **FEX Imager.exe** in the program installation folder, or from the installed **desktop icon**.

When **FEX Imager** is run, the investigator is presented with the **Source** window:

Figure 1: FEX Imager Source

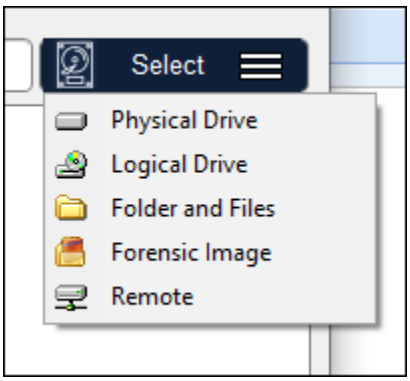


The source refers to the data to be acquired. The source can be:

- A physical drive (i.e. a physical hard disk).
- A logical drive (i.e. a partition such as C:\ or D:\).
- A folder or files located on a partition.
- An existing Forensic Image (i.e. an E01 or DD image file).
- A remoted drive accessed using the Forensic Explorer servlet.

To select the source, click on the **Select** button and chose the required option from the drop-down menu:

Figure 2: Source Window > Select



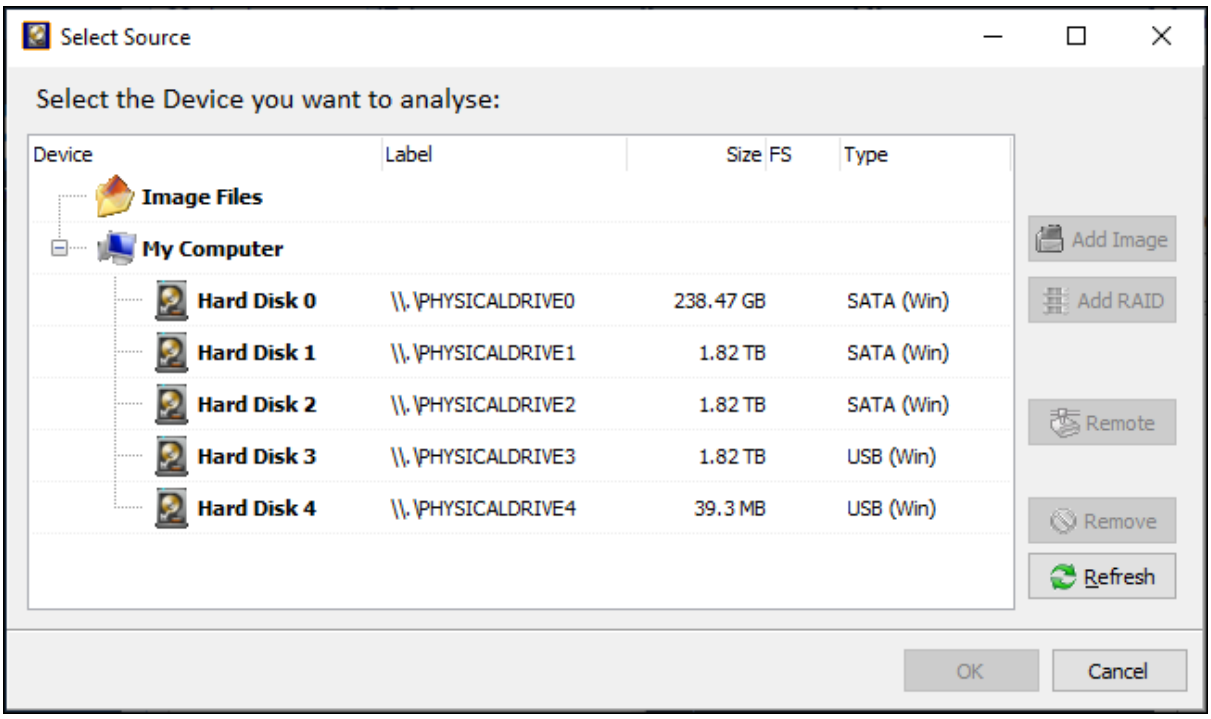
5.2.1 PHYSICAL AND LOGICAL DRIVES

In most situations, pending compliance with any overriding case specific legal requirements, an investigator will forensically image a physical device. Imaging the physical device gives access to the content of the entire media, for example, the space between partitions. Carrier, 2005, observes:

> *"The rule of thumb is to acquire data at the lowest layer that we think there will be evidence. For most cases, an investigator will acquire every sector of a disk".* (1 p. 48)

NOTE: If physical drives are not displayed in this window it is usually because FEX Imager was **not launched as local administrator user** and it does not have sufficient privileges to access the physical drives. Re-launch FEX Imager by right-clicking on the desktop icon and selecting **Run as administrator** from the drop-down menu.

Figure 3: FEX Imager - selecting the source device



The device selection window includes the following information:

Label: Physical drives are listed with their Windows device number. Numbering starts at 0. Logical drives display the drive label (if no label is present then "{no label}" is used). Image files show the path to the image.

Size: The size column contains the size of the physical or logical device, or the size of the image file. (Note that the reported size of a drive is usually smaller than the size printed on the drive label. This is because manufactures report the size in a decimal number of bytes while the Operating System reports the size in 1,024 chunks for each KB).

FS: The File System on the drive, e.g. FAT, NTFS, HFS, APFS.

Type: Describes the way in which the drive is connected to the computer. An image file will show the type of image (e.g. EnCase® or RAW).

5.2.2 ADDING A REMOTE DEVICE

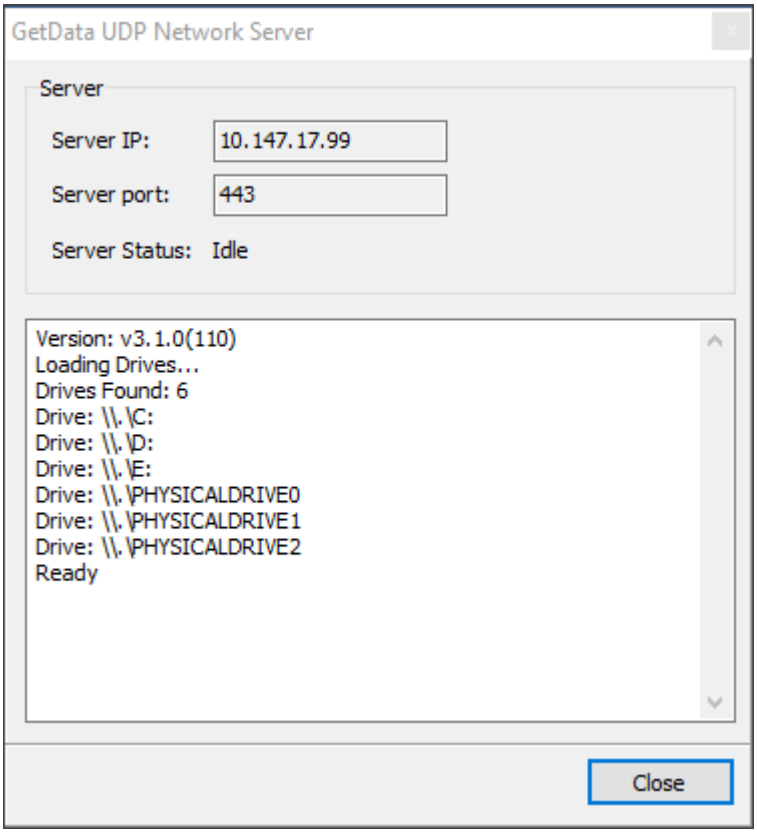
FEX Imager has the capability to examine remote devices across a network using the UDP protocol (User Datagram Protocol is one of the core members of the Internet Protocol Suite, see https://en.wikipedia.org/wiki/User_Datagram_Protocol).

DEPLOY THE GETDATA UDP NETWORK SERVER AS STAND-ALONE

To examine a network device, it is necessary to deploy and run the **GetData UDP Network Server** on the remote computer. It is found in the FEX Imager installation folder, **GetDataNetworkServer.exe**.

When the GetData UDP Network Server is deployed, and run, the following screen appears:

Figure 4: GetData UDP Network Server



Server IP: The IP address of the computer on which the Network Server is running. **IMPORTANT**: When troubleshooting, double check the IP address using CMD line "IPCONFIG" command to ensure the correct machine address.

Server port: The communication port.

Server Status: The server enters "waiting" mode for the connection from Forensic Explorer.

Note that it may be necessary to configure firewall settings on the local and remote computer to enable remote access to the GetData UDP Network Server.

NETWORK SERVER COMMAND LINE OPTIONS

The **GetData UDP Network Server** can be deployed from the CMD line on the remote computer with the following switches:

- /Q Quite Mode (No GUI);
- /P:XXXX Specified port number.

IMPORTANT: When deployed in **Quite Mode:**

- The **GetData UDP Network Server** will appear as a running process in the Windows Task Manager. The name of the process is the name of the executable (i.e. rename "GetData UDP Network Server" as needed).
- The **GetData UDP Network Server** can only be terminated by ending the process in the Windows Task Manager.

DEPLOY THE GETDATA UDP NETWORK SERVER AS A WINDOWS SERVICE

The GetDataNetworkServer can be deployed as a **Windows Service**.

To **install as a service,** use the following command line switch:

- GetDataNetworkServer /install /silent

To **uninstall the service,** use the following switch:

- GetDataNetworkServer /uninstall /silent

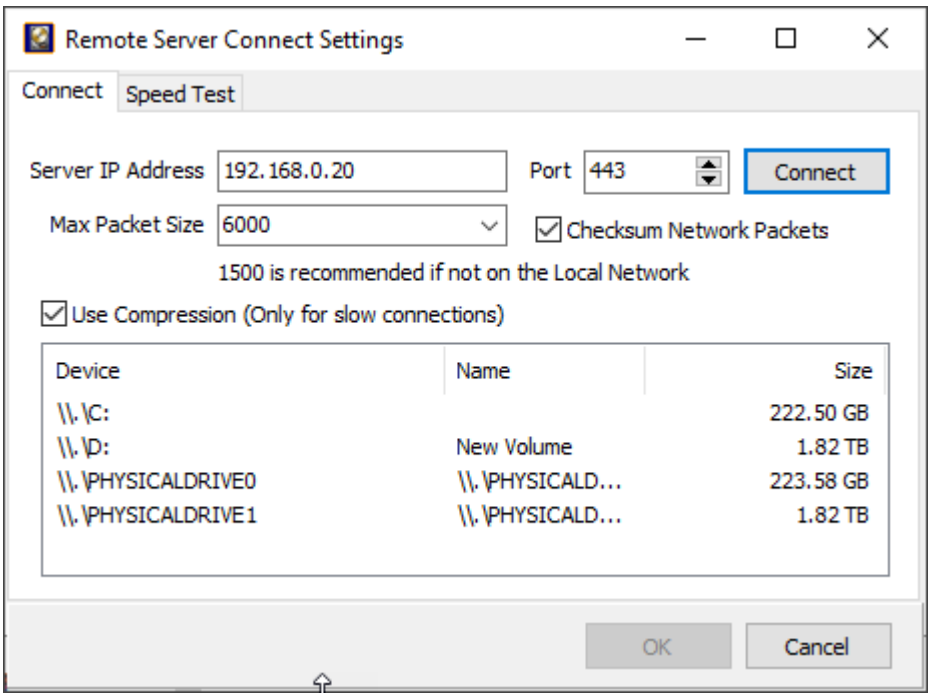
If a non-default port is required (i.e. a port other than 443) the following key must be added to the registry to specify the port number:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GDStreamService\UDPPort(DWORD) = 443

CONNECTING TO THE GETDATA UDP NETWORK SERVER

To connect to the GetData UDP Network Server, run Forensic Imager and in the Source window click on Select > **Remote**:

Figure 5: FEX Imager > Source > Remote > Remote Server Connect Settings



Server IP Address: Enter the IP address of the remote computer as displayed in the **Server IP** field of the **GetData UDP Network Server**.

Max Packet Size: Sets the maximum data packet size to be passed via UDP. On local reliable networks the setting can be higher, which can make the connection more efficient. If not a local network, a maximum packet size of 1500 is recommended (Where possible, test to determine the best settings).

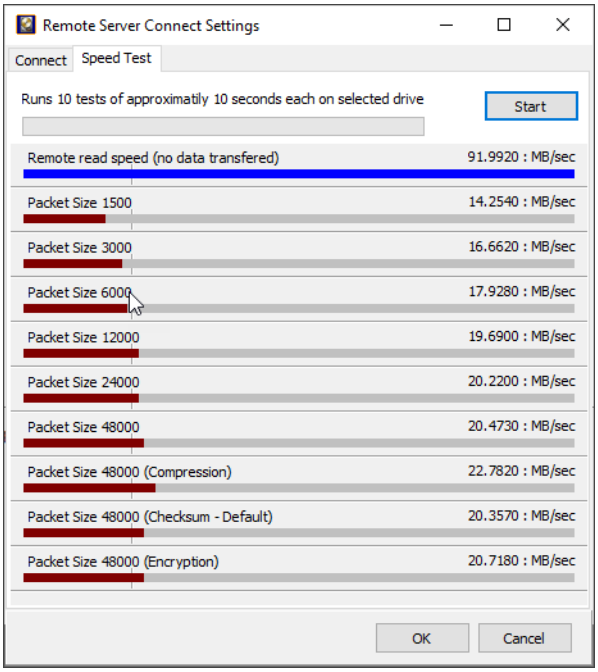
Checksum Network Packets: The checksum field is used for error-checking of the UDP header and data. Whilst it adds an overhead, it is recommended that this setting be applied.

Port: Ensure the Port number uses the same port as the GetData UDP Network Server (default is port 443).

Connect: The connect button activates the connection to the IP Address and Port and lists the available physical and logical devices on the remote computer.

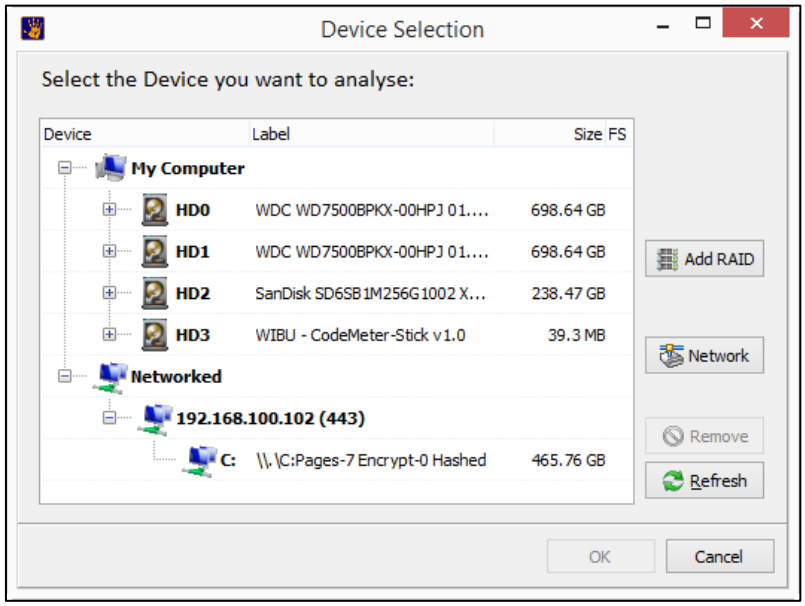
Speed Test: The Speed Test tab test the network connection speed to a specific device. In the **Connect** tab, select the required device, and then change to the **Speed Test** tab. Click **Start** to start the test.

Figure 6: Speed test remote device connection



With the required device selected in the **Connect** tab, click the OK button to connect to the remote device. The selected device should now appear under the **Networked** section of the Device Selection window, as show in Figure 7 below:

Figure 7: Device Selection window showing a UDP connected network device

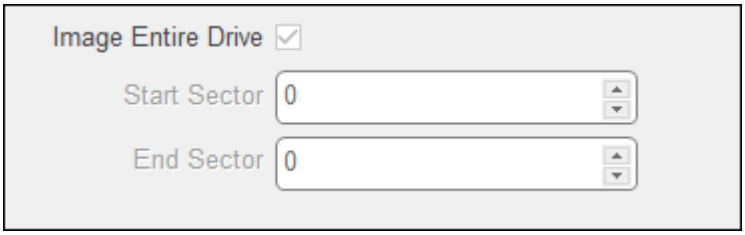


Select the required remote device and click **OK**.

5.2.3 SELECTED SECTORS

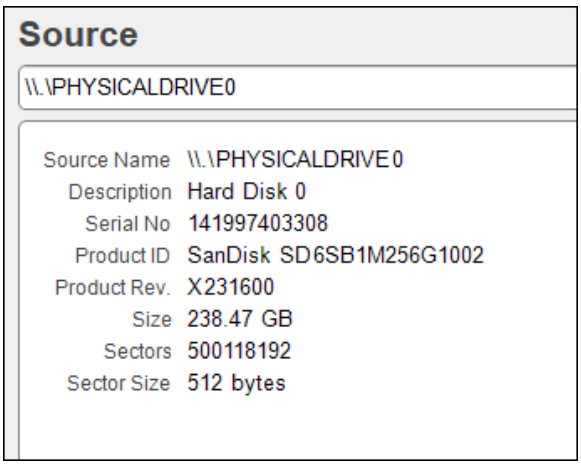
In specific circumstances, an investigator may need to acquire a range of sectors from the device. In this case, start and end sector information in entered in the sector range fields at the bottom of the source selection window.

Figure 8: Select FEX Imager start and end sectors



When a source device is select the source selection window will populate with the device information:

Figure 9: FEX Image source drive information



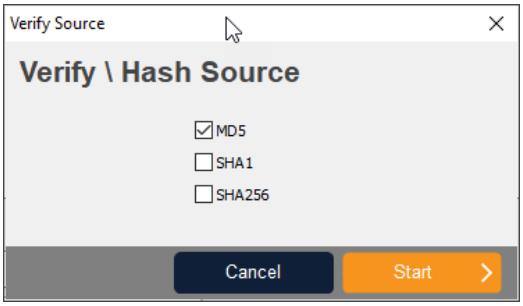
5.2.4 HASH OR ACQUIRE

Once a source is selected, two options become available at the bottom of the **Source** window:

HASH

Hash is selected when the users wishes only to calculate a hash for the device (for example, to verify the hash of an existing forensic image file).

Figure 10: Verify Source



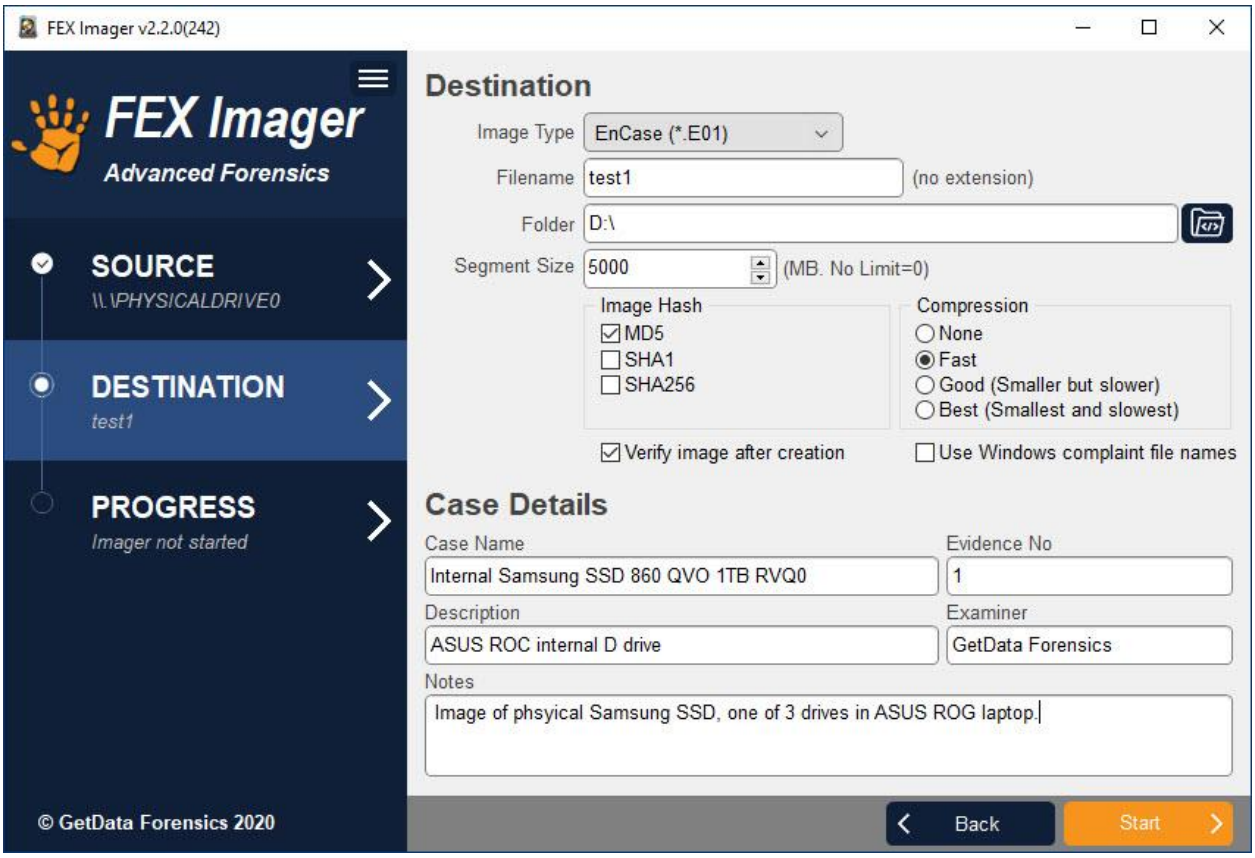
DESTINATION

The **Destination** button is selected to acquire a forensic image. It is described in more detail below.

5.3 DESTINATION WINDOW

The image destination screen, shown in Figure 11 below, is where the parameters for the image file are set, including type, compression, name, location etc.

Figure 11: Setting destination options



5.3.1 IMAGE TYPE

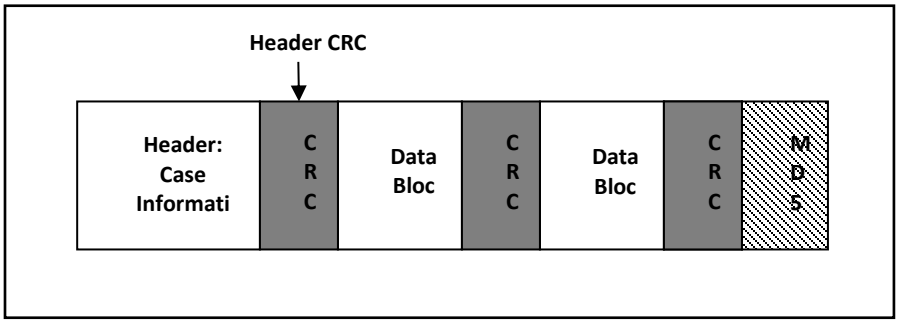
The investigator has the choice of creating the forensic image in one of the following forensic file formats:

DD / RAW

The DD / RAW format originates from the UNIX command line environment. A DD /RAW image is created from blocks of data read from the input source and written directly into the image file. The simplicity of a DD image makes it possible to compare the imaged data to the source, but the format lacks some of the features found in more modern formats, including error correction and compression.

ENCASE®.E01

The EnCase® E01 evidence file format was created by Guidance Software Inc. It is widely accepted in the forensic community as the image file standard. Further information is available at www.guidancesoftware.com. The structure of the EnCase®.E01 format allows for case and validation information (CRC and MD5) to be stored within the image file. The structure of the EnCase® file format is shown below:



5.3.2 FILENAME AND FOLDER

The **Filename** and **Folder** fields set the destination path and file name for the image file. The output file name is the name of the forensic image file that will be written to the investigator's forensic workstation. Click on the folder icon to browse for the destination folder.

5.3.3 SEGMENT SIZE

Segment Size sets the segment size of the created forensic image file. Setting an image segment size is primarily used when the forensic image files will later be stored on fixed length media such as CD or DVD.

For the EnCase®.E01 image format, FEX Imager uses the EnCase® v6 standard and is not limited to a 2 GB segment size. However, if an investigator plans to use larger file segments, they should consider the limitations (RAM etc.) of the systems on which the image files will be processed.

5.3.4 IMAGE HASH

Select and calculate one or more hash values, **MD5, SHA1, SHA256,** for the imaged data. A hash value is a mathematical calculation that is used for identification, verification, and authentication of file data. A hash calculated by FEX Imager during the acquisition of a device (the "acquisition hash") enables the investigator, by recalculating the hash later (the "verification hash"), to confirm the authenticity of the image file, i.e. that the file has not changed. Any change to the acquired image will result in a change to the hash value.

Calculation of HASH values during the acquisition process requires CPU time and will increase the duration of an acquisition. However, it is recommended, in line with accepted best forensic practice, that an acquisition hash is always included when acquiring data of potential evidentiary value. It is also recommended that the investigator regularly recalculate the verification hash during the investigation to confirm the authenticity of the image.

FEX Imager has three independent hash calculation options, MD5, SHA1 and SHA256. The investigator should select the hash option/s which best suits:

MD5 (MESSAGE-DIGEST ALGORITHM 5)

MD5 is a widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). It is a 128-bit hash value that uniquely identifies a file or stream of data. It has been extensively used in computer forensics since the late 1990's.

In 1996 cryptanalytic research identified a weakness in the MD5 algorithm. In 2008 the United States Computer Emergency Readiness Team (USCERT) released vulnerability Note VU#836068 stating that the MD5 hash:

> *"…should be considered cryptographically broken and unsuitable for further use". (2).*

SHA1

In 1995 the Federal Information Processing Standards published the SHA1 hash specification which was adopted in favour of MD5 by some forensic tools. However, in February of 2005 it was announced that a theoretical weakness had been identified in SHA1, which suggests its use in this field may be short lived. *(3) (4)*

SHA-256

From 2011, SHA-256 is expected to become the new hash verification standard in computer forensics. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the National Security Agency (NSA), and published by the USA National Institute of Standards and Technology.

For more detailed information on hashing and how the strength of a hash value applies to the forensic investigator suggested reading includes: "The Hash Algorithm Dilemma–Hash Value Collisions", Lewis, 2009, Forensic Magazine. (5)

5.3.5 COMPRESSION

The EnCase®.E01 file format supports compression of the image file during the acquisition process. Compressing a forensic image file during the acquisition process takes longer, but the file size of the

forensic image on the investigator's workstation will be smaller. The amount of compression achieved will depend upon the data being imaged. For example, with already compressed data such as music or video, little additional compression will be achieved.

DD/RAW image formats do not support compression.

5.3.6 VERIFY IMAGE AFTER CREATION

During the acquisition of a device the **acquisition hash** (MD5 and/or SHA1 and/or SHA256 as per the investigator selection) is calculated as the data is read from the source disk. Once the acquisition is complete, the acquisition hash is reported in the event log in the format:

Acquisition [hash type] Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

For EnCase®.E01 files the MD5 acquisition hash is embedded within the header of the image file.

When the "Verify image after creation" box is selected, at the completion of writing the image file FEX Imager reads the file from the forensic workstation and recalculates the hash. The verification hash is reported in the event log in the format:

Verification [hash type] Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

After the verification process a comparison is made between the source and verification hash. An exact image of the source disk to the image file should result in a "Match":

[hash type] hashes: Match

Should the acquisition and verification hash not match, it is an indication that a problem has occurred, and the device should be re-acquired.

5.3.7 DETAILS

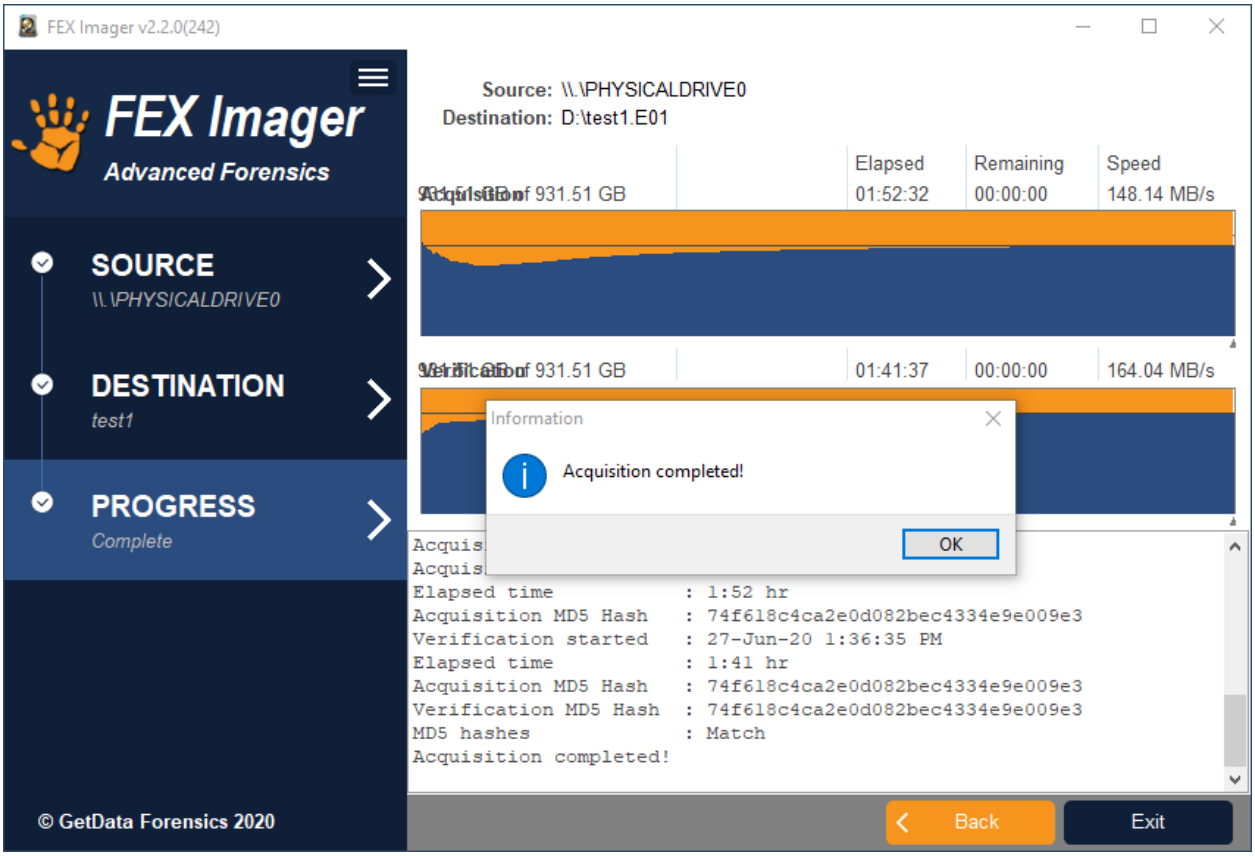
For EnCase®.E01 files, the value of the details field is written into the image file header.

A DD does not store this information as part of the image; however, it must still be entered so that the information can be included in the FEX Imager event log.

5.4 PROGRESS WINDOW

The progress screen displays source information (the drive being acquired) and destination information (location where the forensic image files is being written). Progress information, including elapsed time, time remaining and transfer speed is displayed. The progress window is shown in Figure 12 below:

Figure 12: FEX Imager Progress screen



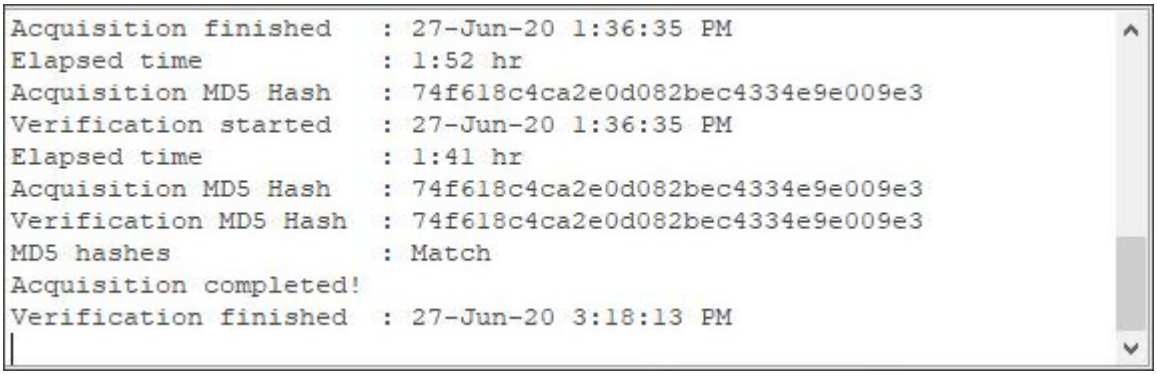
The bottom half of the progress window provides summary information about the acquisition process, including hash information.

If the **E01** image format was selected the **acquisition hash** is stored within the forensic image. If the **verify image after creation** option was selected in the FEX Imager Destination window, the progress window will include a comparison between the:

Acquisition [Hash Type] Hash: A hash of the data taken during the acquisition and stored in the E01.

Verification [Hash Type} Hash: A hash of the data in the forensic image file.

Figure 13: FEX Image Progress window hash information



Note that if the **DD** image format is selected a hash value is not stored within the DD image file.

5.4.1 LOG FILE

The event log for each acquisition is automatically saved to the same folder as the image file/s.

5.4.2 BAD SECTORS AND ERROR REPORTING

Disk errors can occur during the image process due to a problem with the entire drive or a problem isolated to specific sectors. If a bad sector is identified, FEX Imager writes 0's for the data that cannot be read and logs the location of bad sectors in the event log as they are found.

6. DEFINITIONS

.E01	A forensic file format used to create forensic image files of physical devices or partitions (see also .L01). Developed by Guidance Software (http://www.guidancesoftware.com/).
DD	DD (also referred to as RAW) is a disk image format that stems from the DD command on UNIX and Linux operating systems. DD images are considered a forensic format as they are a bit by bit copy of a device.
Forensic Image	A "forensic image is a file (or set of files), is used to preserve an exact "bit-for-bit" copy of data residing on digital media. The most commonly used format is .E01 by Guidance Software (www.guidancesoftware.com). The image contains all data, including deleted and system files, and is an exact copy of the original. Most forensic imaging software integrates additional information into the image file at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an "acquisition hash", which can be later used to validate the integrity of the image. The forensic image file acts as a digital evidence container that can be verified and accepted by courts.
Forensically Sound	Digital evidence by its very nature is volatile. The term forensically sound refers to the accepted industry principle that maintaining the integrity of digital evidence is paramount, and that no action by the investigator should change data that is to be relied upon. FEX Imager collects evidence in a manner that preserves the integrity of evidence and provides an audit trail so that an independent third party can examine the actions undertaken. An investigator should also apply standard principles of crime-scene preservation (photographs, documentation, etc.) to any matter involving digital evidence.
.L01 File	A .L01 file (also commonly referred to as a logical evidence file or LEF) is a forensic file format created by Guidance Software (www.guidancesoftware.com). FEX Imager can export files from a target computer system into a L01 file whilst preserving the integrity of the original file information (dates, times, size, etc.). A .L01 is usually used to store a selection of files, rather than a copy of an entire drive, for which the Guidance Software .E01 format is most frequently used.
MD5	MD5 is a widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). It is a 128-bit hash value that uniquely identifies a file or stream of data. It has been extensively used in computer forensics since the late 1990's. MD5 has been identified to have a theoretical collision weakness (when two files have the same hash). For more information see: - MD5 Collisions, The Effect on Computer Forensics, April 2006, Access. - The Hash Algorithm Dilemma–Hash Value Collisions, Lewis, 2009, Forensic Magazine.
SHA1	SHA1 is a widely used cryptographic algorithm that uniquely identifies a file or stream of data. SHA1 is considered a stronger hash than MD5, but as a result takes longer to calculate. SHA1 has been identified to have a theoretical collision weakness (when two files have the same hash). For more information see: - MD5 Collisions, The Effect on Computer Forensics, April 2006, Access. - The Hash Algorithm Dilemma–Hash Value Collisions, Lewis, 2009, Forensic Magazine.
SHA256	SHA256 is a widely used cryptographic algorithm that uniquely identifies a file or stream of data. It is designed by the United States National Security Agency (NSA) and first published in 2001. SHA256 is a stronger hash than MD5 and SHA1, but as a result takes longer to calculate.
UDP	User Datagram Protocol (UDP) is part of the Internet protocol suite. UDP is a simple message-oriented transport layer protocol that is documented in RFC 768. See https://en.wikipedia.org/wiki/User_Datagram_Protocol. FEX Imager uses UDP to connect to a remote device.

Write Blocker	A write blocker is a tool which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined media. It permits read-only access target data without compromising its integrity. Write blockers exist as both software and as hardware. In computer forensics it is write blocking hardware that is more commonly used as its hardwired configuration provides more certainty as to its use.

7. LICENSE AGREEMENT

GetData® Forensics Pty Ltd ("GetData") – ACN: 143458039

IMPORTANT – END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING FORENSIC EXPLORER ("the SOFTWARE"). BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE SET OUT BELOW. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS SET OUT BELOW, DO NOT INSTALL AND/OR USE THE SOFTWARE. PLEASE TERMINATE INSTALLATION IMMEDIATELY AND DO NOT USE THE SOFTWARE.

1. Software Covered by This License

1.1. This license agreement applies only to the version of the Forensic Explorer software package with which this agreement is included. Different license terms may apply to other software packages from GetData and license terms for later versions of Forensic Explorer may also be changed.

2. General

2.1. GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData.

2.2. The Software and any other materials included under this license, are licensed, not sold to you by GetData for use only under the terms of this Agreement.

2.3. GetData or its licensors own the Software, including all materials included with this package. GetData owns the names and marks of 'GetData,' and 'Forensic Explorer' under copyright, trademark and intellectual property laws and all other applicable laws.

3. Permitted License Uses and Restrictions

3.1. Subject to the terms and conditions of this License, a single License of the Software permits you to run a single Licensed instance of the Software. Where multiple Licenses have been purchased, the License permits you to run concurrent instances of the Software equal to the number of Licenses purchased.

3.2. You are solely responsible for the protection of your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any loss or damage suffered from the use of the Software.

3.3. You and others are not permitted to copy (except as expressly permitted by this Agreement), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify (except to the extent allowed in the documentation accompanying this Agreement) or remove or alter any proprietary legends contained in the Software.

3.4. You are not permitted to share the product activation information provided to you for this Software with other users.

3.5. You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.

3.6. GetData reserves the right to check any and all license details at any time in any reasonable manner.

3.7. GetData may from time to time revise or update the Software and may make such revisions or updates available to you subject to payment of the applicable license fee.

3.8. The Software is protected under United States law and International law and International conventions and treaties. You may not rent, lease, lend, sell, redistribute or sublicense the Software without the express written permission of GetData.

3.9. If you purchase a site license, there will be terms and conditions listed in the appendix of the site license.

4. Disclaimer of Warranty

4.1. To the extent not prohibited by applicable law, by using the Software, you expressly agree that all risks associated with performance and quality of the Software is solely held by you. GetData shall not be liable for any direct, indirect, special or consequential damages arising out of the use or inability to use the software, even if GetData has been advised of the possibility of such damages.

4.2. To the extent not prohibited by applicable law, the Software is made available by GetData 'As Is' and 'With all Faults,' GetData or any GetData authorised representative does not make any representations or warranties of any kind, either expressly or implied concerning the quality, safety, accuracy or suitability of the Software, including without limitation any implied warranties of merchantability, fitness for a particular purpose, non-infringement or that the Software is error free.

4.3. GetData or any GetData authorised representative makes no representations or warranties as to the truth, accuracy or completeness of any information, statements or materials concerning the Software.

4.4. No oral or written information or advice given by GetData or a GetData authorised representative shall create a warranty. Should the Software prove defective, you assume the entire cost of all necessary servicing, repair or correction. Some jurisdictions do not allow the exclusion of implied warranties or limitations on applicable statutory rights of a consumer, the above exclusions and limitations may not apply to you.

5. Limitation of Liability

5.1. To the extent not prohibited by applicable law, in no event will GetData, its officers, employees, affiliates, subsidiaries or parent organisation be liable for any direct, indirect, special, incidental, exemplary, consequential or punitive damages whatsoever relating to the use of the Software.

5.2. Any and all data obtained from the use of the Software becomes the user's sole responsibility and liability.

5.3. Any and all data obtained from the use of the Software in any civil or criminal jurisdiction that results in wrongful conviction, erroneous charges, misrepresentation of data or death or any other

civil or tortious wrong against a person, company, corporation or any other entity, GetData shall bear no liability for any death, wrongful conviction or any other civil or tortious wrong against a person, company, corporation or any other entity.

5.4. Any and all data obtained from the use of the Software is the sole responsibility of the user. In the event the user misconstrues, misinterprets, or misunderstands the data and causes it to be used in any and all civil or criminal jurisdictions, GetData shall bear no liability.

5.5. In no event will GetData's liability to you, whether in contract, tort (including negligence) or otherwise, exceed the amount paid by you for the License under this Agreement.

5.6. In the event that a company bearing the name of GetData operating as a separate legal entity, leases the Software to you, and you misconstrue, misinterpret or misunderstand the data that results in any wrongful conviction, erroneous charges, misrepresentation of data, death or any other civil or tortious wrong against a person, corporation or any other entity, GetData ACN: 143458039 shall bear no liability to you, the liability shall be borne by whatever company bearing the name of GetData operating as a separate legal entity.

6. Applicable Law

6.1. This Agreement and any dispute relating to the Software or to this Agreement shall be governed by the laws of the State of New South Wales and the Commonwealth of Australia, without regard to any other Country or State choice of law rules.

6.2. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to GetData or the matters in this Agreement shall be exclusively in Courts located in NSW, Australia. If any part or provision of this Agreement is held to be unenforceable for any purpose, including but not limited to public policy grounds, then you agree that the remainder of the Agreement shall be fully enforceable as if the unenforced part or provision never existed. There are no third-party beneficiaries, or any promises, obligations or representations made by GetData therein.

7. Export

7.1. You acknowledge that the Software is subject to Australian export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software including destination restrictions issued by GetData.

8. Termination

8.1. This Agreement is effective on the date you receive the Software and remains effective until terminated. If you fail to comply with any and all terms set out above, your rights under this Agreement will terminate immediately without notice from GetData. GetData may terminate this Agreement immediately should any part of the Software become or in GetData's reasonable opinion likely to become the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of and destroy all copies of the Software under your control and confirm compliance in writing to GetData.

9. Entire Agreement

9.1. This Agreement constitutes the entire Agreement between you and GetData relating to the Forensic Explorer Software herein. This Agreement supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement or other communication between the parties relating to its subject matter during the term of this Agreement. No modification, amendment or addendum to this Agreement will be binding, unless it is set out in writing and signed by an authorised representative of each party.

10. Translations

10.1. This agreement is translated into other languages. It is the English version which is the language that will be controlling in all respects. No version of this agreement other than English shall be binding or have any effect.

8. BIBLIOGRAPHY

1. **Carrier, Brian.** *File System Forensic Analysis.* s.l. : Addison Wesley Professional, 2005.

2. **United States Computer Emergency Readiness Team.** US-CERT Vulnerability Note VU#836068. *US-CERT: United States Computer Emergency Readiness Team.* [Online] [Cited: 5 March 2011.] http://www.kb.cert.org/vuls/id/836068.

3. **Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu.** *Collision Search Attacks on SHA1.* 2005.

4. **Merritt, Rick.** Chinese researchers compromise SHA-1 hashing algorithm. *EE Times.* [Online] 16 2 2005. [Cited: 4 May 2100.] http://www.eetimes.com/electronics-news/4051745/Chinese-researchers-compromise-SHA-1-hashing-algorithm.

5. **Lewis, D.** The Hash Algorithm Dilema - Hash Value Collisions. *Forensic Magazine.* [Online] 2008.