Training Manual

Tool Validation Testing

ACCESSDATA®

www.accessdata.com

Information in this training manual, including any URL or other Internet website, is subject to change without prior notice.

Unless otherwise noted, the companies, organizations, products, email addresses, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, email address, person, places, or events is intended or should be inferred. Complying with all copyright laws is the responsibility of the user.

AccessData Group, Inc.
603 East Timpanogos Circle
Orem, UT 84097

Tool Validation Testing

Contents

Module 1 - Introduction

Introduction

This Module will introduce the concept of the validation of forensic software and its place in the forensic 'method' and the validation of that method. A lot of the information drawn from this module is derived from sections of a number of International Standards and procedures. Some of these standards are directed towards an International audience and others are derived from documents which have been created for a specific audience, such as The United Kingdom. Whilst there will always be discrete differences in workflows across various territories, the information contained within this manual will likely still prove useful to a student from any territory. The contents of this and following modules is designed to be as generic as possible but consideration should always be given to local laws and regulations.

What is A Method?

The term 'method is described in The Forensic Science Regulators, Code of Practice and Conduct Appendix: Digital Forensic Services[1] as follows:

'A method is logical sequence of operations or analysis which may include the use of software, hardware and tools'.

More simply, a method is simply another way of describing a process. There are many processes that exist within a forensic workflow. Some examples of processes, or methods might be:

- The creation of a Forensic Image of a SATA hard disk using FTK Imager version 4.3.1.1.
- The processing of data from a Windows 10 operating system using Processing profile 'X' in FTK version 7.4.

Both of the above are fairly standard methods that take place in a Digital Forensic lab. They are also methods which are likely to be repeated time and time again. This is because they are fairly generic. It is this type of method that we would be expected to 'validate'.

We will revisit these methods in a bit more detail later.

---

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912389/107_FSR-C-107_Digital_forensics_2.0.pdf

What does Validation mean?

In general terms, the process of validation could be described as: *'the action of checking or proving the validity or accuracy of something'.* Applying this to a forensic workflow means that we will need to check and prove the validity or accuracy of our method. Before we can understand how this validation will take place and how we can plan for it, we will need to go back to the method and understand all of the different elements that make up that method.

Let's use one of the example methods above:

The processing of data from a Windows 10 operating system using Processing profile 'X' in FTK version 7.4.

We can now break this method down (in simple terms) into its component parts and identify additional elements.

Where does the method start?

In this case, the method would likely start at the point when the investigator would receive the forensic image of the device.

Where does the method end?

The method would likely end at the point of the completion of the processing and at the commencement of the investigation phase.

Details of the Method

The table below provides a **basic** overview of the elements that might be involved in the method described above. As you can see, each element is broken down and consideration is given to environment, hardware, software, the competency of the investigator and the use of test media to be able to validate the results against a control set.

Method starts		
Process	**Considerations**	**Additional**
Receipt of Forensic Image	Depending on the lab environment, consideration may need to be given to use of encryption, network connectivity, storage, security etc.	Competency of Investigators and Technicians involved in each phase of the method to ensure that they are able to competently complete each phase.
Add Forensic image to Forensic workstation	Depending on lab environment	
Verification of Forensic Image	Forensic Tool used for the purpose needs to be tested against a control set.	
Opening of Forensic Software	Confirmation that tools are running as expected and correctly licenced. Hardware considerations.	
Adding Forensic Image to software tool	Confirmation which forensic tool will be used for the specific purpose.	
Choosing Processing profile specific to purpose of investigation	Testing of forensic tool and processing options and confirming the results are accurate and as expected against a control set.	
Processing takes place		
Processing Completed	Validation of results against control set.	

Method ends and next phase commences.

In the table above, the shaded box represents the testing of the forensic software tool and its processing options. The chapters which follow in this training will focus on this area, as it is unrealistic to consider the whole method during this 'tool validation' training.

As we have said before, this method is fairly generic and that is understandable, because many of the processes which take place in a forensic laboratory are standardised and are repeated on a daily basis. Indeed, it is likely that the processes that take place in one laboratory are possibly very similar to those which are used in another. This concept is quite important and we will discuss this in more detail later.

The End Goal

The end goal is that every method which exists in the forensic laboratory has gone through the validation process. The staff members and colleagues that use the method should be confident about whether it is fit for purpose and whether there are any limitations. It should also be shown that the colleagues and staff members who deploy the method are suitably competent to do so.

Where to Start with the Validation Process

In order to start the validation process, it is a good idea to look at the processes which already exist in the forensic lab and document these into a set of Standard Operating Procedures (SOP)'s. Developing SOP's as the first stage provides a foundation for processes moving forward as it encourages you to 'document what you do' rather than 'do what you document'. It may be that you have never broken down the laboratory methods to such a granular level and this may be an additional opportunity to refine some processes within the lab.

Once you are in possession of a full set of SOP's then the method validation process can start.

The Forensic Science Regulator's Code of Conduct and Practice, Draft Guidance: Digital Forensics Method Validation[2] provides a framework for the phases that should follow in the validation process:

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/485037/2015_12_14_-_Digital_Forensics_-_validation_-_draft_guidance.pdf

a. Determining the end-user's requirements;
b. Determining the specification;
c. Risk assessment of the method;
d. A review of the end-user's requirements and specification;
e. Setting the acceptance criteria;
f. The validation plan;
g. The outcomes of the validation exercise;
h. Assessment of acceptance criteria compliance;
i. Validation report;
j. Statement of validation completion; and
k. Implementation plan.

During the chapters that follow, we will look into these sections and consider how these affect our ability to validate the software tool element of the sample method provided in this chapter.

This Page Intentionally Left Blank

In this chapter we will discuss some of features which were mentioned in the previous chapter, in more detail. Where applicable we will discuss the sections featured in the validation process, where they apply to the specifics of the testing of the forensic software.

Determining the End-User's Requirements

The end user's requirements are very important to the process of testing the software tool.

Before we look into the end user's requirements, we need to take a step back and determine who our end user actually is.

In many scenarios, forensic laboratories take their 'instructions' from other internal or external departments. Here are a couple of examples:

A Police Forensic Laboratory in the United Kingdom would receive their forensic submissions from other Police departments within the Police Force.

or

A private organisation may take their instructions from Police forces or from individuals or corporate organisations.

It could be said that The Police, the individual or the corporate organisation could be described as the end user. However, realistically, these entities are only an 'interim' end user. Ultimately, the end user would be the Criminal Justice System, as this could be said to be the final user of the evidential productions a laboratory supplies.

Once the end user has been identified, then it is possible to consider the requirements of the end user.

In **general** terms (and in terms of the software tool specifically), the needs of the end user might include some of the following points:

- The software will be able to obtain an extraction of main types of media, including pictures from the evidence item.

- The software will be able to obtain a comprehensive extraction of all online activity, online file activity, user activity, system information and communication activity from the evidence item

- The software will be able to ensure that all media extracted from the evidence item has associated metadata which is accurate and reliable, where applicable.

- The software will be able to ensure that all internet activity, file activity, user activity, system information and communication activity extracted from the evidence item has associated metadata which is accurate and reliable, where applicable.

- Any reports must be in readable format.

Once the general terms have been documented, they can be further broken down into more specific points which are more focused towards what the software tool is expected to do.

Here are some examples of more focused requirements:

- The software tool will extract all media using file signature search and data carving techniques.

- The software tool will accurately extract all internet related activity and interpret it into a readable format

- The software tool will output all extracted media in its entirety to a conventional reviewing platform.

- The software tool will accurately extract all file related activity and interpret it into a readable format.

- The software tool will accurately extract all system related information and interpret it into a readable format.

- The software tool will accurately extract all user related activity and interpret it into a readable format.

- The software tool will accurately extract all communication related activity and interpret it into a readable format.

- The software tool shall interact with a conventional forensic image file (e.g. E01).

- The integrity of the extracted or analysed data shall be maintained in a manner which is traceable back to the original acquisition from the physical evidence item.

- The software tool will produce the correct MD5 Hash value for all media, (Image and Video files), extracted from the evidence item.

- The software shall not add to, remove or modify the original user-addressable data which is stored on the evidence item.

- The software tool will produce accurate and reliable metadata associated with internet related activity, extracted from the evidence item.

- The software tool will produce accurate and reliable metadata associated with user related activity, extracted from the evidence item.

- The software tool will produce accurate and reliable metadata associated with file related activity, extracted from the evidence item.

By producing a list of the end users requirements, it allows for us to then design the testing specification that will be used during the testing phase.

Remember that this training focusses on the testing of the software tool specifically and all end user requirements should focus on the whole method. The same concept applies to the sections that follow, particularly in relation to risk assessment and specifications.

Determining the Specification

It may be that during the creation of the end user's requirements, it is already known that more than one software tool will be required. This might be because of the limitations of a certain software tools. It makes sense to keep this in mind so that when testing scenarios a produced, they take into account all requirements of the end user. Building test data to test the specific features of one tool is unrealistic to normal investigations practice and is likely to make the testing disproportionate.

We are now able to think about how we will build be our test scenarios for the purposes of testing the software tools as part of the wider method.

In this training, we will deal with the testing of the forensic software tool FTK version 7.4 against a set of control data, namely a forensic image (in E01 format). In a typical laboratory environment, the creation of that forensic image and all associated actions surrounding that, would also be subject to testing and validation. The tests that we will conduct in this class will be carried out on the assumption that the forensic imaging process is one that has been accepted as validated. Therefore, we will continue on the basis that the imaging processes are deemed to be accurate, reliable and fit for purpose.

What will we test?

Forensic Toolkit (FTK) is an examination tool used for the examination of data derived from digital devices. During extraction, the forensic image is mounted into the software which reads the raw data and provides a visual representation as a directory structure. This enables a user to navigate through the files and directories of the imaged device. FTK achieves this by storing the information of all the contents of the forensic image in a database. The database only stores files that are referenced by the regular file system. To forensically extract further data from the volume, FTK allows an analyst to initiate a series of automated operations. FTK refers to this as 'processing options'. The processing options allows an analyst to perform the following tasks on the contents of an exhibit (where applicable):

The full list of processing options available in FTK version 7.4 can be located in Appendix A of this training manual.

The list of expandable compound files is located at Appendix B of this training manual.

Some of our testing will feature samples from the processing options detailed above.

Below are examples of some of the aspects that might be included in the testing specification requirements:

Test	**Details**
Reads the raw data on the image.	The software must display a visual representation as a directory structure to enable the investigator to navigate through the files and directories.
Reporting of Disk Geometry	The software must confirm the same disk geometry as the information noted during the imaging phase and reported in the forensic image.
File System Data Structure Search	The software must allow the investigator to perform tasks on the contents of an exhibit. The investigator must be able to locate records that exist in free space or volume shadow copies that are not present in the $MFT.
File Header Signature Search capability	The software must scan the contents of the image to identify and extract files from unallocated clusters or from used space with 'file signatures' and data carve. The software must Identify 'hex' file headers and footers (signatures) to categorise and reassemble data into readable format. For example, a JPEG has the header ‘FF D8’. The aim of this process is to identify and carve a file based on this signature information alone.
Computing and Matching of Hash Values	The software must be capable of computing a hash value for every file contained on the image.

	The software must be able to apply a comparison of hash values to specific hash database/libraries (Known Not Relevant, NIST, NSRL, etc.)
Verification of File Types	The software must identify file type mismatches subject to a change in file extension. For example, changing the extension of a photograph from '.JPG' to '.DOCX'. This will obfuscate results in live data and portray a picture file as an MS Office Word document.
Extraction of Internal Metadata	The software must be able to extract metadata within files. Metadata is information about the data (data about data), related to file creation date/times, file deletion date/times (maintained in the $MFT of an NTFS file system, for example). The software must be able to extract and report on EXIF data. EXIF data is metadata traditionally associated with pictures taken with a digital camera and can include, access date/times, GPS locations, etc. The software must provide the functionality for recycle bin file recovery. This function is also used to extract original file system metadata, such as file name and timestamps, where applicable. Recycle Bin files, are assigned random names such as, '$I*' to make them unique. The software must provide email header information relating to sender and recipients in readable format. SQLite databases and event logs data are in readable format.
Extraction of E-mail Messages and Attachments	Capability to identify and extract e-mail messages and attachments. Again, as part of this process, any associated metadata is extracted,

	such as the creation date and time, sender and recipient information.
Uncovering Embedded Images	The software must provide the investigator to use file header signatures to search and identify data embedded within another file, common in MS word documents or PDF's, with images often placed alongside text. This process should identify the embedded file and extract it as a child object of the parent file. The software must identify picture files located within thumbnail database files.
Keyword searching	The software indexes data and allows searching across entire dataset and accurately finds lists of keywords and incorporates the power of regular expressions in functionality.

Risk Assessment of the Method

The risk assessment process is a fundamental part of the validation process and is at the core of validation. However, the risk assessment will and should encompass the entire method, to include:

- The Site/Environment
- Personnel
- The Data Network
- Security
- The Organisation
- Hardware
- Software

Risk assessment in the Criminal Justice Process often includes the:

- the risk of wrongful conviction(s);
- the risk of wrongful acquittal(s); and
- the risk of obstructing or delaying investigation(s).

The Forensic Science Regulator's Guidance for Method Validation in Digital Forensics (FSR-G-218)[3] provides an overview of risk assessment and provides some example which are useful when considering this phase.

'It is important to know how a method or tool is to be used and, also important, how they may provide misleading results in certain circumstances. The following summarises some of the sources of potential misleading results.

a. Incompleteness – the inability to recover or find all the data.

b. Inaccuracy:

i.Existence – do all artefacts reported as present actually exist?

ii.Alteration – does a method alter data in a way that changes the meaning, such as updating an existing date-time stamp (for example, associated with a file or email message) to the current date?

iii.Association – for every set of items identified by a given method, is each item truly a part of that set?

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf

iv.Corruption – does the forensic method detect and compensate for missing and corrupted data (including, where relevant, any deliberate editing or manipulation prior to receipt)?

c. Misinterpretation.'

A Review of the End-User's Requirements and Specification

The review of the end user requirements come at this stage in the process so as to provide a checkpoint for review. At this stage the following phases have been undertaken:

- Production of a SOP detailing the proposed method;
- Identification of the End User's Requirements;
- The determination of the Specification
- A risk assessment

Each or any of these phases may have identified issues or observations which may need further review. One of critical considerations during this review would be:

'Is the method fit for purpose?'

Additionally if, during the review, it is identified that there are risks, issues with compatibility, legality or ethical issues, the forensic unit will need to produce a revised end-user's requirements and/or specification.

If at this stage, any changes are required, then it goes without saying that all involved parties are informed and their agreement is confirmed. Any changes to the end user requirements or specification should be documented fully and formally.

Setting the Acceptance Criteria

The Acceptance Criteria provides the validation team with a set of measurable criteria, to establish whether the validation exercise has been successful or unsuccessful.

It is important when setting the acceptance criteria that this isn't something that is collated and produced just by one person. All stakeholders involved in the method should be given the opportunity to agree the acceptance criteria, based on a consensus of their requirements. These stakeholders should include (if they exist)

- The investigations team
- The Quality Manger
- Technical Management
- A sample from the end user/customer base.

The acceptance criteria should be clearly and plainly defined, so that everyone involved in setting the criteria can understand the ideas that are being conveyed.

Some Examples of Acceptance Criteria

- To be able to extract known data from reference key test sample in a manner that does not alter the MD5 hash values in line with the standard operating procedure, and any identified risk as stated within the risk assessment.
- To demonstrate that whilst extracting data no alteration can be made to the reference key sample, thereby proving the functionality container E01 file and protect the integrity of the exhibit/data.
- To accurately identify data type and categorise into user-friendly sets (i.e. pictures, videos, docs, HTML, etc.)

Should the Acceptance Criteria Include Every Function of the Software?

Forensic tools, by their nature, have the ability to interpret and extract vast volumes of data. As such, the validation of each of the individual processing elements would likely result in an unfeasible validation scope.

Dependent upon the review and outcomes of the acceptance criteria, it may be agreeable to focus the validation of the software tools based on data expected to be extracted for the majority of cases.

This will consist of the most commonly seen data throughout the laboratory's casework and will essentially create a pool of known artefacts that are expected to be extracted and to a point in which analysis can be achieved. This significantly cuts the scale of the validation down to a reasonable amount without loss in assurance in the robust testing of the tool.

Successes and Limitations

In some aspects of the validation exercise, it may not be possible to use a simplistic 'yes' or 'no' as a measure of success or failure.

There may be a number of legitimate scenarios where the software cannot/does not produce results.

Examples could be:

A data artefact is placed upon the test device, but the Operating System contained upon that device does not have the capability to store or retain that artifact. In this scenario, the failure of the tool to recover such an item could not be deemed to be failure in terms of the validation exercise. The failure of the software to record this is a limitation of the artefact or Operating System and not a limitation or failure of the tool itself.

A limitation of the tool will be when we know the artefact exists, and has been generated on the source material, but the tool cannot extract and analyse data as per the requirement.

There will be a number of expected and accepted limitations which can be included in the validation plan. These limitations exist primarily as a result of the failure of the Operating System on the test system to store this information, either locally, or at all.

Some examples of acceptable limitations may include:

- **Deleted File Analysis** – Subject to the acceptance criteria, the validation team may accept that not all deleted data is recoverable as deleted files can be "overwritten" making it impossible for data recovery. Further limitations relating to deleted data might be where the file data could be recovered if a file header is identified by the "carving process". A limitation to this may be the loss of metadata and an incomplete file.

- **Web Activity Incognito Mode** – It may be accepted that data will not be recoverable when the browser Google Chrome has been used in incognito mode as it is understood that data is not save to the HDD.

- **Email Activity** - It may be accepted that much of the email data created will be held in cloud storage. Although where and email client is used it may be expected that artefacts may be found.

This Page Intentionally Left Blank

Module 3 - Building the Test Data

In this chapter we will discuss the final planning phases, preparing to build the test data and subsequently building the test data.

The Test Machine

It goes without saying that in order to test the software tool, there needs to be some test material. The creation of the test materials should be carefully planned so as to have the right materials in place before the creation of the testing data takes place. The scope of testing should be clearly defined before the materials are created too, so that the right artefacts can be added to the testing set.

Below is a list of some preliminary considerations that you may wish to take into account before the test data is created.

- Type of machine
- Operating system type
- To image or not to image?
- Scope of artefacts
- Where to place artefacts
- How will you keep notes?
- How will you reliably monitor time and date?

Type of Machine

The type of machine/computer that you use may depend on a number of criteria, including the types of operating systems you wish to add to the testing. It may be that your department does not have the resources to have physical devices available to use for testing. Therefore it may be a consideration whether you wish to use virtual machines for use in testing. Virtual machines provide the opportunity to create test data sets without the need for additional investment in hardware.

Tip: If you intend to use Virtual Machines for use in testing, it is not advisable to utilise linked clones, as this could adversely restrict some of the material which is available in the resulting image file and may cause issues when imaging data.

Operating System Type

It is important to consider that during your investigations, you are likely to be faced with a variety of operating system types. Therefore it should be a consideration that the test data could encompass more than one operating system. The choices that you make regarding the type of Operating System should be a representative sample of the types of operating systems that you are generally faced with in your day to day activities. Some general OS types may include:

- Windows 7
- Windows 10
- MacOS
- Linux

It is also worthy to mention that the artefact types contained within your testing data may need to change to be more reflective of the changes in the OS, for example, the addition of Safari as the default browser in MacOS.

To Image or Not to Image?

As part of the testing plan, it is important to consider whether you will need to create a forensic image of the test data. In the large majority of scenarios, the answer would be 'yes'.

It is possible that the testing which is being conducted is following on from the validation of additional methods including the forensic imaging process and as a consequence, it may be that the forensic images which have been created are also used as part of that validation too. However, for the purpose of this training, it is assumed that the imaging validation has taken place separately and therefore, these processes are unrelated.

If you had decided to use virtual machines to create the testing material, it is possible that the files (such as .vmdk) can be ingested into the forensic tool as an image file (which can be achieved in FTK 7.4). However, the creation of the test materials is to provide a stable and repeatable platform for testing and as such, creating a forensic image is still advisable.

Scope of Artefacts

The scope of the artefacts are likely to have already been planned in your previous phases before reaching this point, but to reiterate, you should be able to show a truly representative sample of the general data that you see in your investigations. If your investigations generally involve the review of illegal imagery, then you would expect to add graphic data, communication data, internet browser data and artefacts which are produced as a consequence of the use of certain software tools which are frequently seen in your investigations. Trying to add artefacts which will cover every imaginable variation of artefacts and crime types could make the testing disproportionately large.

Where to Place Artefacts

During your creation of the testing materials, it may be that you wish to add certain artefacts which already exist and you wish to transfer them onto the testing machine.

The purpose of testing is to **robustly challenge** the software tools. Adding a collection of previously created materials to a folder on the desktop of the testing machine could arguably 'make it easy' for the tool to recover and present the data. It may be more appropriate to introduce the data to the testing machine in a manner which is a more fitting to the scenario and in a way which can also create more useful artefacts such as:

- Downloading data from a cloud instance
- Adding data by introducing a third party device such as a USB device.
- Emailing data to the test machine.

Each one of these concepts provides the ability to introduce data to the testing machine but in doing so will also create additional artefacts of potential forensic interest.

How will you keep notes?

Before you begin to create your test machine, it is really important that you consider how you will take contemporaneous notes during the process. You could do this by asking a colleague to keep a contemporaneous record of notes as you add these to the test evidence, or you could record these yourself. You could also use more novel techniques such as video recording which you could then write up as a set of notes later.

You should assume that you will need to record every action on the test machine, from the moment that it is switched on until the moment that it is shut down. It is particularly important to be able to record when artefacts were created, downloaded, accessed, deleted etc. so that these can be cross referenced during the validation exercise.

Remember that the test data that you are creating should be repeatable and you should also assume that it may not always be the person who is conducting the tests. As a consequence, you should never rely on information from memory. All actions should be physically recorded.

How will you reliably monitor time and date?

The use of a suitable time recording method is crucial to the testing scenario. First of all, it is important that your test machine is reporting the correct time and time zone (or at least the time zone that you 'want to test'). It is also important that you have a reliable time source that you can use within your contemporaneous notes. This way,

you can cross reference the time against the reported time from the test machine and that of the software. The reliability of the time source provides a benchmark for the review. It is not acceptable to use 'time by my watch' as a time source due to the potential for error. Recommendations for reliable time sources include:

- A radio controlled clock
- An internet time source such as time.is

The Expected Outcomes of The Testing

You should note in the validation plan the expected outcomes from the testing. This work has already been done in previous parts of the planning and could be derived from the acceptance criteria. Some examples of expected outcomes could include:

- It is expected that the software will not change the image files.
- It is expected that the software will correctly identify the partitions and file system.
- It is expected that the software will identify the Windows, Linux and MacOS operating systems.
- It is expected that the software will correctly report the file names.
- It is expected that the software will correctly report the file signatures.
- It is expected that hash values will be correctly calculated with the algorithms MD5 and SHA1.
- It is expected that deleted files may or may not be identified.

The Expected Limitations of The Testing

As above, you should also note the expected and accepted limitations of the software used in the testing. As before, this has already been discussed in previous planning. But, some examples are noted below:

- It is accepted that not all deleted data is recoverable as deleted files can be "overwritten" making it impossible for data recovery. Further limitations relating to deleted data might be where the file data could be recovered if a file header is identified by the "carving process" a limitation to this may be the loss of metadata and an incomplete file.

- It is not believed that data will be recoverable when the browser google chrome has been used in incognito mode as it is understood that data is not save to the HDD.

- It is believed that much of the email data created will be held in cloud storage. Although where and email client is used it may be expected that artefacts may be found.

Uncertainty of Measurement

Uncertainty of Measurement is very difficult to calculate scientifically in Digital Forensics, but not impossible. A way of considering Uncertainty of Measurement is, rather than a calculation, to consider it as an expression of the factors that influence measurements of uncertainty, their impacts assessed and a description of your attempts made to mitigate their influence.

To consider this in more detail we can consider some of the factors that may influence this concept.

The first uncertainty is that all data may not have been extracted by the forensic software. This is especially relevant to forensic tools (albeit a remote scenario) as the tool will only be capable of retrieving data which it is programmed to recover. Therefore, if the tool was never programmed to extract a certain type of data, that data will never be extracted until the tool itself has been modified to accommodate it.

The second uncertainty is that it is not possible to be certain if the forensic tool has interpreted the data being extracted correctly just from looking at the software's data output. For example, if a website was using the domain name 'www.nasa.com', and this information is stored in an SQL database controlled by the web browser, there is an uncertainty over the accuracy to which the tool is outputting that data. If the forensic tool interpreted the content of that SQL Database entry as a domain name of 'www.nasa.com'', how can we know whether it is accurate or not? The tool does not provide a level of investigation that permits the user to look at the raw data it has extracted the information from, so verification within the tool is limited.

How to Mitigate Uncertainty of Measurement

The two examples of uncertainty detailed above are quickly mitigated with the use of another analysis tool to cross reference the results. By using the additional software, it is possible to verify that all artefacts are accurately portrayed at a raw level. This in turn verifies the data at the source and allows these results to be compared against the interpreted outputs presented by the original software, thus proving their accuracy.

Building the Test Materials

Now that we have considered how we will build the testing data and which artefacts we will be utilising in this dataset, we can now commence the building of the test data. Below is an example of the test data notes that were taken during the creation of the test data for the use in this training.

03/02/2020	**Prepare MV Test Windows 10 Machine**
Time	**Action**
16:31	Commence creation of Window 10 virtual machine using VMWare workstation
	Using Windows 10 Enterprise
16:43	Automatic restart
16:44	Discoverable to Networks? No
16:44	Install Complete
16:45	Cortana Search box for Updates. Opened Updates window
16:46	Click Check for Updates
16:46	Cortana Search Box for accounts
16:47	click Add, Edit or Remote Users
16:47	Clicked Add Someone Else to This PC
16:48	Commence Creation of LOCAL Account MV TEST password 123, password hint 'first second third'
16:50	Open and Close File Explorer
16:50	Restart
16:56	Open Edge Browser
16:56	Type Google Chrome Download

	https://www.bing.com/search?q=google+chrome+download&form=EDGEAR&qs=EP&cvid=74b7a0792b04483bb9c1f572d1133cf9&cc=US&setlang=en-US
16:58	Click Download Now on search results
	https://www.google.com/chrome/?utm_source=bing&utm_medium=sem&utm_campaign=1001342%7CChromeWin10%7CGB%7Cen%7CHybrid%7CText%7CBKWS~Exact&brand=CHBF&ds_kid=43700010204856413&utm_source=bing&utm_medium=cpc&utm_campaign=1008138%20%7C%20Chrome%20Win10%20%7C%20DR%20%7C%20ESS01%20%7C%20EMEA%20%7C%20GB%20%7C%20en%20%7C%20Desk%20%7C%20BING%20SEM%20%7C%20BKWS%20~%20Exact&utm_term=install%20chrome%20web%20browser&utm_content=Install%20-%20Exact&gclid=CMuVzp_ttecCFYJ2GwodJI8CmQ&gclsrc=ds
16:59	Clicked Download Now
16:59	Clicked Accept and Install
17:00	Close Edge
17:00	Open File Explorer - navigate to Downloads
17:00	Install Chrome
17:01	Chrome install complete - icon present on desktop
17:02	Click Chrome icon
17:02	Google search for accessdata
17:02	https://www.google.com/search?q=accessdata&oq=accessdata&aqs=chrome..69i57j0l7.6766j1j8&sourceid=chrome&ie=UTF-8
17:03	Click AccessData Homepage from Google page

17:03	Opens https://accessdata.com/
17:04	type bbc.co.uk in chrome search bar
17:05	Click link for Soho streets evacuated over WW2 bomb find
17:05	https://www.bbc.co.uk/news/uk-england-london-51361924
17:06	use Chrome search bar for term Nasa
	https://www.google.com/search?q=nasa&rlz=1C1CHBF_enGB887GB887&oq=nasa&aqs=chrome..69i57j0l7.2782j1j4&sourceid=chrome&ie=UTF-8
17:07	Click Nasa Wikipedia page from Google results
	https://en.wikipedia.org/wiki/NASA
17:08	Right click Nasa Logo - save image as
17:08	Save as Nasa Image to delete and save onto desktop
17:08	close Chrome browser
17:08	Open Nasa Image to delete png image from desktop in Photos App
17:09	Close Photos App
17:10	Drag Nasa Image to delete to recycle bin
17:10	Open Chrome Browser
17:11	Open New Incognito Window
17:12	Search for ccleaner download
	https://www.google.com/search?q=ccleaner+download&rlz=1C1CHBF_enGB887GB887&oq=ccleaner+download&aqs=chrome..69i57.5447j0j1&sourceid=chrome&ie=UTF-8
17:12	Click ccleaner homepage from google results

	https://www.ccleaner.com/ccleaner?source=cpc&gclid=EAIaIQobChMIkPCorfC15wIVRLTtCh2UdwDXEAAYASAAEgKNSPD_BwE
17:13	Click Download free version
17:13	Click free download
17:14	Click download on free version and download commences
17:14	ccsetup 563.exe downloaded
17:15	Close Incognito window
17:16	Google search for 'Pictures of racing cars'
17:16	search auto completes to Pictures of racing cars to colour in
17:17	click Images
17:18	right click on image and name Racing car 1 and save to documents racing car 1.jpg
17:18	right click on image and name Racing car 2 and save to documents racing car 2.jpg
17:20	Insert USB device
17:20	Use VMWare to bring in removable device
17:20	USB Device identified as SARAH 1
17:21	close Chrome browser
17:21	Open File Explorer
17:22	Accessed Sarah 1 USB device
17:23	Drag Win 10 Manual October 2017.pdf to desktop
17:24	Eject SARAH 1

17:34	Empty recycle bin
04/02/2020	
07:34	Shut down
05/02/2020	
09:58	Start machine
09:59	open edge browser
	bing search for 'pictures of cats'
09:59	https://www.bing.com/search?q=pictures+of+cats&form=EDGHPC&qs=PF&cvid=65603938ad584decb62e883d93fd21eb&cc=US&setlang=en-US
10:00	click on 'images' on results page
10:01	right click on image and save to desktop as Picture cat saved for deletion via recycle bin
10:02	right click on image and save to desktop as Picture cat saved for deletion via shift delete
10:03	close Edge browser
10:04	cortana search box for Windows Store - open windows store from results
10:05	search for mail app
10:05	change search to Windows mail app
10:06	close windows store
10:07	Open Chrome Browser
10:07	search for gmail
	open gmail result from results window

10:11	https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GlifWebSignIn&flowEntry=ServiceLogin
10:13	sign into gmail account oliking585@gmail.com with password PasswordABC123
10:14	sending an email to shargreaves@accessdata.com. Title This is a test email. Body I am sending this email to test gmail
	cortana search box for Mail
10:17	open microsoft mail app
10:20	sign in with user account credentials for oliking585@gmail.com
	Compose email to dmenzies@accessdata.com
	This is a Test Message from MV Test Image
	HI Daz,
	This is a test message from MV Test Image (Sarah).
10:23	Please reply.
10:24	Send message
10:27	Synchronise sent messages to populate send items box
10:34	Reply from shargreaves@accessdata.com
10:35	Close mail app
10:35	Drag Picture cat saved for deletion via recycle bin from Desktop to recycle bin
10:36	Delete Picture cat saved for deletion via shift delete using Shift and Delete

10:52	Empty recycle bin
10:53	Connect USB device SARAH 1
10:54	Open File Explorer
10:59	Install FTK Imager 4.2.1.exe
11:00	Open FTK Image 4.2.1
	Commencing imaging of MV Test Windows 10 .E01 mage with full compression
	Sending to SARAH 1
	Imaging Complete

This Page Intentionally Left Blank

Conducting the Tests

The process of testing will include the actions of bringing the test data into the forensic tool and then conducting an analysis to ensure that the results are available and accurately reported. What is critical to this phase is to understand which processing options will apply to ensure that the relevant artefacts are parsed/processed/mounted for evaluation. Therefore it is important to consider which of these processing options will be applicable. You should refer back to the information that you already have gathered and it may be the case that you have already decided which 'processing profile' you will use. The processing used should be reflective of the type of processing that would be undertaken in general cases and should be proportionate to the objectives of the testing. In other words, the processing should be planned so that the tool is prepared to extract the data which has been placed on the test data.

Example - Explicit Image Detection

When explicit material is suspected in a case, the Explicit Image Detection feature allows for easier location and identification of those files. When creating the case, there are options for identifying explicit material. Explicit Image Detection (EID) reads all graphics in a case and assigns them a score according to what it interprets as being possibly illicit content.

EID contains three options for processing:

Name	Level	Description
X-DFT	Default (XS1)	This method the most generally accurate. This is selected by default when EID is turned on.
X-FST	Fast (XTB)	This is the fastest method of conducting EID. It scores a folder by the number of files it contains that meet the criteria for a high likelihood of explicit material. It is built on a different technology than X-DFT and does not use theory to process. It is designed for very high volumes, or real-time page scoring. Its purpose is to quickly

		reduce, or filter, the volume of data to a meaningful set.
X-ZFN	Less False Negatives (XT2)	This is a profile similar to X-FST but with more features and fewer false negatives than X-DFT. You can apply this filter after initial processing to all evidence, or to only the folders that score highly using the X-FST option. Check-mark or highlight those folders to isolate them for Additional Analysis. In Additional Analysis, the option for File Signature Analysis must be selected for EID options to work correctly.

EID Scoring

Each folder is given a score that indicates the percentage of files within the folder that have an EID score that is above 50.

For example, if the folder contains 8 files and three of them score over 50, the folder score will be 38 (3 is 37.5% of 8). Now, a folder score of 38 does not mean there is no objectionable material in that folder, it only means that there is not a high concentration of objectionable material found there.

Explicit Image Detection filtering assigns ratings to pictures according to the presence or absence of skin/flesh tones in graphic files. In addition, it not only looks for flesh tone colours, but it has been trained on a library of approximately 30,000 pornographic images. It assesses actual visual content. This capability increases the speed with which investigators can handle cases that involve pornography.

Successfully filtered pictures are issued a score between 0 and 100 (0 being complete absence of skin tones, and 100 being heavy presence of skin tones). A score above 100 indicates that no detection could be made. When you set filters for analysing the scored data, you specify your own acceptance threshold limit for images you may consider to be inappropriate. Negative scores indicate a black and white, or grayscale image where no determination can be made, or that some error occurred in processing the file.

If EID is likely to be used as part of the processing on most (or all) cases within the lab environment, then this should be tested. Data should exist within the test data

which will allow for skin tones to be identified in the truest sense (image of people with different skin tones). Data should also be present within the test sample which will allow for 'false positives' In other words, data which is of a similar colour to skin tones, but is not, such as animals or other such images.

It is likely that EID when processed, will pick up not only the images which contain 'skin' but also images which contain media including 'skin tones'.

The fact that the EID process identifies more than those images containing 'skin' in the truest sense, may be **expected** and **accepted**. If so, this should be documented as such. This is because EID is designed to identify colour tones and not physical 'skin'. This limitation may mean that although the process has accurately recovered the data containing skin, it has recovered additional data, which may require manual filtering to remove it. This would not be deemed to be a failure of the tool.

If the testing media did not contain any images which were designed to test the functionality of the EID process and subsequently no images were recovered during this process, then it would remain that the testing materials were not suitable for the purpose. This would not be deemed to be a failure of the tool.

If suitable images (positive) were placed on the testing materials and EID did not recover these using of the options, then this would be deemed to be a **failure** of the tool in testing and should be marked as a **limitation** of the functionality of the tool post testing.

Class Activity – Identification of Data Processed and Extracted with FTK 7.4 using test data using Test Data Set.

The Outcomes of the Validation Process

Once the testing is complete, then it is important to be able to document the results of these tests. These outcomes should be documented in a way which is understandable and straight forward. The outcomes can be produced in a list based format. Some examples of reported outcomes would be:

1	Forensic Image File Integrity	The integrity of the image file containers were preserved and not affected by the data processing in any way.
2	Partition and File System Recognition	The partition and file system details are recovered as expected in Windows 10
3	Operating System Recognition	The OS version was identified.

4	User Account Recognition	User accounts for Windows 10 are identified.
5	File Metadata Reporting	File metadata was reported correctly for all tested operating systems.
6	File Signature Recognition	File signature recognition was reported correctly for all tested operating systems.

Review of the Validation Outcomes Against the Acceptance Criteria

Now that you have produced and documented the outcomes, you should refer back to the acceptance criteria that was laid down during the planning phases. This is to enable you to confirm that the outcomes of the testing are acceptable, or indeed unacceptable. The objective here is to show that the testing that has been conducted has fulfilled the objectives required and it can be shown that the testing has enabled you to demonstrate that the tool is capable of achieving the outcomes as documented.

During the review of the Acceptance criteria, it may become apparent that some areas of testing were not appropriate to fulfil the requirements of the Acceptance Criteria. It may also be that there were insufficient artefacts present within the testing materials to demonstrate the criteria sufficiently. If this is the case then it is necessary to go back to the testing phase and repeat the process so as to ensure that the said criteria can be tested and fulfilled.

This Page Intentionally Left Blank

Producing the Final Report

The production of the validation report would naturally be produced at this stage. The final report would obviously encompass the whole method and not just the testing of the software tool.

Validating the Tool Only

The Forensic Regulators Draft Guidance: Digital Forensics Method Validation (FSR-G-218 Second consultation)[4] states:

> *'It is a method that produces the results, a tool is only part of a method. For example, a write blocker is a device that allows a storage device from an exhibit to be connected to a forensic examiner's computer, whilst preserving evidential integrity during preview or forensic imaging. It is important to verify that the write blocker is not malfunctioning, e.g. allowing data to be written back to the storage device or corrupting data as they are read through it. However, if this is the only part of the forensic imaging method that is checked or validated, it cannot be known whether consistent and full results are produced on each occasion. It is therefore important to validate the entire forensic imaging method, from the continuity and handling of the original exhibit through to the production of a verified set of forensic images for analysis, and including all intermediate steps.'*

The Validation Report

A report should be constructed that details the validation process performed. This should include the following:

a. The original requirement.

b. Reference to what is, and is not, validated.

c. A summary of the strategy, tests performed and the outcome of each test.

---

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/485037/2015_12_14_-_Digital_Forensics_-_validation_-_draft_guidance.pdf

d. Reference to the data used and any limitations accepted from the onset these may have on the tests performed and therefore what caveats apply.

e. Whether the method is fit for purpose: this should state whether the method is fully approved, partially accepted or not recommended for use.

f. A caveat to suggest that reliability and uncertainty measures have been considered and what impact these may have should be included.

g. Recommendations for use:

i. to include any limitations of the method, the impact of these limitations and any additional steps required to detect and mitigate for them;

ii. define the required on-going quality regimen (e.g. quality assurance tests); and

iii. Effect of new approach/technique/equipment on existing methods: whether existing methods become obsolete and should be superseded or whether the method should be used as an alternative or in parallel.

During the testing, it is important that you noted important information which can be brought through to the final report including:

a. who undertook the test;

b. when the test took place;

c. what the test assessed;

d. what equipment was used;

e. the expected outcome;

f. what the results were; and

g. any other appropriate information (e.g. the raw results or a link to them and where the test was performed, if this may affect findings).

The writing of the final report might feel like a daunting task but in actual fact, this is mainly a collation of the data which has already been collected and documented during the previous phases.

Referring back the first module in this training we discussed the phases of this process in line with the recommendations laid down by the Forensic Regulator. These are a great foundation to use as the skeleton for your report.

l. Determining the end-user's requirements;
m. Determining the specification;
n. Risk assessment of the method;
o. A review of the end-user's requirements and specification;
p. Setting the acceptance criteria;
q. The validation plan;
r. The outcomes of the validation exercise;
s. Assessment of acceptance criteria compliance;
t. Validation report;
u. Statement of validation completion; and
v. Implementation plan.

Statement or Certificate of Validation Completion

If the process of method validation was being undertaken as part of an accreditation process, then it would follow that the laboratory would have to produce a Statement or Certificate of Validation Completion.

The aim of this statement is to provide those making decisions on the use of the results, a short executive summary of the validation steps performed, and key issues surrounding the validation. The intention is that the statement will be no more than two sides of A4 paper in plain language.

The Implementation Plan

The implementation plan is where you would document your plans for executing the method and using it in the lab environment. This might include your plans for:

a. Staff competency training
b. How the new method might be integrated with existing methods in the lab
c. The monitoring mechanisms to be used to demonstrate that the method remains under satisfactory control during its use
d. The protocols for calibration, monitoring and maintenance of any equipment

Post Implementation Maintenance

Once the validation is complete and implemented, it is important that you consider when this needs to be reviewed. As far as software tools are concerned, it follows that

as they are updated and new versions are released, then your review of the release notes are paramount to understanding whether your use of the new version impacts the current validation or whether a re-validation should take place.

Re-Validation – Some Examples

- A new version of the software is released which contains a bug fix. The bug in the current software impacted the lab's ability to recover data types which were pertinent to the investigation process. This meant that this was previously marked as a limitation in the current validation. Re-Validation would be required so as to confirm that they bug fix was working appropriately, that it was able to recover and produce the artefacts as required and was therefore no longer noted as a limitation.
- A new version of the software was released which contains a bug fix. The bug fix has no impact on the validation which currently exists because it falls outside of the scope of the validation requirements for the lab. It could be argued that if the new release of the software has no impact on the current validation, then re-validation would not be necessary.
- A new version of the software was released which handled a new artefact (or new version of an artefact) which you have seen in your investigations. Re-validation would be necessary in order to add this process to the scope of the validation as the results of this new processing should be tested. It would follow that the testing materials may need to be adjusted to take into account the new or updated artefact.

This Page Intentionally Left Blank