



CARDIFF UNIVERSITY SCHOOL OF COMPUTER SCIENCE AND INFORMATICS

CM3203 One Semester Project: 40 Credits

Author: Benjamin Ajax-Lewis

Supervisor: Michael Daley

Moderator: Alun Preece

Final Project

“Application of ISO 17025 with Inter-Laboratory Testing”

Abstract

I want to streamline the Integration of ISO 17025 [1] into today's digital forensic investigations so that my research can be used to help police forces prove that the tools they use are backed up by scientific research by running tests following the ISO 17025 [1] standard that will be enforced onto the UK police departments as of October 2017 and from these tests I will outline a general procedure of how I conducted my tests to meet the requirements of this ISO so that others can use it to conduct their own scientific tests on forensic tools in the future.

If there are any acronyms that you do not understand, the full meanings of each can be found in the glossary at the back of the report.

Acknowledgement

I would like to thank Michael Daley for supervising my project, giving me flexible meeting times and consistently fast communication and useful advice throughout this project. I would also like to thank Paul, Tim and Mark from Gwent police for giving me lots of real world scenarios to help me understand what they needed from me and finally I would like to thank my family for helping me proof read and improve the flow of my report.

Contents

1. Introduction	5
1.1 Intended Project Audience and Beneficiaries	5
1.2 Project Scope	5
1.3 Project Aims and Objectives.....	6
2. Background	7
2.1 Initial Meeting with Gwent Police.....	7
2.2 Encase	8
2.3 C4ALL	8
2.4 Internet Evidence Finder (IEF)	8
2.5 Griffeye Analyse	8
2.6 ACPO Good Practice Guidelines.....	8
2.7 Guidelines for OLAF Staff (EU).....	9
2.8 ISO 27001 Information security management	9
2.9 27037 [2] Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence	9
2.10 ISO/IEC 17025 [1] General requirements for the competence of testing and calibration laboratories.....	11
2.11 Forensic Science Regulator Codes of Practice and conduct issue 3, February 2016	12
2.12 Conclusions from background resources.....	13
3. Approach.....	14
3.1 Mapping ISO 17025 [1]	14
3.2 Proficiency Testing	14
3.2.1 Initial Scenarios for Raw Images.....	16
3.2.2 Justification of Image Scenario's	16
3.3 Training Quality of the Analyst	17
3.4 Outline Structure of how to conduct testing using ISO 17025 [1]	17
4. Implementation.....	18
4.1 Mapping ISO 17025 [1]:	18
4.2 Creating Finalised Digital Images	20
4.2.1 Setting up the Samples:.....	21
4.2.2 Persona for Scenario 1:.....	21
4.2.3 Conventional Hard Drive Scenario:.....	21
4.2.5 USB scenario:.....	22
4.2.6 Questions for Scenario 1:.....	22
4.2.7 Answers for Scenario 1:	23

4.2.8 Persona for scenario 2:	23
4.2.9 SSD Scenario:.....	23
4.2.9.1 Content of SSD:.....	23
4.2.10 DVD Scenario:	24
4.2.11 Questionnaire for Scenario 2:.....	24
4.2.12 Answers for Scenario 2:	24
4.3 Forensic Tool Proficiency Testing.....	26
4.3.1 Encase v8.02.01 Tests.....	26
4.3.3 AXIOM Examine v1.0.11.4067 (IEF included) Tests	68
4.3.4 Griffeye v17.0 Tests.....	84
4.3.5 C4All Test	97
4.4 Procedure to meet the needs of ISO 17025 [1]	98
5. Results and Evaluation	99
6. Future Work.....	103
7. Conclusions	104
8. Reflection and Learning.....	106
9. Glossary	108
10. Appendix.....	109
10.1 Diary of Gantt chart	109
11. References.....	114

1. Introduction

The problem I will be aiming to solve is that with the enforcement of ISO 17025 "General requirements for the competence of testing and calibration laboratories" (ISO/IEC 17025 [1]) will mean that digital forensic tools that have always been used now need to have proficiency testing conducted on them and the laboratory methods that are used will need to be validated otherwise they won't meet the requirements of this ISO, and if they can't get accreditation from this ISO standard then forensic analysts will have to state this in a coversheet in their reports that the tools and methods they have been used are not backed up by scientific results and haven't been validated, this can immediately cast doubt on the evidence that they will present in court. ISO17025 [1] was published in 2005 and is only now being enforced onto digital forensic laboratories because there is no accreditation needed for people to set themselves up as "digital forensic specialists" in the UK, meaning that there are currently under qualified people dealing with digital forensics that are not moderated and hopefully with this ISO being enforced will make the field of digital forensics more creditable. The approach I intend to take for this project will be to look at the current standards and guidelines that are in place such as ISO 27037 (ISO/IEC 27037 [2]) which covers the overall procedures of conducting a digital investigation and then I will focus on the main guidelines that have been adopted by the police inside Europe such as ACPO Good Practice Guidelines (DAC Janet Williams QPM, ACPO [4]), from there I will be able to work out how an investigation should be carried out and what methods forensic analysts currently have to abide by.

With this knowledge, I will use ISO 17025 [1] to work out how it will change or evolve the current procedures for carrying out a case from the beginning to the end of an investigation. I will also be conducting proficiency tests on selected tools that are used daily by the South Wales Police to help them meet the accreditation for the testing of tools within ISO 17025 [1] so that they can use my test results to prove that the forensics tools that they use have been thoroughly tested, and to say that if anyone with forensics expertise using the same tools that were used in my tests on the same data images that I will produce should find the same/similar results. From the tests that will be conducted I want to make an overall procedure for being able to test digital forensic tools so that others can follow on from my research and so they can conduct their own scientific tests from a similar foundation.

1.1 Intended Project Audience and Beneficiaries

The test results from this project will assist Gwent Police's in getting their accreditation for ISO 17025 [1]. These results will be added to the work that they have already completed in validating the forensic equipment that they use and be presented in the form of Inter-laboratory testing. My Work from this project will hopefully go towards helping other police forces navigate ISO 17025 [1] accreditation.

1.2 Project Scope

The main scope of this project is to focus research around ISO 17025 [1] that looks at General requirements for the competence of testing and calibration laboratories this ISO is set to be enforced as of October 2017 in the United Kingdom, and with this enforcement I intend to help provide useful research for local police forces to use to meet the requirements of this ISO before the deadline. This project scope has changed from the initial plan as the amount of research that needed to be done

around all the aspects described in that first plan would have been too ambitious to fit into my timescale so I have decided to narrow it to try and get a more detailed focus at this specific ISO as supposed to a shallow view of many standards. I will be working with Gwent police to help narrow the sorts of tools that they use frequently to help focus the testing I will conduct and cover the most common devices that they recover from a crime scenes to help assist in making the proficiency testing as useful and realistic as possible for them.

1.3 Project Aims and Objectives

Primary Aims and Objectives:

Mapping ISO 17025 to currently used guidelines – I will look at the current policies that European digital forensic police departments use to conduct their investigations and I will show how ISO 17025 [1] links to these guidelines and what will be expected to be achieved to make sure that laboratories adhere to this ISO standard.

Proficiency Testing of Frequently Used tools – I will get together frequently used tools by the Welsh Police force and following ISO 17025 [1] I will make digital images that will be put onto clean devices. Then I will test what evidence I can find using the forensic tools that the police force will have specified and then hand the images over to the police for them to conduct the same tests to see if we have same or similar results using the tools that they have recommended.

Training Digital Forensic Analysts – From the images that will be made I will make questionnaires that will range from easy questions on how to identify the hash of that given device to harder questions on how you would find certain deleted information. These questions will be aimed at digital Forensic Analysts that have had 2-3 years' experience

Outline Structure of how to conduct testing using ISO 17025 – I will write a procedure on how to conduct a proficiency tests using this ISO with the goal of outlining a clear structure of how I conducted my tests on digital forensic tools with the aim of this structure being adopted by others to test other forensic tools in the future.

2. Background

In this section of the report I will give an outline of the main points on all the resources that have been collected, to provide you with the context and understanding of the project I am undertaking and to give incite for anyone to the struggles that must be overcome to solve the problems that I intend to achieve at the end of this project.

2.1 Initial Meeting with Gwent Police

On the 10th February 2017, I met with three members of the Gwent Police force. two of the members were forensics analysts and one was the quality manager for the division; the meeting was set up by my supervisor Michael Daley and the main topic of the meeting was ISO 17025 (ISO/IEC 17025:2005 [1]) which is soon to be enforced by the digital forensics division and the meeting was to see how my project could help them to achieve the integration of this ISO into their current way of practice and to provide me with invaluable information on how their current procedures work in practice.

From my discussion with them it became clear that making a list of recommended tools that I would test would not be as useful to produce as they mentioned having many certificates from the manufacturers stating that these leading tools have been tested thoroughly and that all their features work as expected, but they did need me to test some tools for them but not to verify if features worked from these tools but to see if when independent data is produced for these tools that they should be able to find this data and have the same results when they carry out their own tests on these same images. They narrowed down their daily forensic tools to four tools that they use on nearly every investigation; these tools are Encase, C4All, Internet Evidence Finder (IEF) and Griffeye. They want this data and information to be generated to help them have an inter-laboratory testing of the tools that they use and to make sure they meet their targets for accreditation with ISO 17025 (ISO/IEC 17025:2005 [1]). With this data, they can then back up the forensic tools they use with scientific evidence. It was agreed that they would need images made on clean devices and that the scenarios and evidence to be produced on these devices should be aimed at a forensic analyst who has at least 2-3 years' experience and the best way to document the findings of the test would be in the form of a type of questionnaire that would be split into sections that ranged in difficulty from easy, medium and hard, that way a forensic analyst with only a few years of experience should be able to document and report things from the device from the easy and medium sections and still collect all the needed evidence to build a case against a suspect but the hard section would challenge them to find more concrete evidence that would only improve their case against the suspect while making it difficult to find the data needed.

The meeting confirmed a few assumptions I had about how they acquire devices from crime scenes and especially with the increasing number of devices people own in the emerging era of the Internet of Things it would be unnecessary to collect every possible device and would only make it more difficult to extract the relevant data by being buried under the masses of irrelevant data that we all generate. The meeting with the police was invaluable as it gave me a more practical view of the world of forensics that would not have been possible through the sources I had read about in theory and it also helped to narrow down my field of study.

2.2 Encase

This is one of the oldest forensic tools out there that was created by guidance software in 1998 (Guidance Software [8]). Encase features cover the complete processing and extraction of data from the file system and once that's done it has built in filters to be able to narrow down the evidence you are looking for. In recent years, it has added in more modularity functions to give analyst the ability to write their own scripts that can be integrated into the core system of Encase and they call these scripts "En-scripts".

2.3 C4ALL

Categorizer for all is a tool that takes images and videos that have been flagged in another tool such as Encase, it can then export and analyse these files against a database of indecent images or videos so that it can categorize the severity of each media file in relation to the current investigation (C4All [9]).

2.4 Internet Evidence Finder (IEF)

IEF is a tool that was created by the Magnet Forensic (Magnet Forensic [10]) that's aimed at extracting all the possible information from internet files and their respective artefacts to then present them in a user-friendly way so that analysts can filter the search engine results and browser history to build the evidence for their case. IEF is better equipped than a program like Encase at presenting browser history and is what the police use instead of solely relying on Encase to get all their meaningful data.

2.5 Griffeye Analyse

This tool specializes in analysis of media files as it allows for instant frame by frame playback on video files, which can then be flagged for further inspection. It boasts a wide range of filters that can be applied to the raw image file with the most notable of them being the nudity filter which breaks down images into percentage of nudity found in those folders to assist analysts in being able to find indecent images (Griffeye [11]).

2.6 ACPO Good Practice Guidelines

ACPO follows 4 main principles that I will paraphrase and outline below:

Principle 1: No actions taken by police officers or people employed by the police force should change any data that will be needed in court.

Principle 2: If a person needs to have access to the original image of the data, that person must be experienced and competent in carrying out that task and be able to explain why it was necessary to do so.

Principle 3: All actions taken in the investigation should be documented so that it can be stored and replicated by an independent third party if needed.

Principle 4: The person in charge of the investigation must enforce the law and these principles

ACPO covers details about what devices you should capture data from, by selecting the most relevant devices that would have the best evidence to extract data from, for example collecting a suspect's personal computer would have more relevant data

than trying to collect information from a family shared computer that might only have a fraction of the useful data needed to build evidence of the crime. When conducting an acquisition of the devices you want to capture data from, it makes mention of using “trusted tools” (ACPO, Live forensics approach, p.26 [4]). This is where the policies would change under ISO 17025 [1] because where in ACPO guidelines it mentions “trusted” tools which will be brought under scrutiny of what a trusted tool can be in this new ISO unless laboratories can prove that these tools are trusted with proper accreditation to back it up when ISO 17025 [1] is installed. There are also procedures outlined on how things should be documented and what rules need be followed when writing your report (ACPO, Data Reporting, p.38 [4]).

2.7 Guidelines for OLAF Staff (EU)

These guidelines concentrate around having high security standards for a forensic laboratory and go into more details about having procedures in place to protect acquired data by producing back-ups that will be held in different locations to mitigate against any kind of loss or contamination of the original image (Article 8, 8.1, [5]). The general investigation and collection of data guidelines that are followed by police forces within the EU are the same as the ACPO Good Practice Guidelines as they have adopted the 4 main principles as a base to follow and use that alongside ISO 27037 [2] to conduct their digital forensic investigations. (Introduction, Paragraph 3 [5])

2.8 ISO 27001 Information security management

This ISO looks at how information should be handled when collected and stored by an organisation. Some of the content mentioned in this ISO already seems to have been adopted by the OLAF guidelines in terms of how to mitigate against the loss of data. This is done by producing secure encrypted back-ups to the data that has been collected and making sure that access to the data is monitored and made secure to reduce any accidental or intentional changes to the information. It also mentions the need to make sure that average users should be provided with training to help understand the data that they produce and how they can secure their own information. Getting certified in this ISO is important as it shows that the business/organisation have the willingness to protecting acquired data. This ISO is useful for Digital forensics because of the amount of data that needs to be collected for an investigation. The laboratory needs to make sure that the information on those devices are looked after and steps are taken to protect that information which could be laid dormant for several months or years depending upon the swiftness of the law courts. (ISO 27001:2013 [6])

2.9 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

This ISO outlines the main processes that must be carried out in a digital forensic investigation, from how to identify a crime has taken place, to being able to preserve the data at the end of the investigation to ensure the fullest integrity when it is presented in a court of law. It also clearly states that it should be used as a guide and understands that things may change when it comes to how laws are applied in different countries around the world and that it doesn't supersede that law. It

provides formal definitions for the four main processes of any given digital investigation (Mapping the Forensic Standard ISO/IEC 27037, p.11-12 [3]):

- Identification is the “process involving the search for, recognition and documentation of potential digital evidence”
- Collection is the “process of gathering items that contain potential digital evidence”
- Acquisition is the “process of creating a copy of data within a defined set”
- Preservation is the “process to maintain and safeguard the integrity and /or original condition of potential digital evidence”

From these four main sections of an investigation the main areas of this ISO are around the collection and acquisition of the evidence, as these areas build up most of the digital evidence that will be used to create a case against the suspect. It goes into more detail about how every piece of evidence needs to be put onto clean devices to ensure that no residual data were left behind from a previous use of that device and to minimize contamination of the evidence. Along with this making sure all these clean devices are hashed and maintain a chain of custody once the evidence has been collected through a bit by bit image to help document and know who is accessing which piece of information and why. From this it says that the processes used must be well understood, defensible and well documented as to make sure the case is coherent and can justify its actions. When it comes to analysing the data collected and trying to acquire the evidence from these devices this ISO sets some parameters to make sure that tests conducted on this data to carve/filter it should be repeatable to ensure that another investigator can perform the same tests “using the same measurement procedures and method using the same instrument under the same conditions and can be repeated at any time after the original test” and also asks for it to be reproducible if they use “the same measurement method but different instruments and under different conditions” (Mapping the Forensic Standard ISO/IEC 27037, p.14 [3]) they should be able to get similar results and all actions should be able to be justified as to why they were conducted on all actions and methods used in the investigation and that final part is pretty much the same as the 2nd principle of the ACPO guidelines.

When it comes to the preservation of evidence this ISO outlines the need for strict access to the evidence to help protect the items from accidental or deliberate modification and covers general rules to take into account such things as making sure to minimize handling of data to ensure that it doesn't become contaminated and to ensure that changes are accounted for by documenting everything and to prevent analysts from taking actions that are beyond their competence or understanding, as well as having appropriate environmental controls for the physical evidence because once the evidence is collected and the report written the case could remain dormant for a long time before it reaches the law courts. Once the case has been concluded analysts must be sure that their report and processes used are all audited thoroughly just in case an independent assessor needs to evaluate the activities performed by that analyst/first responder (ISO/IEC 27037:2012, [2]).

2.10 ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

This ISO was written to work within a laboratory that revolves around more of the hard sciences such as biology and chemistry and makes many references towards meeting the needs of the customer or client so much of the context of the procedures that it has in place must be adapted for a digital forensic environment. This ISO covers many procedures on how documentation must be made for every process of testing (ISO/IEC 17025, p.24, Section 5.6.2.2 [1]) from the tools being used, any changes or issues that need to be assessed in the documentation (ISO/IEC 17025, p.10, Section 4.3.2 [1]), what were their findings and general lab conditions (ISO/IEC 17025, p.8, Section 4.1.5 [1]). This ISO also introduces a new role that needs to be assigned which is that of being a quality manager who can have the ability to change procedures if they are not working efficiently within the workplace and being able to have access to the highest forms of management within the organisation so that they can be kept informed and work to better improve the quality of their division with these procedures. They also have responsibility for running scheduled audits of the procedures outlined in this ISO to make sure that they are up to standard. The tools and procedures need to have proficiency testing to reinforce that they are working and that these results can be repeatable by an independent agency if needed. Because of the possible research and data being collected by this ISO it covers what should be done in terms of storing the data and protecting the client's information but for the police most of those procedures are already in place with the Data Protection Act (Data Protection Act, 1998 [13])

This ISO also covers what to do when computers are used for the acquisition, processing, recording, reporting, storage or retrieval of test or calibration data and then the laboratory must ensure that:

- The computer software developed by the user is documented in sufficient detail and is suitably validated as being adequate for use
- Procedures are established and implemented for protecting the data; such procedures shall include but not be limited to the integrity and confidentiality of data entry or collection, data storage, data transmission and data processing
- Computers and automated equipment are maintained to ensure properly functioning and are provided with the environmental and operating conditions necessary to maintain the integrity of the test and calibration data

From these point's, I can see that interpretation in order to focus it towards digital forensics can be difficult as most of the ISO states "if" you are using a computerised system where as with digital forensics it is exclusively a computerised approach and as for the first point it makes about the "software developed by the user" that would be through companies such as Guidance Software who create the forensic tool "Encase" (Guidance Software [8]) and they provide certificates to validate their products. Their next section on making sure to protect the data is already of the utmost importance to a digital investigator to minimize contamination of the evidence that they collect through write blockers.

2.11 Forensic Science Regulator Codes of Practice and conduct issue 3, February 2016

This document covers the police interpretation of ISO 17025 [1] and aims to try and help integrate changes in the way forensics in police departments carry out their everyday tasks. This document looks at digital forensics, forensic pathology, toxicology and many more areas as these are the departments that will be affected by the introduction of this ISO. As I have already outlined the contents of ISO 17025 [1] previously in the background section I will only briefly mention some areas where the police have gone into more detail about how it will fit in with this ISO. They make mention of document control and making sure to handle information correctly with a set time to dispose of this information/documents in an appropriate manner e.g. shredding/incinerating. Documents and reports need to be written in a way to allow anyone with the expertise in that field to be able to pick and understand how that report was carried out and can be replicated without the need for the original practitioner. When it comes to the training of individuals, procedures need to be put in place to keep documentation of each expert's qualifications and to make sure that these are kept up to date to ensure that experts remain competent to carry out tasks within their own field. This document's interpretation of lab conditions is much the same as mentioned in my reading of ISO 17025 [1] (Forensic Science Regulator [7]).

The most detailed section of this document's codes of practice comes in with what needs to be done to carry out a validation procedure; these are the list of things needed to validate a procedure where relevant to the situation:

- Determine end user requirements and specification
- Risk assessment
- Review of the end user requirements
- Acceptance criteria
- Validation plan
- Outcome of validation exercise
- Assessment of acceptance criteria compliance
- Validation report
- Statement of validation completion
- Implementation plan

all of this is what takes place when producing a new procedure to follow and in terms of my project the area that is most important to me is the validation plan, this goes into more detail of validation testing (Forensic Science Regulator, p.30 , Section 20.7.3 [7]) and states "the validation shall be carried out using simulated casework material in the first instance and subsequently where possible permitted and appropriate with actual casework material to confirm its robustness" so this shows the need for me to produce digital images to make sure that tools are validated in accordance with ISO 17025 [1] and the other notable section of this document is validation of interpretive methods (Forensic Science Regulator, p.31, Section 20.9.1 [7]) and it says to "demonstrate that they can provide consistent reproducible , valid and reliable results that are compatible with the results of other competent staff" and then lists four different ways tests can be carried out by people but the one relevant for this project is "Participating in inter-laboratory comparisons(Forensic Science Regulator, p.32 [7])" as tests will be conducted within Cardiff University to prove the validity of digital forensic tools and the research and results will then be taken by

Gwent police to help go towards getting their accreditation for ISO 17025 [1] (ISO/IEC 17025 [1]).

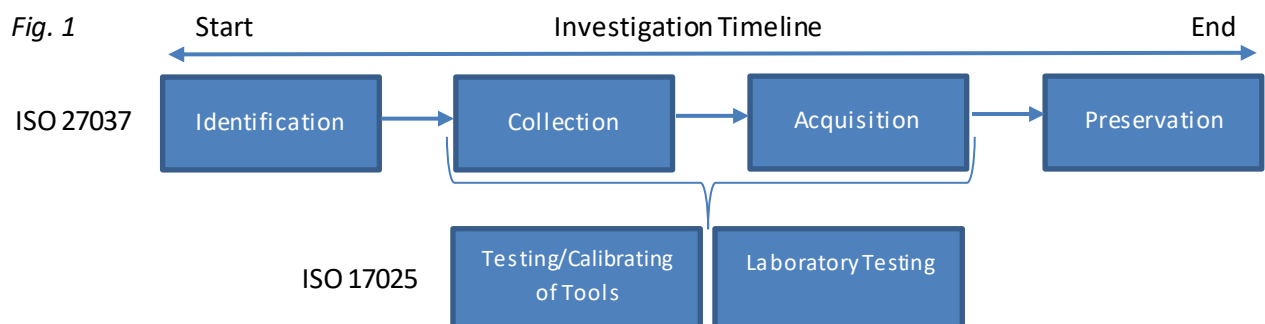
2.12 Conclusions from background resources

From the background sources that I have collected and outlined it is obvious that there is a lot of overlap between different standards and guidelines on how to run an investigation, from ACPOs focus around their 4 main principles to conduct a case to how those have had to be generalised in ISO 27037 [2] to make sure that it doesn't obstruct the way some police forces conduct their investigations around the world. Having also read Forensics Science regulators codes of practice and conduct it gave me a better understanding of the impact that ISO 17025 [1] will have on all fields of forensics within the police and will be invaluable to assisting me in achieving the requirements for ISO 17025 [1]. My focus for this project is to conduct proficiency tests on forensic tools to help validate them, a constraint to this task will be obtaining the forensic tools that have been mentioned by the police as most of them are licenced towards law enforcement with no straight access for academia but Gwent police should hopefully assist in all problems that may arise. If all the tools are obtained then the only other constraint to this part of the project will be my competence at using the tools they have outlined because most of them are new to me so I will be leaning on guides and forums to assist me in navigating the tools that needed to be tested. From the background resources that have been collected it is obvious that I should be looking in more detail on how the collection and acquisition of evidence is performed and what level of testing needs to be conducted in these areas to ensure the tools used by the investigators and the condition of their labs are tested in conditions expected to meet ISO 17025 [1]. Once I have built the images that will be tested I will also follow the procedures stated in ISO 27037 [2] to make sure that my tests and images are carried out in the same manner as a professional digital forensic analyst would be expecting to obtain with no contamination of evidence.

3. Approach

3.1 Mapping ISO 17025

I will take the research that I have gathered in the background section of my report and produce a clear diagram from the start to the end of an investigation and then I'll outline where ISO 17025 [1] will be used and what additions or changes it will make to the way an investigation had been conducted before police forces needed to meet the specifications of this ISO, I will also draw out a table comparing where ISO 17025 [1] will be applying changes compared to the current guidelines that are followed and what documentation needs to be considered. From this approach, I should be able to build a good foundation of what aspects need to be considered for me to help assist police in tailoring my results towards this ISO, with the intention of giving another interpretation of this ISO with un-bias test results.



In figure 1 I have outlined the main sections of ISO 27037 [2] and ISO 17025 [1]. From this diagram, it shows the four sections that will be carried out in a forensic investigation following ISO 27037 [2] and I've highlighted the areas of ISO 17025 [1] that will be integrated into the everyday tasks of a forensic analyst so my concentration will need to be around the collection of evidence which will involve the raw images I intend to create for collection. Acquisition of the evidence will be the inter-laboratory testing of the forensic tools and making sure that these proficiency tests are conducted in as fair an environment as possible that a forensic analyst would have access to.

3.2 Proficiency Testing

From my discussion with the police it became apparent the sorts of tools that they use daily and what devices that they typically extract data from. They have provided me with a list of devices and content they expect to find in the raw images that will be producing for inter-laboratory testing, these Devices are:

- Conventional Hard Disk Drives
- Solid State Drives
- Compact Disk
- DVD
- USB
- Memory card
- Mobile phone (not Smart Phone)

The Content Expected to be found in general on most of these devices are:

- Images - Live
- Images - Deleted
- Videos - Live
- Videos - Deleted
- Internet History
- Documents e.g. Word, Excel, and PDF etc.
- Chat
- Windows Metadata e.g. Bios, Registry etc.
- Cloud e.g. Dropbox (if possible)
- Email e.g. Outlook
- Social Networking e.g. Facebook
- File Sharing
- Webmail e.g. Gmail

Additional Content for some of the Devices:

- Some Hidden areas (HPA and DCO)
- Some hidden files
- Some deleted files
- Some encrypted data

To help assist in the making of these images I will write up initial scenarios for the content on each device so that I will have a rough structure of what content needs to be included and these scenarios will help to provide context as to what evidence a forensic analyst should be looking to document when viewing these images, most scenarios obviously cannot do anything illegal but to make them authentic for analysts to view they have to be based around hiding documents and media that are either explicit or can be seen as illegal when posed in a scenario as these are the types of cases that a digital forensic analyst has to deal with on a daily basis.

The tools that will be tested are Encase, IEF, C4All and Griffeye and most of these tools are for law enforcement but I should have access to them through Gwent police who can provide this software to the forensics labs at Cardiff University, the only tool that might be subject to change is Griffeye as that is strict on the licencing and is only normally allowed for the police and I may not be granted access to it.

A possible approach for the raw images could be to create them inside a virtual machine and then populating the data produced in these machines onto clean devices that will be provided by Gwent Police, another method could be to produce these images on physical devices that might be accessible from the forensic department in Cardiff university but that would also have the constraint of needing access to the labs for long hours as these devices are populated and then imaged. I have looked at programs like forGE (Hannuvisiti, Forensic test image generator [12]) that attempts to dynamically hide files within a file system in a variety of methods such as alternate data streams and steganography, I will try exploring other possible methods to dynamically create the forensic scenarios that I want to populate on these devices as this could save me a lot of time in the labs or at home depending on which approach I end up choosing when it comes to generating the raw images for each device.

To begin imaging I will start with a standard conventional hard disk drive and other smaller devices such as a memory card, DVDs and USBs to put images on first as I

am most comfortable with these devices and then with time permitting I will produce digital images for an SSD and mobile device, with the mobile phone being lowest on my priority as I am very unfamiliar with mobile forensics and unsure what additional data can be extracted from that type of device apart from incoming/outgoing phone calls and text message threads.

3.2.1 Initial Scenarios for Raw Images

Scenario 1:

An initial scenario involving the trafficking of a type of animal from one country to another. The evidence for this type of image could be hidden media files documenting the range of animals that the suspect is trying to sell and documentation of those animals possibly in the form of a spreadsheet of payments for the suspect to keep track of what they have been purchasing and selling.

Scenario 2:

Another scenario that might be possible for the raw images could be money laundering. The evidence for this would be a series of documents that are hidden/encrypted and point towards how much money the suspect has been laundering and where they have been concealing the money. With possible correspondence between them and another person via email and could show that it goes further than this original suspect.

Scenario 3:

A scenario that is just a standard user who's just trying to hide explicit images on their computer. The evidence for this would just been different forms of media that the user has tried to hide/encrypt on their machine in various locations as to believe that these images would not be found with a search of their device. An additional facet to this scenario could be the case of sharing explicit images via emails or by more secure transfer means and the evidence for this would be hidden in the networking traffic that would be taken from the live machine.

Scenario 4:

The last scenario that would be feasible to work in a forensic image would be a collection of torrent files that would be marked as explicit so that the analyst knows what they need to be looking for this type of file. The evidence for this image would be the torrent files that the user doesn't want to be found along with other documents/emails that point towards the user conversing with other people in a shared peer to peer connection to enforce that this person is the distributor of these files.

3.2.2 Justification of Image Scenario's

Looking at the rough scenarios that I have outlined I think some of them are a bit too ambitious in terms of the amount of content that would need to be placed to populate the device and provide evidence without making it too obvious to find, for example the money laundering scenario would need a lot of information and spreadsheets generated to find the evidence but would be difficult to generate enough trivial documents to hide that evidence among them. Some of the evidence that was thought of in the initial scenarios would go beyond the capabilities of the forensic

tools that need to be tested, for example the networking traffic would be an addition that could not be tested by the forensic tools that the police have chosen so for the moment that should be suspended unless more content for training the analyst would be needed. Having looked closer at the features that the forensic equipment could manage I think leaning towards scenarios that involve heavy amounts of media would play towards the strength of the tools that will be tested but also allow for more thorough proficiency testing to be conducted as more of features could be covered. So that is why I would choose scenario 1 and scenario 3 as these two have the most media content to be introduced and the devices that the police have chosen could be combined into one scenario that would spread out the evidence that they would be looking for.

3.3 Training Quality of the Analyst

From the raw data images that will be created from the devices I will produce a questionnaire for each device outlined in the proficiency testing that is intended to help train future digital analysts who have about 2-3 years' experience on how to use these tools effectively and to help continue to support the inter-laboratory testing on these tools. The intention is to make a questionnaire that contains about 15 questions at most, ranging from easy to hard on the content they need to find inside these devices. I decided on 15 questions initially to have an even split of 5 easy, 5 medium, and 5 hard questions but I can see this possibly changing in my outcome depending on the content that is on the devices and the need to challenge the analysts in the hard questions but also making sure that if they have answered the easy and medium questions correctly then they should be able to get enough evidence to build a strong case. The hard questions are there to really challenge the analysts and are not expected to be completed correctly by everyone who undertakes these tests. I will make a few varying questions that I will get the Gwent Police to validate to make sure that they questions are challenging enough for analysts of that experience level. The questions difficulty will range from things like being able to identify the hash of that drive to then identify what environment this image was created in and possibly a question to make sure that the tools they are using find the same amount of data every time so that their results can be added to the proficiency tests already carried out on these tools to validate them further.

3.4 Outline Structure of how to conduct testing using ISO 17025

From the tests and questionnaires that will be made I intend to use these results as a basis to outline a general structure/procedure of the way proficiency tests were conducted on digital forensic tools to meet the requirements of this ISO in the hope that more testing can be conducted by other people into validating the large variety of tools that are out there and so it becomes a lot easier for people to have one structure to follow and build tests and results from a similar foundation.

I will aim to draw out a clear diagram of the testing process that I have conducted and write it up in more detailed clear steps of what should be expected to be done to test a forensic tool thoroughly to meet the requirements of ISO 17025 [1]. The end deliverable for this target will be a summary of the tasks that were conducted so that people can just read that to understand the specifications needed to conduct a fair test in the same way under similar or same conditions that the tests were run in without the need for people to read through this entire project report before they can get started with their tests

4. Implementation

4.1 Mapping ISO 17025:

Here I have taken the main areas of ISO 17025 [1] and I am going to go through all the relevant background resource material I collected and line it up with the current guidelines used by police forces to show where things will be new or adapted for digital forensic departments to become accredited through scientific practices.

ISO 17025 [1]	Current Digital Forensic Guidelines
Document Control (ref 4.3 [1])	ISO 27001 and ISO 27037 [2] cover these topics by stating how to manage evidence and the best ways to secure your documents
Review of requests, tenders and contracts (ref 4.4 [1])	ISO 27037 [2] covers procedures when areas of the investigation go beyond the boundaries of the police force and goes into detail about dealing with network contracts like an SLA or just search warrants
Subcontracting (ref 4.5 [1])	ACPO guidelines covers sub-contracting in terms of first responders or experts in a field that other members of the team are not competent in
Packaging and general chemicals and materials (section 4.6 [1])	ACPO guidelines outlines details making sure that forensic analysts use and have been provided with a useful first response kit that has all the equipment needed for extraction and packaging of the evidence
Complaints (ref 4.8 [1])	Through all the sources that I have covered in the background section none of them have any policies for dealing with complaints so this is a relatively new section that the ISO has introduced to be applied into digital forensics but I assume that being a sub-department of the police force means that this section falls under policies that are outlined in general for the whole police department
Control of non-conforming tests (ref 4.9 [1]) the lab will have a procedure for when they can't follow their current procedures	This is another new section that is to be brought in with ISO 17025 [1] as there has never been a focus for documenting non-conforming test in any of the other sources that I have covered, but in terms of digital forensics this would be a very positive procedure to enforce as anything involving technology moves quickly so having the flexibility to document new procedures as your tackling new problems is useful

Control of records (ref 4.13 [1])	ISO 27037 [2] covers processes around dealing with records for collection, storage, indexing and maintenance of quality and technical records as within the field of digital forensics it is of the utmost importance to maintain the chain of custody
Technical records (ref 4.13.2 [1])	ACPO goes into details on report writing and how it must make sure that steps taken in an investigation are written in a way to be presented in court to a laymen audience and to make sure the steps taken in the report are able to be replicated by other forensic experts in the field if needed
Internal audits (ref 4.14 [1]) Conduct internal audits on their procedures and activities periodically to a predetermined schedule to ensure they meet the needs of this ISO	ACPO covers areas of auditing cases, but the ISO puts more of a focus on audits being conducted frequently to increase the validity of tests and procedures within the laboratory rather than just auditing reports that have been made from past investigations
Technical requirements (ref 5.2 [1]) Training, Background checks, competence	This is new as none of the sources I have covered go into any detail on the constant training needed to be a forensic analyst, and it also has a focus on needing to make sure analysts qualification are kept at a consistently high level to remain competent within their field and the need for background checks must be covered in the more general employment policies of the police force.
Test methods and method validation (ref 5.4 [1])	This is another new area that is being introduced as tools have never needed to be validated in this way before so when conducting my tests, I need to make sure to follow aspects of areas outlined in this section of the ISO
Validation of methods (ref 5.4.5 [1])	This is a new area that the ISO has introduced, as most of the everyday processes that are conducted within the department now need to fit in with the way that validation has been structured within the ISO
Control of data (ref 5.4.7 [1])	OLAF guidelines and ISO 27001 cover areas on the control of data and making sure to protect the data that is integral to the case by setting up security procedures and multiple back-ups of the

	images obtained
Equipment (ref 5.5 [1])	OLAF guidelines talk about the lab conditions but doesn't go into detail on making sure that needed equipment is obtained for digital analysts
Handling of test items (ref 5.8 [1])	ACPO guidelines covers procedures on how to look after items to make sure they don't get contaminated, damaged or mislabelled when moving them from location to location
Assuring the quality of test results (ref 5.9 [1])	This is the main new area that's being enforced with this ISO that is important to this report, as testing has never been something that digital forensics has needed to do as all testing is conducted by the companies who manufacture the equipment/software. So, conducting your own proficiency tests on digital forensic tools has never needed to be done before
Reporting the results (ref 5.10 [1])	Much the same as the previous section this is new and just goes into details about making sure that when you report the results you fill out all the sections that they have outlined in the ISO when writing your report

From this table I can see that the new sections to focus around for this ISO are Control of non-conforming tests (ref 4.9 [1]), Technical requirements (ref 5.2 [1]), Test methods and method validation (ref 5.4 [1]), Validation of methods (ref 5.4.5 [1]), assuring the quality of test results (ref 5.9 [1]) and reporting the results (ref 5.10 [1]). These areas are the most impactful on the current structures in digital forensics and my focus is already aimed at running tests on the tools that get used within the Gwent police department so now I will make sure to conduct them in accordance with assuring the quality of test and calibration results (ref 5.9 [1]) and Validation of methods (ref 5.4.5 [1]) to make sure that I meet the requirements of this standard.

4.2 Creating Finalised Digital Images

In this section I will explain how the images were created and how they will be used for proficiency testing. I have taken the specification of content that the police usually find in a typical image and mapped what type of content I would put in each area and then after each scenario I have written up a questionnaire and answers for the evidence you would be expected to find.

These are the devices obtained from Gwent police:

500 Gb Hard drive

120 Gb SSD

64 Gb USB

Couple CDs and DVDs

Mobile Phone

The devices that will be imaged and tested in this report are the Hard drive, SSD, DVD and USB as I ran out of time to generate and image a mobile phone into the scenarios that have been finalised below.

4.2.1 Setting up the Samples:

To start building the images that would be used as samples in the testing four 500Gb Hard drives were digitally sterilized and then two of these drives were used to make the original digital scenario images that would be imaged onto the police's Hard drive and SSD. It was done in this way as a precaution in case anything went wrong when working on the obtained devices. I then proceeded to make multiple scenarios for these devices as these images would be serving two purposes by the end of this project, one being samples that would be used to test the validity of the forensic tools outlined and secondly as possible training images for future forensic analyst to use when learning how to use said forensic tools. To make the scenarios seem as authentic as possible I made personas so that no matter what situation that was finalised I would have an idea of what this person would do and it made outlining the scenario's a lot easier.

4.2.2 Persona for Scenario 1:

Aaron loves collecting animals and pets, he is 28, he has a typical 9 to 5 job repairing computers and barely makes enough money to satisfy his need for collection creatures, his hobbies include watching his favourite football team Everton, and getting out into the fresh air when he goes hiking. To try and solve his money issues he has taken time to become an animal breeder but the animals he breeds are illegal to own within the United Kingdom as that's where the most money is for him to make. By importing and trafficking Bears into the UK.

4.2.3 Conventional Hard Drive Scenario:

The suspect you are investigating is suspected of smuggling exotic animals from America into the UK a Hard drive and USB have been recovered from the residence of the suspect and a dd image has been taken and copied onto a clean 500Gb hard drive and 64Gb USB you'll need to find evidence of Bears on their system.

4.2.3.1 Content of the Hard Drive Image:

Live images – football pictures, Landscape pictures for hiking, pet images and some computing images from Work

Deleted Images – old landscape pictures, Stock Images and 2 Bear pictures

Videos Live –videos of landscapes/hiking, videos of animals and videos of exploring scenery

Videos Deleted – 3 Bear Videos

Documents – Spreadsheets for managing Money, wish list of Presents for him/others, password hint in a text file (Alternate Data Stream), PC parts list and setup guides for software/hardware

Internet Search History: Location to hike, looking up tickets for an Everton match, general pc troubleshooting problems and Private Browser Searches for how to buy Bears

Hidden and Encrypted Folder in Pictures: Containing 5 pictures of bears

HPA: 10 Bear Pictures

VM: 10 Bear Pictures, Finance Spreadsheet for selling bears and partition encrypted with Everton as password

Emails: Yahoo Account to set up a drop box to store files

Dropbox: Contains a back-up of all the contents in the documents

Torrents: ISO of Linux OS torrent for the Virtual machine

Alternate data stream: password hint.txt: Actual Hint.txt

4.2.5 USB scenario:

To fit in with the persona laid out for this scenario I thought it would be useful to make the USB image a tool that was used in his job as a computer technician and has some tools that may hint towards files being hidden within the hard drive and adds more to the profile that this suspect knows his way around computers.

4.2.5.1 Content of the USB:

Live Images: Computing and networking pictures of possible past systems they worked on

Documents: Old School IT work and Networking assignment/Guides

Software installers: executable files for Virus software and VM Software

Digital tools: SD Burner Tool, HPA Creation Tool

4.2.6 Questions for Scenario 1:

1. What type of file system is the hard drive dd image?
2. Is there anything that points towards a HPA?
3. Is there any evidence in their search history?
4. What type of browser was the suspect using to conduct these searches?
5. Were there any unusual file types that point towards more on the system?
6. Have you noticed any additional partitions that might contain information?
7. Are there any files that are hiding more information in a non-conventional means?
8. Where were the image and media files found?
9. How did the user try to cover up the images?
10. Can you decrypt the files?
11. Can you recover any documents that point towards the user smuggling/purchasing these animals?
12. What are their capabilities at using a computer?

4.2.7 Answers for Scenario 1:

1. It is a NTFS file system as used by windows operating systems
2. The ATA Tool found on the USB points towards a HPA as well as the Hard drive being a wrong size to the one it was advertised as
3. The Suspect tries to find how to "Sell bears"
4. The browser was in Private/incognito mode in the users attempt for the system not to log its details
5. The user has a torrent for a Linux based operating system
6. The HPA you should have noticed by now and additional partition for the Virtual machine
7. The password hint.txt has an unusual alternate data stream hidden behind it that gives you the actual hint to the password that is on the encrypted VM partition
8. The pictures are found in the pictures folder, videos folder (once recovered from being deleted), 2 bear pictures were deleted and removed from the recycle bin, 10 bear pictures can be found in HPA and 10 bear pictures can be found in the Virtual machine if you have gained access to it
9. The files were deleted, hidden, encrypted or stored in the HPA
10. The files use the base Microsoft encryption from windows 7 professional and forensic tools should be able to recover these files
11. If access to the virtual machine is gained then you can find a spreadsheet in the documents that lists pricing of different types of bear
12. This user is clearly experienced with computers as it evident with the addition of a virtual machine in the system and a HPA on the drive

4.2.8 Persona for scenario 2:

Bill is 26 years old, likes consuming all types of media as quickly as possible as most people of his generation do, his evenings are spent watching videos on YouTube and Twitch, he likes playing videos games and keeping up to date in social media. He has a job at a local supermarket and works Monday to Friday and spends weekends playing on his computer. His outward personality doesn't compare to his online one and he is hiding more of on his computer than he shows in his social media.

4.2.9 SSD Scenario:

A law has been passed in the UK that makes pictures of puppies illegal to have and if you are found in the possession 16 or more images of puppies then this is a serious crime. An SSD and DVD have been recovered from the suspect and dd images have been made and put on to clean devices. Your job will be to find at least 16 unique images of puppies

4.2.9.1 Content of SSD:

Live images – videos games/computers, stock windows images, images of pets, Movie backgrounds, Holiday pictures and pictures of food

Deleted Images - old animal pictures and old holiday pictures and food pictures

Hidden Folder: 5 Puppy Pictures

Encrypted and Hidden Folder: 12 puppy pictures

Encrypted and Deleted Folder: 3 puppy pictures

Videos Live –stock videos from windows, Holiday videos, videos exploring the countryside, videos of pets

Videos Deleted – old videos of landscape and animals

Documents – Wish list of video game, Documents of “To do lists”, old school work and backup file of encryption key from windows

Internet Search history: YouTube searches, twitch searches, social media searches and Private browser searches for puppies

Items are hidden at: (hidden and encrypted folders) (some are deleted)

C:/Program files/\$old Stuff (5 puppy pictures)

Pictures/\$stuff (3 pictures of puppies) Deleted)

Pictures/\$Things (12 puppy pictures)

4.2.10 DVD Scenario:

The persona for this suspect made them a lot less computer literate so their attempts to hide these images are very simplistic and when it came to populating the DVD I didn't see them being as obvious to hide things on a separate disc that could be found and accessed so easily so this image is more of a red herring of images, music and documents to look through than any actual evidence to be found on it

4.2.10.1 Content of the DVD:

Images Live: old design drawings and scanned images of old work

Music: video game type music and generic music

Documents: Old school work and general notes

4.2.11 Questionnaire for Scenario 2:

1. What type of file system is the SSD dd image?
2. Where were the images found?
3. How did the user try to cover them up?
4. Can you decrypt the files?
5. Were there any unusual file types that might help gain access to these files?
6. What are their capabilities at using a computer?
7. Is there any evidence in their search history?
8. What type of browser was the suspect using to conduct possible searches?
9. What are the users most frequented sites?

4.2.12 Answers for Scenario 2:

1. It is an NTFS file system that is typically from a windows operating system
2. Items are hidden at: (hidden and encrypted folders) (some are deleted):
C:/Program files/\$old Stuff (5 puppy pictures)

Pictures/\$stuff (3 pictures of puppies) Deleted)

Pictures/\$Things (12 puppy pictures)

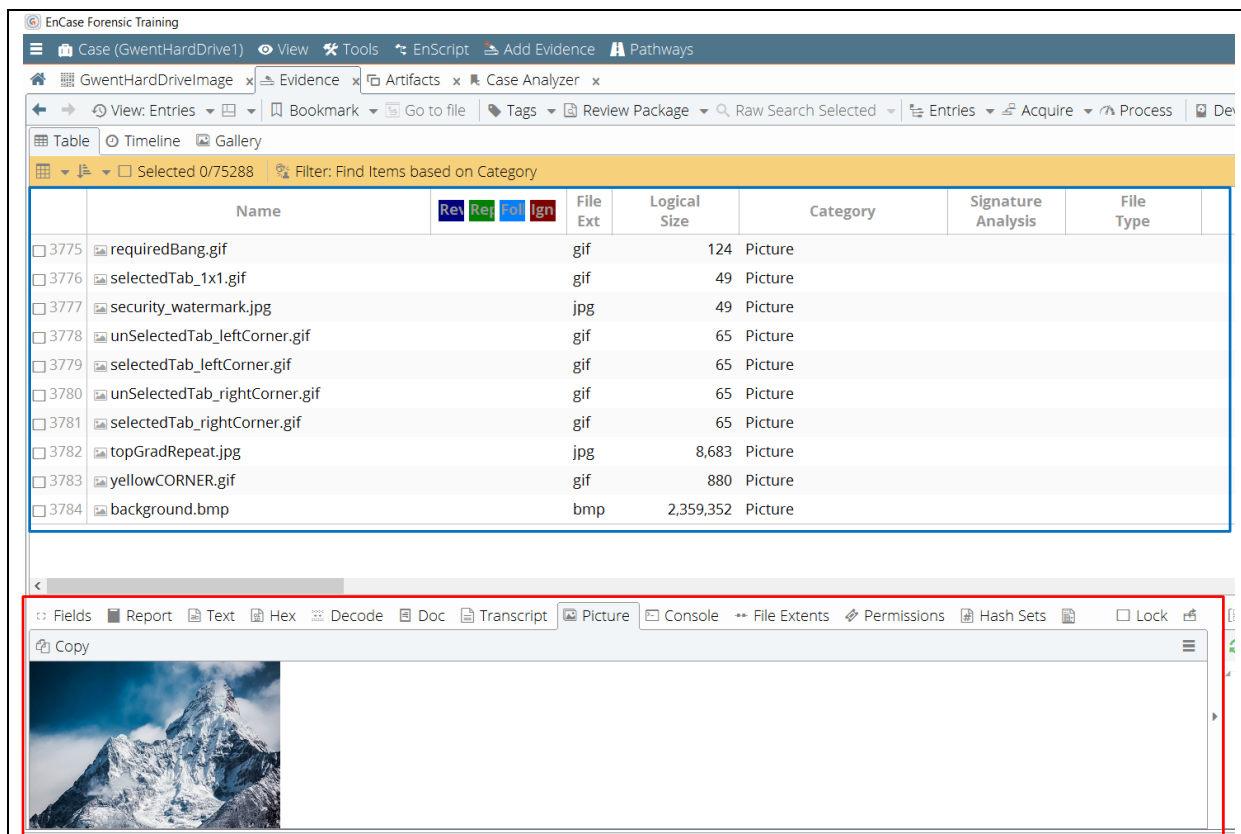
3. The files were deleted, Hidden and Encrypted
4. The files were encrypted with Microsoft standard encryption and a backup key is found in the documents if you find it otherwise forensic tools should be able to decrypt it
5. a backup key is found in the documents if you find it to help decrypt the files
6. very basic use as is evident with their attempts to hide the explicit images and use built in operating system encryption
7. The suspect searches for puppy pictures
8. The browser was in a private/incognito mode when they were searching for those images
9. Facebook, Twitter and YouTube

4.3 Forensic Tool Proficiency Testing

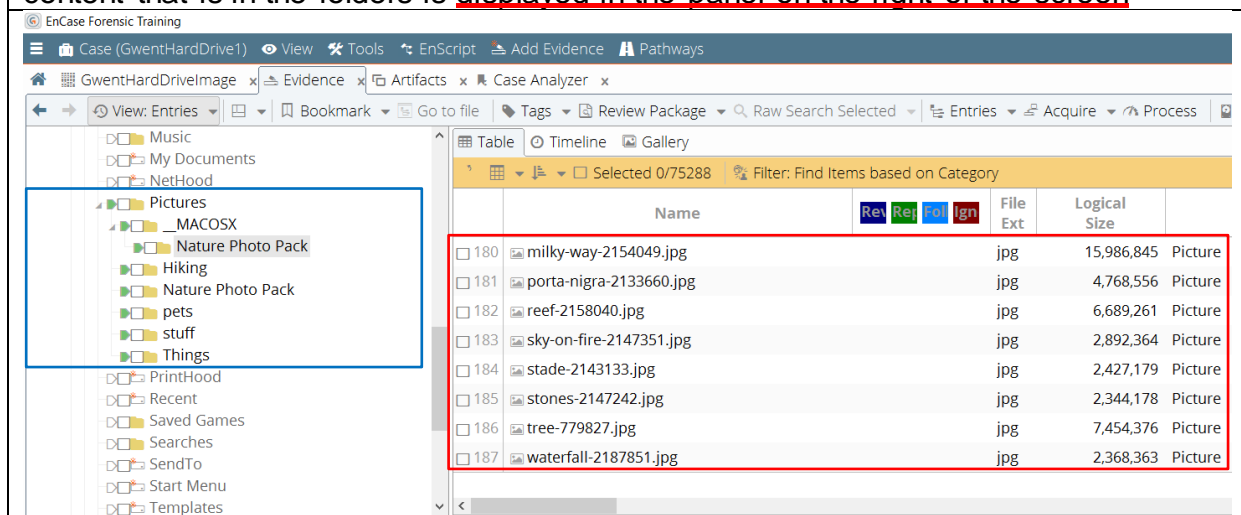
Now that I have moved onto testing the forensic tools, a few things have changed since my initial approach as some of the forensic tools have changed from what I expected such as IEF which is now incorporated into a bigger tool called AXIOM from Magnet Forensics (Magnet Forensics [10]) so I couldn't just get the base IEF software anymore as the company Magnet Forensics is pushing for only AXIOM to be an all-round tool that includes their IEF software. Another change that I found from testing was the C4ALL tool is more an add-on for Encase and when I tried to export my marked images to be categorized by C4ALL I couldn't get it working and it wouldn't give me access to the tool so I have abandoned tests from that tool and instead added in the forensic tool of FTK which works much in the same way as Encase does and these two tools are direct rivals of each other and for the sake of testing these tools I thought it would be useful to see the differences between what each one provides over the other. The Tests are laid out with a name, description, result and evidence of the result in the form of a screenshot with a detailed description of what is being displayed underneath with each important detail underlined in either blue, red or green with corresponding boxes highlighted on the actual screenshot proof.

Before going through the tests, I want to clarify that I am not trained in any of these tools and have only had limited experience in Encase and FTK, so some of the results of these tests might be different from what a trained analyst would find.

4.3.1 Encase v8.02.01 Tests		
Laboratory Location: Digital Forensic Laboratory Cardiff University Queens Building 5 The Parade, Roath, Cardiff CF24 3AA, UK		Tests Carried out on: 10/4/2017 Tested by: Ben Ajax-Lewis
4.3.1.1 Test for Convention Hard Drive (500Gb)		Drive Serial Number: W2ASSTVA
Test Name	Test Description	Result
Live Images	Does the tool find the bear pictures that are hidden along with the trivial stock images used to pad the digital image	Yes, encase can process and display all the live images from this device
This screenshot shows a small <u>section of all the live images</u> available from the device when I filtered them in encase, and the <u>bottom panel</u> has been set to preview one of the images from the many that are available on the drive		



This screenshot displays all the images live and deleted that can be found in the pictures folder and the structure on the left shows a green arrow that highlights the content that is in the folders is displayed in the panel on the right of the screen



Deleted files

Does the tool find all the deleted bear videos

Yes, but the way that it automatically recovers items didn't make it easy to filter just deleted items

This screenshot shows the folder of videos that were deleted when making the raw image and it has recovered them but not marked them as deleted as shown in the panel at the bottom

The screenshot shows the EnCase Acquisition interface. On the left, a file tree lists various folders including 'Videos'. The main pane displays a table of files:

	Name	Rev	Ref	Pol	Ign	File Ext	Logical Size	Cat
1	Bear2.mp4					mp4	16,402,658	Multimedia
2	Bear2.mp4-\$EFS						672	Unknown
3	Bear.mp4					mp4	5,194,721	Multimedia
4	Bear.mp4-\$EFS						672	Unknown
5	Bear1.mp4					mp4	49,119,038	Multimedia
6	Bear1.mp4-\$EFS						672	Unknown

Below the file list, the 'Fields' tab is active, showing details for the selected file:

Name	Value
Entropy	
Item Path	GwentHardDriveImage\Users\Aaron\Videos\More stuff\Bear2.mp4
True Path	GwentHardDrive1\GwentHardDriveImage\Users\Aaron\Videos\More stuff\Bear2.mp4
Description	File, Hidden, Archive, Encrypted
Is Deleted	

Videos Live	Are all the Live videos recovered containing sweeping landscapes	Yes, this tool displays all expected media files
-------------	--	--

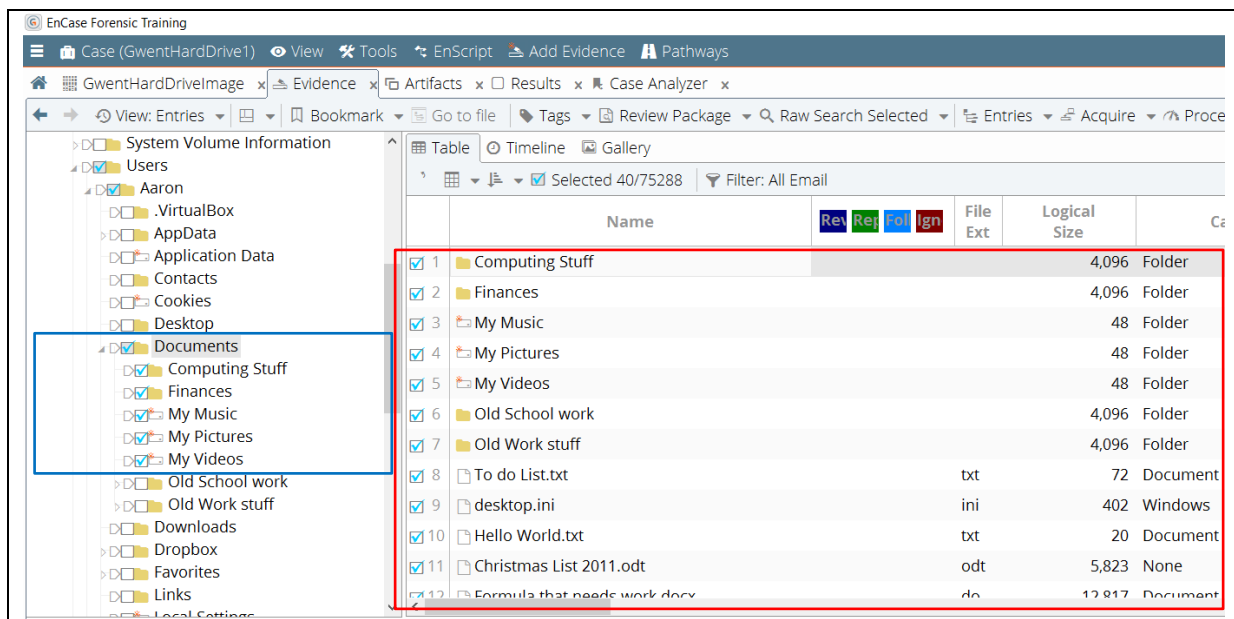
This screenshot shows the video folder that contains all the live videos that encase has processed from the digital image in the panel on the right

The screenshot shows the EnCase Forensic Training interface. On the left, a file tree lists various folders including 'Documents'. The main pane displays a table of files:

	Name	Rev	Ref	Pol	Ign	File Ext	Logical Size	Cat
37	Stream - 7433.mp4					mp4	30,478,928	Multimedia
38	Sunset - 7052.mp4					mp4	4,821,191	Multimedia
39	Surf - 2694.mp4					mp4	311,260,566	Multimedia
40	Waterfall - 7428.mp4					mp4	61,373,065	Multimedia
41	Wave Of Fog - 7102.mp4					mp4	54,923,083	Multimedia
42	WhatABeautifulSunset!.mp3					mp3	3,669,397	Multimedia
43	Winter - 6683.mp4					mp4	20,331,720	Multimedia
44	Winter - 7327.mp4					mp4	25,366,445	Multimedia
45	More stuff-\$EFS						672	Unknown

Documents	Are the "old school" and computing tech guides recovered and displayed	Yes, it can extract the documents from the image
-----------	--	--

This is a screenshot of the Documents folder from the digital image and the expected contents of which is shown in the panel on the right

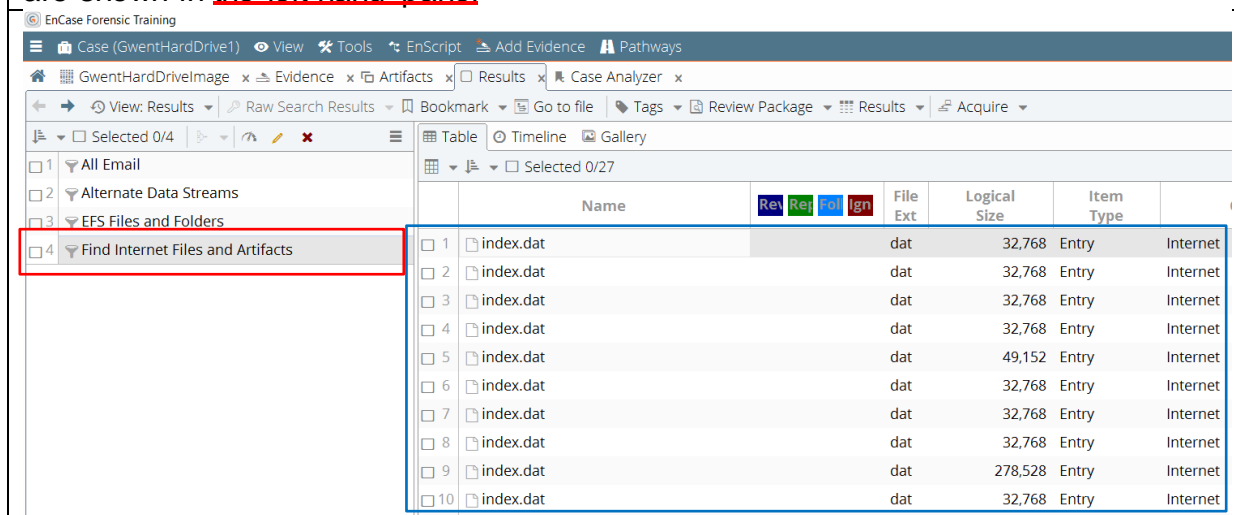


Internet Search History files

Does it find internet history files and display what mode a browser was in when they were being viewed

No, it found the internet files through the filters built-into the tool but it could not find the much more detail from these documents using the filters available

This screenshot shows the index.dat files that contain search information from the Internet explorer browser, these were filtered using the built-in filters in encase that are shown in the left-hand panel



Encrypted Files

Does encase show and label files that are encrypted

Yes, it does show files that are encrypted

The screenshot below shows the content of all folders that were encrypted and these were extracted through the default filters shown on the left and it has labelled the files correctly as in encrypted in the bottom panel.

EnCase Forensic Training

Case (GwentHardDrive1)

View

Tools

EnScript

Add Evidence

Pathways

GwentHardDriveImage

Evidence

Artifacts

Results

Case Analyzer

View: Results

Raw Search Results

Bookmark

Go to file

Tags

Review Package

Results

Acquire

Selected 0/4

1 All Email

2 Alternate Data Streams

3 EFS Files and Folders

4 Find Internet Files and Artifacts

Table

Timeline

Gallery

Selected 0/10

	Name	Rev	Rel	Fol	Ign	File Ext	Logical Size
1	Things						4,096
2	brown-bear-2011584.jpg					jpg	10,093,287
3	european-brown-bear-2185337.jpg					jpg	4,785,056
4	european-brown-bear-2186748.jpg					jpg	3,984,600
5	grizzly-bear-600559.jpg					jpg	453,126
6	water-1282937.jpg					jpg	12,263,854
7	More stuff						360
8	Bear2.mp4					mp4	16,402,658
9	Bear.mp4					mp4	5,194,721
10	Bear1.mp4					mp4	49,119,038

Fields

Report

Text

Hex

Decode

Doc

Transcript

Picture

Review

Console

Name	Value
s URL Host	
s URL Host Name	
s URL Name	
s True Path	GwentHardDriveImage\Users\Aaron\Pictures\Things
s Description	Folder, Hidden, Archive, Encrypted

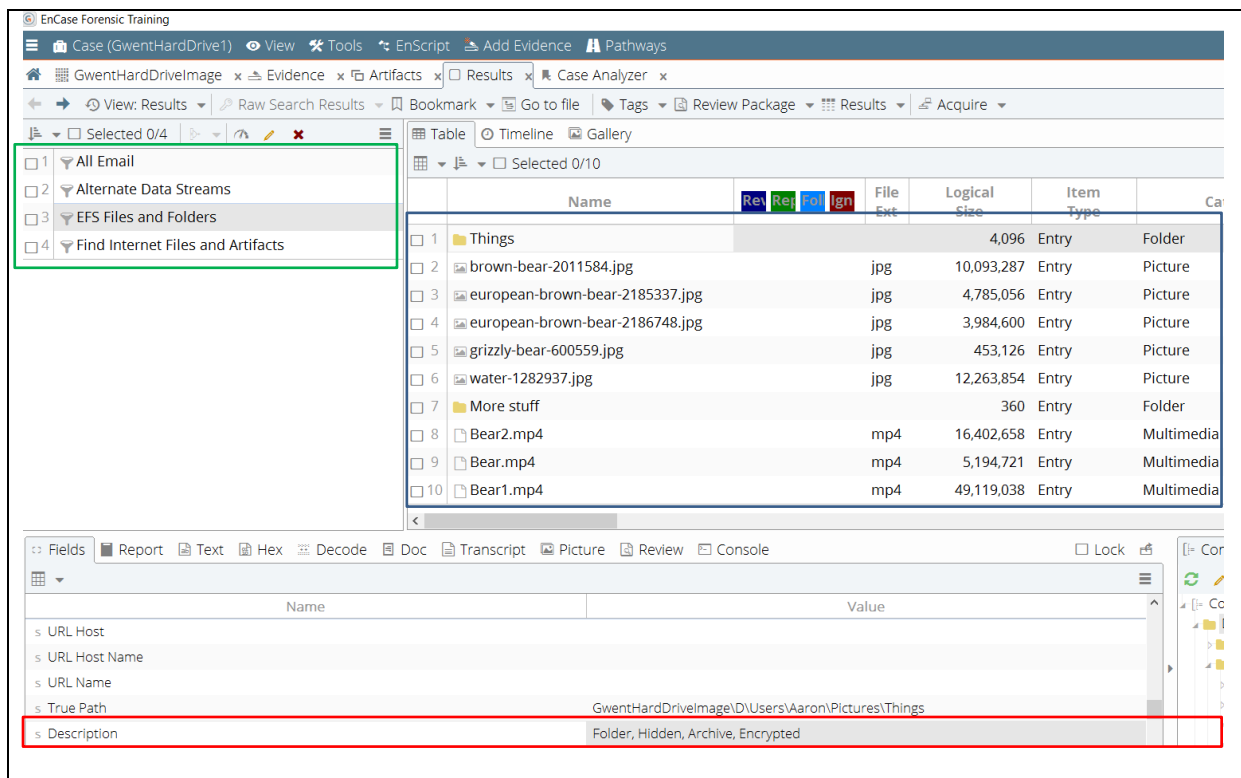
Hidden Folders

Does it show hidden folder from within the image

Yes, it shows hidden folders and states this in the description

This screenshot shows the pictures contained inside the hidden folders that were expected to be found in the raw image and it displays the files as hidden in the description panel underneath and these files were discovered using the built-in filters of encase shown on the left

30

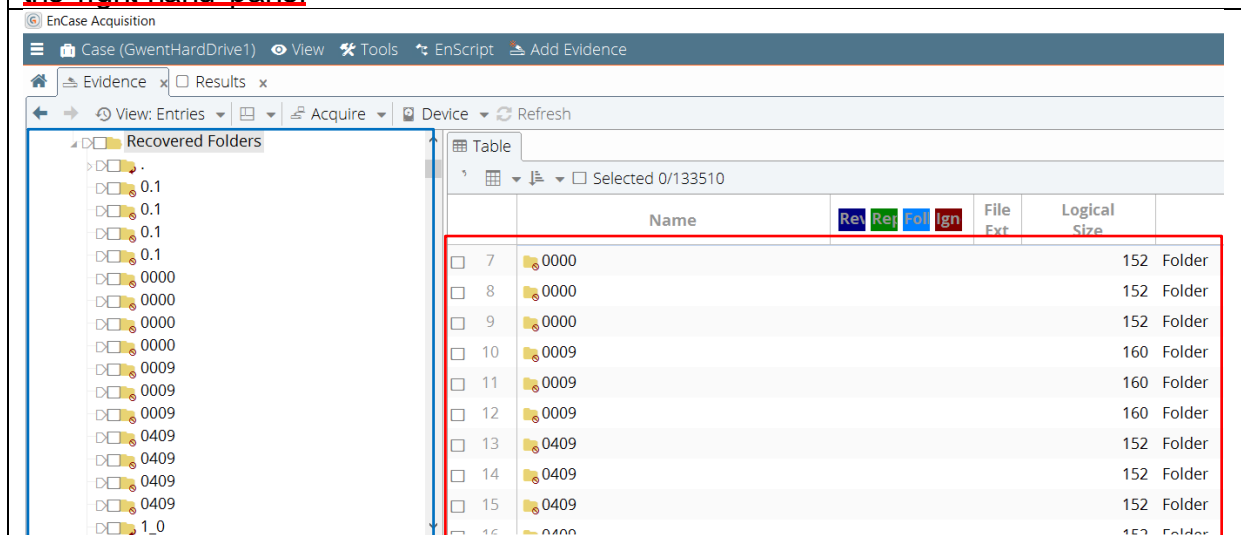


HPA Files

Can it see and recover the bear pictures that are hidden in the unallocated space

No, it recovered a lot from the unallocated space with old deleted files from past windows updates but it did not recover the pictures that I hid in there on purpose

Here is a screenshot of the recovery folder that was extracted from the drive and is highlighted on the left-hand side and the preview content from that folder is shown in the right-hand panel

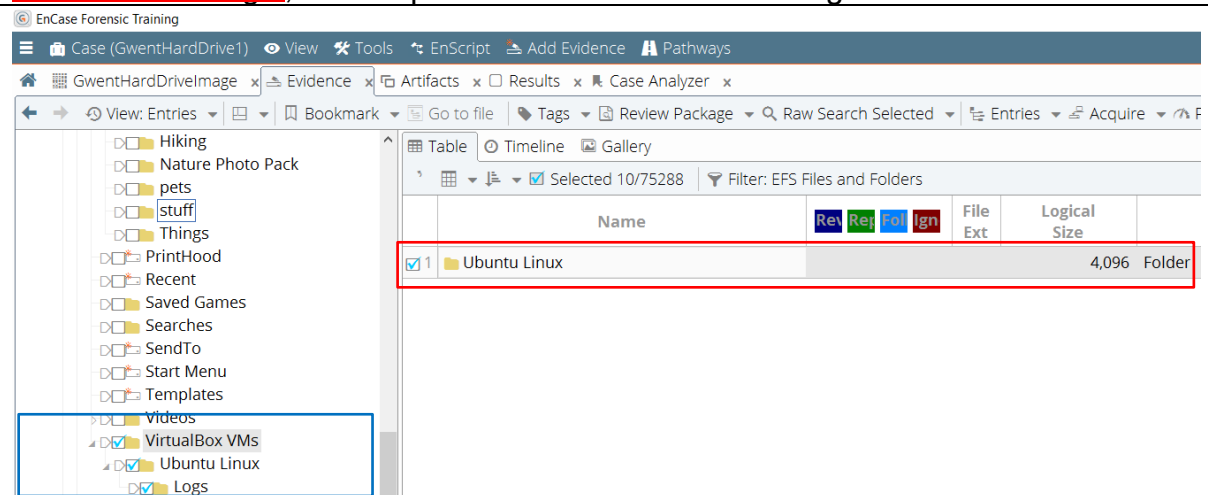


Virtual Machine Partition

Can the tool find and display content that is stored within a virtual machine

No, they will need to extract it and boot up the system to access it (via a VM probably)

This screenshot shows the virtual box folder shown on the left and previews the content on the right, but the partition isn't accessible through this forensic tool

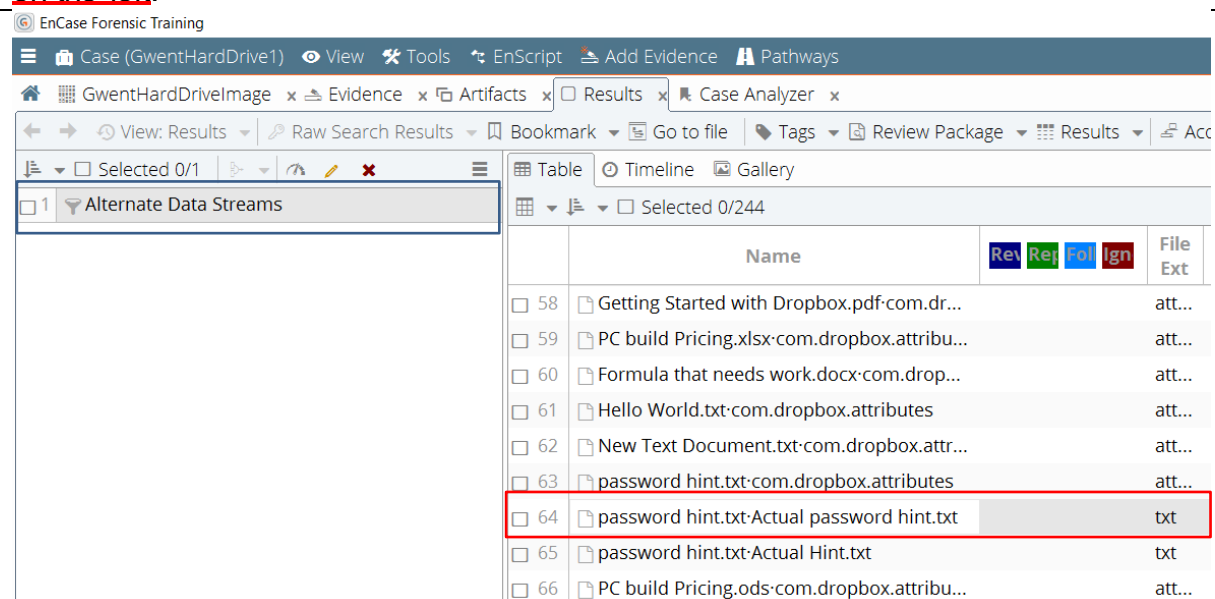


Alternate Data Stream

Can it display the alternate data streams and specifically the password hint at the back of the text file

Yes, it shows ADS with its full extension when the file is shown in the display panel

Here is a screenshot showing the alternate data stream that was expected to be found that contains the actual password hint that was hidden on the other side of the password hint.txt file. This file was found using the alternate data stream filter shown on the left.



Emails

Does it display the information around the user's yahoo email and messages from dropbox

Using default filters, it finds some category email files but doesn't find items the files that were to be expected

This screenshot shows the built-in filters on the left that has found all the information which it has then categorised into files that it deemed to be of email content as shown on the right

	Name	Rev	Ref	Fol	Ign	File Ext	Logical Size	Item Type	Category
1	Windows.edb					edb	42,008,576	Entry	Email
2	config.dbx					dbx	6,144	Entry	Email
3	instance.dbx					dbx	5,120	Entry	Email
4	host.dbx					dbx	205	Entry	Email
5	WindowsMail.MSMessageStore					M...	2,121,728	Entry	Email
6	WindowsMail.MSMessageStore					M...	2,113,536	Entry	Email
7	MainQueueOnline1.que					que	27,468	Entry	Email
8	MainQueueOnline0.que					que	28,770	Entry	Email
9	secedit.sdb					sdb	1,056,768	Entry	Email
10	DataStore.edb					edb	8,454,144	Entry	Email

Dropbox

Can the tool find the files stored for dropbox

Yes, displays all files that have been backed up from the documents folder as expected

Here is the proof of the dropbox folder as highlighted on the left and the previews of the files and folders contained within it on the right

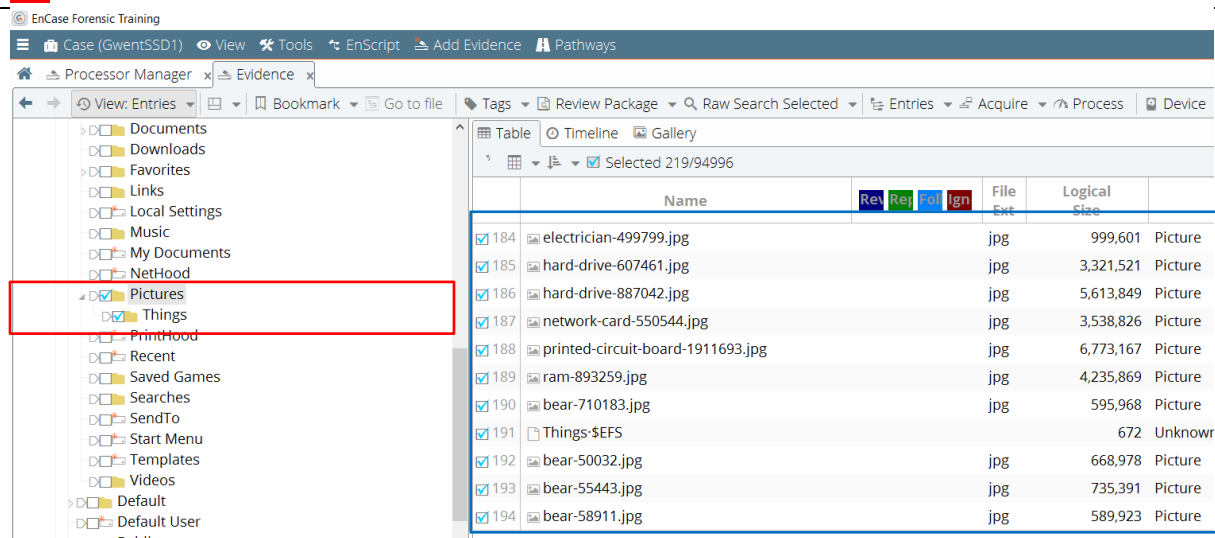
	Name	Rev	Ref	Fol	Ign	File Ext
1	..dropbox.cache					ca...
2	Computing Stuff					
3	Finances					
4	Computing Stuff-com.dropbox.attributes					att...
5	Finances-com.dropbox.attributes					att...
6	Payslip management.ods					ods
7	Payslip management.ods-com.dropbox.attr...					att...
8	.dropbox					dr...
9	desktop.ini					ini
10	Getting Started with Dropbox.pdf					pdf
11	Getting Started with Dropbox.pdf-com.drop...					att...
12	PC build Pricing.xlsx					xlsx

4.3.1.2 Tests for SSD (120Gb)

Device Serial Number: W2ASSTY6

Test	Description	Result
Live Images	Does it find all the live images such as holiday, pet and food pictures	Yes, it does extract the images that are expected to be found in the pictures folder

This screenshot shows the expected live images that were processed from the device previewed on the right and shows the pictures folder that is selected on the left



Deleted Files	Does it recover the deleted such as the old animal pictures and school documents	No, because of the way that encase seems to be set up I could not find any expected deleted files as there was no default filter that could find the media content that had been deleted
Hidden Folders	Can it display the hidden folders containing the explicit images within the system	Yes, it has found the explicit content that was hidden in the folders

This screenshot shows the hidden folder that was placed in the program files as highlighted on the left, it shows the explicit images that are contained within that folder shown in the panel on the right and it is labelled as hidden below in the description

The screenshot shows the EnCase Forensic Training interface. On the left, a tree view under 'PerfLogs' shows a folder named 'Old Stuff' containing several files. On the right, a table lists these files with their names, extensions, and logical sizes. Below the table, a 'Fields' panel shows details for the selected file, including its item path, true path, and description.

	Name	Rev	Rel	File	Logical Size
1	chihuahua-621112.jpg			jpg	2,613,884
2	adorable-1846555.jpg			jpg	10,331,808
3	adorable-1851108.jpg			jpg	1,423,836
4	animal-1846557.jpg			jpg	4,465,331
5	bulldog-1047518.jpg			jpg	2,114,094

Name	Value
Entropy	
Item Path	GwentSSDImage\D\Program Files\Old Stuff\chihuahua-621112.jpg
True Path	GwentSSD1\GwentSSDImage\D\Program Files\Old Stuff\chihuahua-621112.jpg
Description	File, Hidden, Archive

Encrypted Files	Does the tool find and flag encrypted files and their contents	Yes, this tool finds encrypted files and labels them in the description
-----------------	--	---

Here is a screenshot of the encrypted content that is previewed on the right and it can be found in the pictures folder as shown on the left and it labels these files correctly in the description panel down below

EnCase Forensic Training

Case (GwentSSD1) View Tools EnScript Add Evidence Pathways

Processor Manager Evidence

View: Entries Bookmark Go to file Tags Review Package Raw Search Selected Entries Acquire P

Documents Downloads Favorites Links Local Settings Music My Documents NetHood **Pictures Things** PrintHood Recent Saved Games Searches SendTo Start Menu Templates Videos Default Default User Public Windows

Table Timeline Gallery

Selected 25/94996 Filter: Find Pictures

	Name	Rev	Ref	Pol	Ign	File Ext	Logi
<input checked="" type="checkbox"/>	1					rottweiler-2160307.jpg	jpg 1,
<input checked="" type="checkbox"/>	2					rottweiler-2160307.jpg-\$EFS	
<input checked="" type="checkbox"/>	3					adorable-1846555.jpg	jpg 10,
<input checked="" type="checkbox"/>	4					adorable-1846555.jpg-\$EFS	
<input checked="" type="checkbox"/>	5					adorable-1851108.jpg	jpg 1,
<input checked="" type="checkbox"/>	6					adorable-1851108.jpg-\$EFS	
<input checked="" type="checkbox"/>	7					animal-1846557.jpg	jpg 4,
<input checked="" type="checkbox"/>	8					animal-1846557.jpg-\$EFS	
<input checked="" type="checkbox"/>	9					bulldog-1047518.jpg	jpg 2,
<input checked="" type="checkbox"/>	10					bulldog-1047518.jpg-\$EFS	
<input checked="" type="checkbox"/>	11					chihuahua-621112.jpg	jpg 2,
<input checked="" type="checkbox"/>	12					chihuahua-621112.jpg-\$EFS	

Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets

Name	Value
Entropy	
Item Path	GwentSSDImage\Users\Bill\Pictures\Things\rottweiler-2160307.jpg
True Path	GwentSSD1\GwentSSDImage\Users\Bill\Pictures\Things\rottweiler-2160307.jpg
Description	File, Hidden, Archive, Encrypted

Live Videos	Does the forensic tool show all live video files on the processed image	Yes, it can filter the data to find the live videos that have populated on this image
-------------	---	---

Here is the evidence of all the expected live videos that have been accessed through the videos folder on the image and processed by Encase, and then previewed in the panel on the right

EnCase Forensic Training

Case (GwentSSD1) View Tools EnScript Add Evidence Pathways

Processor Manager Evidence

View: Entries Bookmark Go to file Tags Review Package Raw Search Selected Entries Acquire Process Device

Favorites Links Local Settings Music My Documents NetHood Pictures Things PrintHood Recent Saved Games Searches SendTo Start Menu Templates **Videos** Default Default User Public Windows Lost Files

Table Timeline Gallery

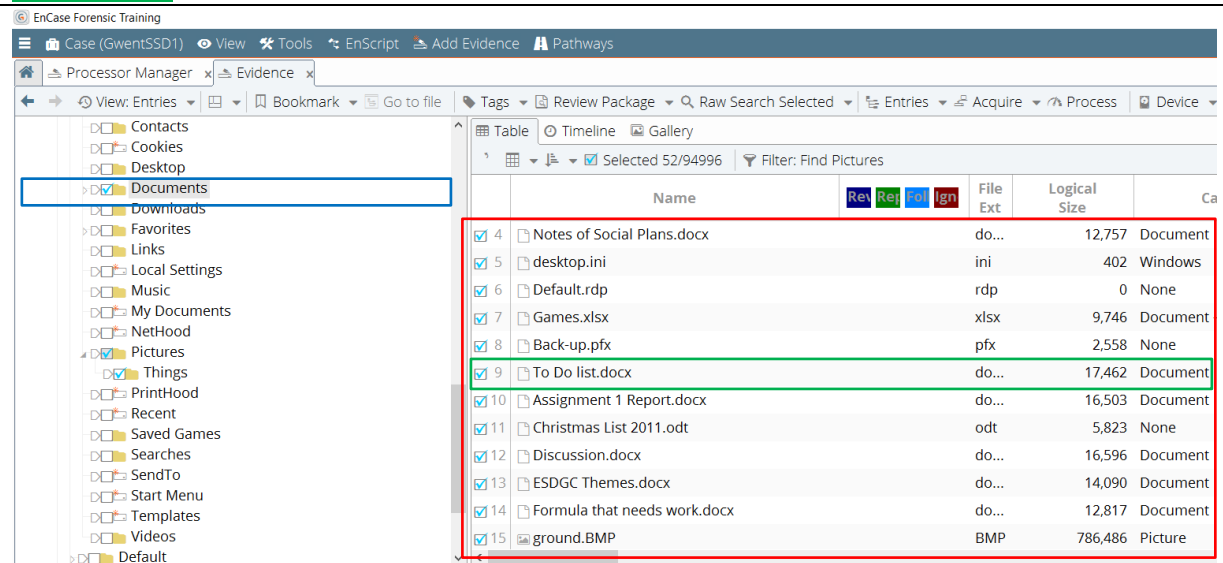
Selected 24/94996

	Name	Rev	Ref	Pol	Ign	File Ext	Logical Size	Cat
<input checked="" type="checkbox"/>	13					Stream - 7432.mp4	48,541,972	Multimedia
<input checked="" type="checkbox"/>	14					Stream - 7433.mp4	30,478,928	Multimedia
<input checked="" type="checkbox"/>	15					Sunset - 7052.mp4	4,821,191	Multimedia
<input checked="" type="checkbox"/>	16					Surf - 2694.mp4	311,260,566	Multimedia
<input checked="" type="checkbox"/>	17					tree-779827.jpg	7,454,376	Picture
<input checked="" type="checkbox"/>	18					Waterfall - 7428.mp4	61,373,065	Multimedia
<input checked="" type="checkbox"/>	19					waterfall-2187851.jpg	2,368,363	Picture
<input checked="" type="checkbox"/>	20					Wave Of Fog - 7102.mp4	54,923,083	Multimedia
<input checked="" type="checkbox"/>	21					WhatABeautifulSunset!.mp3	3,669,397	Multimedia
<input checked="" type="checkbox"/>	22					Winter - 6683.mp4	20,331,720	Multimedia
<input checked="" type="checkbox"/>	23					Winter - 7327.mp4	25,366,445	Multimedia

Documents	Does the tool find all the variety of documents such as old school work and "To do lists"	Yes, document files are extracted and displayed as expected from this processed image
-----------	---	---

This screenshot shows the documents folder highlighted on the left and the contents

that is expected to be found displayed on the right-hand panel with the “to do lists” inside them

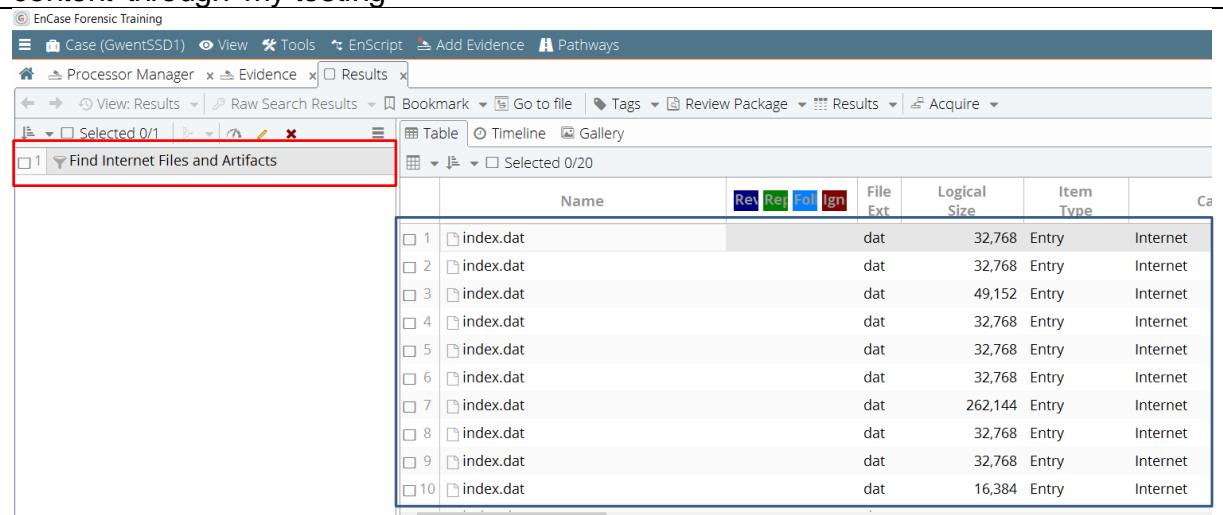


Internet Search History

Can it find and display all the search history from this user that were in browsers in normal and private mode

No, through encases default filters I could only find limited files containing information on the history that the user has been viewing and even then, it would not display which type of browser that information came from

Here is the screenshot of the index.dat files as displayed on the right which were extracted through encases default filter on the left, but no more knowledge around the browser types could be found using these features in encase to narrow down it content through my testing



4.3.1.3 Tests for USB (64 Gb)

Device Serial Number:
AA0000000000485

Test	Description	Results
Documents	Does it find and display the networking documents stored on the USB	Yes, all the networking documents are discovered and displayed in the tool

This is a screenshot that shows the list of folders processed from the USB image on the left and then displays the evidence of the expected documents in the panel on the right

Name	File Ext	Logical Size	Category
Addressing the Network.docx	do...	164,284	Document
Assessment 2 draft.docx	do...	5,951,400	Document
Comms Cisco.docx	do...	25,219	Document
lan devices mod 4.ppt	ppt	987,136	Document - Presentation
osi model.ppt	ppt	1,651,712	Document - Presentation

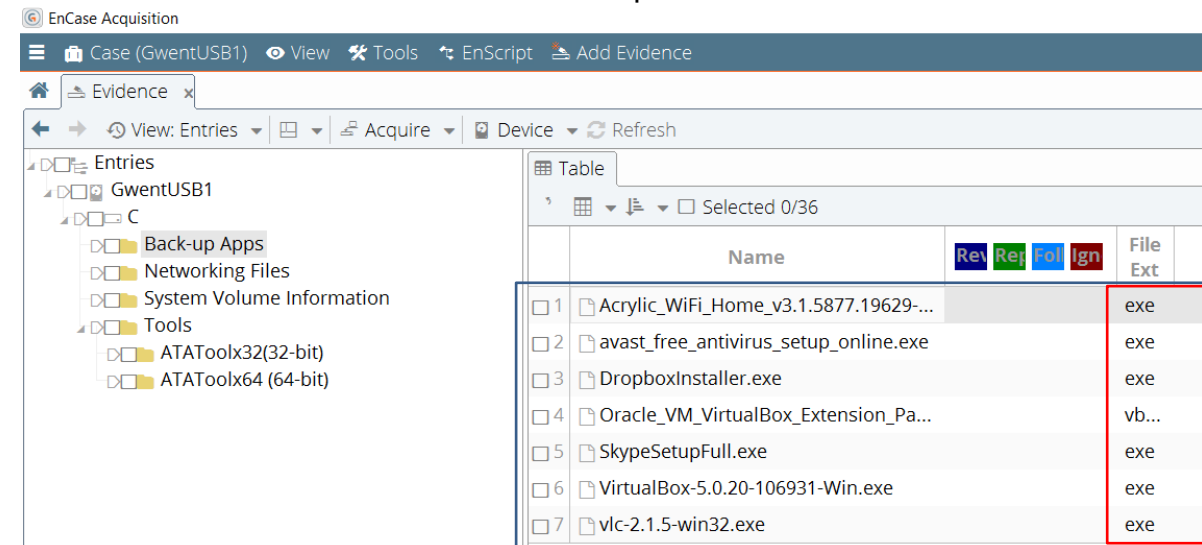
Live Images	Does it show all the computer networking images that should be found in this raw image	Yes, it does display the live images that are expected to turn up when examining the processed image
-------------	--	--

Here is the screenshot evidence of the expected pictures to be found on the device and they are displayed in the right-panel

Name	File Ext	Logical Size	Category
control-cabinet-2147373.jpg	jpg	3,588,827	Picture
network-1572617.jpg	jpg	2,621,603	Picture
network-cables-494649.jpg	jpg	1,807,950	Picture
router-157597.png	png	232,145	Picture
usb-686359.jpg	jpg	239,557	Picture

Application Files	Are the application files found and categorized with the right extensions	Yes, it shows the application files from the image and the correct extensions are labelled on each of them.
-------------------	---	---

This is a screenshot of all the application installers that have been processed from the USB image displayed in the panel on the right with the correct extensions for each file labelled in the column in the same panel

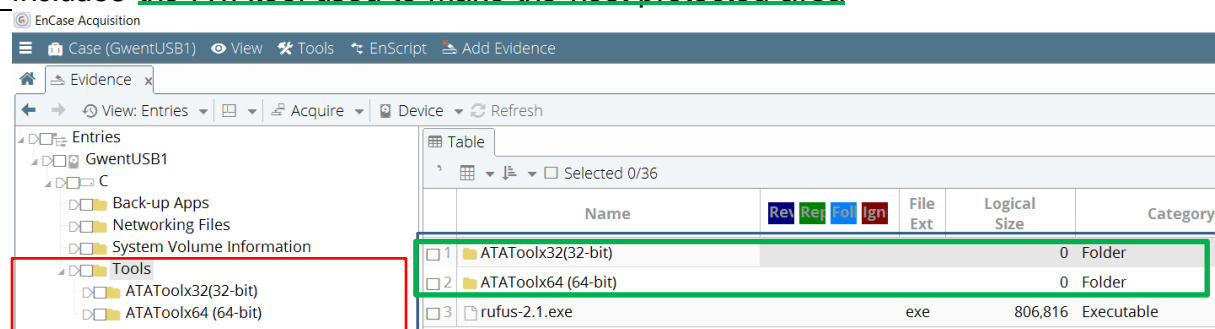


Digital Tools

Does it show and categorize the software tools on this USB

Yes, it displays the tool and categorizes them under executable as expected

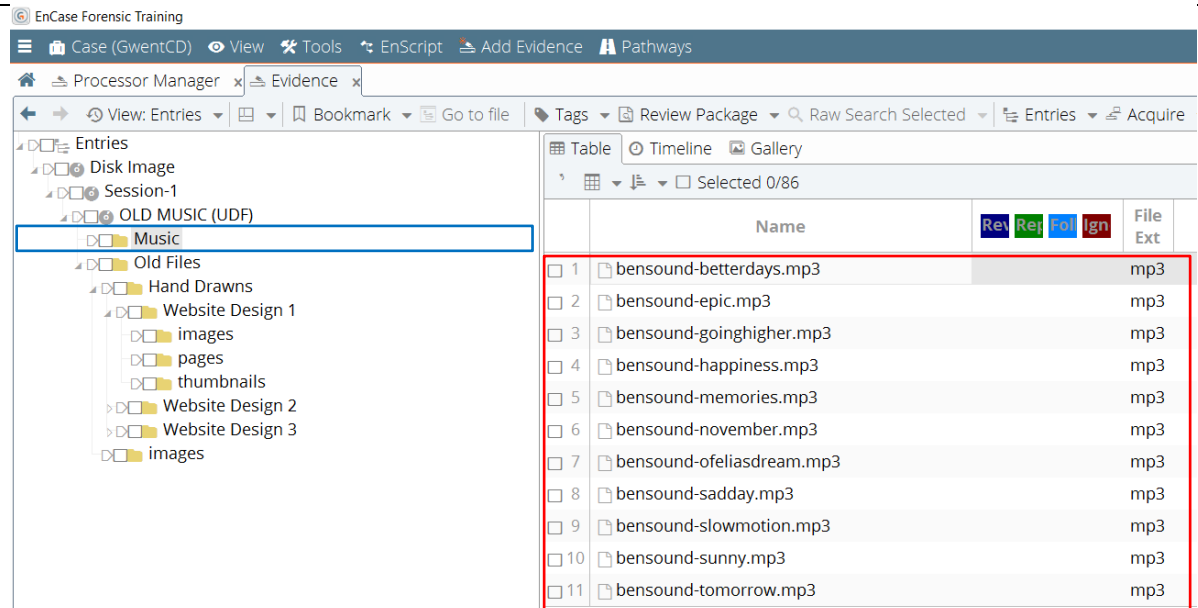
This screenshot shows the software tools that have been displayed in the panel on the right and are stored on this device in the tool folder highlighted on the right, this includes the ATATool used to make the host protected area



4.3.1.4 Tests for DVDs	Device Name: Optiarc DVD RW AD-5280S	
------------------------	--------------------------------------	--

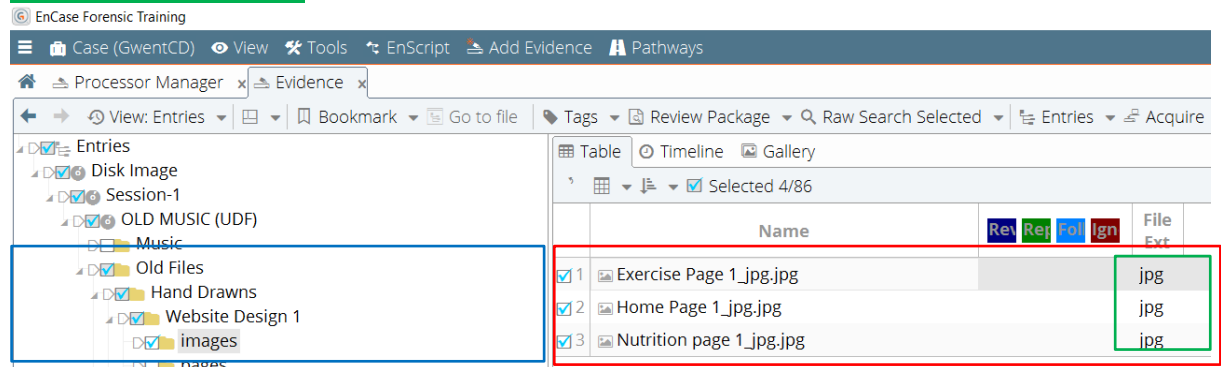
Test	Description	Results
Music	Are the music files displayed and classified correctly by encase from the rest of the standard documents	Yes, it does filter and correctly classify all the music files that can be found the DVD image

This screenshot shows the music folder highlighted on the left in encase and it correctly categorizes music files and displays them on the right with the expected file extensions



Live Images	Does it show all the old-school design work that is expected to be on the DVD	Yes, it can filter and process all the design pictures that are on the DVD image
-------------	---	--

This screenshot shows the design work files from the "Hand Drawns" folder on the left which has then been previewed on the right with the correct extensions to be found which are jpeg



Documents	Does it display the documents stored on this device	Yes, it does display the documents that have been stored on this DVD image
-----------	---	--

Here is screenshot proof that shows the expected documents from all the highlighted folders that were stored on the image shown on the left and then they have been

processed and displayed on the right-hand panel

EnCase Forensic Training

Case (GwentCD) View Tools EnScript Add Evidence Pathways

Processor Manager Evidence

View: Entries Bookmark Go to file Tags Review Package Raw Search Selected Entries Acquire Process Device

Entries

- Disk Image
 - Session-1
 - OLD MUSIC (UDF)
 - Music
 - Old Files
 - Hand Drawns
 - Website Design 1
 - images
 - pages
 - thumbnails
 - Website Design 2
 - Website Design 3
 - images

Table Timeline Gallery

Selected 78/86

	Name	Rev	Rel	Col	Ign	File Ext	Logical Size	Cal
<input checked="" type="checkbox"/> 1	Music						964	Folder
<input checked="" type="checkbox"/> 2	Old Files						156	Folder
<input checked="" type="checkbox"/> 3	Design ideas.docx					do...	14,426	Document
<input checked="" type="checkbox"/> 4	Notes for assessment 1.docx					do...	12,937	Document

4.3.2 FTK v6.1.0.130 Tests

Laboratory Location:

Digital Forensic Laboratory
Cardiff University
Queens Building
5 The Parade, Roath,
Cardiff CF24 3AA, UK

Tests Carried out on: 11/4/2017

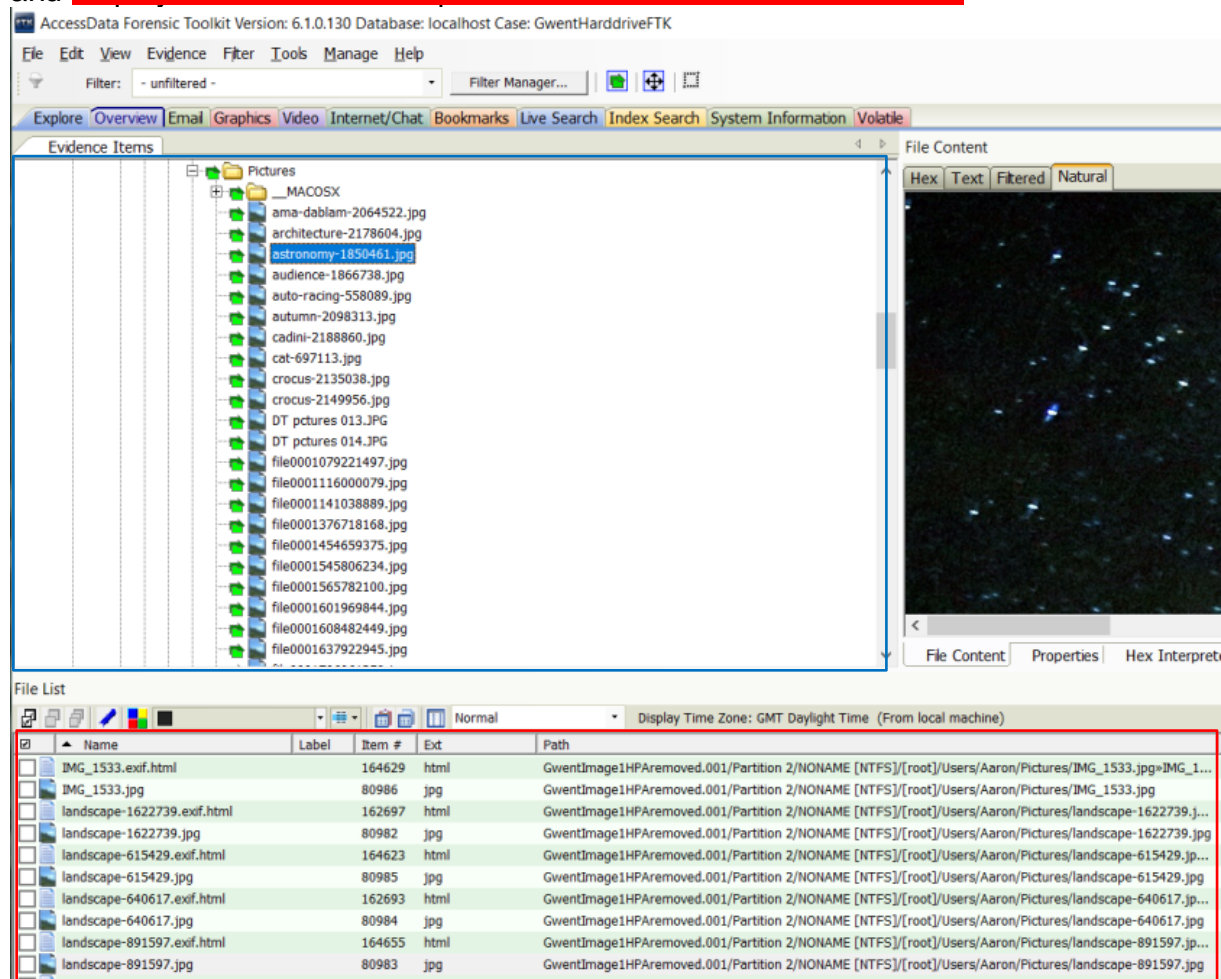
Tested by: Ben Ajax-Lewis

4.3.2.1 Test for Convention Hard Drive (500Gb)

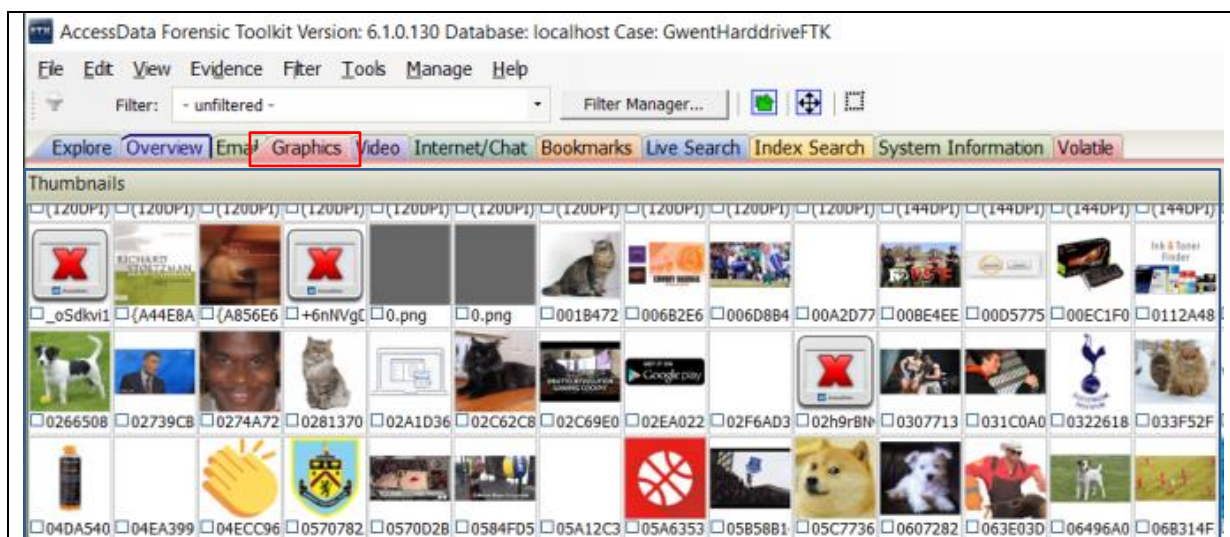
Device Serial Number: W2ASSTVA

Test	Description	Result
Live Images	Does the tool find the bear pictures that are hidden along with the trivial stock images	Yes, FTK can find and filter all the images from the processed device

This screenshot shows all the live pictures that have been highlighted from the pictures folder in the processed image and the contents that is expected to be found and displayed is shown in the panel at the bottom of the screenshot



This screenshot shows all the live images that can be found on the device which have mostly been scrapped from web pages when the use has been accessing different web pages and it is shown in the graphics tab in FTK

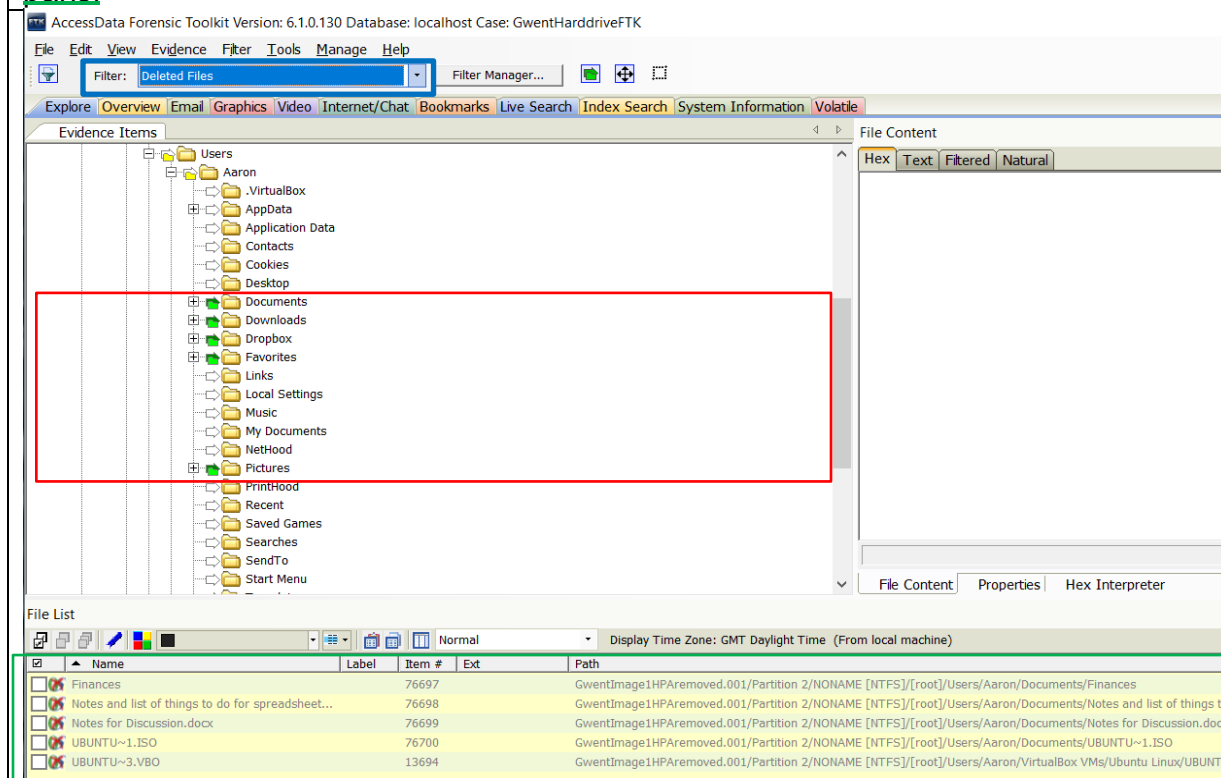


Deleted Files

Does the tool find deleted files that are expected to be found on the device such as the torrent file

Yes, it does recover them, there was a default filter that looked for all deleted files which made finding them very easy

This screenshot shows the deleted files filter being used in the top left corner and it highlights the folders that contain the expected content underneath it on the left and the details of each file that has been deleted from the image is shown in the bottom panel

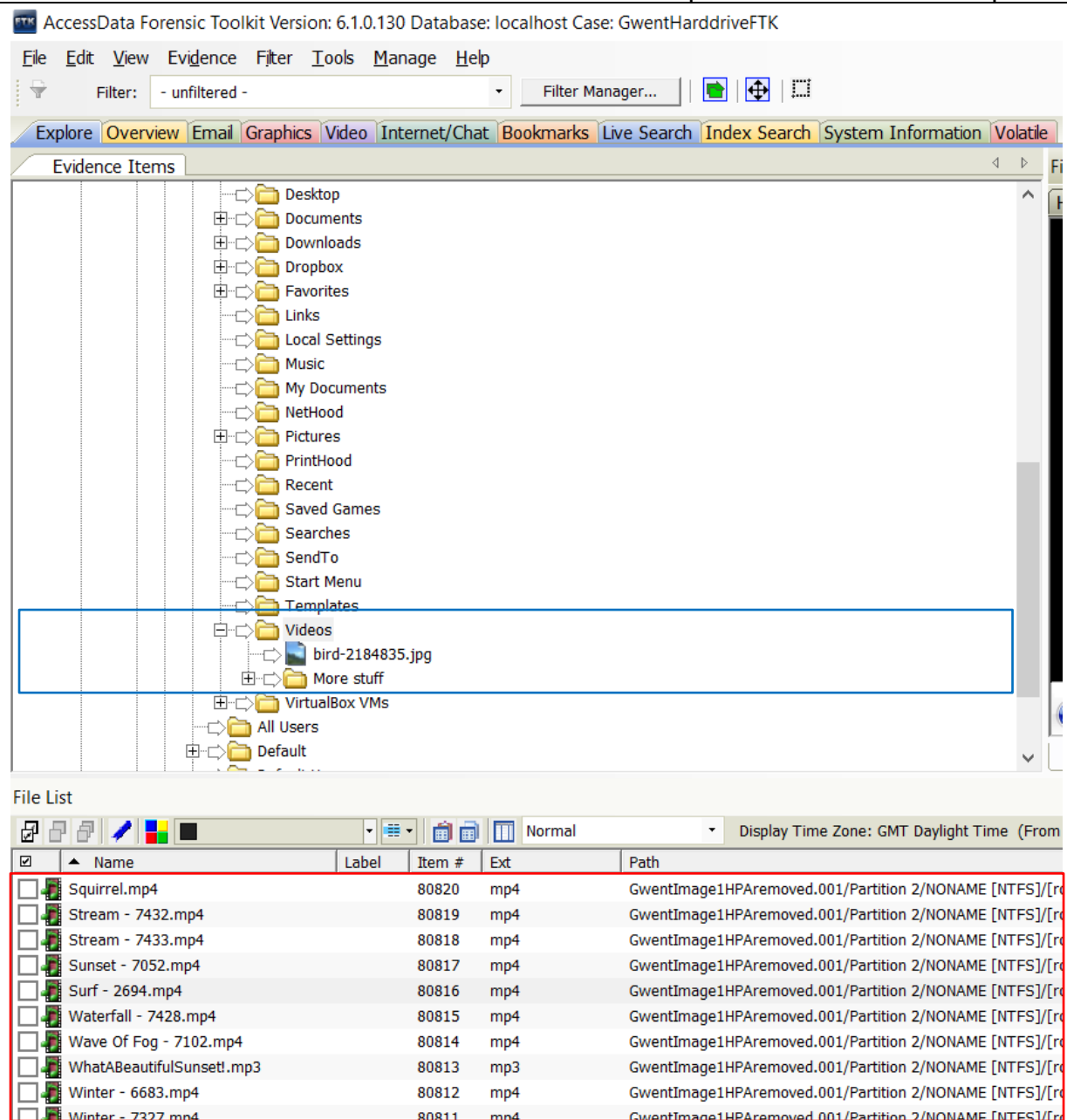


Live Videos

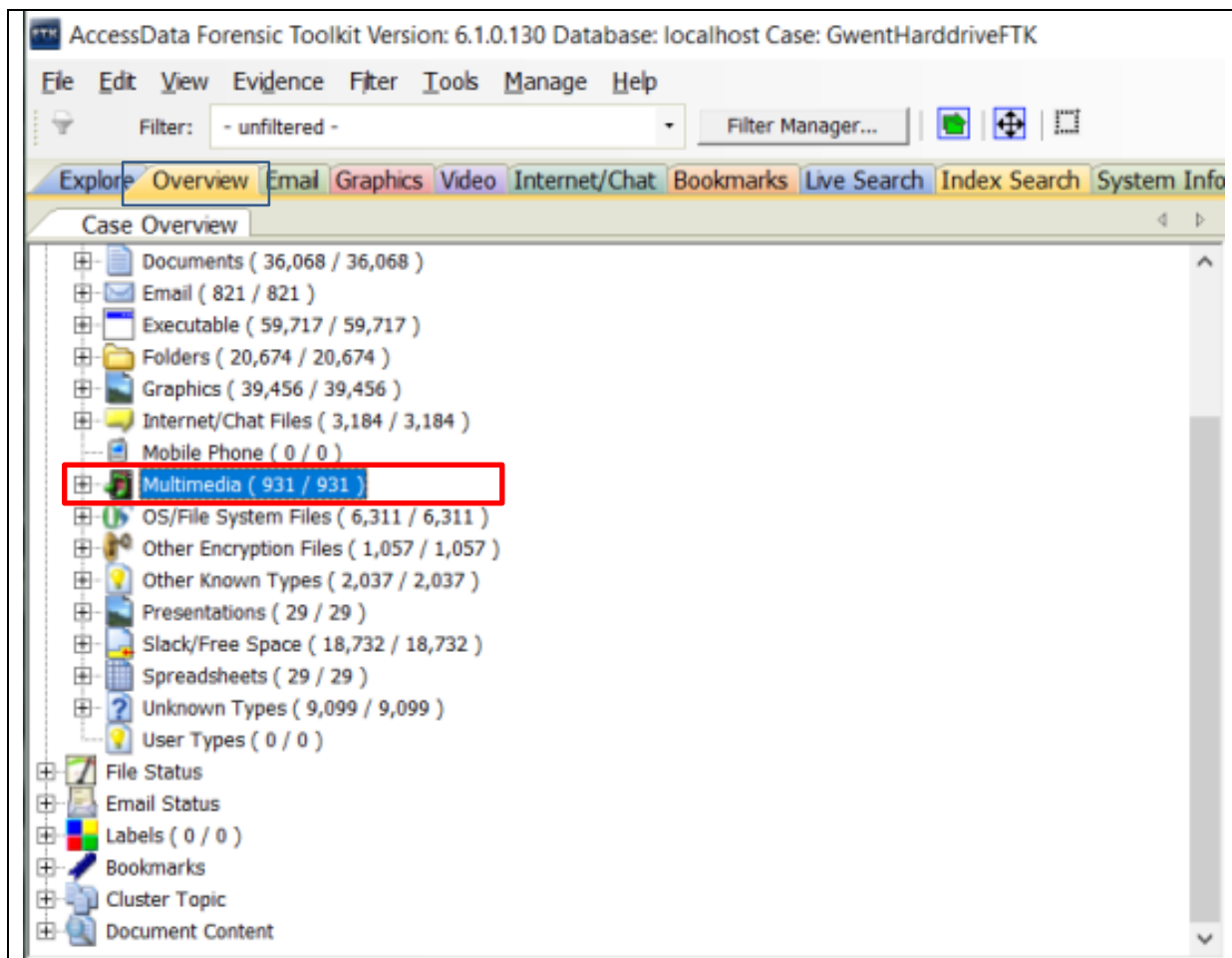
Are all the Live videos recovered such as the once containing sweeping landscapes

Yes, it can filter all the necessary multimedia files and displays them from the videos folder

Here is a screenshot of all the expected videos that can be found in the “Videos” folder shown on the left and the details of that folder is previewed in the bottom panel



Here's another screenshot from the overview tab that easily displays all multimedia content to be found in this digital image as it automatically filters the content in various categories shown on the left



Documents	Are the “old school” and computing tech guides recovered and displayed	Yes, it does process and find all the guides that have been populated on this digital image
-----------	--	---

Here is the screenshot of the documents folder that have been highlighted on the left and it is currently displaying the contents of the “pc parts” spreadsheet from the user that is selected in the bottom panel and displayed on the right hand-side

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered -

Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Users

Aaron

.VirtualBox

AppData

Application Data

Contacts

Cookies

Desktop

Documents

Christmas List 2011.odt

Computing Stuff

Finances

Formula that needs work.docx

My Music

My Pictures

My Videos

Old School work

Old Work stuff

password hint.bt

PC build Pricing.ods

PC build Pricing.xlsx

Project Specification.docx

Downloads

Dropbox

File Content

Hex Text Filtered Natural

	A	B	C	D	E
1	Alice Mk1				
2		item	Price		
3	Graphics Card	Geforce GTX 980	£465		£279
4	Processor	Intel i5	£179		£179
5	Hard drive	1 Tb	£43		£43
6	SSD	120Gb	£42		£42
7	RAM	8Gb			
8	PSU				
9	Cooling				
10	Motherboard				
11	Case				
12					
13			£729		£543
14					
15					
16					

File Content Properties Hex Interpreter

File List

Normal

Display Time Zone: GMT Daylight Time (From local machine)

	Name	Label	Item #	Ext	Path	Category
	PC build Pricing.ods		76685	ods	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/PC build Pricing.ods	ApacheOffice 4 Calc
	PC build Pricing.ods.FileSlack		200452		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/PC build Pricing.ods.FileSlack	Slack Space
	PC build Pricing.xlsx		76691	xlsx	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/PC build Pricing.xlsx	Excel 2010
	Pictures		140121		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old School work/Spanish Culture.odp>...	Placeholder
	pillier_D.dds		82749	dds	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Unknown
	pillier_D.dds.FileSlack		100176		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Slack Space
	pillier_D2.dds		82748	dds	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Unknown
	pillier_D2.dds.FileSlack		100175		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Slack Space
	pillier_I.dds		82747	dds	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Unknown
	pillier_I.dds.FileSlack		100174		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/Old Work stuff/texturebank/Metro Thea...	Slack Space

Internet Search History

Does it find internet history files on the processed image

Yes, FTK does find the expected history files and displays them in an internet/chat tab where it has categorised all the history files

This screenshot shows FTK being able to filter out the internet files through the internet/chat tab shown in the top left panel and the details on the files that have been filter is shown underneath them with a preview of the selected file on the right

46

AccessData Forensic Toolkit Version: 6.10.130 Database: localhost Case: GwentHarddriveFTK

File List

Name	Item #	Last Visit Time	URL
IE site on Microsoft.com.url	81277		
index.dat	82140		
index.dat	17604		
index.dat	30777		
index.dat	30779		
index.dat	31130		
index.dat	31136		
index.dat	34232		
index.dat	34508		
index.dat	34517		
index.dat	80918		
index.dat	81809		
index.dat	81855		
index.dat	81813		
index.dat	81858		
index.dat	81679		

File Content

IE History Index

URL	:2017040420170405: Aaron@--mmc:pagebreak.1
file:	
user name:	
response:	
accessed time:	04/04/2017 13:36:31 +0100
modified time:	04/04/2017 14:36:31 +0100
expiration time:	30/04/2017 13:36:32 +0100
hits:	1
use counts:	0
URL	:2017040420170405: Aaron@:Host: Computer
file:	
user name:	
response:	
accessed time:	04/04/2017 13:36:31 +0100
modified time:	04/04/2017 14:36:31 +0100
expiration time:	
hits:	1
use counts:	0
URL	:2017040420170405: Aaron@--mmc:pagebreak.2
file:	
user name:	

This screenshot show a more detailed display of the users search history with most of his searches seeming to involve football as displayed in the panel on the right

File List

Name	Item #	Last Visit Time	URL
History	20328		
History	217393		
History	237407		

Item #	URL	Search Results	Hits	Use Counts
47	https://www.google.co.uk/?gws_rd=ssl#q=everton+fc&*	everton fc - Google Search	1	0
48	http://www.evertonfc.com/	Home Everton Football Club	2	0
49	http://www.evertonfc.com/news	News Everton Football Club	1	0
50	http://www.evertonfc.com/fixtures	Fixtures Everton Football Club	2	0
51	http://www.evertonfc.com/evertontv/highlights?fixtureId=c7ca6e94-9c45-40d5-8cf8-3f51c45a5f98	Highlights Everton Football Club	1	0
52	http://www.evertonfc.com/fixtures	Fixtures Everton Football Club	2	0
53	http://www.bbc.co.uk/news/		2	0
54	http://www.bbc.co.uk/news/world-europe-39486640	St Petersburg metro bombing 'possibly a suicide attack' - BBC News	1	0

Encrypted Files

Does FTK find the encrypted files that are stored on this raw image

Yes, FTK can filter the encrypted files and display them

This screenshot shows all the encrypted files on the image as highlighted in the left-hand panel and then the bottom panel shows the details of the files contained in this image and the right-hand panel previews the content which has come up as encrypted

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

Presentations (29 / 29)

Slack/Free Space (18,732 / 18,732)

Spreadsheets (29 / 29)

Unknown Types (9,099 / 9,099)

User Types (0 / 0)

File Status

Bad Extensions (24,592 / 24,592)

Data Carved Files (0 / 0)

Decrypted Files (0 / 0)

Deleted Files (3,737 / 3,737)

Duplicate Items (0 / 0)

Email Attachments (0 / 0)

Email Related Items (From Email) (1,616 / 1,616)

Encrypted Files (22 / 22)

Flagged Ignore (0 / 0)

Flagged Privileged (0 / 0)

From Recycle Bin (16 / 16)

KFF Alert Files (0 / 0)

KFF Inoperable (0 / 0)

File Content

Hex Text Filtered Natural

Unable to View

Document is encrypted

File Content Properties Hex Interpreter

File List

Normal

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size
Bear.mp4		81702	mp4	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff/Bear.mp4	EFS Encrypted Files	5076 KB	5072 KB
Bear1.mp4		81657	mp4	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff/Bear1.mp4	EFS Encrypted Files	46.84 ...	46.84 ...
Bear2.mp4		81445	mp4	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff/Bear2.mp4	EFS Encrypted Files	15.64 ...	15.64 ...
brown-bear-2011584.jpg		81659	jpg	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/brown-bear-201158...	EFS Encrypted Files	9860 KB	9856 KB
config.dbx		17616	dbx	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Dropbox/instance1/C...	SEE-Encrypted SQLit...	8192 B	6144 B
european-brown-bear-2185337.jpg		81480	jpg	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/european-brown-be...	EFS Encrypted Files	4676 KB	4672 KB
european-brown-bear-2186748.jpg		81600	jpg	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/european-brown-be...	EFS Encrypted Files	3892 KB	3891 KB
grizzly-bear-600559.jpg		81478	jpg	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/grizzly-bear-600559...	EFS Encrypted Files	444.0 ...	442.5 ...
instance.dbx		17618	dbx	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Dropbox/instance_db...	SEE-Encrypted SQLit...	8192 B	5120 B
Login Data		20307	<miss...	GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/ProgramData/AVAST Software/SZBrowser/profile...	Login Data File	20.00 ...	18.00 ...
More stuff		81415		GwentImage1HPAreMOVED.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff	Folder	360 B	360 B

Hidden Folders

Does it show hidden folder from within the image

Yes, but it doesn't filter just hidden files and I know that these files were hidden because I put them there otherwise I don't think I could have known they were hidden

Here is the screenshot of the hidden folder that has also been encrypted which seems to take president over hidden folders in FTK the details of this folder are displayed in the bottom panel with the highlighted content in the left panel

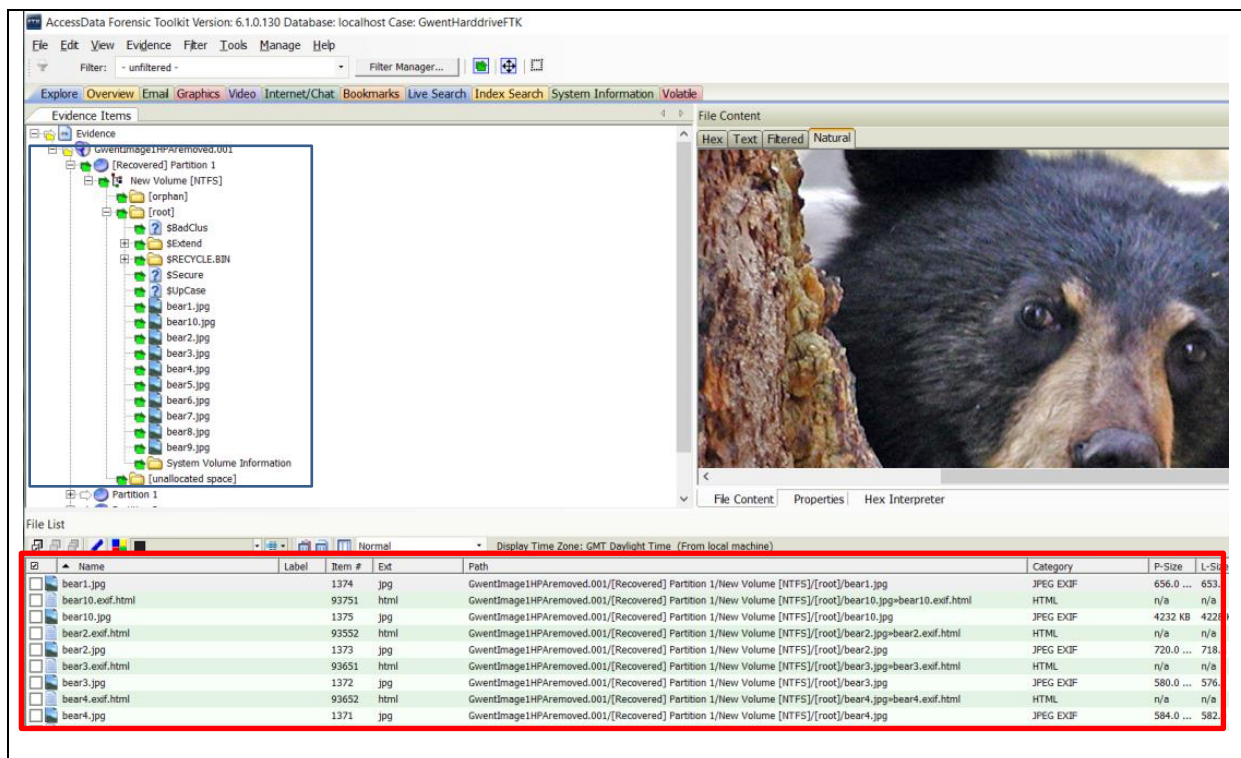
48

AccessData Forensic toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddrive1.K
File Edit View Evidence Filter Tools Manage Help
Filter: Encrypted Files Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Documents and Settings
PerfLogs
Program Files
ProgramData
Recovery
System Volume Information
Users
Aaron
.VirtualBox
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Dropbox
Favorites
Links
Local Settings
Music
My Documents
NetHood
Pictures
...
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
Bear2.mp4	81445	mp4	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff/Bear2.mp4	
brown-bear-2011584.jpg	81659	jpg	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/brown-bear-2011584.jp	
config.dbx	17616	dbx	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Dropbox/instance1/config	
european-brown-bear-2185337.jpg	81480	jpg	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/european-brown-bear-2	
european-brown-bear-2186748.jpg	81600	jpg	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/european-brown-bear-2	
grizzly-bear-600559.jpg	81478	jpg	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/grizzly-bear-600559.jpg	
instance.dbx	17618	dbx	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Dropbox/instance_db/inst	
More stuff	81415		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Videos/More stuff	
Things	81245		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things	
water-1282937.jpg	81655	jpg	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Pictures/Things/water-1282937.jpg	

HPA Files	Can it see and recover the bear pictures that are hidden in the unallocated space	Yes, it recovers all the files from the unallocated space without any extra work needed to be done
-----------	---	--

Here is the screenshot of files recovered from the HPA including the 10 bear pictures that was expected to be found and are highlighted on the left and with more details of the contents of the HPA found in the panel at the bottom



Virtual Machine Partition	Can the tool find and display content that is stored within a virtual machine	No, FTK couldn't find the files for the VM partition
Alternate Data Stream	Can it display the alternate data streams and specifically the password hint at the back of the text file	Yes, FTK had a put in function to find Alternate data streams

Here is the screenshot of the alternate data stream filter being run in the top left and the data streams appear as separate files underneath the original files they are attached to in the bottom panel. The actual content of the file is displayed on the right showing the text inside of "actual password hint.txt" file

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK
File Edit View Evidence Filter Tools Manage Help
Filter: Alternate Data Streams Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Partition 2
NONAME [NTFS]
[orphan]
[root]
\$BadClus
\$Extend
\$Recycle.Bin
\$Secure
\$UpCase
Documents and Settings
PerfLogs
Program Files
ProgramData
Recovery
System Volume Information
Users
Aaron
.VirtualBox
AppData
Application Data
Contacts
Cookies
Desktop
Documents
File Content
Hex Text Filtered Natural
View Text As: Windows 1252 (Latin 1, ANSI)
hint for password:
its your Favourite Football team , capital at the start
File Content Properties Hex Interpreter
File List
Normal Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Categ...	P-Size
Actual Hint.txt		13022		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/password hint.txt/Ac...	Zero L...	0 B
Actual Hint.txt		81237		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/password hint.txt/Ac...	Zero L...	0 B
Actual password hint.txt		13023		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/password hint.txt/Ac...	7 bit t...	80 B
Actual password hint.txt		81238		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Documents/password hint.txt/Ac...	7 bit t...	80 B
com.dropbox.attributes		13667		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/har...	Altern...	88 B
com.dropbox.attributes		13669		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/dat...	Altern...	88 B
com.dropbox.attributes		13671		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/cpu...	Altern...	88 B
com.dropbox.attributes		13673		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/net...	Altern...	88 B
com.dropbox.attributes		13675		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/cool...	Altern...	88 B
com.dropbox.attributes		13677		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/co...	Altern...	88 B
com.dropbox.attributes		13679		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/Dropbox/Computing Stuff/co...	Altern...	88 B

Emails

Does it display the information around the user's yahoo email and messages from drobox

Yes, it does filter the email information from the processed image

This screenshot shows all the files that have been categorized as email files and highlighted on the left in FTK and displays the details of each one in the panel at the bottom

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

- Evidence Groups
- File Items
 - File Extension (147,024 / 147,024)
 - File Category (200,073 / 200,073)
 - File Status
 - Email Status
 - Email Attachments (0 / 0)
 - Email Related Items (From Email) (1,616 / 1,616)
 - Email Reply (0 / 0)
 - Forwarded Email (0 / 0)
 - Labels (0 / 0)
 - Bookmarks
 - Cluster Topic
 - Document Content

File Content

Hex	Text	Filtered	Natural
000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
060	00 00 00 00 5B 45 AD A9-18 E1 1B 86 C4 1A 07 19		...E-@-á-Ä...
070	05 60 00 00 36 F7 4C 65-7E B8 18 63 B7 24 07 19		...6+Le-,c-6...
080	91 72 01 00 85 BA 40 4C-D6 5A 64 2C 41 28 07 19		...°@LÖZd,A(...
090	15 06 00 00 1D 2A 2E 16-05 7B 38 0A B4 2E 07 19		...*....{8-...
0a0	05 3B 00 00 17 C9 02 D6-16 E1 81 F0 09 2F 07 19		...Ë-Ö-á-8-/...
0b0	95 7E 05 00 9F CD 4A 80-D6 78 6C 43 4A 2F 07 19		...~ÏJ-Öx1CJ/...
0c0	01 95 0B 00 A4 81 9D CD-73 5A 1D B9 E7 31 07 19		...x-ÏsZ-³g1...
0d0	95 6A 03 00 47 E9 49 04-93 B4 B4 7E 0F 32 07 19		...j-ËéI-...2...
0e0	15 6A 03 00 3B 7E 3A 3A-51 18 37 6B C2 36 07 19		...j-...:Q-7kÅ6...
0f0	15 14 0A 00 AF 22 7B 26-C7 DF 56 F1 24 3C 07 19		...""[sBVñs<...

Cursor pos = 0; clus = 3029929; log sec = 24239437; phy sec = 24446285

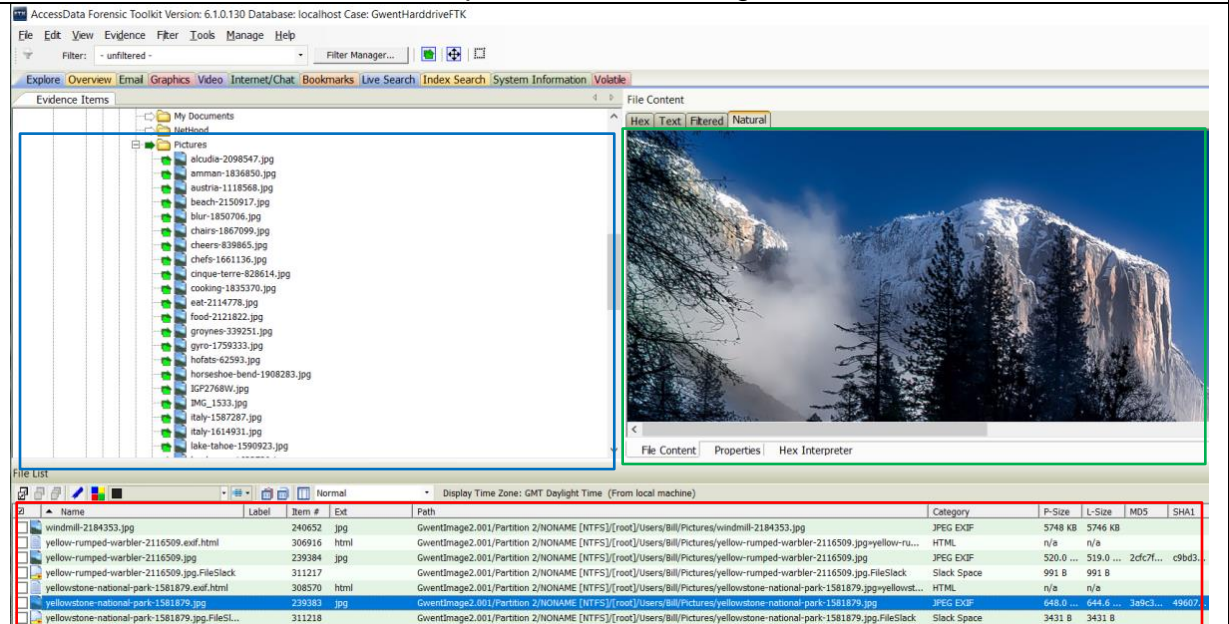
File Content Properties Hex Interpreter

File List

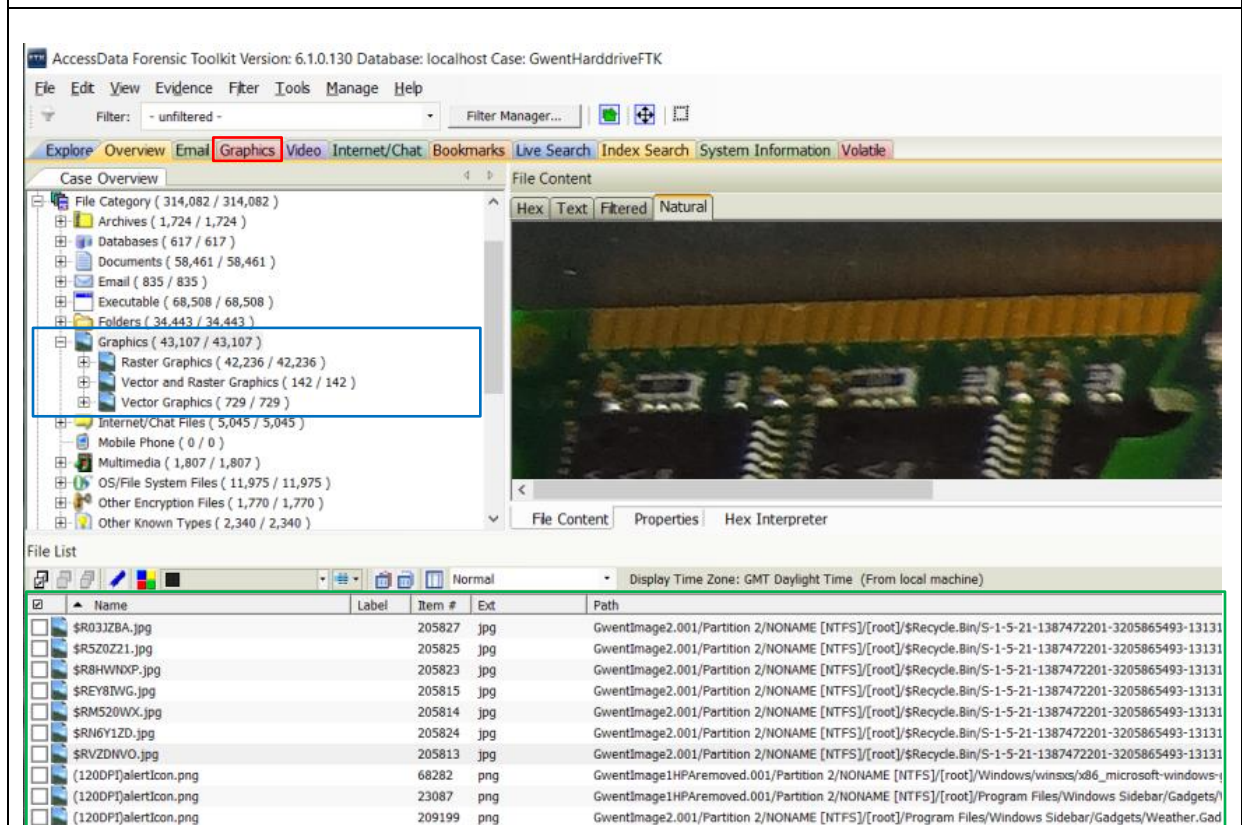
Name	Label	Item #	Ext	Path
1A9A5B38B01B2218F6555A1F1EEB0D844939...		48997	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1A9A5B38B01B2218F6555A1F1EEB0D844939...		141622		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1AC23ECB61668E8C3B43A68F9EC0072E5EE1...		33886	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1AC23ECB61668E8C3B43A68F9EC0072E5EE1...		128886		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1AE6E62744C27BF596C20119B7E80E83375F...		25394	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B0B0690FD3F24D2F8757AEDD1E1440A4222...		79811	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B0B0690FD3F24D2F8757AEDD1E1440A4222...		46818		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B29D78663875054C724F557573882CB85E3...		32421	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B5CA197C3F9879770C4F45BD016BE898818...		55806	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B5CA197C3F9879770C4F45BD016BE898818...		100121		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B994BCD445DEA86396365D2E6242F2AE3AF...		51636	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B82022E34C2857E18B643E4C000711703D3...		72491	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1B82022E34C2857E18B643E4C000711703D3...		200253		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1BD15578B8228775DA1BA7EF5556FD168D59...		43186	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1BD15578B8228775DA1BA7EF5556FD168D59...		46388		GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1C11CB99B0623C952BC13CF12BD068C1C9F...		71647	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A
1C54986C1C9827C3D09702FEC1E419C42804...		24360	<missing?>	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/A

4.3.2.2 Tests for SSD (120Gb)		Device Serial Number: W2ASSTY6
Test	Description	Result
Live Images	Does it find all the live images such as holiday, pet and food pictures	Yes, encase does find all the expected live pictures from the SSD image

This is a screenshot of all the expected live images that can be found from highlighting the users picture folder displayed on the left, with details down below of which item is selected and then previewed on the right

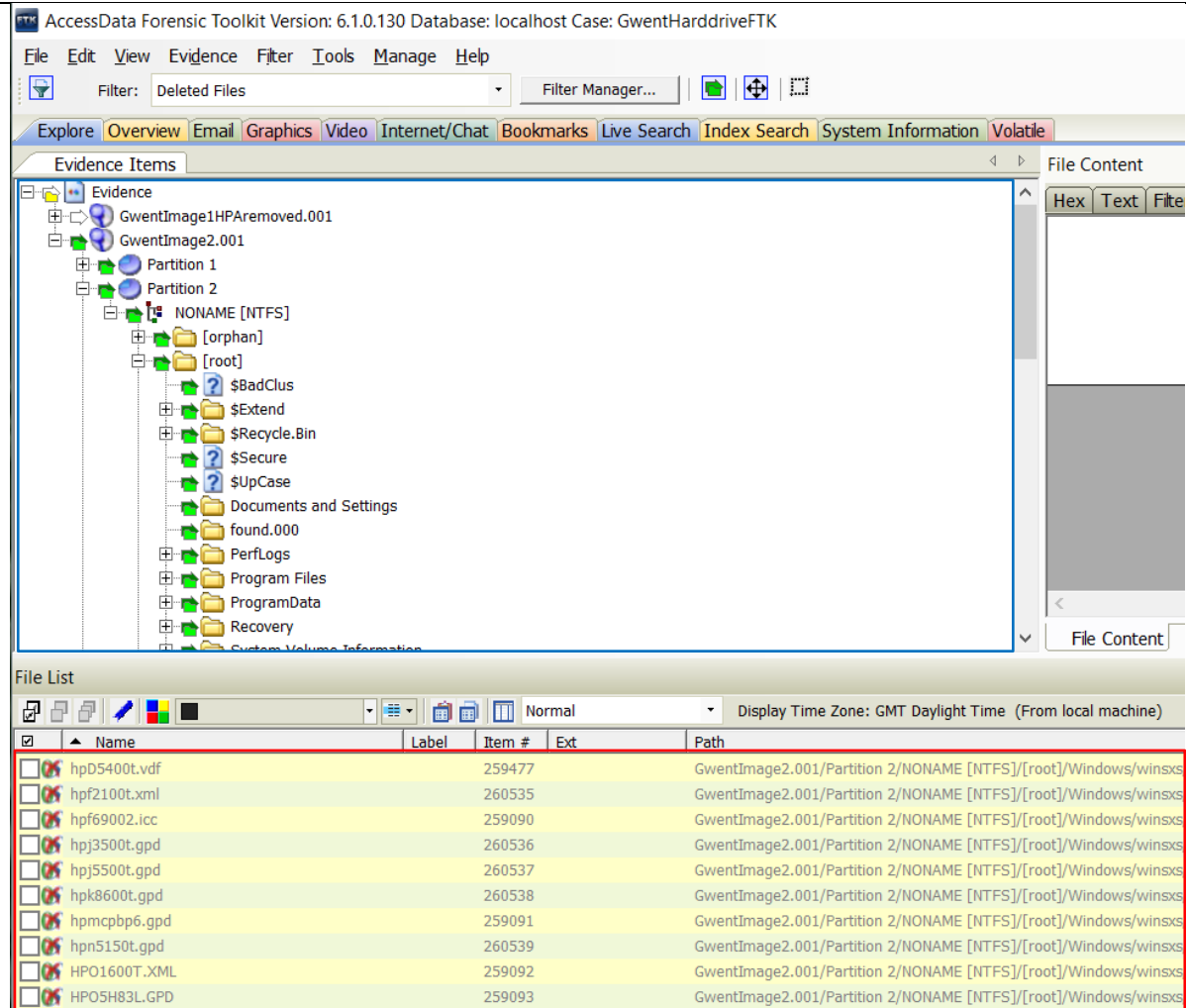


This screenshot shows all the media files that it has filtered in the graphics tab with details down in the bottom panel each one specific location on the device



Deleted Files	Does it recover the deleted files such as the old animal pictures and school documents from the raw image	No, it does find some files with FTK's easily built in filter that highlights all deleted files from the image but I could not find the expected files in the filter
---------------	---	--

Here is the screenshot of all the available deleted files from [this device](#) as [highlighted on the left](#) with more specific details of each [file recovered in the panel underneath](#)



Hidden Folders	Can it display the hidden folders containing the explicit images within the system	It doesn't make it easy to find these files and without knowing that they were hidden I cannot sure how you would be able to filter just these files in FTK
----------------	--	---

This screenshot shows the hidden folder that was placed in the program files containing [the "explicit" images highlighted on the left](#) with details of each image contained [inside the folder in the panel down below](#)

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Program Files

AVAST Software
Common Files
DVD Maker
GIMP 2
Google
Internet Explorer
MSBuild
Old Stuff
Reference Assemblies
Uninstall Information
Windows Defender
Windows Journal
Windows Mail
Windows Media Player

File Content

Hex Text Filtered Natural

A viewer for

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
\$B0		205715		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/\$B0
adorable-1846555.exif.html		324115	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/adorable-1846555.jpg>adorable-1846555...
adorable-1846555.jpg		205719	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/adorable-1846555.jpg
adorable-1851108.exif.html		324271	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/adorable-1851108.jpg>adorable-1851108...
adorable-1851108.jpg		205718	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/adorable-1851108.jpg
animal-1846557.exif.html		324490	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/animal-1846557.jpg>animal-1846557.exif...
animal-1846557.jpg		205717	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/animal-1846557.jpg
bulldog-1047518.exif.html		324354	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/bulldog-1047518.jpg>bulldog-1047518.exif...
bulldog-1047518.jpg		205716	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/bulldog-1047518.jpg
chihuahua-621112.exif.html		324511	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/chihuahua-621112.jpg>chihuahua-621112...
chihuahua-621112.jpg		205720	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/chihuahua-621112.jpg
chihuahua-621112.jpg.FileSlack		326520		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Old Stuff/chihuahua-621112.jpg.FileSlack

Encrypted Folders

Does the tool find and flag encrypted files and their contents

Yes, it does and clearly flags and classifies that those files are encrypted

This screenshot shows all the encrypted files on the system using FTK's default filters and the expected files that were encrypted and marks them all in red making them easy to find in the panel at the bottom

55

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: Encrypted Files Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Evidence

GwentImage1HPAremoved.001

GwentImage2.001

Partition 1

Partition 2

NONAME [NTFS]

[orphan]

[root]

[unallocated space]

Unpartitioned Space [basic disk]

File Content

Hex Text Filtered Natural

File Content Properties Hex Interpreter

File List

Normal

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
!CreateFolder	322233			GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Temp/OpenOffice 4.1.3 (en-US) Installati...
adorable-1846555.jpg	239368	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/adorable-1846555.jpg
adorable-1851108.jpg	239366	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/adorable-1851108.jpg
animal-1846557.jpg	239364	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/animal-1846557.jpg
Back-up.pfx	237442	pfx		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Documents/Back-up.pfx
bulldog-1047518.jpg	239362	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/bulldog-1047518.jpg
chihuahua-2101658.jpg	240222	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/chihuahua-2101658.jpg
chihuahua-621112.jpg	239360	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/chihuahua-621112.jpg
chihuahua-624924.jpg	239358	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/chihuahua-624924.jpg
dog-1027549.jpg	239352	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/dog-1027549.jpg
dog-279698.jpg	239356	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/dog-279698.jpg
dog-589002.jpg	239354	jpg		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/dog-589002.jpg
Login Data	217351	<missing?>		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Google/Chrome/User Data/Default/Login ...
MsiDigitalCertificate.CertificateForPatching	324253			GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Program Files/Google/Update/1.3.32.7/GoogleUpdateHelper.msi*M...
net-472388.inn	240220	inn		GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/Pictures/Things/net-472388.inn

Videos Live

Does the forensic tool show all live videos files on the image

Yes, it processes all the videos and displays them as expected

This screenshot shows the expected videos that are found in the video directory highlighted on the left, with more specific details of the contents of the directory found in the panel underneath

56

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

- Desktop
- Documents
- Downloads
- Favorites
- Links
- Local Settings
- Music
- My Documents
- NetHood
- Pictures
- PrintHood
- Recent
- Saved Games
- Searches
- SendTo
- Start Menu
- Templates
- Videos
 - tree-779827.jpg
 - waterfall-2187851.jpg
 - winter-mountain-2130872.jpg
- Default
- Default User
- Public

File List

Name	Label	Item #	Ext	Path
tree-779827.jpg		240672	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
waterfall-2187851.exif.html		308242	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
waterfall-2187851.jpg		240670	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
waterfall-2187851.jpg.FileSlack		315097		GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
Waterfall - 7428.mp4		240671	mp4	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
Wave Of Fog - 7102.mp4		240669	mp4	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
WhatABeautifulSunset!.mp3		240668	mp3	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
winter-mountain-2130872.exif.html		318017	html	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
winter-mountain-2130872.jpg		240686	jpg	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo
Winter - 6683.mp4		240667	mp4	GwentImage2.001/Partition 2/NONAME [NTFS]/[roo

This screenshot shows all the multimedia content that has be processed from this digital image of the SSD with details of each one's location shown in the panel at the bottom

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Case Overview

Archives (1,734 / 1,734)

Databases (666 / 666)

Documents (62,837 / 62,837)

Email (840 / 840)

Executable (70,124 / 70,124)

Folders (34,515 / 34,515)

Graphics (43,092 / 43,092)

Internet/Chat Files (5,113 / 5,113)

Mobile Phone (0 / 0)

Multimedia (1,809 / 1,809)

Audio (1,374 / 1,374)

Not Verified (12 / 12)

RIFF File (6 / 6)

Video (386 / 386)

Windows Media (6 / 6)

WMP Playlist (25 / 25)

OS/File System Files (11,980 / 11,980)

File Content

Hex Text Filtered Natural

```

000 3C 3F 77 70 6C 20 76 65-72 73 69 6F 6E 3D 22 31 <?wpl version="1
010 2E 30 22 3F 3E 0D 0A 3C-73 6D 69 6C 3E 0D 0A 20 .0"><aml>...
020 20 3C 69 65 61 64 3E 0D-0A 20 20 20 3C 6D 65 <head>...
030 74 61 20 6E 61 6D 65 3D-22 47 65 6E 65 72 61 74 ta name="Generat
040 6F 72 22 20 63 6F 6E 74-65 6E 74 3D 22 4D 69 63 or" content="Mic
050 72 6F 73 6F 66 74 20 57-69 6E 64 6F 77 73 20 4D rossoft Windows M
060 65 64 69 61 20 50 6C 61-79 65 72 20 2D 20 31 edia Player -- 1
070 31 2E 30 2E 35 34 32 38-2E 34 39 34 33 22 2F 3E 1.0.5428.4943"/>
080 0D 0A 20 20 20 3C 74-69 74 6C 65 3E 4D 75 73 <title>Mus
090 69 63 20 61 75 74 6F 20-72 61 74 65 64 20 61 74 ic auto rated at
0a0 20 35 20 73 74 61 72 73-3C 2F 74 69 74 6C 65 3E 5 stars</title>
0b0 0D 0A 20 20 3C 2F 68 65-61 64 3E 0D 0A 20 20 3C </head>... <
0c0 62 6F 64 79 3E 0D 0A 20-20 20 3C 73 65 71 3E body>... <seq
0d0 0D 0A 20 20 20 20 20 3C 73 6D 61 72 74 50 6C <smartPl
0e0 61 79 6C 69 73 74 20 76-65 72 73 69 6F 6E 3D 22 aylist version="
0f0 31 2E 30 2E 30 2E 30 22-3E 0D 0A 20 20 20 20 20 1.0.0.0">...

```

Cursor pos = 0; clus = 443383; log sec = 3547064; phy sec = 3753912

File Content Properties Hex Interpreter

File List

Normal

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
\$R05K87B.mp4		15883	mp4	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-1033339973-3797219707-...
01_Music_auto_rated_at_5_stars.wpl		228230	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
01_Music_auto_rated_at_5_stars.wpl		80948	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
02_Music_added_in_the_last_month.wpl		228229	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
02_Music_added_in_the_last_month.wpl		80947	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
03_Music_rated_at_4_or_5_stars.wpl		80946	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
03_Music_rated_at_4_or_5_stars.wpl		228228	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
04_Music_played_in_the_last_month.wpl		228227	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
04_Music_played_in_the_last_month.wpl		80945	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
05_Pictures_taken_in_the_last_month.wpl		228226	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
05_Pictures_taken_in_the_last_month.wpl		80944	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
06_Pictures_rated_4_or_5_stars.wpl		80943	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
06_Pictures_rated_4_or_5_stars.wpl		228225	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
07_TV_recorded_in_the_last_week.wpl		80942	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
07_TV_recorded_in_the_last_week.wpl		228224	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
08_Video_rated_at_4_or_5_stars.wpl		228223	wpl	GwentImage2.001/Partition 2/NONAME [NTFS]/[root]/Users/Bill/AppData/Local/Microsoft/Media Player/Sync Playlists...
08_Video_rated_at_4_or_5_stars.wpl		80941	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...
08_Video_rated_at_4_or_5_stars.wpl		80940	wpl	GwentImage1HPAremoved.001/Partition 2/NONAME [NTFS]/[root]/Users/Aaron/AppData/Local/Microsoft/Media Play...

Documents

Does the tool find all the variety of documents such as old school work and "To do lists"

Yes, FTK can find and display all the expected documents from the description

This screenshot shows all the expected files to be found on the device highlighted on the left with details of each show in the bottom panel

58

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentHarddriveFTK

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Documents

Assignment 1 Report.docx

Christmas List 2011.odt

Discussion.docx

ESDGC Themes.docx

Formula that needs work.docx

Games.xlsx

HW LIST.odt

Inventory.xlsx

Maths.xlsx

MI VIDA LOCA.odt

My Music

My Pictures

My Videos

Notes and list of things to do for spreadsheet.docx

Notes for Discussion.docx

Notes of Social Plans.docx

Project Specification.docx

Spanish Culture.odp

Technical documentation - Database.docx

File Content

Hex Text Filtered Natural

IF(I5="Monthly Membership", G5+30, IF(Or(I5="Annual M

This is meant to work out the date and add on either a m monthly or yearly

To Do List for assignment 1 Spreadsheets

Password to unlock the worksheets is the same as the on

File Content Properties Hex Interpreter

File List

Normal

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path
CompObj		308843		GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Technical documentation - Database.docx...
DocumentSummaryInformation		308844		GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Technical documentation - Database.docx...
SummaryInformation		308845		GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Technical documentation - Database.docx...
\$I30		237423		GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/\$I30
.rels		313777	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Notes for Discussion.docx>.rels
.rels		317773	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Project Specification.docx>.rels
.rels		317759	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/To Do list.docx>.rels
.rels		312234	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Notes of Social Plans.docx>.rels
.rels		317902	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Maths.xlsx>.rels
.rels		318059	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/To Do list 2.5.2013.docx>.rels
.rels		318254	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/ESDGC Themes.docx>.rels
.rels		308848	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Games.xlsx>.rels
.rels		312249	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Inventory.xlsx>.rels
.rels		317858	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Notes and list of things to do for spreadsheet...
.rels		317791	<missing?>	GwentImage2.001/Partition 2/NO NAME [NTFS]/[root]/Users/Bill/Documents/Formula that needs work.docx>.rels

Internet Search History

Can it find and display all the search history from this user in browsers in normal and private mode

Yes, it does find all the search history from the user but doesn't make it easy to specify which browser that search was conducted in unless you know the content of the sample before hand

This screenshot shows the search history from the user who was mostly frequenting Facebook and when it comes to safe searches the tool managed to extract the puppies search term that the user didn't want to found

59

Hex	Text	Filtered	Natural					
	tr-8#q=s ony+plays tation+fac ebook&*							
63	https://w ww.facebo ok.com/So nyPlaystati on/	[NULL]	Sony PlayStation - Home Facebook	1	0	no	05/04/2017 13:33:39 +0100	05/04/2017 13:33:39 +0100
64	https://w ww.facebo ok.com/pu shsquare/? ref=py_c	https:// www.fac ebook.co m/SonyP laystatio n/	Push Square - Home Facebook	1	0	no	05/04/2017 13:33:55 +0100	05/04/2017 13:33:55 +0100
65	https://w ww.facebo ok.com/PS 4DailyNew s/?ref=py_ c	https:// www.fac ebook.co m/pushs quare/?r ef=py_c	PS4 Daily News - Home Facebook	1	0	no	05/04/2017 13:46:50 +0100	05/04/2017 13:34:05 +0100
66	https://w ww.googl e.co.uk/we bhp?sourc eid=chrom e-instant& rlz=1C1AV FA_enGB7 39GB739& ion=1&esp v=2&ie=U TF-8	[NULL]	puppies - Google Search	20	0	no	07/04/2017 12:29:07 +0100	05/04/2017 13:34:36 +0100
67	https://w ww.googl	[NULL]	puppies - Google Search	20	0	no	07/04/2017 12:29:07	05/04/2017 13:34:36

4.3.2.3 Tests for USB (64 Gb)		Device Serial Number: AA00000000000485
Test	Description	Results
Documents	Does it display all the documents from the raw image	Yes, it does process all the documents from the USB

Here is the screenshot of the documents from the USB highlighted on the left with details of each shown in the panel underneath

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemoveable Devices

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Evidence

- GwentImageUSB.001
 - Partition 1
 - TRANSCEND [FAT32]
 - [root]
 - Back-up Apps
 - control-cabinet-2147373.jpg
 - network-1572617.jpg
 - Networking Files
 - Addressing the Network.docx
 - Assessment 2 draft.docx
 - Comms Cisco.docx
 - lan devices mod 4.ppt
 - osi model.ppt
 - System Volume Information
 - Tools
 - usb-686359.jpg

File Content

Hex Text Filtered Natural

A viewer for this format

File List

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Addressing the Net...		1152	docx	GwentImageUSB.00...	Micro...	164.0 ...	160.4 ...	9e8d8...	df83d...	8883c...	11/04/2017 ...	11/04/2017	16/05/2013 ...
app.xml		1497	xml	GwentImageUSB.00...	XML	n/a	714 B	7bd96...	8fa02...	261b5...	n/a	n/a	n/a
app.xml		1482	xml	GwentImageUSB.00...	XML	n/a	992 B	78fe8...	8ecab...	98f6c...	n/a	n/a	n/a
app.xml		1364	xml	GwentImageUSB.00...	XML	n/a	1004 B	e90e1...	65c28...	c9cac...	n/a	n/a	n/a
Assessment 2 draft...		1153	docx	GwentImageUSB.00...	Micro...	5812 KB	5811 KB	92ca5...	79128...	62cf1...	11/04/2017 ...	11/04/2017	10/04/2017 ...
Comms Cisco.docx		1154	docx	GwentImageUSB.00...	Micro...	28.00 ...	24.63 ...	a42b8...	55841...	5cbb6...	11/04/2017 ...	11/04/2017	10/04/2017 ...
core.xml		1498	xml	GwentImageUSB.00...	XML	n/a	643 B	c80b9...	64c7d...	46767...	n/a	n/a	n/a
core.xml		1483	xml	GwentImageUSB.00...	XML	n/a	646 B	6c998...	b2523...	8fd1d...	n/a	n/a	n/a
core.xml		1365	xml	GwentImageUSB.00...	XML	n/a	647 B	4dbea...	64fb9...	6b7d6...	n/a	n/a	n/a
Current User		1378		GwentImageUSB.00...	OLE S...	n/a	74 B	b1ad9...	51453...	27c7f...	n/a	n/a	n/a
Current User		1353		GwentImageUSB.00...	OLE S...	n/a	4096 B	c7918...	bc6af...	405bd...	n/a	n/a	n/a
customXml		1478		GwentImageUSB.00...	Place...	n/a	n/a				n/a	n/a	n/a
customXml		1360		GwentImageUSB.00...	Place...	n/a	n/a				n/a	n/a	n/a
docProps		1496		GwentImageUSB.00...	Place...	n/a	n/a				n/a	n/a	n/a
docProps		1481		GwentImageUSB.00...	Place...	n/a	n/a				n/a	n/a	n/a
docProps		1363		GwentImageUSB.00...	Place...	n/a	n/a				n/a	n/a	n/a
document.xml		1500	xml	GwentImageUSB.00...	XML	n/a	14.25 ...	07e95...	eb8c9...	af78a...	n/a	n/a	n/a
document.xml		1485	xml	GwentImageUSB.00...	XML	n/a	2211 KB	787d5...	ae7ff7...	9dcea...	n/a	n/a	n/a

Loaded: 102 | Filtered: 102 | Total: 102 | Highlighted: 0 | Checked: 0 | Total LSize: 17.48 MB

Live Images	Does it show all the images from the USB	Yes, it does find all the expected pictures that were stored on the USB
-------------	--	---

Here is the screenshot using [the built-in graphics filter to get the live images in FTK](#) with [details of each image shown below](#)

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemoveable Devices
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Category (252 / 252)
Archives (2 / 2)
Databases (0 / 0)
Documents (58 / 58)
Email (0 / 0)
Executable (27 / 27)
Folders (37 / 37)
Graphics (24 / 24)
Internet/Chat Files (0 / 0)
Mobile Phone (0 / 0)
Multimedia (0 / 0)
OS/File System Files (3 / 3)
Other Encryption Files (0 / 0)
Other Known Types (10 / 10)
Presentations (2 / 2)
Slack/Free Space (38 / 38)
Spreadsheets (0 / 0)
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
image13.png		1510	png	GwentImageUSB.00...	PNG	n/a	212.0 ...	823c7...	31aa9...	4efaf6...	n/a	n/a	n/a
image14.png		1511	png	GwentImageUSB.00...	PNG	n/a	212.0 ...	823c7...	31aa9...	4efaf6...	n/a	n/a	n/a
image15.png		1512	png	GwentImageUSB.00...	PNG	n/a	210.7 ...	b10d2...	02a82...	88165...	n/a	n/a	n/a
image16.png		1513	png	GwentImageUSB.00...	PNG	n/a	236.2 ...	7d359...	4fc71...	72505...	n/a	n/a	n/a
image17.png		1514	png	GwentImageUSB.00...	PNG	n/a	208.4 ...	83fdb...	0a456...	99845...	n/a	n/a	n/a
image18.png		1515	png	GwentImageUSB.00...	PNG	n/a	214.9 ...	7a0cc...	bc2f5...	92412...	n/a	n/a	n/a
image2.png		1516	png	GwentImageUSB.00...	PNG	n/a	252.0 ...	8b4bb...	6a254...	38677...	n/a	n/a	n/a
image3.png		1517	png	GwentImageUSB.00...	PNG	n/a	252.0 ...	8b4bb...	6a254...	38677...	n/a	n/a	n/a
image4.png		1518	png	GwentImageUSB.00...	PNG	n/a	260.3 ...	c4d7e...	a05c5...	57dc3...	n/a	n/a	n/a
image5.png		1519	png	GwentImageUSB.00...	PNG	n/a	260.3 ...	c4d7e...	a05c5...	57dc3...	n/a	n/a	n/a
image6.png		1520	png	GwentImageUSB.00...	PNG	n/a	237.8 ...	8b3ca...	ecc36...	70b98...	n/a	n/a	n/a
image7.png		1521	png	GwentImageUSB.00...	PNG	n/a	241.0 ...	a15fc...	8ddb1...	f8fffd...	n/a	n/a	n/a
image8.png		1522	png	GwentImageUSB.00...	PNG	n/a	209.9 ...	306fe...	7bf9f1...	cf196...	n/a	n/a	n/a
image9.png		1523	png	GwentImageUSB.00...	PNG	n/a	241.0 ...	a15fc...	8ddb1...	f8fffd...	n/a	n/a	n/a
network-1572617.jpg		1010	jpg	GwentImageUSB.00...	JPEG ...	2564 KB	2560 KB	27b55...	0e126...	8d79b...	11/04/2017 ...	11/04/2017	10/04/2017 ...
network-cables-494...		1011	jpg	GwentImageUSB.00...	JPEG	1768 KB	1765 KB	4f0e7...	068b5...	d1b84...	11/04/2017 ...	11/04/2017	10/04/2017 ...
router-157597.png		1012	png	GwentImageUSB.00...	PNG	228.0 ...	226.7 ...	c87bff...	da517...	b1bf6...	11/04/2017 ...	11/04/2017	10/04/2017 ...
usb-686359.jpg		1013	jpg	GwentImageUSB.00...	JPEG ...	236.0 ...	233.9 ...	40e78...	d9ef0f...	a55ed...	11/04/2017 ...	11/04/2017	10/04/2017 ...

Loaded: 24 Filtered: 24 Total: 24 Highlighted: 1 Checked: 0 Total Size: 12.36 MB

Application Files

Does it display the application files on this image

Yes, it does display all the application files with the correct extensions

This screenshot shows the content that is expected to be found which has all the application installers in the folder on the USB with details of each shown in the panel down below

62

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemovable Devices

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

Evidence
GwentImageUSB.001
Partition 1
TRANSCEND [FAT32]
[root]
Back-up Apps
Oracle_VM_VirtualBox_Extension_Pack-5.0.20
Untitled0
darwin.amd64
linux.amd64
linux.x86
solaris.amd64
win.amd64
win.x86
control-cabinet-z147373.jpg

File Content
Hex Text Filtered Natural

A viewer for this form

File Content Properties Hex Interpreter

File List

Normal
Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
.		1401		GwentImageUSB.00...	Folder	n/a	0 B				n/a	n/a	28/04/2016 ...
Acrylic_WIFI_Home_...		1102	exe	GwentImageUSB.00...	Exe	4472 KB	4471 KB	77e14...	ea6d1...	96042...	11/04/2017 ...	11/04/2017	06/03/2016 ...
avast_free_antivirus...		1103	exe	GwentImageUSB.00...	Exe	4892 KB	4889 KB	1ac91...	e8b3f...	7ea88...	11/04/2017 ...	11/04/2017	10/01/2015 ...
darwin.amd64		1409		GwentImageUSB.00...	Folder	n/a	0 B				n/a	n/a	28/04/2016 ...
DropboxInstaller.exe		1104	exe	GwentImageUSB.00...	Exe	320.0 ...	316.5 ...	e1fce...	c292b...	df902...	11/04/2017 ...	11/04/2017	15/01/2015 ...
ExtPack-license.html		1402	html	GwentImageUSB.00...	HTML	n/a	9546 B	b2e8c...	ceca8...	30c2a...	n/a	n/a	28/04/2016 ...
ExtPack-license.rtf		1403	rtf	GwentImageUSB.00...	Micro...	n/a	21.37 ...	0f954...	af4a5...	a3b42...	n/a	n/a	28/04/2016 ...
ExtPack-license.bdt		1404	bd	GwentImageUSB.00...	7 bit t...	n/a	8998 B	1271f...	65a86...	4b5e5...	n/a	n/a	28/04/2016 ...
ExtPack.manifest		1405	manif...	GwentImageUSB.00...	7 bit t...	n/a	29.12 ...	ea7d5...	b15ba...	5bba2...	n/a	n/a	28/04/2016 ...
ExtPack.signature		1406	signat...	GwentImageUSB.00...	7 bit t...	n/a	6 B	6179f...	2ea29...	08ceb...	n/a	n/a	28/04/2016 ...
ExtPack.xml		1407	xml	GwentImageUSB.00...	XML	n/a	481 B	8e849...	ddb3c...	f74ea...	n/a	n/a	28/04/2016 ...
linux.amd64		1419		GwentImageUSB.00...	Folder	n/a	0 B				n/a	n/a	28/04/2016 ...
linux.x86		1432		GwentImageUSB.00...	Folder	n/a	0 B				n/a	n/a	28/04/2016 ...
Oracle_VM_VirtualB...		1105	<miss...	GwentImageUSB.00...	GZip	15.66 ...	15.66 ...	ad35e...	17660...	11f40...	11/04/2017 ...	11/04/2017	07/06/2016 ...
PXE-Intel.rom		1408	rom	GwentImageUSB.00...	Unkno...	n/a	48.00 ...	70dfa...	62954...	fb079...	n/a	n/a	28/04/2016 ...
SkypeSetupFull.exe		1106	exe	GwentImageUSB.00...	Exe	41.04 ...	41.04 ...	c3f05...	0d975...	b1408...	11/04/2017 ...	11/04/2017	24/05/2015 ...
solaris.amd64		1445		GwentImageUSB.00...	Folder	n/a	0 B				n/a	n/a	28/04/2016 ...
Untitled0		1351	<miss...	GwentImageUSB.00...	Tar	n/a	43.79 ...	8eb2c...	a3254...	1cda5...	n/a	n/a	28/04/2016 ...

loaded: 82 Filtered: 82 Total: 82 Highlighted: 0 Checked: 0 Total LSize: 285.1 MB

Digital Tools

Will it show and categorize the software tools on this USB image

Yes, it processes and finds all the software tools that were stored on this image

It shows all the expected executable files and most importantly the tool used to make the HPA

63

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemoveable Devices

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

- [root]
 - Back-up Apps
 - control-cabinet-2147373.jpg
 - network-1572617.jpg
 - Networking Files
 - Addressing the Network.docx
 - Assessment 2 draft.docx
 - Comms Cisco.docx
 - lan devices mod 4.ppt
 - osi model.ppt
 - System Volume Information
 - Tools
 - ATAToolx32(32-bit)
 - ATAToolx64 (64-bit)
 - usb-686359.jpg
 - [unallocated space]
- Unpartitioned Space [basic disk]

File Content

Hex Text Filtered Natural

A view

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: GMT Daylight Time (From local machine)

	Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
<input checked="" type="checkbox"/>	ATATool.exe		1204	exe	GwentImageUSB.00...	Exe	52.00 ...	50.50 ...	98955...	92526...	334fe...	11/04/2017 ...	11/04/2017
<input checked="" type="checkbox"/>	ATATool.exe		1252	exe	GwentImageUSB.00...	Exe	720.0 ...	717.5 ...	1ef42...	fba51...	18d77...	11/04/2017 ...	11/04/2017
<input checked="" type="checkbox"/>	ATAToolx32(32-bit)		1251		GwentImageUSB.00...	Folder	4096 B	4096 B				11/04/2017 ...	11/04/2017
<input checked="" type="checkbox"/>	ATAToolx64 (64-bit)		1203		GwentImageUSB.00...	Folder	4096 B	4096 B				11/04/2017 ...	11/04/2017
<input checked="" type="checkbox"/>	rufus-2.1.exe		1202	exe	GwentImageUSB.00...	Exe	788.0 ...	787.9 ...	d8422...	e51a7...	284c0...	11/04/2017 ...	11/04/2017

4.3.2.4 Tests for DVDs	Device Name: Optiarc DVD RW AD-5280S
------------------------	--------------------------------------

Test	Description	Results
Music	Does it categorise music files from standard documents	Yes, FTK extracts the music files and correctly categorises the information from the disc

This screenshot shows the music files that have been filter from the information processed from the image and displays the details down below

The screenshot displays the AccessData Forensic Toolkit (FTK) interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, Manage, and Help. The main window is divided into several panes. On the left, the 'Evidence Items' pane shows a tree structure of the DVD image, with 'GwentImageDVD.iso' selected. The 'File Content' pane on the right shows a list of files, with 'Music' selected. The 'File List' pane at the bottom shows a detailed list of music files, including their names, labels, item numbers, extensions, paths, categories, sizes, and creation/modification dates. The list is filtered to show only music files, and the 'Music' category is selected.

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
bensound-betterday...		2102	mp3	GwentImageDVD.iso...	MP3 ...	2103 KB	2103 KB	277ad...	ed60e...	c700d...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-epic.mp3		2103	mp3	GwentImageDVD.iso...	MP3 ...	2441 KB	2441 KB	78046...	6ea7e...	fdbc1...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-goinghigh...		2104	mp3	GwentImageDVD.iso...	MP3 ...	3343 KB	3343 KB	2057e...	9acda...	2b1da...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-happines...		2105	mp3	GwentImageDVD.iso...	MP3 ...	3577 KB	3577 KB	3479c...	36837...	11a9c...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-memorie...		2106	mp3	GwentImageDVD.iso...	MP3 ...	3148 KB	3148 KB	fa278...	7e89f...	ea8f8...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-novembe...		2107	mp3	GwentImageDVD.iso...	MP3 ...	2899 KB	2899 KB	a016c...	5fe6f5...	48824...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-ofeliasdre...		2108	mp3	GwentImageDVD.iso...	MP3 ...	4084 KB	4084 KB	e3228...	2a87e...	ea691...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-sadday.m...		2109	mp3	GwentImageDVD.iso...	MP3 ...	2032 KB	2032 KB	fa4e0...	d5948...	a132b...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-slowmoti...		2110	mp3	GwentImageDVD.iso...	MP3 ...	2829 KB	2829 KB	e0e75...	5aa7d...	dbf07...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-sunny.mp3		2111	mp3	GwentImageDVD.iso...	MP3 ...	1914 KB	1914 KB	15e0a...	1501f...	58fd6...	10/04/2017 ...	n/a	10/04/2017 ...
bensound-tomorrow...		2112	mp3	GwentImageDVD.iso...	MP3 ...	4030 KB	4030 KB	63cc0...	5ffa8b...	00024...	10/04/2017 ...	n/a	10/04/2017 ...

Live Images	Does it show all images from that DVD	Yes, it does find the expected images from the DVD
-------------	---------------------------------------	--

Here is the screenshot of the expected live images from the DVD that have been selected on the left with a preview of the image on the right

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemoveable Devices

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

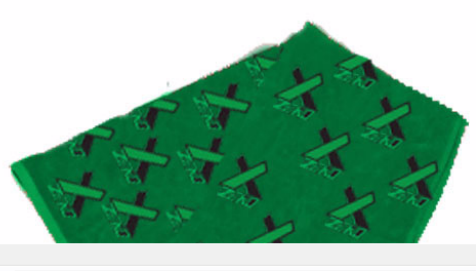
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

- Evidence
 - GwentImageDVD.iso
 - OLD MUSIC [CDFS]
 - Session 1
 - Track 01
 - OLD MUSIC [UDF]
 - Design ideas.docx
 - Music
 - Notes for assessment 1.docx
 - Old Files
 - Hand Drawns
 - images
- GwentImageUSB.001

File Content

Hex Text Filtered Natural



File Content Properties Hex Interpreter

File List

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Nutrition page 3_jpg...		2308	htm	GwentImageDVD.iso...	HTML	565 B	565 B	747b7...	dd573...	66939...	17/04/2012 ...	n/a	17/04/2012 ...
Nutrition page 3_jpg...		2214	jpg	GwentImageDVD.iso...	JPEG	1409 B	1409 B	c2f5d...	29edf...	e05f7f...	17/04/2012 ...	n/a	17/04/2012 ...
Nutrition page 3_jpg...		2258	jpg	GwentImageDVD.iso...	JPEG	84.73 ...	84.73 ...	a21f3...	9b3fd...	1b312...	17/04/2012 ...	n/a	17/04/2012 ...
pages		2305		GwentImageDVD.iso...	Folder	296 B	296 B				10/04/2017 ...	n/a	10/04/2017 ...
pages		2063		GwentImageDVD.iso...	Folder	296 B	296 B				10/04/2017 ...	n/a	10/04/2017 ...
pages		2206		GwentImageDVD.iso...	Folder	296 B	296 B				10/04/2017 ...	n/a	10/04/2017 ...
Promotional Hat_jpg...		2057	jpg	GwentImageDVD.iso...	JPEG	40.19 ...	40.19 ...	5a095...	83773...	ded17...	02/02/2012 ...	n/a	02/02/2012 ...
Promotional Hat_ps...		2058	jpg	GwentImageDVD.iso...	JPEG	36.57 ...	36.57 ...	4c4ef...	14429...	d94e4...	02/02/2012 ...	n/a	02/02/2012 ...
Promotional Towel_...		2059	jpg	GwentImageDVD.iso...	JPEG	30.65 ...	30.65 ...	c5d37...	85e34...	6e7f2...	02/02/2012 ...	n/a	02/02/2012 ...
Promotional Towel ...		2060	ipq	GwentImageDVD.iso...	JPEG	27.89 ...	27.89 ...	43ea8...	9938c...	2dd03...	02/02/2012 ...	n/a	02/02/2012 ...

Documents

Will it display the documents from this type of device

Yes, FTK does process documents from the DVD

This screenshot shows the documents processed from the DVD and displayed in the panel at the bottom

AccessData Forensic Toolkit Version: 6.1.0.130 Database: localhost Case: GwentRemoveable Devices

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

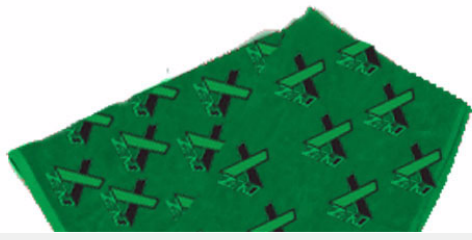
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Evidence Items

- Evidence
 - GwentImageDVD.iso
 - OLD MUSIC [CDFS]
 - Session 1
 - Track 01
 - OLD MUSIC [UDF]
 - Design ideas.docx
 - Music
 - Notes for assessment 1.docx
 - Old Files
 - Hand Drawns
 - Images
- GwentImageUSB.001

File Content

Hex Text Filtered Natural



File Content Properties Hex Interpreter

File List

Display Time Zone: GMT Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Categ...	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
.rels		2353	<miss...	GwentImageDVD.iso...	XML	n/a	590 B	77bf6...	9d7ab...	e1923...	n/a	n/a	n/a
.rels		2370	<miss...	GwentImageDVD.iso...	XML	n/a	590 B	77bf6...	9d7ab...	e1923...	n/a	n/a	n/a
[Content_Types].xml		2351	xml	GwentImageDVD.iso...	XML	n/a	1422 B	d2b47...	d09f0...	688dc...	n/a	n/a	n/a
[Content_Types].xml		2368	xml	GwentImageDVD.iso...	XML	n/a	1422 B	d2b47...	d09f0...	688dc...	n/a	n/a	n/a
_rels		2263		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
_rels		2259		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
_rels		2352		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
_rels		2369		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
app.xml		2355	xml	GwentImageDVD.iso...	XML	n/a	709 B	ae26d...	53077...	26574...	n/a	n/a	n/a
app.xml		2372	xml	GwentImageDVD.iso...	XML	n/a	980 B	cb99c...	9d38c...	17a75...	n/a	n/a	n/a
core.xml		2356	xml	GwentImageDVD.iso...	XML	n/a	749 B	da0c6...	99948...	b7a19...	n/a	n/a	n/a
core.xml		2373	xml	GwentImageDVD.iso...	XML	n/a	635 B	9cc77...	0fe50...	a1fbb...	n/a	n/a	n/a
docProps		2354		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
docProps		2371		GwentImageDVD.iso...	Place...	n/a	n/a				n/a	n/a	n/a
document.xml		2375	xml	GwentImageDVD.iso...	XML	n/a	8049 B	60d0f...	8d71e...	22297...	n/a	n/a	n/a
document.xml		2358	xml	GwentImageDVD.iso...	XML	n/a	2443 B	94cdb...	544b7...	85bf9...	n/a	n/a	n/a
document.xml.rels		2260	rels	GwentImageDVD.iso...	XML	n/a	953 B	eaf7b...	5d7ce...	31f4f4...	n/a	n/a	n/a
document.xml.rels		2264	rels	GwentImageDVD.iso...	XML	n/a	953 B	eaf7b...	5d7ce...	31f4f4...	n/a	n/a	n/a

4.3.3 AXIOM Examine v1.0.11.4067 (IEF included) Tests

Laboratory Location:
Digital Forensic Laboratory
Cardiff University
Queens Building
5 The Parade, Roath,
Cardiff CF24 3AA, UK

Tests Carried out on: 12/4/2017
Tested by: Ben Ajax-Lewis

4.3.3.1 Test for Convention Hard Drive (500Gb)

Device Serial Number: W2ASSTVA

Test	Description	Result
Browser Types	Does it find different types of browser and if they were in private mode or not from the image, the expected browsers are Firefox and Avast Safe Search	Yes, it does along the side it clearly categorizes the different browsers used by the user and if they were in safe/private mode

This screenshot shows the types of browsers down the left side and a search for bears that the user conducted while in a safe browser mode

The screenshot displays the Magnet AXIOM Examine v1.0.11.4067 interface. On the left, the 'WEB RELATED' section shows 12,655 artifacts, including Chrome/360 Safe Browser Carved Session/Tabs (9), Chrome/360 Safe Browser/Opera Carved Web History (156), Firefox Bookmarks (48), Firefox Cache Records (5,867), Firefox Cookies (630), Firefox Downloads (9), Firefox Favicons (40), Firefox FormHistory (9), Firefox Input History (2), Firefox SessionStore Artifacts (250), Firefox Web History (252), Firefox Web Visits (313), Google Analytics First Visit Cookies Carved (46), Google Analytics Referral Cookies Carved (21), Google Analytics Session Cookies Carved (29), Google Analytics URLs Carved (54), IE InPrivate/Recovery URLs (30), and Internet Explorer Cache Records (706). The main pane shows 'EVIDENCE (9)' with a table of search results. The first result is highlighted with a red box: URL: https://uk.search.yahoo.com/yhs/search;_ylt=A7x9U... Title: bears - Avast Yahoo Search Results. Below this, the 'DETAILS' section shows 'ARTIFACT INFORMATION' for the same URL. The 'TAGS AND COM' section on the right shows 'TAGS (0)' with a note 'No tags have been added' and an 'ADD NEW TAG' button. There are also checkboxes for 'Select an existing tag: Bookmark, Evidence, Of interest'.

Internet Search Terms	Does it display the internet search terms	Yes, AXIOM extracts all the search terms that the user inputted
-----------------------	---	---

This screenshot neatly filters the google search terms and displays a sample of the search terms from the user that were expected to be found

Magnet AXIOM Examine v1.0.11.4067 - GwentHardDriveImg
File Tools Help

Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results

FILTERS

Skin tone Media categories

«
Artifacts

EVIDENCE (329)
Column view

Dating Sites URLs1
Facebook URLs108
Google Analytics First Visit Cookies9
Google Analytics Referral Cookies9
Google Analytics Session Cookies9
Google Analytics URLs52
Google Searches329
Identifiers970
Parsed Search Queries55
Rebuilt Webpages135
Social Media URLs58
Tax Site URLs1
Torrent URLs1
Web Chat URLs1

CHAT10,338
EMAIL15
WEB RELATED12,655
Chrome/360 Safe Browser Carved Session/Tabs9

Search Term	URL
long hair cat breeds	https://www.google.co.uk/search?q=long+hair+c
long hair cat breeds	https://www.google.co.uk/search?q=long+hair+c
black bear cubs	https://www.google.co.uk/search?q=bear+cubs&
download firefox	https://www.google.co.uk/search?hl=en-GB&sou
everton fc	https://www.google.co.uk/?gws_rd=ssl#q=everto
long hair cat breeds	https://www.google.co.uk/search?q=long+hair+c
yahoo mail	https://www.google.co.uk/?gws_rd=ssl#q=yahoo
youtube	https://www.google.co.uk/?gws_rd=ssl#q=youtut
download firefox	https://www.google.co.uk/search?hl=en-GB&sou
HPA	https://www.google.co.uk/?gws_rd=ssl#q=HPA&?
ninite	https://www.google.co.uk/?gws_rd=ssl#q=ninite&
computer parts builder	https://www.google.co.uk/?gws_rd=ssl#q=compu
black bear cubs	https://www.google.co.uk/search?q=bear+cubs&
ergonomic chair	https://www.google.co.uk/?gws_rd=ssl#q=ergonx
32 bity	https://www.google.co.uk/?gws_rd=ssl#q=32+bit
utorrent	https://www.google.com/search?q=utorrent&ie=
anti static wrist strap ebayer	https://www.google.co.uk/?gws_rd=ssl#q=anti+s
bear cubs	https://www.google.co.uk/?gws_rd=ssl#q=bear+c

Live Images	Can the tool find all the pictures that are live from the Hard Drive Image	Yes, this tool extracts all the pictures from the hard drive
Here is a screenshot of an expected pictures to be found that have been filtered through <u>AXIOMs filters shown the left</u> with <u>details and preview of the images on the right</u>		

69

Filters: Evidence, Artifacts, Content types, Date, Time, Tags and comments, Profiles, Partial results, Keyword lists

EVIDENCE (36,127)

Image	Created Date/T...	Last Accessed...	Last Modified...	Size (B...	Date/TI...	Origina...	SI
				1264			0.0
				1069			0.0
	04/04/2017 09:59:45	07/04/2017 22:06:20	03/04/2017 21:06:12	511038			10.
				37645			0.0
				10700			74.
				1056			0.0
				97505			79.
				6917			42.
				1478			0.0
				11752			0.0
				1695			79.
				56176			0.0
				3894			0.0
				3517			2.3
				51288			29.
				12133			8.4
				10947			0.0
				7582			0.0

6917

PREVIEW

DETAILS

ARTIFACT INFORMATION

Size (Bytes) 6917
Skin Tone Percentage 42.6
MDS Hash 154b28e56146c49da4b4f6ff603c61e2
SHA1 Hash 377bb9ea31e6bfb844c566aeebb822

Time zone: UTC+000

Deleted Files

Does AXIOM find and recover all the deleted files this image

Yes, AXIOM allows for assess to contents found in the recycling bin showing that it recovers deleted files

Here is a screenshot of the files found inside the recycle bin through the filters selected on the left with the contents of the bin shown in the middle panel

Filters: Evidence, Artifacts, Content types, Date, Time, Tags and comments, Profiles, Partial results, Keyword lists

EVIDENCE (2)

File Na...	Deleted Date/T...	User Security Identifier	Original Path
Bird.mp4	04/04/2017 13:37:14	S-1-5-21-1033339973-3797219707-1025835211-10...	C:\Users\Aaron\Videos\Bird.mp4
New folder	04/04/2017 13:51:25	S-1-5-21-1033339973-3797219707-1025835211-10...	C:\Users\Aaron\Documents\New folder

Bird.mp4

DETAILS

ARTIFACT INFORMATION

File Name Bird.mp4
Deleted Date/Time 04/04/2017 13:37:14
User Security Identifier S-1-5-21-1033339973-3797219707-1025835211-1000
Original Path C:\Users\Aaron\Videos\Bird.mp4
Type File
Current Location \$ROS87B.mp4
File Size (bytes) 8756563

EVIDENCE INFORMATION

Source GwentImage1HPAreMOVED.001 - Partition 2 (Microsoft NTFS, 399.9 GB)\\$Recycle.Bin (S-1-5-21-1033339973-3797219707-1025835211-1000)\\$ROS87B.mp4
Location n/a
Evidence number GwentImage1HPAreMOVED.001

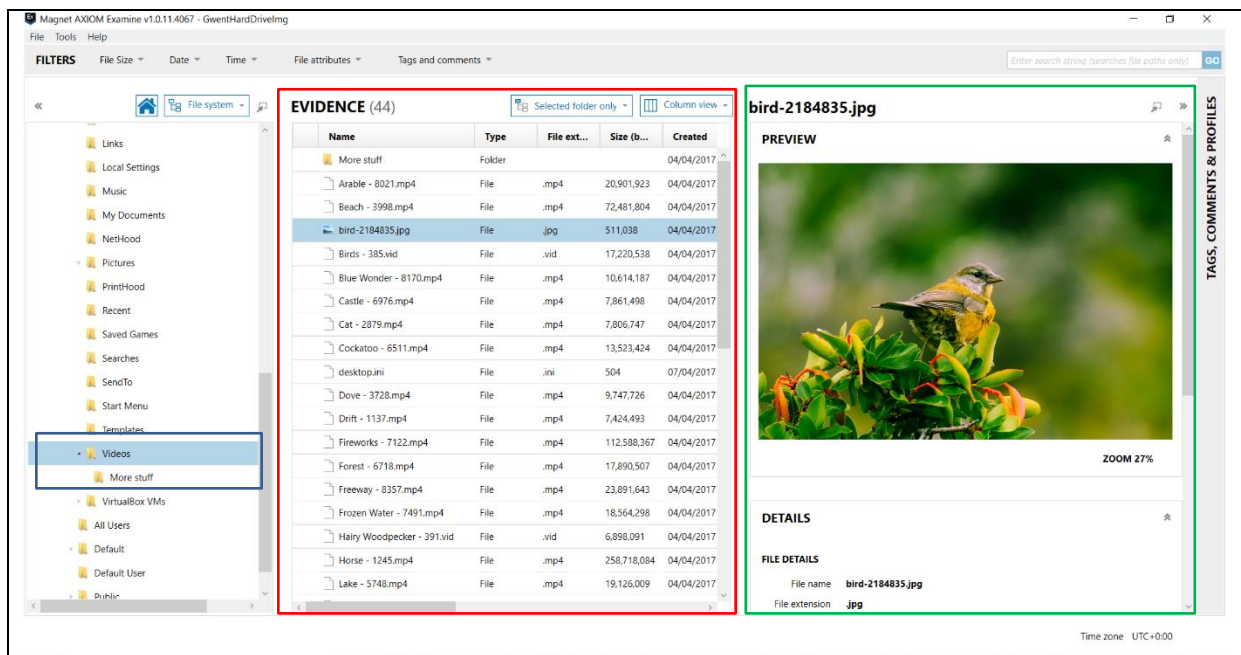
Time zone: UTC+000

Live Videos

Are all Live videos processed and found from the device

Yes, it finds all the live videos from the hard drive

The Screenshot shows all the live videos found inside the "Videos" folder which is selected on the left with details of the contents of the folder shown under the evidence heading in the middle, and a preview of the selected image on the right

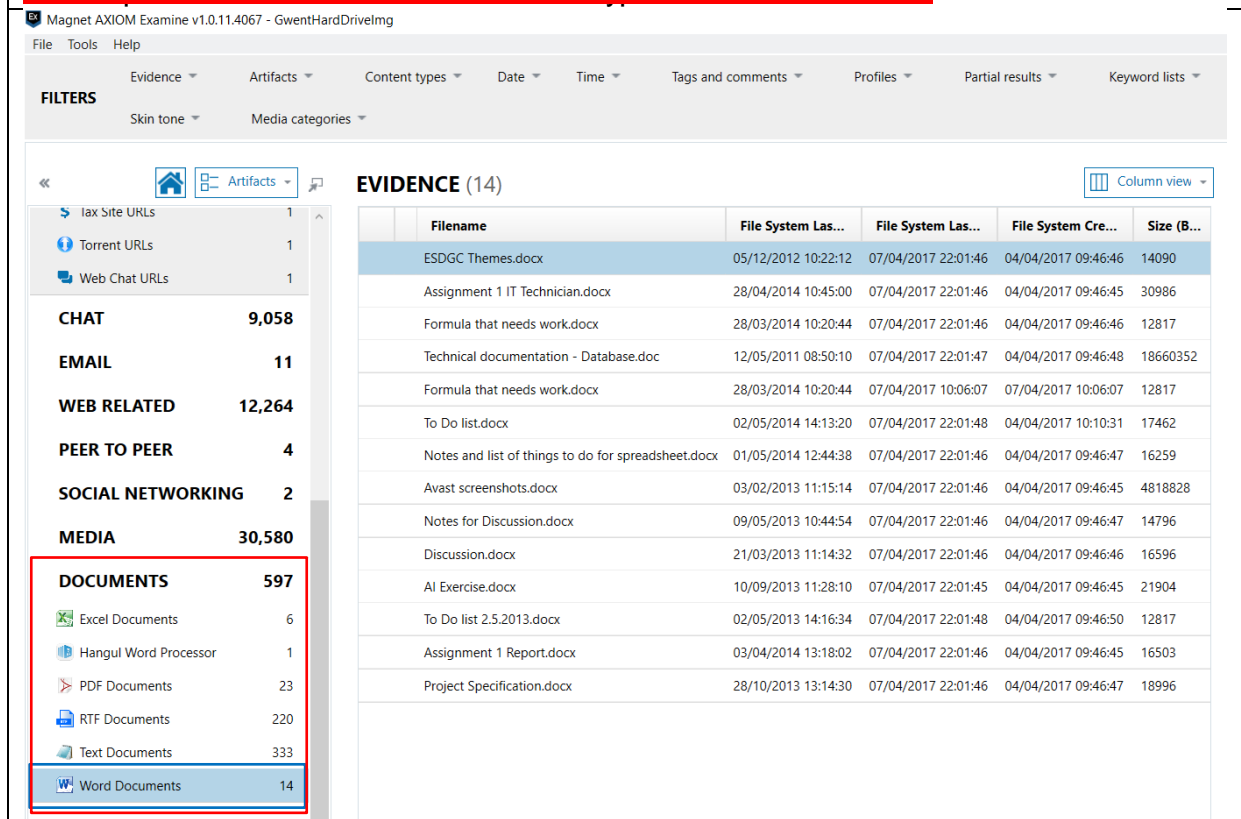


Documents

Does it display all files and their contents from the image

Yes, it does and it categorizes all the documents under the different software that each were created in

This screenshot shows all the word documents from the hard drive image and has more options to filter different document types down the left side



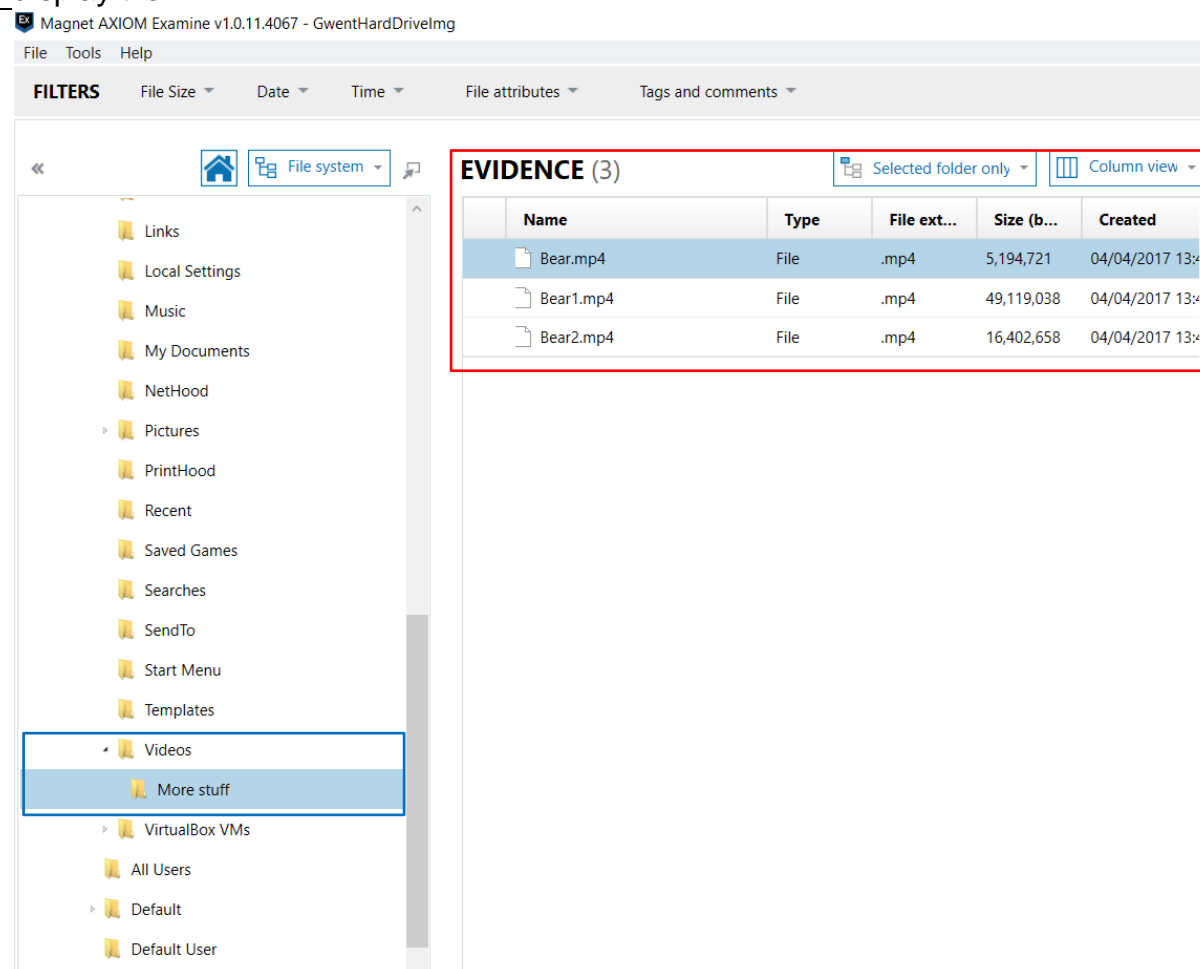
Encrypted Folders

Can it find and differentiate between

Yes, it can display the files that are encrypted but

	normal files and encrypted ones	doesn't have a filter to find them and only because I know its destination can I find the files that were encrypted
--	---------------------------------	---

Here is a screenshot of the folder that contains the files that are known to be encrypted but the tool doesn't have a specific filter to find these files but it does display them



Hidden Folders	Does it show hidden folders from within the image	Yes, it finds and displays hidden folders from the hard drive
----------------	---	---

This screenshot shows the hidden folder containing the images needed for evidence and in the details down the right side shows that the file is hidden in the attributes

Magnet AXIOM Examine v10.11.4067 - GwentiHardDrivelmg

File Tools Help

FILTERS File Size Date Time File attributes Tags and comments Enter search string (searches file p

File system

EVIDENCE (5) Selected folder only Column view

Name	Type	File ext...	Size (byt.
brown-bear-2011584.jpg	File	.jpg	10,093,287
european-brown-bear-2185337.jpg	File	.jpg	4,785,056
european-brown-bear-2186748.jpg	File	.jpg	3,984,600
grizzly-bear-600559.jpg	File	.jpg	453,126
water-1282937.jpg	File	.jpg	12,263,854

brown-bear-2011584.jpg

DETAILS

FILE DETAILS

File name: brown-bear-2011584.jpg
File extension: .jpg
Logical size: 10,093,287 bytes
Created: 05/04/2011 16:00:55
Accessed: 05/04/2011 16:00:55
Modified: 05/04/2011 16:00:55
Cluster: 5502291
Cluster count: 2465
Physical location: 22537383936
Physical sector: 44018328
MD5 hash: 39cb5ae92895cf96db2cf0127ddb2781
File attributes: Archive, Encrypted, Hidden

EVIDENCE INFORMATION

Source: GwentiImage1HPAremoved.001 - Partition 2 (Microsoft NTFS, 399.9 GB)\Users\Aaron\Pictures\Things\brown-bear-2011584.jpg
Evidence number: GwentiImage1HPAremoved.001

HPA Files

Can it see files that are in unallocated space

No, it cannot recover the files from the HPA that were populated on the image

Dropbox

Will AXIOM show files that are kept in dropbox

Yes, it can find these files and shows when the user accessed the website of dropbox

Here is the proof of AXIOM being able to find the files and know it was a picture file when it was sent to the dropbox cloud, and the tool also labels the type of URL that it has processed which in this case is "cloud services URLs"

iDrivelmg

Content types Date Time Tags and comments Profiles Partial results Keyword lists Type a search term... GO

EVIDENCE (125) Column view

Item	Type	Category
http://talkrtv.com/ad/channel.php?*", "domains": ["tal...	Cloud Services URLs	Refined Results
https://www.google.co.uk/url?sa=t&rct=j&q=&esrc...	Cloud Services URLs	Refined Results
https://www.dropbox.com/home	Cloud Services URLs	Refined Results
https://www.google.com/ads/user-lists/1000051215...	Cloud Services URLs	Refined Results
https://photos-2.dropbox.com/t/2/AABCy1-f4_FGjX...	Cloud Services URLs	Refined Results
https://www.dropbox.com/log/csp_enforced	Cloud Services URLs	Refined Results
https://www.dropbox.com/pagelet/files/browse?top...	Cloud Services URLs	Refined Results
https://dl-web.dropbox.com/installer?authenticcode_...	Cloud Services URLs	Refined Results
https://www.dropbox.com/static/images/teams/onb...	Cloud Services URLs	Refined Results
https://www.dropbox.com/download?os=win	Cloud Services URLs	Refined Results
https://www.dropbox.com/log/csp_enforced	Cloud Services URLs	Refined Results
https://www.dropbox.com/personal	Cloud Services URLs	Refined Results
https://www.dropbox.com/log/csp_enforced	Cloud Services URLs	Refined Results

https://photos-2.dropbox.com/t/2/AABCy1-f4_FGjX...

DETAILS

ARTIFACT INFORMATION

URL: https://photos-2.dropbox.com/t/2/AABCy1-f4_FGjXKOG_s3Kx6YZ4hwOjwuiY0iVHe8gjZR9Q/12/661596827/jpeg/32x32/1/_/1/2/Getting%20Started%20with%20Dropbox.pdf/EMenprFG8ogAigC/LiKDtWYdKc4fsgRAZdok9KHJrzfj8Dkx4Kh2Q0Ooo?size=32x32&size_mode=1
Site Name: Dropbox
Date/Time: 07/04/2017 10:13:29
Original artifact: Firefox Cache Records

EVIDENCE INFORMATION

Source: GwentiImage1HPAremoved.001 - Partition 2 (Microsoft NTFS, 399.9 GB)\Users\Aaron\AppData\Local\Mozilla\Firefox\Profiles\yv29u01l.default\cache2\entries\44006E29A4200ACAF4FB9B2AF1619130E35F3665
Location: n/a
Evidence number: GwentiImage1HPAremoved.001

Social Media

Does this tool label and filter social media content from the standard search terms

Yes, it can find and show information about the social media sites visited by the user

Here is the screenshot of all the Facebook information that the user has accessed using the built-in filters of AXIOM

Magnet AXIOM Examine v1.0.11.4067 - GwentHardDriveImg

File Tools Help

Evidence ▾ Artifacts ▾ Content types ▾ Date ▾ Time ▾ Tags and comments ▾ Profiles ▾ Partial results ▾

FILTERS

Skin tone ▾ Media categories ▾

« Artifacts ▾ **EVIDENCE (108)** Column view ▾

ALL EVIDENCE 69,578

REFINED RESULTS 1,893

- Classifieds URLs 30
- Cloud Services URLs 125
- Dating Sites URLs 1
- Facebook URLs 108**
- Google Analytics First Visit Cookies 9
- Google Analytics Referral Cookies 9
- Google Analytics Session Cookies 9
- Google Analytics URLs 52
- Google Searches 329
- Identifiers 970
- Parsed Search Queries 55
- Rebuilt Webpages 135
- Social Media URLs 58
- Tax Site URLs 1
- Torrent URLs 1
- Web Chat URLs 1

URL	Date/Time	Pot
https://www.facebook.com/rsr.php/v3icMq4/yG/l/e...	04/04/2017 20:10:05	Unk
https://www.facebook.com/tr/?id=95846670754566...	04/04/2017 10:45:56	Unk
https://www.facebook.com/LinusTech/about/?ref=p...		Unk
https://www.facebook.com/tr/?id=84657989874066...	04/04/2017 11:53:53	Unk
https://www.facebook.com/tr/?id=84657989874066...	04/04/2017 11:54:12	Unk
https://www.facebook.com/tr/?id=26118338100622...	05/04/2017 10:21:57	Unk
https://www.facebook.com/plugins/comments.php?...	04/04/2017 11:50:32	Unk
https://www.facebook.com/tr/?id=26118338100622...	05/04/2017 10:20:32	Unk
https://www.facebook.com/tr/?id=14551466252578...	04/04/2017 11:47:49	Unk
https://www.facebook.com/rsr.php/v3iZKe4/yv/l/e...	01/04/2017 05:46:16	Unk
https://www.facebook.com/pg/LinusTech/about/?ref...	05/04/2017 09:55:45	Unk
https://www.facebook.com/rsr.php/v3ivSr4/y0/l/en...	03/04/2017 20:01:33	Unk
https://www.facebook.com/plugins/comments.php?...	04/04/2017 11:47:51	Unk
http://staticxx.facebook.com/connect/xd_arbiter/r/1...		Unk
https://www.facebook.com/rsr.php/v3/yP/r/vOuzD...	29/03/2017 20:43:37	Unk
https://www.facebook.com/tr/?id=14551466252578...	04/04/2017 11:48:56	Unk
https://www.facebook.com/rsr.php/v3/y_r/KFLGp...	04/04/2017 05:05:52	Unk
https://www.facebook.com/tr/?id=26118338100622...	05/04/2017 10:22:05	Unk

Reconstruct web pages

Can the tool rebuild web pages from the users typed search history

Yes, the AXIOM tool can extract and rebuild the web pages from the internet history

This screenshot shows the rebuilt webpages filter being selected and the user searching in dropbox and looked for computing troubleshooting with the preview page being on the download for the Ubuntu ISO

Magnet AXIOM Examine v1.0.11.4067 - GwentHardDriveImaging

File Tools Help

Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists

Filters Skin tone Media categories

Artifacts

- Google Analytics Referral Cookies 9
- Google Analytics Session Cookies 9
- Google Analytics URLs 52
- Google Searches 329
- Identifiers 970
- Parsed Search Queries 55
- Rebuilt Webpages 135**
- Social Media URLs 58
- Tax Site URLs 1
- Torrent URLs 1
- Web Chat URLs 1

CHAT 10,338

EMAIL 15

WEB RELATED 12,655

- Chrome/360 Safe Browser Carved Session/Tabs 9
- Chrome/360 Safe Browser/Opera Carved Web History 156
- Firefox Bookmarks 48
- Firefox Cache Records 5,867

EVIDENCE (135)

Page Title	URL
	http://eticketing.evertonfc.co...
	https://d14qd3he45186l.clo...
Directory Listing: /	https://releases.mozilla.com...
	https://www.youtube.com/y...
Dropbox	https://marketing.dropbox.co...
	https://6266175.files.doublecl...
How to Install Windows 7 (Beginners) (with Pictures)...	http://www.wikihow.com/In...
	https://www.snapengage.co...
	https://cdn.doubleverify.com...
	http://pagead2.googlesyndi...
Tickets Everton Football Club	http://www.evertonfc.com/t...
	http://cdn.doubleverify.com...
Apache OpenOffice - Official Site - The Free and Op...	https://www.openoffice.org/...
	https://syimg.com/zz/comb...
	https://www.youtube.com/y...
	http://emp.bbc.co.uk/emp/5...
Home Everton Football Club	http://www.evertonfc.com/...
Google	https://www.google.co.uk/?l...

Column view

https://www.ubuntu.com/download/ubuntu-fl...

PREVIEW

[Jump to site nav](#)

[Jump to content](#)

- Cloud
 - [Overview](#)
 - [OpenStack](#)
 - [Managed cloud](#)
 - [Public cloud](#)
 - [IaaS](#)
 - [Storage](#)
 - [Partners](#)
 - [Training](#)
 - [Plans and pricing](#)
- Server
 - [Overview](#)

DETAILS

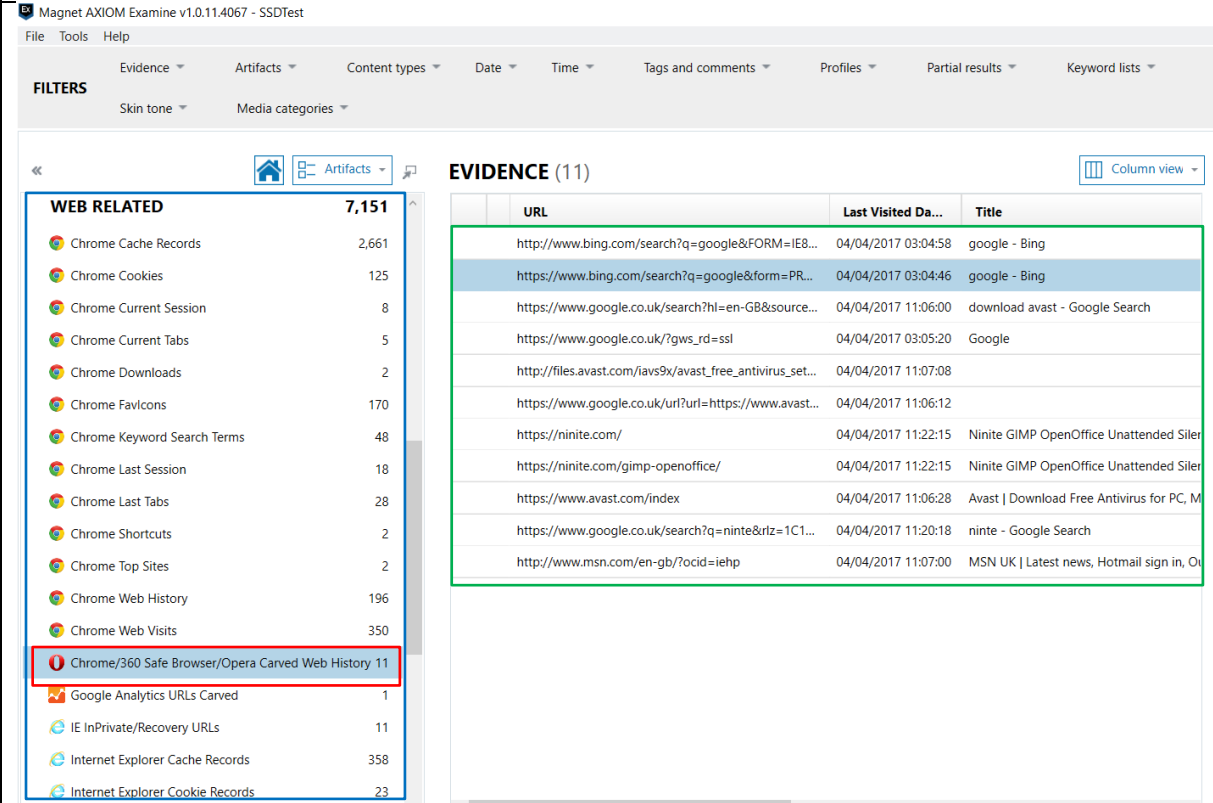
ARTIFACT INFORMATION

URL <https://www.ubuntu.com/download/ubuntu-flavours>

Page Title Ubuntu flavours | Ubuntu

Created Date/Time 05/04/2017 10:05:42

Domain www.ubuntu.com

4.3.3.2 Tests for SSD (120Gb)		Device Serial Number: W2ASSTY6
Test	Description	Result
Browsers Types	Does the tool find the different types of browsers used such as Internet Explorer and Chrome and in the different modes such as Normal and Incognito mode	Yes, the AXIOM tool can extract all this information from the SSD image
<p>This screenshot shows <u>Chrome and Internet explorer as the expected browsers</u> used by the user and <u>the safe search filter has been selected</u> with the contents of what <u>the user was searching for under the evidence heading</u></p> 		
Shows internet History	Does the tool find and display the user's internet history	Yes, it does find the search history of the user
<p>This screenshot shows the user <u>searching for "puppies" in incognito mode for google chrome</u> <u>as well as a few other things</u> with the <u>keywords filter selected on the left</u></p>		

Magnet AXIOM Examine v1.0.11.4067 - SSDTest
File Tools Help
Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists
FILTERS
Skin tone Media categories
Artifacts
EVIDENCE (48)
Column view
EMAIL 2
WEB RELATED 7,151
Chrome Cache Records 2,661
Chrome Cookies 125
Chrome Current Session 8
Chrome Current Tabs 5
Chrome Downloads 2
Chrome Favicons 170
Chrome Keyword Search Terms 48
Chrome Last Session 18
Chrome Last Tabs 28
Chrome Shortcuts 2
Chrome Top Sites 2
Chrome Web History 196
Chrome Web Visits 350
Chrome/360 Safe Browser/Opera Carved Web History 11
Google Analytics URLs Carved 1
IE InPrivate/Recovery URLs 11
Keyword Search Term URL Source
breeds of dogs https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
sony playstation facebook https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Dachshund https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Australian Cattle Dog https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Shetland Sheepdog https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Maltese https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Boxer https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
imdb https://www.google.co.uk/search?q=imdb&rlz=1C1... GwentImage2.001 - Partition 2 (N
youtube https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
puppies https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
French Bulldog https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
German Shepherd https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Australian Cattle Dog https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Shetland Sheepdog https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
Dachshund https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
twitich https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
youtube https://www.google.co.uk/webhp?sourceid=chrome... GwentImage2.001 - Partition 2 (N
ninte https://www.google.co.uk/search?q=ninte&rlz=1C1... GwentImage2.001 - Partition 2 (N
Live Images Will the forensic tool find and filter all the live images on the device Yes, it can find all the expected images from the device and displays them
Here is the screenshot of expected live images that have been processed from the device shown under the evidence heading with the pictures folder selected on the left

Magnet AXIOM Examine v1.0.11.4067 - SSDTest
File Tools Help

FILTERS
File Size
Date
Time
File attributes
Tags and comments

File system

Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
Pictures
PrintHood
Recent
Saved Games
Searches
SendTo
Start Menu
Templates
Videos
Default
Default User
Public
Windows

EVIDENCE (193)
Selected folder only
Column view

Name	Type	File ext...	Size (b...	Created	Accessed	Modified
dunes-2191641.jpg	File	.jpg	2,023,282	07/04/2017 11:13:15	07/04/2017 11:23:47	07/04/2017
eat-2114778.jpg	File	.jpg	2,957,666	07/04/2017 11:11:32	07/04/2017 11:23:47	07/04/2017
electrician-499799.jpg	File	.jpg	999,601	05/04/2017 13:05:11	05/04/2017 13:05:11	05/04/2017
file0001079221497.jpg	File	.jpg	5,123,538	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001116000079.jpg	File	.jpg	309,747	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001141038889.jpg	File	.jpg	3,665,801	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001176452626.jpg	File	.jpg	1,734,458	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001376718168.jpg	File	.jpg	2,516,390	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001454659375.jpg	File	.jpg	2,489,067	05/04/2017 13:04:12	05/04/2017 13:04:12	25/08/2017
file0001545806234.jpg	File	.jpg	4,480,979	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001565782100.jpg	File	.jpg	3,161,797	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001601969844.jpg	File	.jpg	2,435,531	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001608482449.jpg	File	.jpg	1,599,705	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001625591306.jpg	File	.jpg	1,119,395	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001637922945.jpg	File	.jpg	592,615	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001706961259.jpg	File	.jpg	885,555	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001735386118.jpg	File	.jpg	271,060	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001750264747.jpg	File	.jpg	2,301,205	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017
file0001817248786.jpg	File	.jpg	756,345	05/04/2017 13:04:13	05/04/2017 13:04:13	25/08/2017

Deleted files

Does AXIOM find all the deleted files stored on the device

Yes, AXIOM does find deleted files

This screenshot shows the deleted content from the recycle bin shown in the evidence panel, with the recycle bin filter selected on the left

78

Magnet AXIOM Examine v1.0.11.4067 - SSDTest
File Tools Help

Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists

FILTERS
Skin tone Media categories

<<
Home
Artifacts

EVIDENCE (7)
Column view

MEDIA 18,736
DOCUMENTS 592
OPERATING SYSTEM 6,039

File System Information 1
Jump Lists 21
LNK Files 160
Network Interfaces (Registry) 5
Network Profiles 3
Operating System Information 2
Recycle Bin 7
Shellbags 33
Startup Items 5
Timezone Information 2
USB Devices 24
User Accounts 12
UserAssist 40
Windows Event Logs 5,667
Windows Drafted Files 57

File Name	Deleted Date/T...	User Security Identifier	Original Path
world-1264062.jpg	05/04/2017 13:46:24	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\world-12
saturn-341379.jpg	05/04/2017 13:46:24	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\saturn-3
ram-921458.jpg	05/04/2017 13:23:46	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\ram-921
poster-76647.jpg	05/04/2017 13:46:24	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\poster-7
file8261246814968.jpg	05/04/2017 13:23:41	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\file82612
travel-1749508.jpg	05/04/2017 13:46:24	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\travel-17
file0001792779106.jpg	05/04/2017 13:23:36	S-1-5-21-1387472201-3205865493-1313131780-10...	C:\Users\Bill\Pictures\file00017

Live Videos

Are all Live videos discovered from this raw image

Yes, AXIOM does process all the live videos from the hard drive image

Here is the screenshot showing all the expected live videos in the videos folder in the file system view

Magnet AXIOM Examine v1.0.11.4067 - SSDTest

File Tools Help

FILTERS File Size Date Time File attributes Tags and comments

« File system

Desktop

Documents

Downloads

Favorites

Links

Local Settings

Music

My Documents

NetHood

Pictures

PrintHood

Recent

Saved Games

Searches

SendTo

Start Menu

Templates

Videos

Default

Default User

EVIDENCE (26) Selected folder only Column view

Name	Type	File ext...	Size (b...	Created	Accessed
My Music	Folder			04/04/2017 03:02:15	04/04/2017 0...
My Pictures	Folder			04/04/2017 03:02:15	04/04/2017 0...
My Videos	Folder			04/04/2017 03:02:15	04/04/2017 0...
Assignment 1 Report.docx	File	.docx	16,503	05/04/2017 12:30:31	05/04/2017 1...
Back-up.pfx	File	.pfx	2,558	07/04/2017 11:26:40	07/04/2017 1...
Christmas List 2011.odt	File	.odt	5,823	05/04/2017 12:30:31	05/04/2017 1...
Default.rdp	File	.rdp	0	07/04/2017 14:14:46	07/04/2017 1...
desktop.ini	File	.ini	402	04/04/2017 03:02:28	04/04/2017 0...
Discussion.docx	File	.docx	16,596	05/04/2017 12:30:31	05/04/2017 1...
ESDGC Themes.docx	File	.docx	14,090	05/04/2017 12:30:31	05/04/2017 1...
Formula that needs work.docx	File	.docx	12,817	05/04/2017 12:30:31	05/04/2017 1...
Games.xlsx	File	.xlsx	9,746	05/04/2017 13:48:13	05/04/2017 1...
ground.BMP	File	.BMP	786,486	05/04/2017 12:30:31	05/04/2017 1...
HW LIST.odt	File	.odt	5,539	05/04/2017 12:30:31	05/04/2017 1...
Inventory.xlsx	File	.xlsx	10,887	05/04/2017 12:30:31	05/04/2017 1...
Maths.xlsx	File	.xlsx	34,799	05/04/2017 12:30:31	05/04/2017 1...
MI VIDA LOCA.odt	File	.odt	1,594,494	05/04/2017 12:30:31	05/04/2017 1...
Notes and list of things to do for spreadsheet.do...	File	.docx	16,259	05/04/2017 12:30:32	05/04/2017 1...
Notes for Discussion.docx	File	.docx	14,796	05/04/2017 12:30:32	05/04/2017 1...

Hidden Folders

Does it show the hidden folders that are on the image

Yes, the AXIOM tool can find and display the hidden folders from this device

Here is a screenshot from AXIOM showing the pictures that are inside a hidden folder and it clearly states the status of the folder inside the right panel under "File attributes" as "hidden"

time File attributes Tags and comments Enter search string (searches file paths or

EVIDENCE (5) Selected folder only Column view

Name	Type	File ext...	Size (b...	Created	Accessed
adorable-1846555.jpg	File	.jpg	10,331,808	05/04/2017 13:12:28	05/04/2017 13:12:28
adorable-1851108.jpg	File	.jpg	1,423,836	05/04/2017 13:12:28	05/04/2017 13:12:28
animal-1846557.jpg	File	.jpg	4,465,331	05/04/2017 13:12:28	05/04/2017 13:12:28
bulldog-1047518.jpg	File	.jpg	2,114,094	05/04/2017 13:12:28	05/04/2017 13:12:28
chihuahua-621112.jpg	File	.jpg	2,613,884	05/04/2017 13:12:28	05/04/2017 13:12:28

adorable-1846555.jpg

DETAILS

FILE DETAILS

File name **adorable-1846555.jpg**

File extension **.jpg**

Logical size **10,331,808 bytes**

Created **05/04/2017 13:12:28**

Accessed **05/04/2017 13:12:28**

Modified **03/04/2017 22:25:12**

Cluster **3187134**

Cluster count **2523**

Physical location **13054500864**

Physical sector **25497072**

MDS hash **6ae00a451ba02eb0f84fe459787099f9**

File attributes **Archive, Hidden**

EVIDENCE INFORMATION

Source **GwentImage2.001 - Partition 2 (Microsoft NTFS, 115.62 GB)\Program Files\Old Stuff\adorable-1846555.jpg**

Evidence number **GwentImage2.001**

Social Media

Will the tool find all

Yes, this tool can show all

	interaction with social media content such as Facebook and Twitter	the social media content that the user looked at
--	--	--

This is a screenshot shows proof of all the Facebook pages that the user has visited with the currently highlighted Facebook page of “The Syndicate project”

Magnet AXIOM Examine v1.0.11.4067 - SSDTest

File Tools Help

Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists

FILTERS

Skin tone Media categories

« Artifacts

EVIDENCE (269) Column view

URL	Date/Time	Potential Activity
https://www.facebook.com/rsrc.php/v3/yx/r/aYl2pK...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/rsrc.php/v3/yw/r/NE61o...		Unknown
https://www.facebook.com/rsrc.php/v3/yN/r/Ru6Q...	05/04/2017 12:46:50	Unknown
https://www.facebook.com/rsrc.php/v3/zCt4/yZ/l/en...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/rsrc.php/v3/INDj4/yZ/l/en...		Unknown
https://www.facebook.com/rsrc.php/v3/yX/r/Yxc2id4...	07/04/2017 10:56:46	Unknown
https://www.facebook.com/rsrc.php/v3/yA/r/9fr_ePv...	05/04/2017 12:46:50	Unknown
https://www.facebook.com/rsrc.php/v3/yz/r/tia2K7w...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/rsrc.php/v3/yf/r/u0RLOS...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/TheSyndicateProject/		Looking at Facebook profile with profile id: TheSynd
https://www.facebook.com/rsrc.php/v3iZaJ4/yu/l/en...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/rsrc.php/v3/yz/r/WfGolkj...	07/04/2017 10:56:46	Unknown
https://www.facebook.com/rsrc.php/v3/inse4/y/l/en...	07/04/2017 10:53:16	Unknown
https://www.facebook.com/rsrc.php/y/l/r/H3nktOa7Z...		Unknown
https://www.facebook.com/rsrc.php/v3/y4/r/-PAXP-...	07/04/2017 10:56:46	Unknown
https://www.facebook.com/rsrc.php/v3/ye/r/7cdUH_...	05/04/2017 12:46:51	Unknown
https://www.facebook.com/pushsquare/?ref=py_c		Unknown
https://www.facebook.com/PS4DailyNews/?ref=py_c	05/04/2017 12:46:50	Unknown

ALL EVIDENCE 45,862

REFINED RESULTS 2,149

- Classifieds URLs 46
- Cloud Services URLs 1
- Dating Sites URLs 1
- Facebook URLs 269**
- Google Analytics First Visit Cookies 6
- Google Analytics Referral Cookies 6
- Google Analytics Session Cookies 2
- Google Searches 231
- Identifiers 1,096
- Parsed Search Queries 58
- Rebuilt Webpages 106
- Social Media URLs 324
- Tax Site URLs 1
- Torrent URLs 1
- Web Chat URLs 1

CHAT 11,153

Reconstructed Web pages	Can the tool reconstruct web pages from the users typed search history	Yes, the AXIOM tool can reconstruct web pages from the search history that it recovers
-------------------------	--	--

Here is a screenshot of the rebuilt webpage filter and a sample of the reconstructed webpages that have been remade from the users search history in the browsers and displayed on the right

Magnet AXIOM Examine v1.0.11.4067 - SSDTest

File Tools Help

Evidence Artifacts Content types Date Time Tags and comments Profiles Partial results Keyword lists

FILTERS Skin tone Media categories

Artifacts

ALL EVIDENCE 46,369

REFINED RESULTS 2,155

- Classifieds URLs 46
- Cloud Services URLs 1
- Dating Sites URLs 1
- Facebook URLs 269
- Google Analytics First Visit Cookies 6
- Google Analytics Referral Cookies 6
- Google Analytics Session Cookies 2
- Google Searches 232
- Identifiers 1,096
- Parsed Search Queries 60
- Rebuilt Webpages 106**
- Social Media URLs 327
- Tax Site URLs 1
- Torrent URLs 1
- Web Chat URLs 1

CHAT 11,184

EVIDENCE (106) Column view

Page Title	URL	Created Date/T...	Dom
Twitter web player	https://www.youtube.com/yts/jsbin/player-en_US-vfl...	07/04/2017 10:46:38	www.y
Twitter web player	https://twitter.com/i/videos/tweet/85012085894542...	07/04/2017 10:52:15	twitter
Twitter web player	https://twitter.com/i/videos/tweet/84929859883575...	05/04/2017 12:49:39	twitter
Twitter web player	https://twitter.com/i/videos/tweet/84994742817859...	07/04/2017 10:52:15	twitter
Twitter web player	https://twitter.com/i/videos/tweet/84994742817859...	07/04/2017 10:50:38	twitter
Twitter web player	https://aax-eu.amazon-adsystem.com/s/lu37d=imdb...	07/04/2017 10:53:06	aax-eu
Twitter web player	https://twitter.com/i/videos/tweet/84916378453510...	05/04/2017 12:48:23	twitter
Twitter web player	https://www.googletagmanager.com/gtm.js?id=GT...	04/04/2017 11:06:59	www.g
Twitter web player	https://twitter.com/i/videos/tweet/85028953495690...	07/04/2017 10:49:38	twitter
Twitter web player	https://twitter.com/i/videos/tweet/84985295543616...	07/04/2017 10:51:25	twitter
download avast - Google Search	https://www.google.co.uk/search?hl=en-GB&source...	04/04/2017 11:05:58	www.g
google - Bing	http://www.bing.com/search?q=google&FORM=IE8...	04/04/2017 03:04:57	www.b
Twitter web player	https://twitter.com/i/videos/tweet/84990394905864...	07/04/2017 10:51:25	twitter
Twitter web player	https://twitter.com/i/videos/tweet/85029636085106...	07/04/2017 10:47:18	twitter
Bing	http://www.bing.com/Passport.aspx?popup=1	04/04/2017 03:04:58	www.b
	https://securepubads.g.doubleclick.net/gpt/pubads_...	07/04/2017 10:57:20	secure
	https://pubads.g.doubleclick.net/gampad/ads?ad_ru...	07/04/2017 10:46:37	pubad
Twitter web player	https://twitter.com/i/videos/tweet/84952548876272...	05/04/2017 12:48:23	twitter

PREVIEW http://www.bing.com/search?q=...

google

Web Images Videos

53,700,000 RESULTS Date

Google

www.google.co.uk

A day in the lives of a billion people. Watc
Programmes Business Solutions + Google

Search

DETAILS

ARTIFACT INFORMATION

URL http://www.bing.com/search?
q=google&FORM=IE8SRIC

Page Title google - Bing

Created Date/Time 04/04/2017 03:04:57

Preview

4.3.4 Griffeye v17.0 Tests

Laboratory Location:
Digital Forensic Laboratory
Cardiff University
Queens Building
5 The Parade, Roath,
Cardiff CF24 3AA, UK

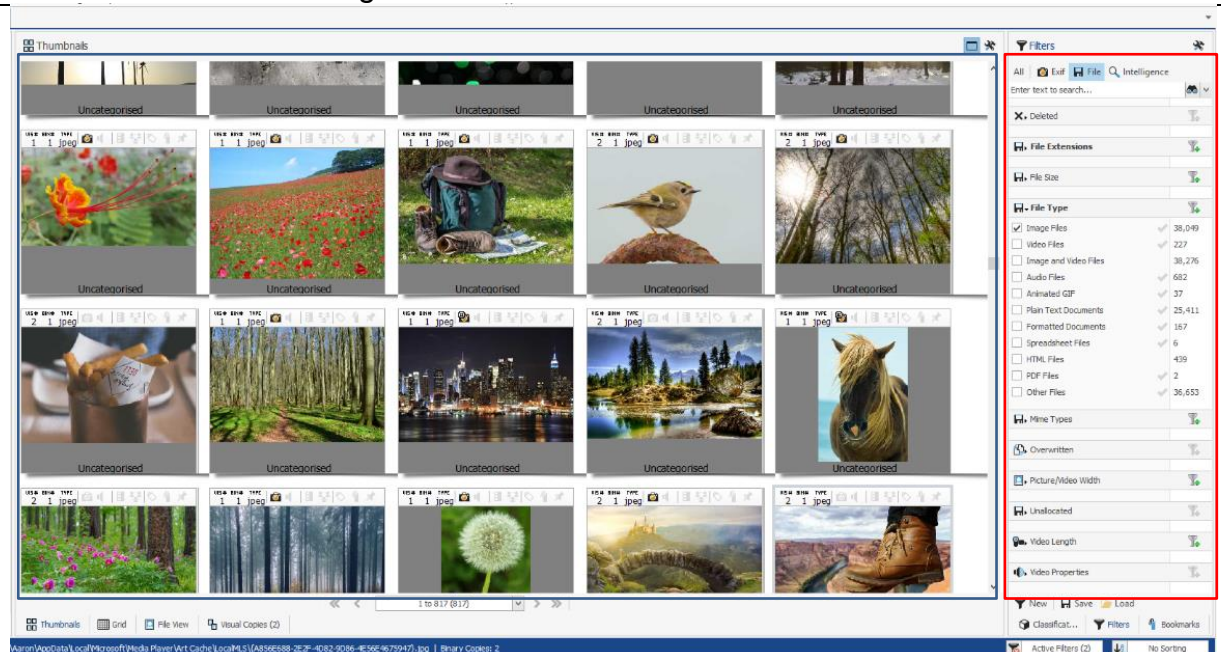
Tests Carried out on: 13/4/2017
Tested by: Ben Ajax-Lewis

4.3.4.1 Test for Convention Hard Drive (500Gb)

Device Serial Number: W2ASSTVA

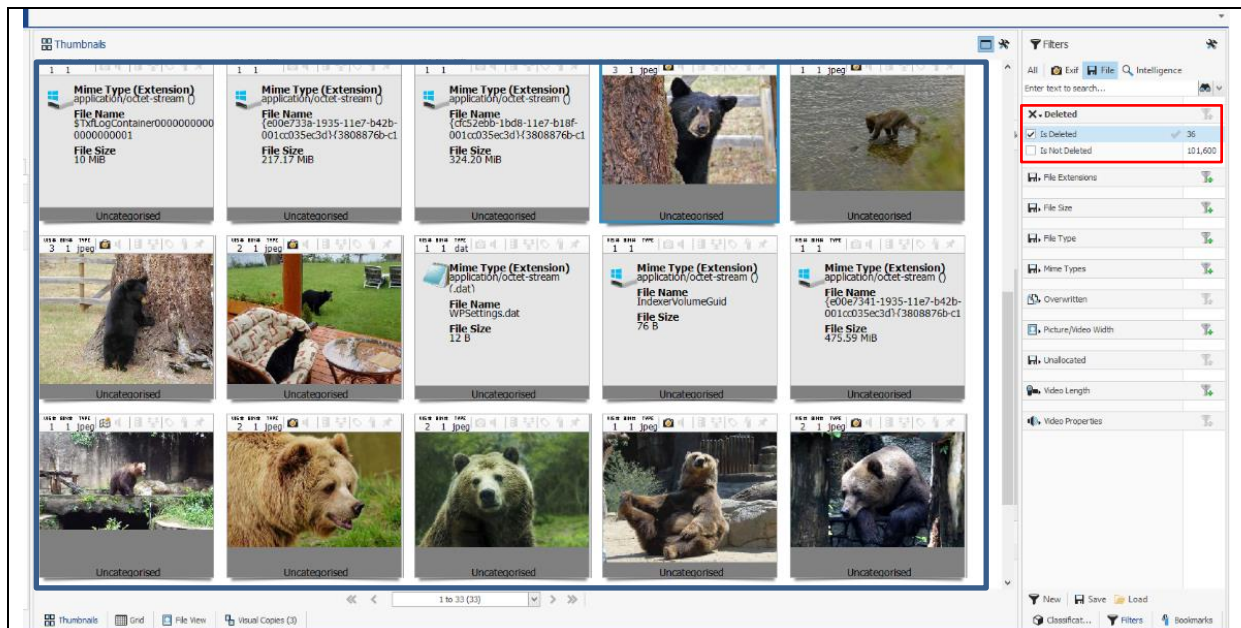
Test	Description	Result
Live Images	Are the live images displayed and filtered correctly	Yes, griffeye finds all the live images from this processed image

Here is the screenshot from griffeye showing a sample of the live images and a list of default filters down the right-hand side



Deleted Files	Does Griffeye find and recover all deleted files from the hard drive image	Yes, Griffeye recovers deleted files, but also marks files in the host protected area as deleted files as well when searching
---------------	--	---

Here is a screenshot of all the deleted files that griffeye has recovered from the image previewed in the thumbnails panel and shows the filter for deleted objects selected on the right-hand side

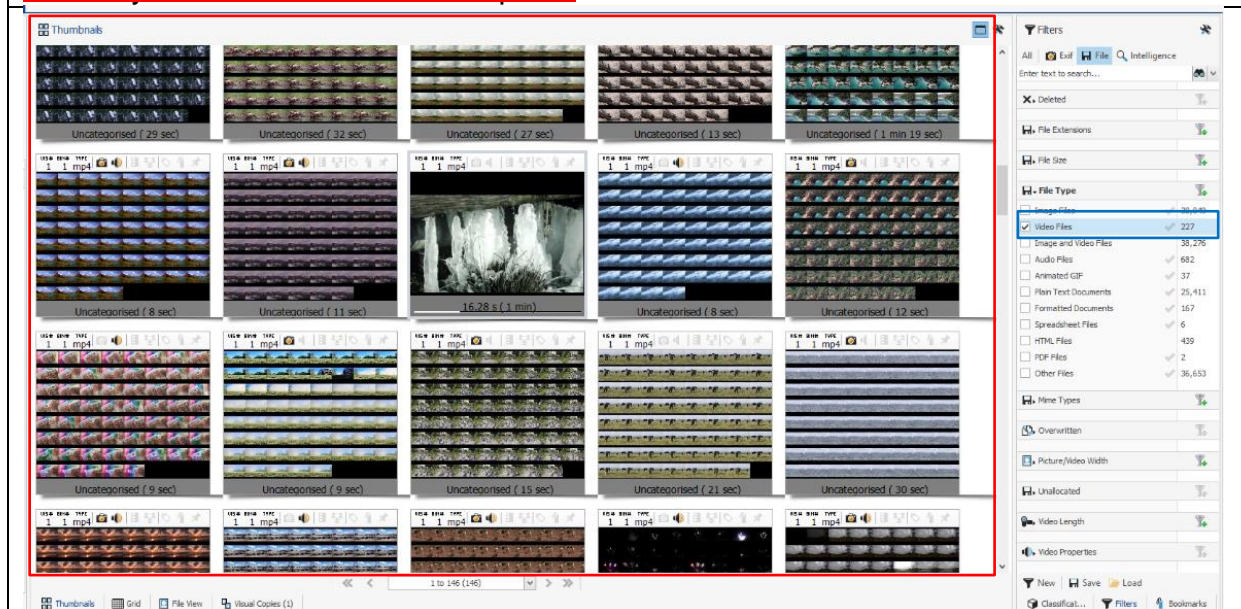


Live Video

Are the expected videos that are on this device processed and categorized correctly

Yes, Griffey does find the videos and it also allows for immediate playback when you scroll over a video so you can check it frame by frame

This is the screenshot from griffey shows the videos filter selected on the right that looks for all the live videos that has be processed from the SSD image and displayed frame by frame in the thumbnails panel

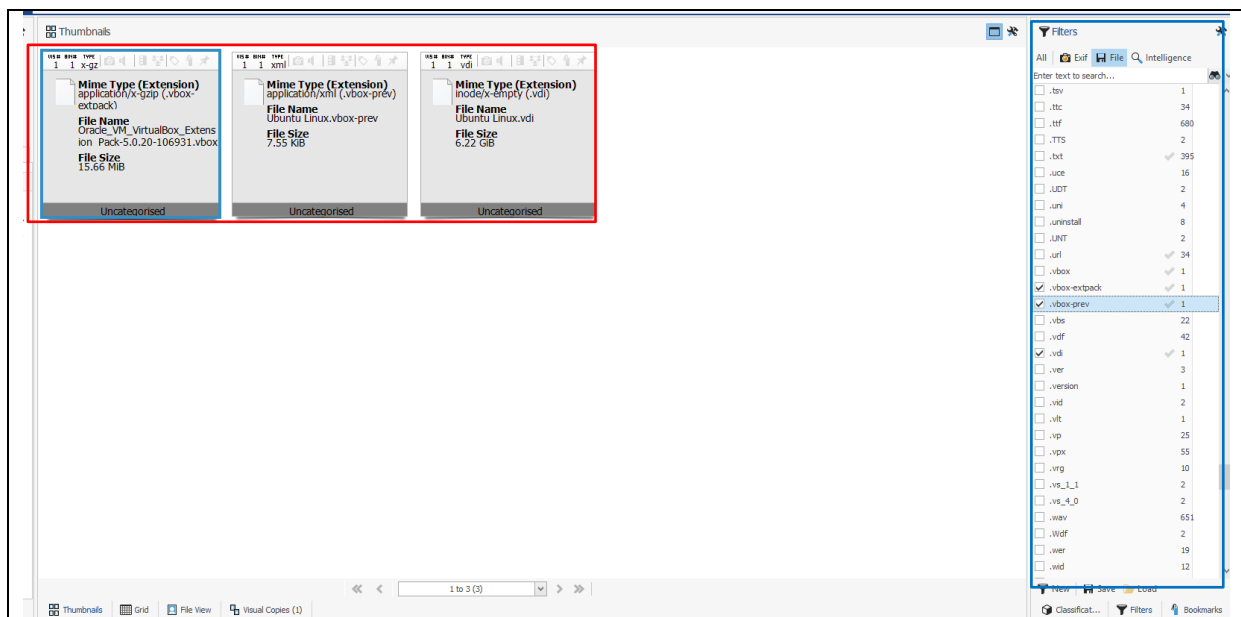


Virtual Machine

Will the Griffey tool find the information about virtual machines

Yes, it does find the virtual box files that are on the system but doesn't have access to partition files

This a screenshot shows that the default filters have a wide range of files types that can be used to find what you are looking for and in this example, it is showing the vdi files from the virtual machine

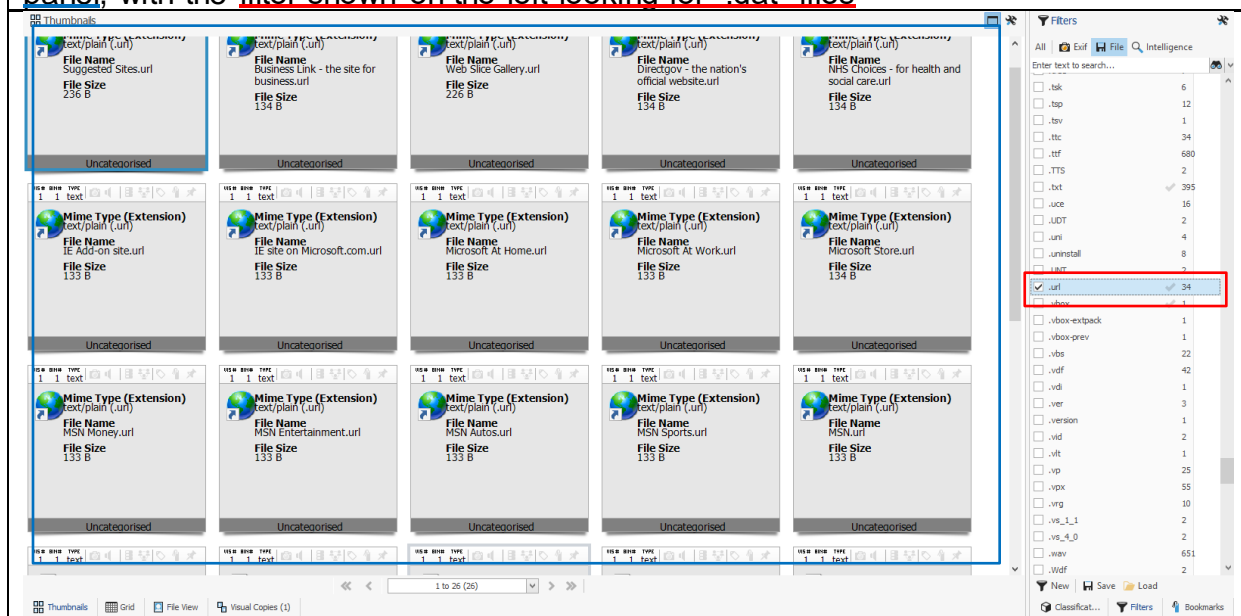


Internet Files

Does Griffey find internet files and display their content

Yes, it finds the files and displays some of the content that it can read

Here is the screenshot proof of the internet search files shown in the thumbnail panel, with the filter shown on the left looking for ".dat" files

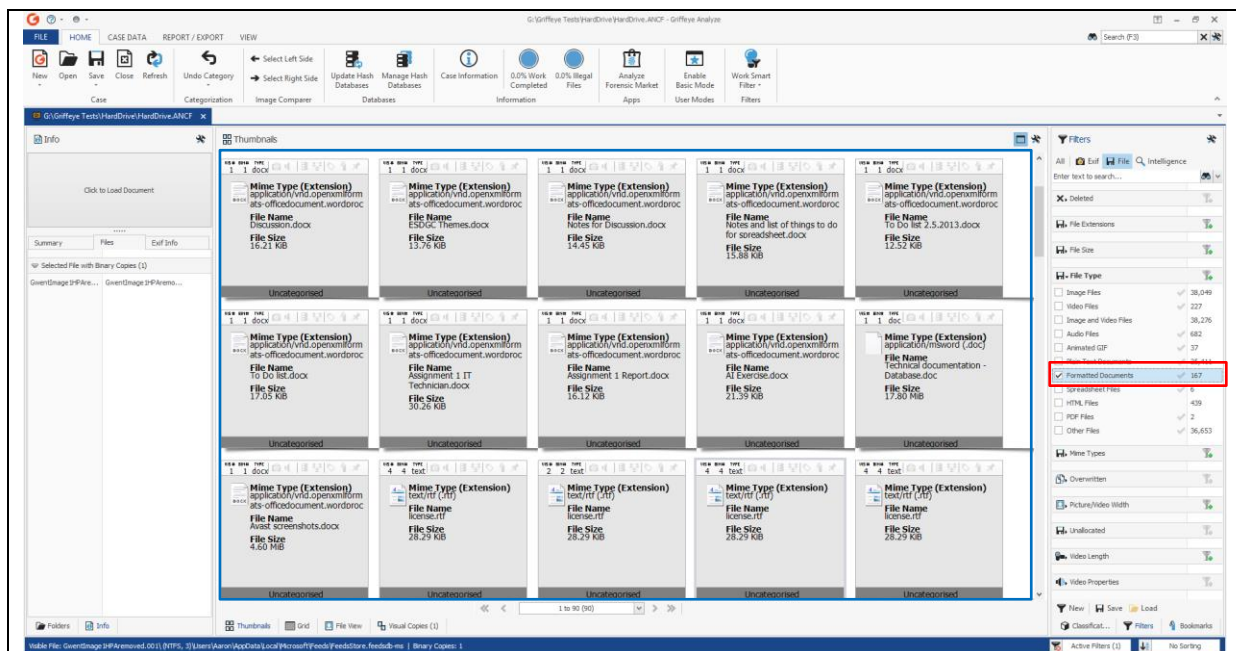


Documents

Are all the documents on this digital image shown correctly

Yes, the griffey tool can extract document files and display them

This is the screenshot of the expected documents that were extracted from the image and displayed under the thumbnail panel, with the formatted documents filter selected on the right

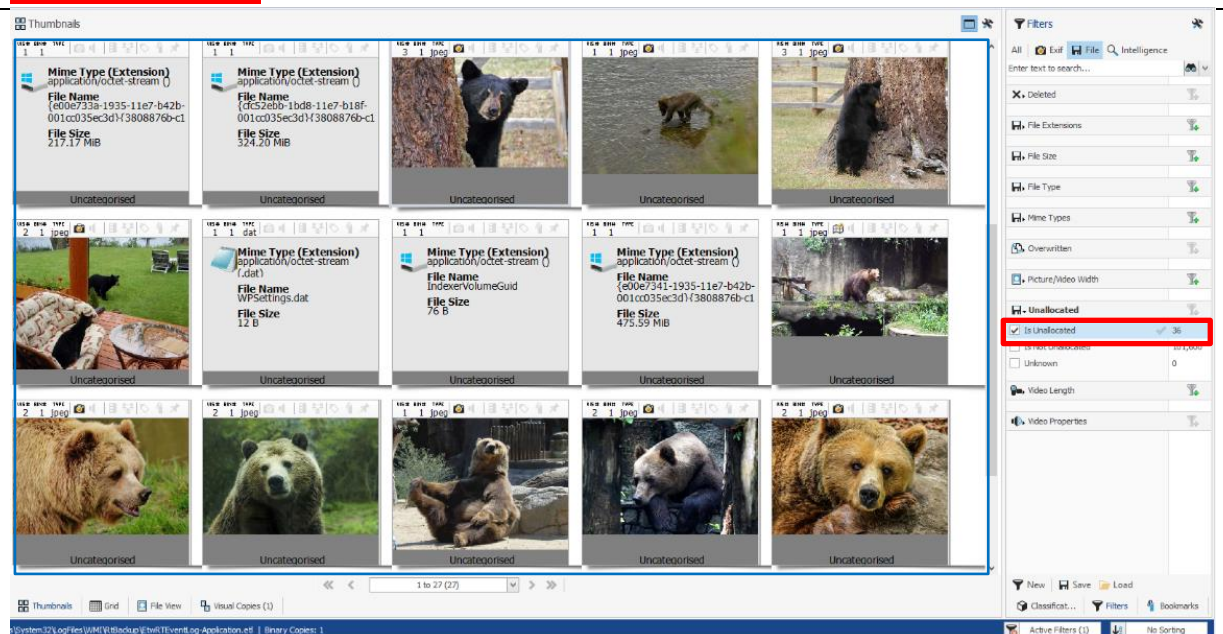


HPA files

Will the Griffeye tool be able to find and display files found in unallocated space

Yes, it does have a built-in function for unallocated space and from this it finds the images that were hidden from within

Here is the screenshot of Griffeye finding all 10 bear images that were placed on the HPA displayed in the thumbnail panel and the filter selected on the right is for “unallocated” files



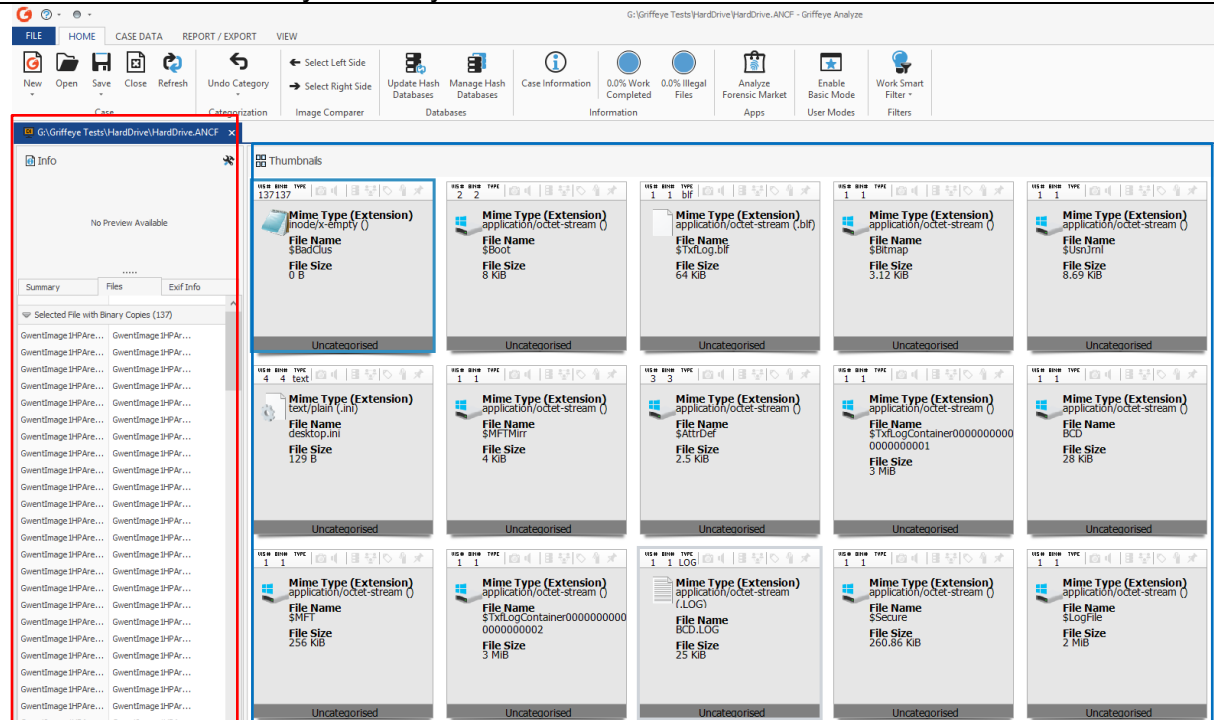
Hidden Files

Does the Griffeye tool show hidden files and folders

Yes, it does show hidden folders but it doesn't have a filter to find just the hidden files and folders on the image

This screenshot shows examples of known hidden files that are on the device in the thumbnail section and lists more details for each down the left-hand side, but it didn't

find and filter them dynamically

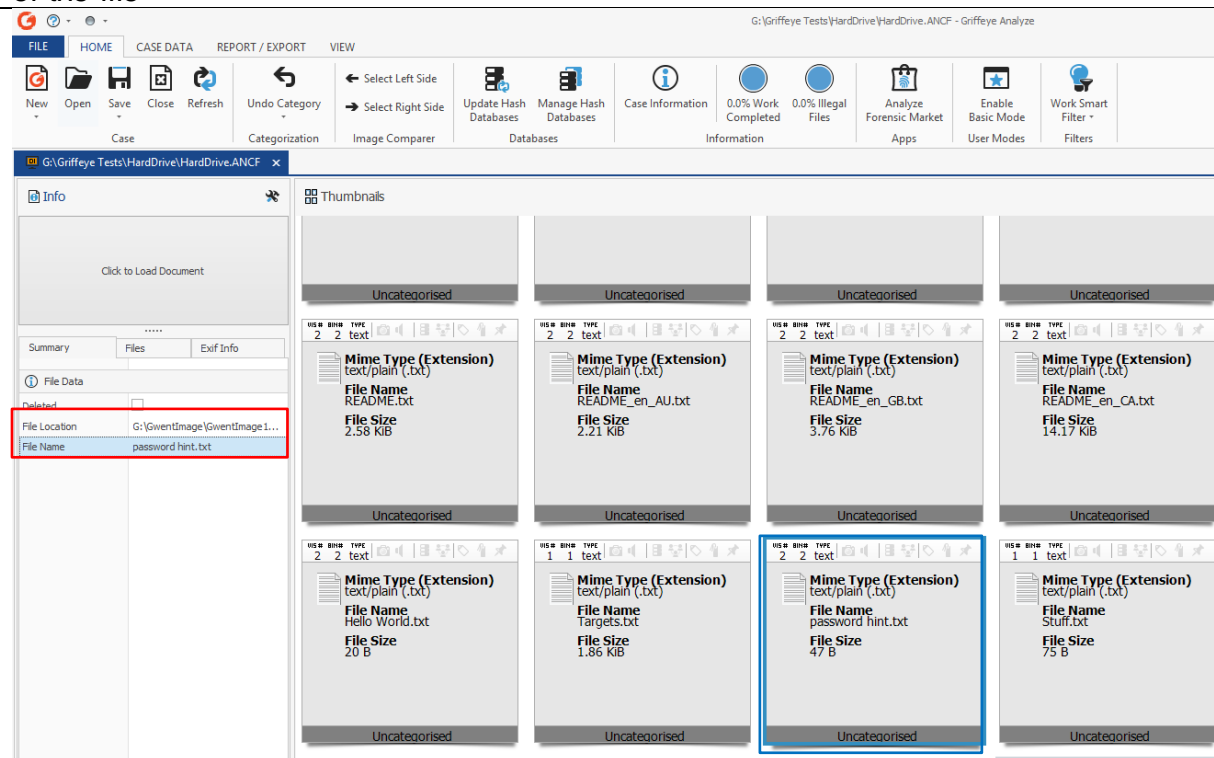


Alternate Data Streams

Will the Griffeye tool find and show the ADS attached to the files

No, it does not show alternate data streams from files and there is no filter to search for them

Here is a screenshot of the file that has an Alternate Data Stream that was manually assigned to it and griffeye only displays the first section of its extension not the rest of the file



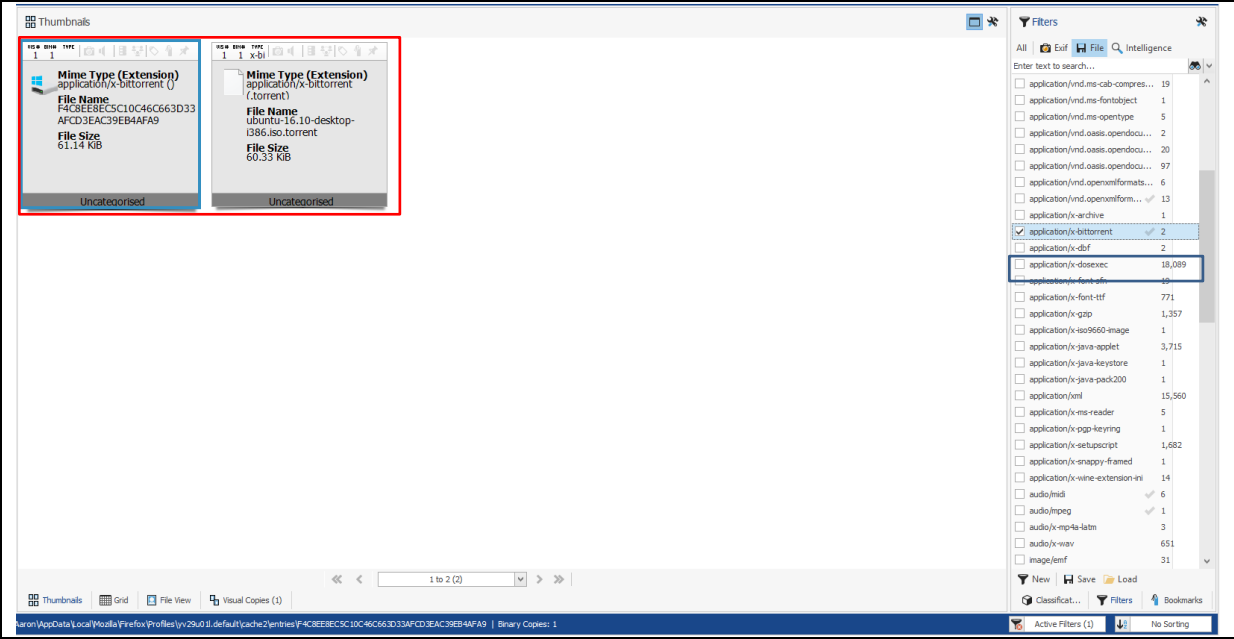
Torrents

Can the Griffeye tool filter

Yes, this tool can use filter

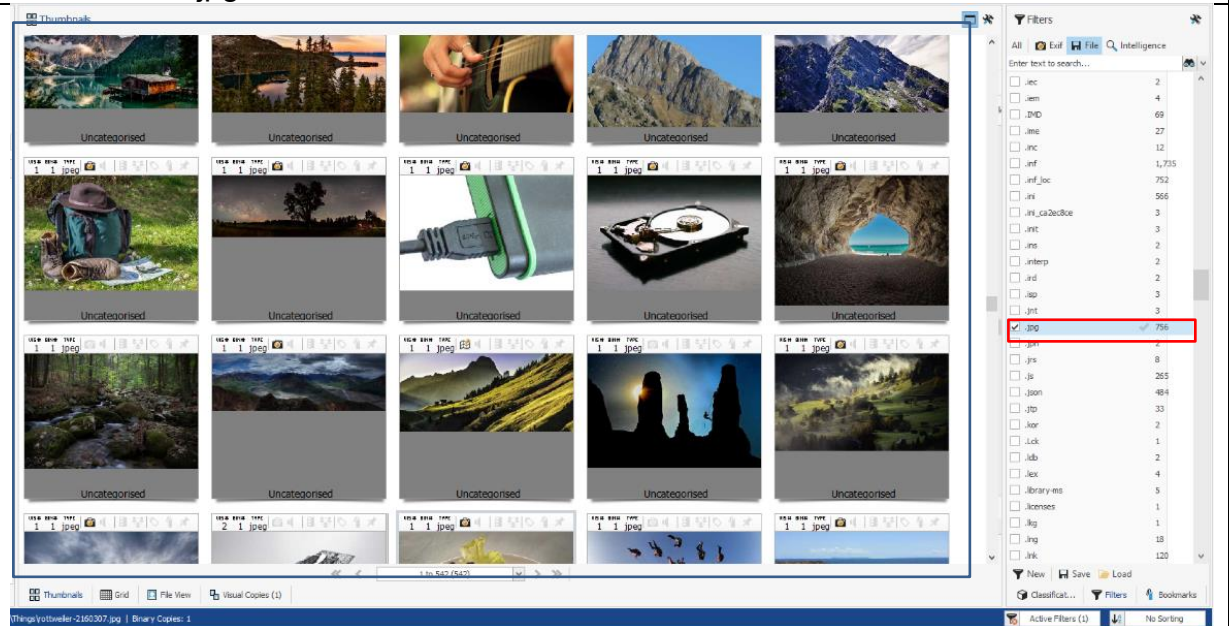
	out torrent files found on the device	options to find torrent file types
--	---------------------------------------	------------------------------------

This is a screenshot from using the built-in filters that can process all the torrents the user has downloaded and in this example, it shows the Linux ISO file



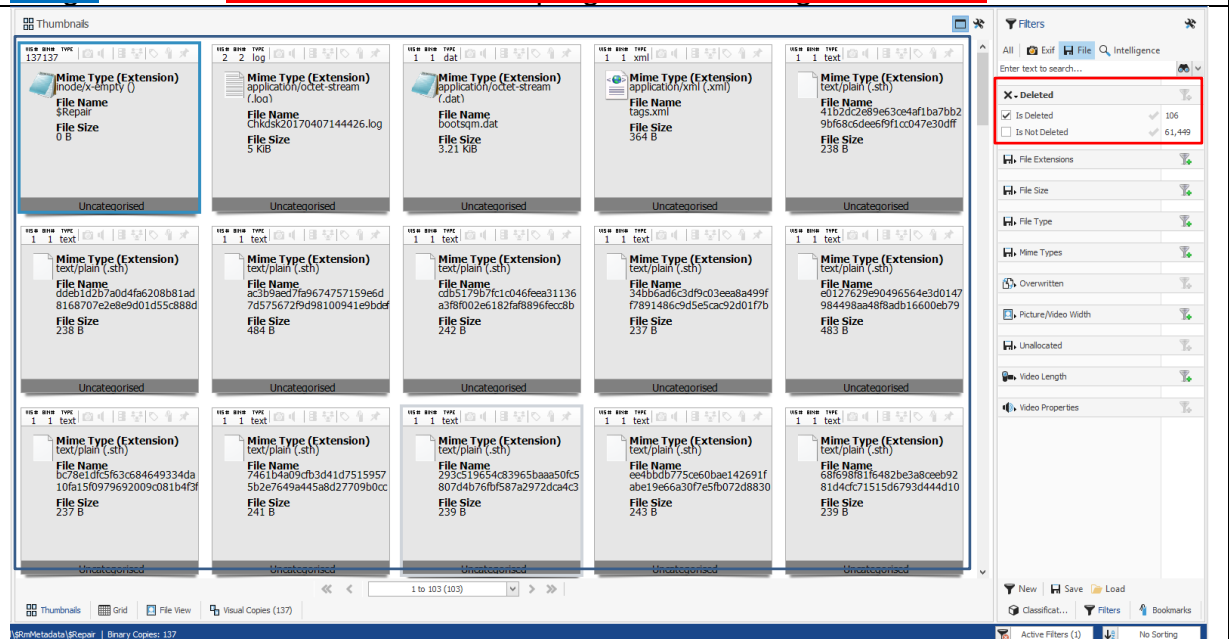
4.3.4.2 Tests for SSD (120Gb)		Device Serial Number: W2ASSTY6
Test	Description	Result
Live Images	Are the expected socializing and adventurous live pictures found on the SSD image	Yes, the Griffeye tool does process live images from this device

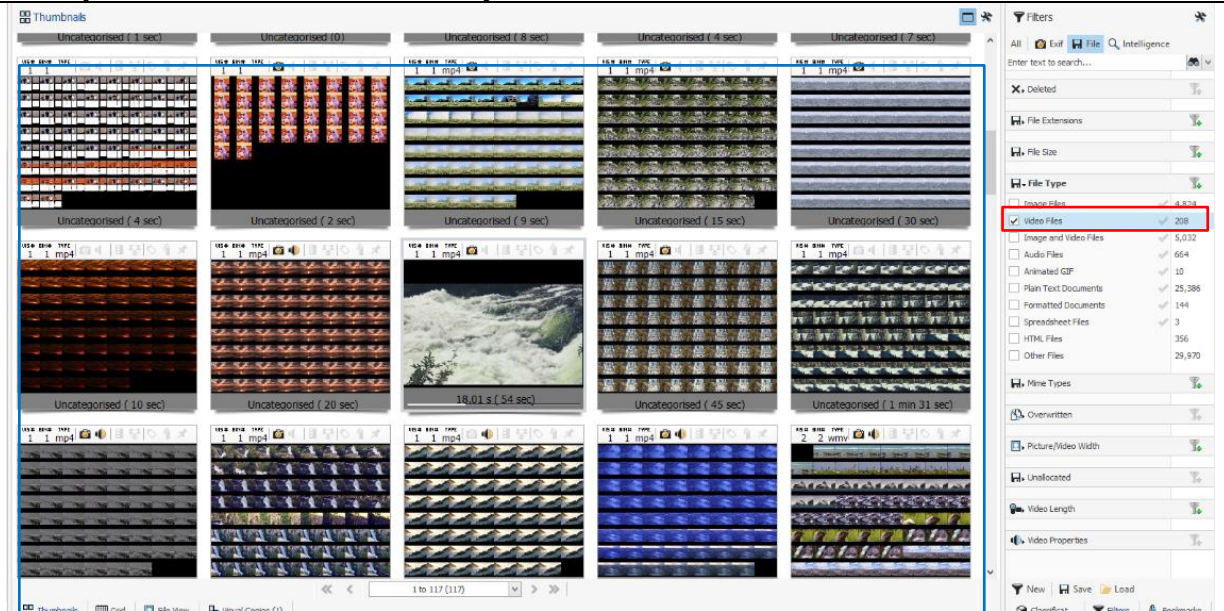
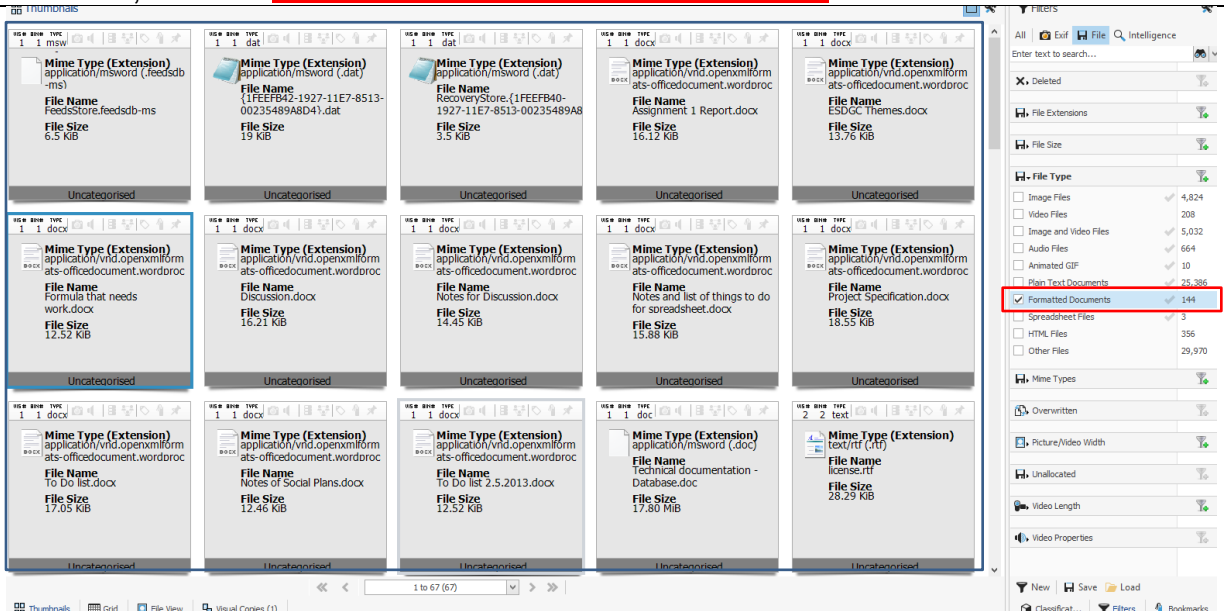
Here is the screenshot of the images that are were expected to be found on the populated SSD image displayed in the thumbnail panel, with the default filter selected as “.jpg”



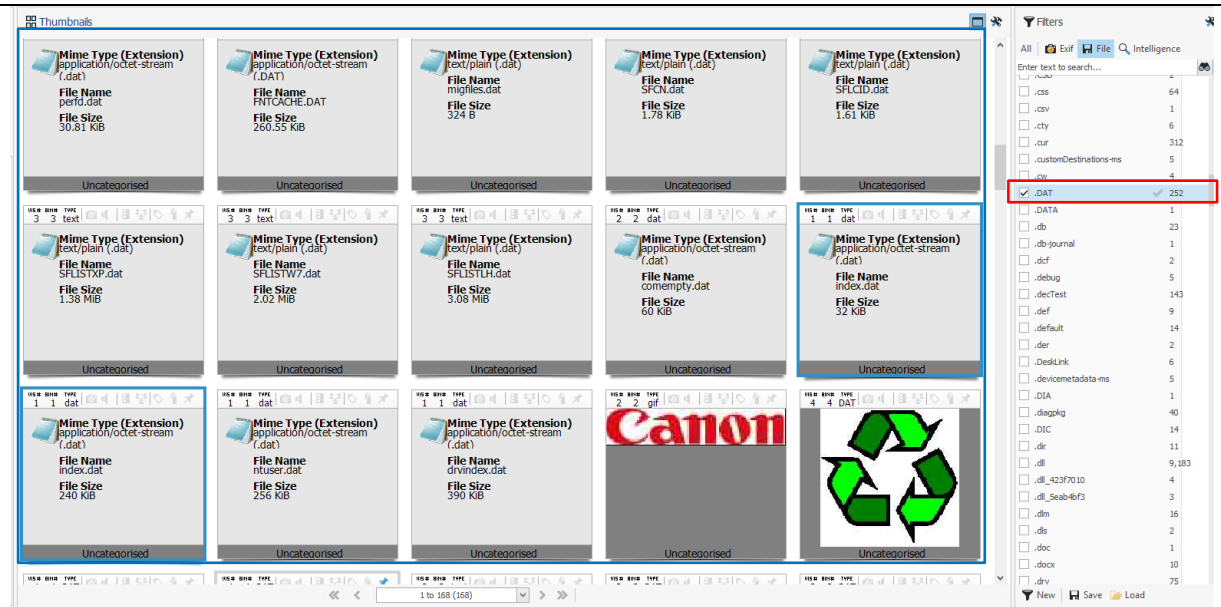
Deleted Files	Will the Griffeye tool recover the deleted files from the device image	Yes, it recovers some deleted files but I couldn't find the expected files that had been deleted
---------------	--	--

Here is the screenshot of the deleted files that griffeye has recovered from the digital image with the filter selected in the top right corner being “Is Deleted”



Live Video	Are all the expected live videos displayed within the Griffeye tool	Yes, the Griffeye tool can extract these files and classifies them correctly
This is screenshot of <u>a sample of the expected live videos</u> that can be found through Griffeye's <u>filters which are currently selected for "Video files"</u>		
		
Documents	Can the Griffeye tool display and correctly filter all the documents on the raw image	Yes, this device can display all the document from the SSD image
This is the screenshot of <u>all the expected document files</u> that had been populated on this drive, with the <u>filter selected as "formatted documents"</u>		
		
Internet Files	Will the Griffeye forensic tool show internet files and their respective browsers	Yes, the Griffeye tool does process internet files but it is very limited with the content that it displays

This screenshot shows the index.dat files that it has found and could be extracted from this tool as they contain the internet explorer history data, the filter on the right is selected as ".dat"

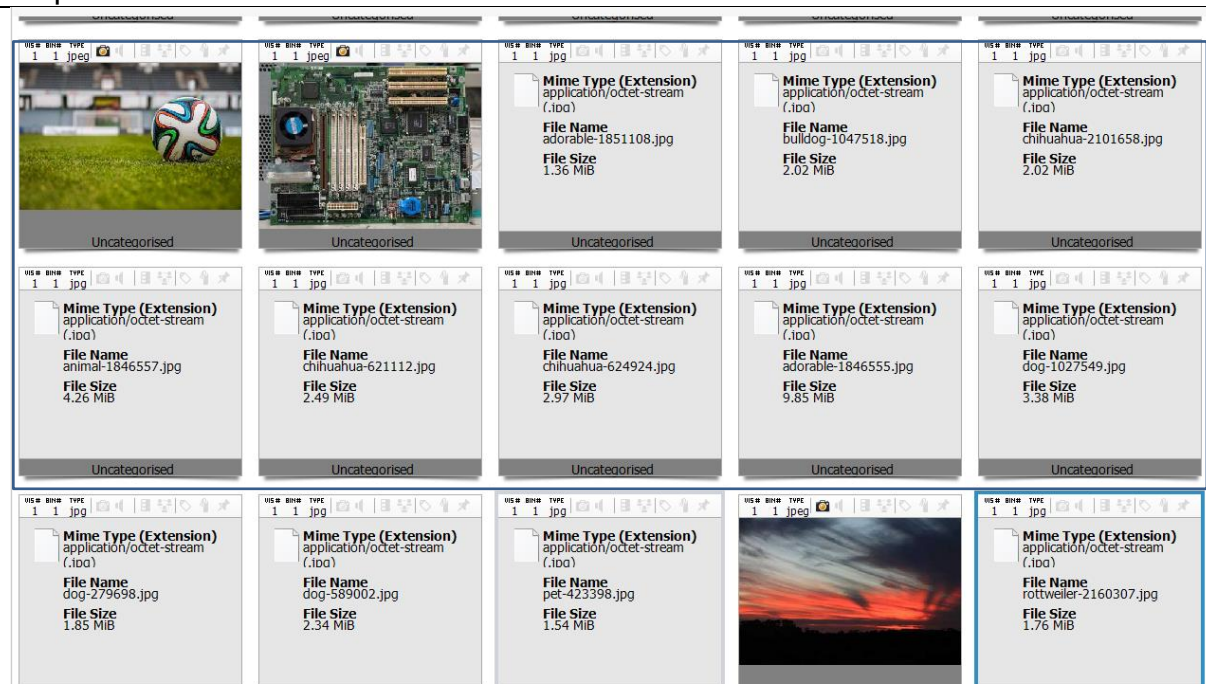


Hidden Files

Does the Griffeye forensic tool show and label the hidden files on this image correctly

Yes, it does display the hidden folders but it doesn't have a method to filter hidden folders and doesn't state that a file is hidden when looking at the details of the file

This screenshot shows all the files that have been populated onto the SSD image that are hidden or encrypted files and they stand out from other files and they cannot be previewed in the thumbnail tab



Software used

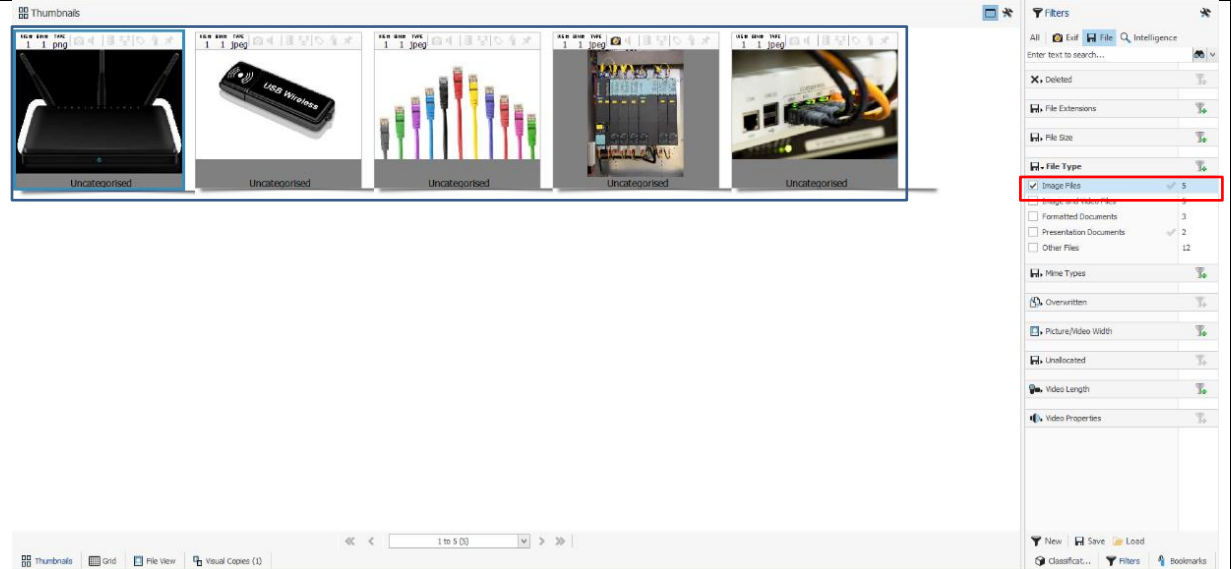
Does it show software

Yes, it does extract this

4.3.4.3 Tests for USB (64 Gb) Device Serial Number: AA0000000000485

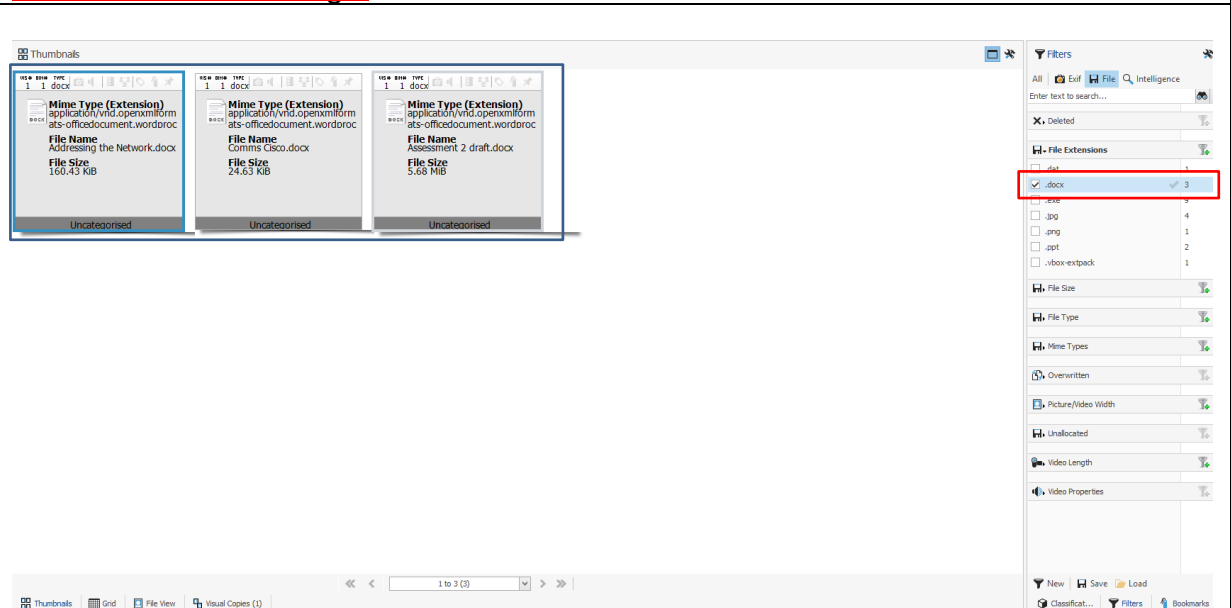
Test	Description	Results
Live Images	Does the Griffeye tool extract and display the images on the USB device	Yes, The Griffeye tool does find and display the live images from the USB

Here is the screenshot showing the images that have been taken from the USB and were found using the "image Files" filters shown on the right



Documents	Does the Griffeye tool find and display the networking documents stored on the USB image	Yes, Griffeye does show the documents that are on this USB device
-----------	--	---

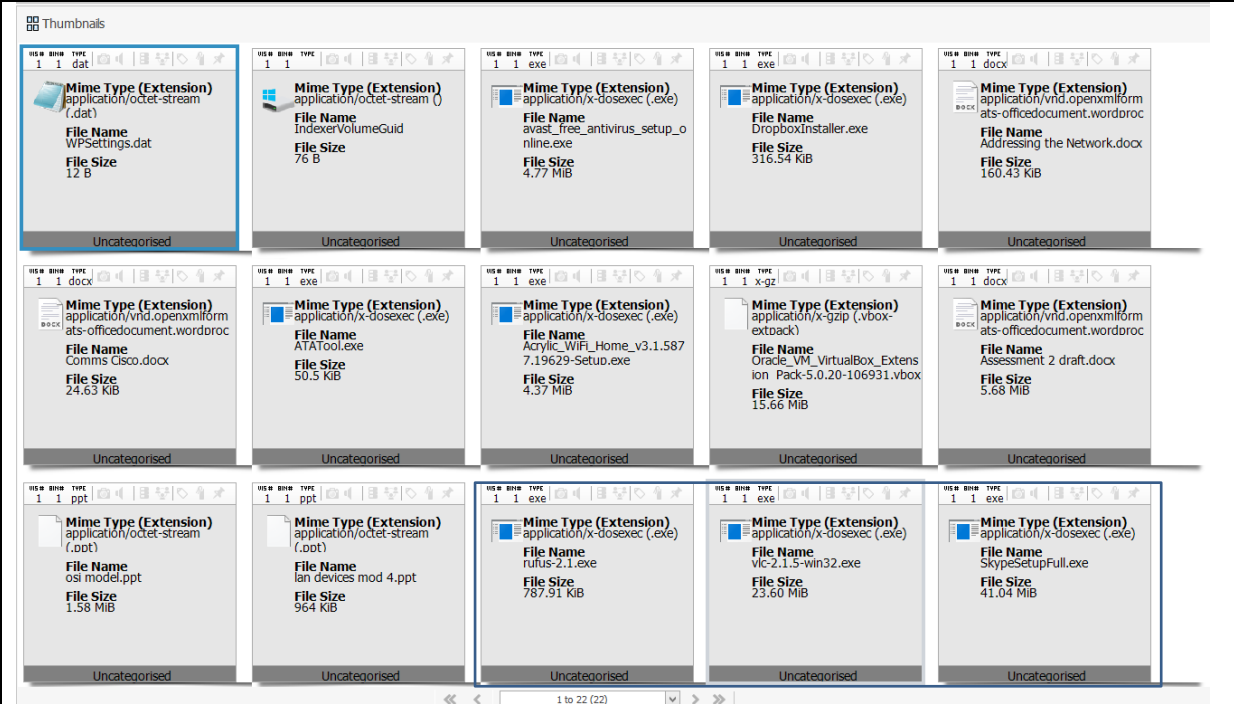
Here is the screenshot showing the documents from the USB device with the "docx" filter selected on the right



Application Files	Does the Griffeye tool display the application files on this USB image	Yes, the Griffeye tool allows for a lot of filters which can display the application files
-------------------	--	--

on the USB

This screenshot shows the application installers that are on the USB drive

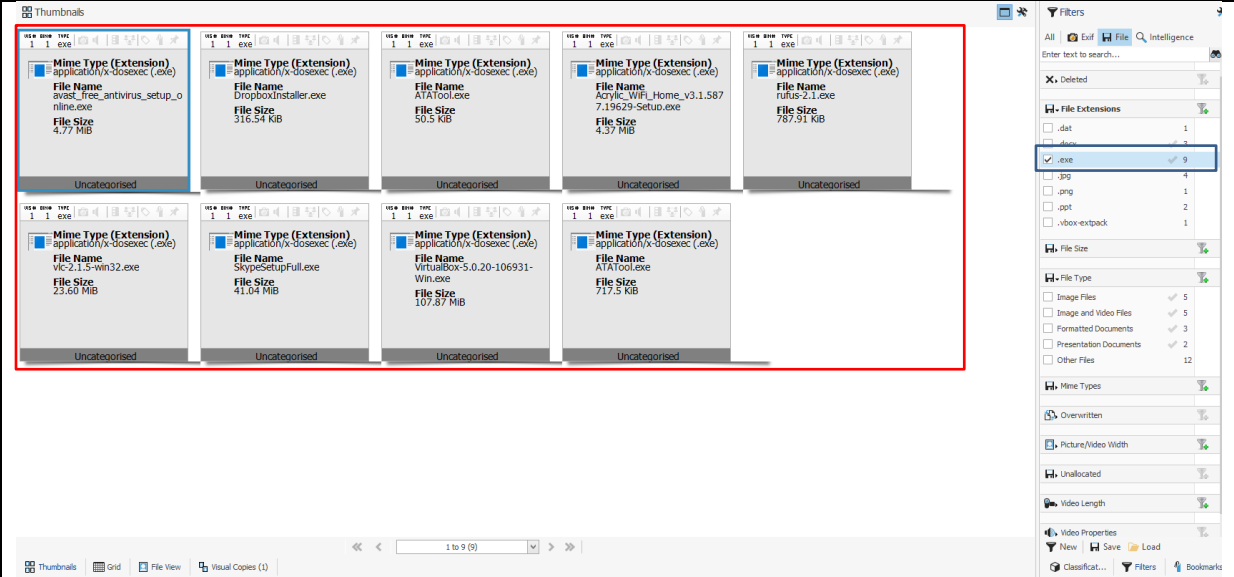


Digital Tools

Will it show and
categorise the software
tools on the USB image

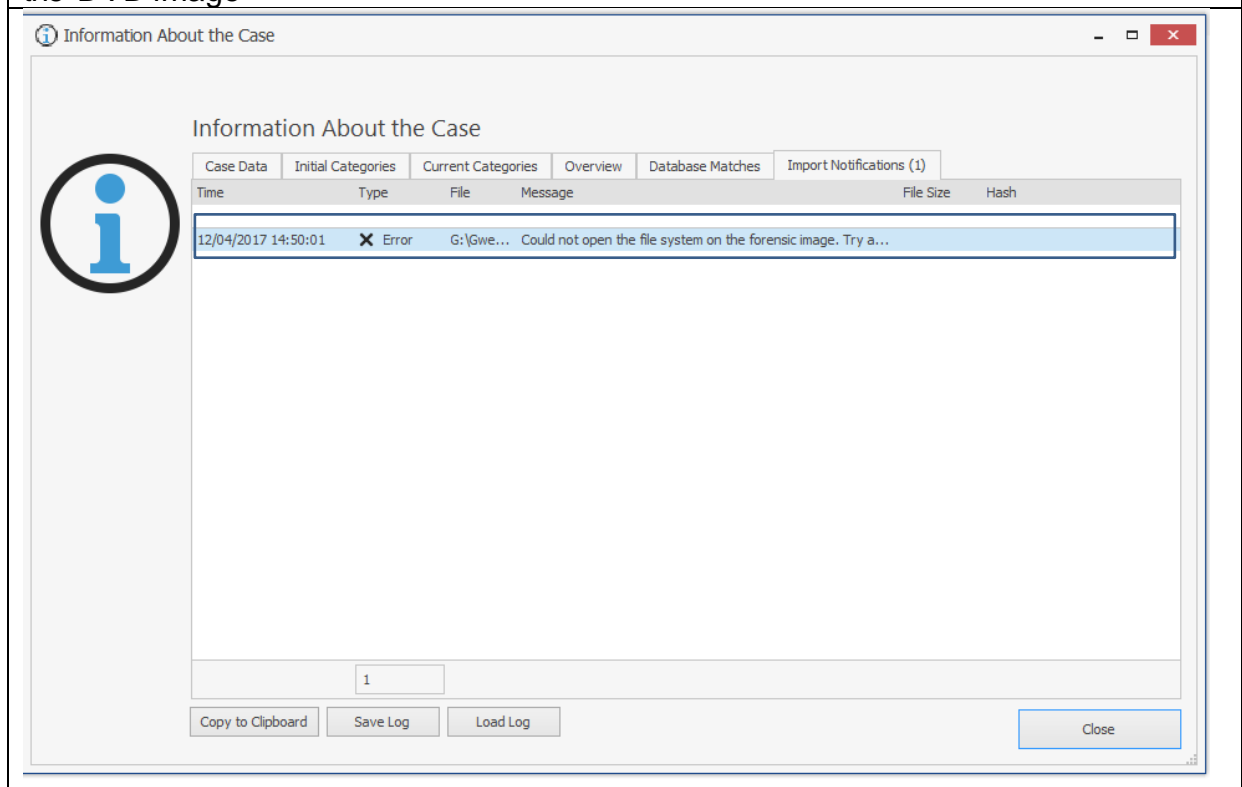
Yes, it processes and
categorises the software
tools from the USB image

This screenshot shows the ".exe" files on the USB device and displayed in the thumbnail panel.



4.3.4.4 Tests for DVDs		Device Name: Optiarc DVD RW AD-5280S
Test	Description	Results
Testing Stopped	-	Griffey couldn't open the DVD raw image and an error message appeared every time it tried to mount and process that image so I couldn't test it on this type of device

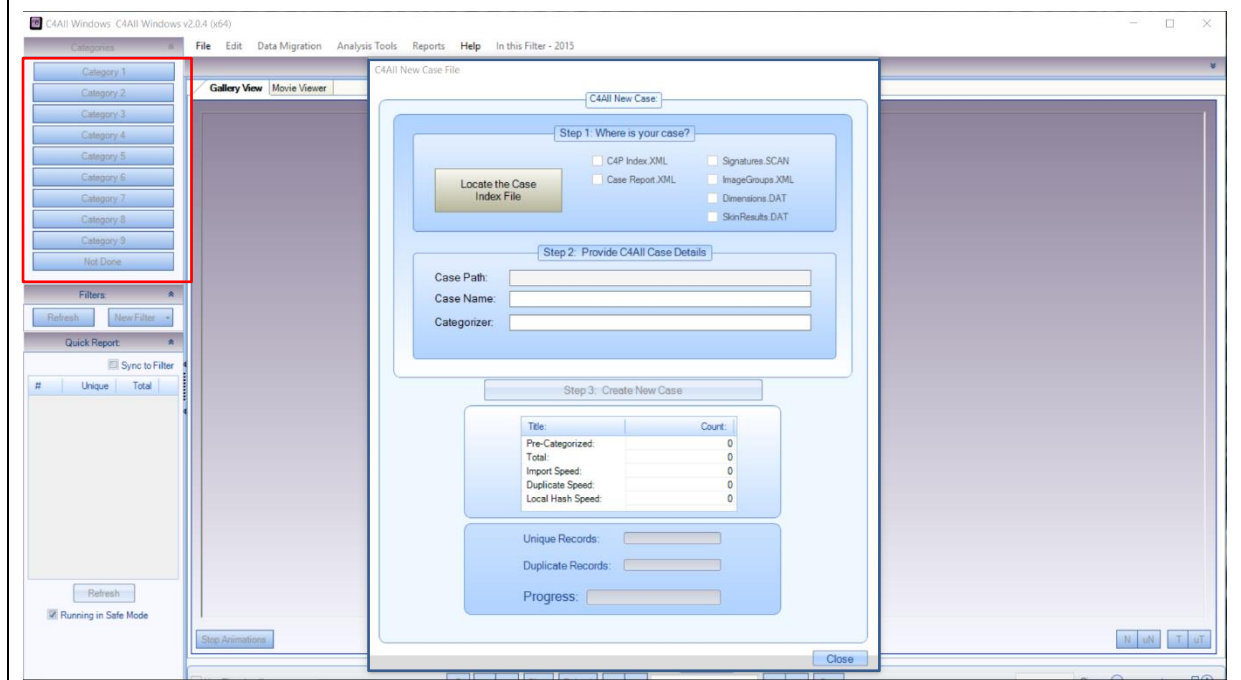
This screenshot shows the error information that came up when it refused to read the DVD image



4.3.5 C4All Test

Test	Description	Result
Testing Stopped	-	This tool would not take any images that had been marked to be analysed from Encase and it didn't have any way to categorize the images without them being of explicit nature

This screenshot shows the main menu of the C4ALL tool and some of the different features that it could have employed to categorise the seriousness of certain images when conducting a case



4.4 Procedure to meet the needs of ISO 17025

I will summarize step by step what was done to set up the samples and environment for testing the various forensic tools in this report:

- a) Before starting work on your sample images make sure to sterilise all device(s) that you will be using, if they are not already brand new devices
- b) Make sure to have at least two back-up devices of the same type as a precaution in case anything happens when populating the image
- c) When creating the samples make sure cover live, deleted, hidden and encrypted files and ensure to have at least two files/folders in each of these sections to solidify test results
- d) When the device(s) need to be imaged ensure you have tested the write blocker that will be used on the devices
- e) Image each of the device(s) you will test directly onto the computer system where you will be running your tests
- f) Ensure you create a test plan in compliance with ISO 17025 [1] using section 5.9 on "Assuring the quality of test and calibration results" (ISO/IEC 17025 [1], p.20 Section 5.9 [1])
- g) - When writing out your tests ensure to tailor your testing towards the content that is populated on the imaged devices and not the forensic tools capabilities
- h) an example test plan table is displayed below:

"Name of Tool that will be testing"		
Laboratory Location:		Tests Carried out on: (Date) Tested by: (Name of Analyst)
"Device image you would be testing"		"Device Identifier"
Test	Description	Result
"Name of Test"	"Specific Description of what you expect from the test"	"Details of if the test succeeds or failed"
"Detailed description of what the screenshot depicts"		
"Screenshot of evidence goes here"		

- i) The test plan covers enough detail to provide proof of a successful/failed test and when, where and who conducted said test in accordance with ISO 17025 [1].
- j) The tests are laid out to cover all the content that had be populated onto the images and if the forensic tools could process and extract this content then the test was deemed to be a successful and proved the validation of that forensic tool.

5. Results and Evaluation

Here is a summary of the results from my proficiency testing on the Hard drive, SSD, USB and DVD images, the table below shows when a test was passed (✓), Failed (✗) or Not Applicable (-):

<u>Encase Results</u>	<u>Hard Drive</u>	<u>SSD</u>	<u>USB</u>	<u>DVD</u>
Live Images	✓	✓	✓	✓
Live Videos	✓	✓	-	-
Live Music	-	-	-	✓
Live Documents	✓	✓	✓	✓
Deleted Files	✓	✗	-	-
Internet files and search history	✗	✗	-	-
Hidden Files	✓	✓	-	-
Encrypted Files	✓	✓	-	-
HPA files	✗	-	-	-
VM partition	✗	-	-	-
Alternate Data Streams	✓	-	-	-
Emails	✓	-	-	-
Dropbox	✓	-	-	-
Application Files	-	-	✓	-
Digital Tools	-	-	✓	-

When running through the testing of encase it was difficult to navigate around the tool to begin with as I hadn't spent much time using it before testing so it took a little while to get used to how the filters worked and what were the limits of the version that I had at my disposal. After conducting my tests on the Hard drive image it processed most of the file system without any problem so the live files were extracted and filtered with ease, then it came to the deleted files and no matter what I found I could not see an easy way to look for just deleted files when filtering and the tool seemed to automatically recover these files and that didn't make it easy to see if a file was deleted or not, so for that test I resorted to finding files that I knew had been deleted just to prove that this tool does display deleted folders, the hard drive also failed on finding meaningful data from the internet search history as it only recovered the index.dat files from the image but could not present them in a meaningful way that was desired to be found in this test. The next few tests on the Hard drive image I expected would be more of a challenge for the tool to find but to my surprise the "alternate data streams" were recovered instantly and it found all the hidden and encrypted folders that were on the image when it was processed, there were only two areas that the tool didn't gain access to and that was the virtual machine partition and it could not recover the expected folders from the "host protected area". On the SSD image the only tests that failed were the deleted folders test as I could not find the content that had be purposely deleted for this test and the internet history test which failed the same way that it did in the review of the Hard drive image. The USB and DVD images passed all the tests that were presented with but they only had a small amount of content to test. Encase is a very solid tool that recovers almost anything and with the encase scripts it allows for this software tool to be highly modular, and even though the encase didn't manage to recover the HPA files or the files from a virtual machine I know that there are more methods to

extract that data that goes beyond this tool but there is enough evidence for an analyst to know that both these areas exist and need further examination when it is being used in an investigation.

FTK Results	Hard Drive	SSD	USB	DVD
Live Images	✓	✓	✓	✓
Live Videos	✓	✓	-	-
Live Music	-	-	-	✓
Live Documents	✓	✓	✓	✓
Deleted Files	✓	x	-	-
Internet files and search history	✓	✓	-	-
Hidden Files	✓	✓	-	-
Encrypted Files	✓	✓	-	-
HPA files	✓	-	-	-
VM partition	x	-	-	-
Alternate Data Streams	✓	-	-	-
Emails	✓	-	-	-
Dropbox	✓	-	-	-
Application Files	-	-	✓	-
Digital Tools	-	-	✓	-

FTK came in as a last minute substitute for C4ALL to make up the numbers for forensic tools that I would be testing and as FTK is the straight competitor to Encase I thought looking at the comparison between these two tools would be useful and interesting to see what each tool had to offer and for the most part they were identical in what they managed to extract from the live files and when it came to deleted files FTK had a built in filter that would recover all files that had been deleted which it managed to recover the expected files from the Hard drive but like encase it could not find them on the SSD image and when a file was flagged as deleted it even marked them in red to help them stand out from all the other files when you were looking at them it definitely felt like a more user friendly tool to pick up. The tests that FTK beat encase on were the recovery of the HPA files as the moment I processed the image it found all ten hidden pictures in the HPA instantly and the internet files test that was run on the Hard drive and SSD images found and presented a lot more information through the default filters from the tool but apart from that the two forensic tools were identical in their recover of the rest information from the different dd images.

AXIOM Results	Hard Drive	SSD
Browser Types	✓	✓
Internet Search Terms	✓	✓
Social Media	✓	✓
Reconstructed web pages	✓	✓
Live Images	✓	✓
Live Videos	✓	✓
Live Documents	✓	✓
Deleted Files	✓	✓
Hidden Files	✓	✓

Encrypted Files	✓	✓
HPA files	✗	-
VM partition	✗	-
Alternate Data Streams	✓	-
Emails	✓	-
Dropbox	✓	-

AXIOM was a forensic tool that I wasn't expected to have so much functionality from as I was planning to be testing IEF, but in the interest of time I couldn't wait on hearing back from the police if they had a copy of just "Internet Evidence Finder (IEF)" so I conducted my tests within the AXIOM application and came up with a few more tests that were aimed around Internet and browser files that I would expect to find and in the interest of these tests being more centred around just internet files I chose not to test the USB and DVD images as these didn't have any content of that sort within the images. As FTK and Encase both weren't made to extract much information from browsers it was going to be interesting to see what this tool could extract, and I was impressed at how well AXIOM pulled out the information from the user's internet history and presented it with very easy to understand filters that would allow you to filter for things like which browser the user had been in and which google search had typed in making it very easy to narrow down your evidence when I was conducting my tests. For the general content that was local to the user it found almost everything except the HPA and VM files which all the tools so far have struggled with.

Griffeye Results	Hard Drive	SSD	USB	DVD
Torrent	✓	-	-	-
Software Used	-	✓	-	-
Camera Types	-	✓	-	-
Live Images	✓	✓	✓	-
Live Videos	✓	✓	-	-
Live Documents	✓	✓	✓	-
Deleted Files	✓	✓	-	-
Internet files and search history	✓	✓	-	-
Hidden Files	✓	✓	-	-
Encrypted Files	✓	✓	-	-
HPA files	✓	-	-	-
VM partition	✗	-	-	-
Alternate Data Streams	✗	-	-	-
Emails	✓	-	-	-
Dropbox	✓	-	-	-
Application Files	-	-	✓	-
Digital Tools	-	-	✓	-

Griffeye as a forensic tool focuses around all types of media content so I wasn't expecting much when it came to the documents and others text based files that would be found when testing the images, but it processed and extracted most of the images and had a wide range of file types that you could use to narrow your

searches, but when it came to searching for the alternate data streams it couldn't show me any alternate data streams from within this tool and failed on that test as it also did on the virtual machine partition which every tool has failed on so far. Its biggest strength was the ease at which you could look through videos frame by frame by just hovering your mouse over the object you wanted to look at and the amount of meta data it could extract was fascinating as all the images were royalty free but it could tell me what camera those pictures had been taken on which could help when processing evidence from a crime scene. This tool along with FTK were the only ones that managed to recover the pictures from the HPA and it displayed them when filtering for unallocated space and under deleted jpeg files and the only major problem that I couldn't resolve in my tests of griffey were that it refused to accept and process the raw image from the DVD.

After finishing my tests, it was plain to see that no matter what you tried to do to hide incriminating evidence these tools together could find all the content that would be hidden and I tried my best to vary the digital images to include every piece of content that the police had specified in our earlier meetings. It was a shame C4ALL wouldn't work in my testing but considering that it's a tool aimed at categorizing sexually explicit images and all my images were aimed around finding bears and puppies I could not see how I could test it thoroughly without it having actual explicit images for this tool to be able to distinguish between them and the trivial content. If I was to conduct more testing in future I would aim it around a more in depth image with multiple users to see how it would separate out the different user's files when it processed them inside the tool. Overall all the tools managed to read the content I had put in the images to varying degrees and my proficiency tests reflect the digital tools capabilities to find all the evidence I had placed within them. When investigating, it would be ignorant to rely solely on one forensic tool to collect your evidence so where some of these tools have struggled to extract meaningful information other tools have picked up the slack to cover that forensic tools weaknesses.

6. Future Work

From my work on this project I can see that there is still much that will need to be done in the future as ISO 17025 [1] is all about keeping analysts and their equipment up to date and in this report I only covered four forensic tools that were frequently used so if work needed to continue there are a lot more forensic tools that could use more proficiency testing to help validate them in the future, and the current tools I tested will constantly be updating and changing to meet the new requirements of technology in the future. With that said the generation that is currently growing up is the first one that grew up with the internet as we know it and being able to have access to documents and files through the cloud so I see more forensic work turning towards dealing with external storage that won't be easily extracted and these forensic tools will need to adapt to counter this movement, along with files being stored in offsite locations the desire for everyone to encrypt their data is more important than ever and this can prove to be a problem for forensic analysts and their software manufacturers in future when trying to obtain evidence from encrypted machines. So, a future goal would be to conduct more tests into encrypted files and files that would be stored on a cloud device to help proficiency tests in forensics remain relevant to the type of content that would be expected to find on everyone's machines these days.

Another area for study that I didn't manage to delve into in this project is mobile forensics as I ran out of time to try and make a realistic image for that device and then to test the data that could be extracted from that, and with everyone having access to some kind of mobile device the need to have more research and tests into this area of forensics to meet the requirements of ISO 17025 [1] is invaluable and my recommendation is to approach it in the same way I did by making images using a persona for a suspect in a scenario so that when it comes to making the image you can differentiate between what evidence you want to put on that mobile device and also what would the suspect have on their phone as just standard trivial data be it notes, photos, videos etc.

The last piece of future work that I would have been useful to have working in this project would be a dynamic test image generator for the content that you are trying to hide in an image and I know that forGE (Hannuvisiti, Forensic test image generator [12]) has done some work into this area but their tools I couldn't get working with my project, that meant that I created my images manually which allowed me to put things in where I wanted them to be but it took a lot of time that could have been saved and used to conduct some more meaningful tests on the forensic tools. This last piece of additional work is more a project that could be undertaken adjacent to this project that assists in the building of forensic images dynamically so that analysts don't have to waste time creating their own test images.

7. Conclusions

These are my 4 main report requirements that were needed to complete this project:

1. Mapping ISO 17025 to currently used guidelines
2. Proficiency Testing of Frequently Used tools
3. Training Digital Forensic Analysts
4. Outline Structure of how to conduct testing using ISO 17025

The first requirement I had decided upon having in this report was to help me and other possible readers understand what the big changes were going to be from how operations were currently conducted in a police forensic environment, so analyzing the current guidelines and standards that were being enforced on a UK police force was my first main task to complete. The work from mapping ISO 17025 [1] allowed me to see that “Assuring the quality of test and calibration results (ref 5.9)” and “Validation of methods (ref 5.4.5)” were the sections that were most important to completing my deliverables for this project so that compliance with ISO 17025 [1] was met and from that I had a clear structure of how my later tests should be presented when they were being conducted as proficiency tests on forensic tools as there is no current universal structure of what tests need to be run in order to ensure validation on forensic tools.

The next requirement that I had was to conduct my own proficiency tests on selected forensic tools that had been outlined by Gwent police, this was to assist in their accreditation for ISO 17025 [1]. To prove the validity of each tool I made as authentic an image as possible for a Hard drive, SSD, USB and DVD so that when it was tested it would cover the main features that each of these tools were capable of and if these tools could find and display the expected content that had been hidden and put onto these devices then they would pass my tests proving that they could deliver the features they advertise and so they would be validated.

Setting out the test plans I made sure to follow the outline laid out in ISO 17025 [1] in section 5.10.2 that covers “Tests reports and calibration certificates”, this section lists what is required to be in a test report as the bare minimum, I will list the ones relevant to my testing down below:

- A report title
- Name and address of the laboratory, and the location where the tests and/or calibrations were carried out
- Identification of the method used
- A description of, the condition of, and unambiguous identification of the items(s) tested
- The date(s) of performance of the test
- Test results
- The name(s), functions(s) and signatures(s) or equivalent identification of person(s) authorizing the test report.

Following these I created my test plans to conform to what information needed to be presented when writing out the test results.

For the third requirement in my report I made sure that when I was creating my test images I would build a persona of suspects that had used the device to make it seem like a user had actually been using these devices rather than just getting a lot

of media assets and packing them into a drive without any narrative, but as one of my requirements was that these images might be used to test other forensic analysts in future I needed to add some restrictions to myself when creating these images, so when it came to putting information on these devices I had to justify why this person would have a picture of a mountain or a document detailing how they managed their money and as long as these files fit with the persona I had envisioned for that scenario then the narrative I wanted to have on that device would work. I had decided to pair up the devices together as having an independent USB and DVD scenario didn't make much sense with how my suspects would operate so I had the hard drive and USB together and the SSD and DVD together as one and wrote out a summary of the scenario and questionnaires for each so that an analyst would have a direction of what content they would be looking for and how to conduct their investigation within the tool they were training in.

The Last requirement about outlining a structure of how to conduct testing using ISO 17025 [1] I had put in myself because when talking to Gwent police about this ISO it was clear that many different police departments were all working out how to help accomplish testing and validating using this ISO so writing up a summary of how I had set up my testing and what devices had been used to conform with ISO 17025 [1]. I thought it would be useful to have this summary be available so that if others wanted to build upon my work and how I had tested these forensic tools then they would only need to check on this procedure summary at the end of my report without needing to read through the entire report unless they wanted more detail on what had occurred in my testing.

Overall I have delivered something in each of the requirements that I had set out at the beginning of this project. From these deliverables, I have discovered along the way that creating the samples and pre-processing of those samples takes up so much more time that I had initially assumed but the extent at which the forensic tools once processed could find all the evidence that I had attempted to hide was astonishing and there is no data that you could possibly hide when an analyst works their way through these tools from the tests carried out. The other thing I learnt from my testing was making sure that the tests were fair by testing them in the same environment and creating the samples under the same lab conditions to ensure that only the content that I expected to go on the devices did. but also, I know I could have added more depth to some of these requirements such as mapping ISO 17025 [1] or the procedure on conducting testing in ISO 17025 [1] as with these requirements I felt I didn't get as much practicality out of these sections and they could have been more background additions rather than full requirement goals and if the meeting with Gwent police had happened sooner in my projects conception I could have saved two weeks from refocusing my goals and got more requirements for this project. Finally, I believe I made the right approaches for each of these requirements by doing a lot of research into ISO 17025 [1] which helped me understand the problem that I would need to overcome in proficiency testing and the testing procedure and the best deliverables that were produced from this project were the ones that will be handed over to Gwent police for their accreditation so I believe I have succeeded in solving the overall problem of this project to help get accreditation in ISO 17025 [1].

8. Reflection and Learning

Now that the project has concluded I can take a step back and reflect on what I accomplished over the 15 weeks. The beginning foundations of this project were very unstable as my project scope from my initial plan had been thought up because I had heard that a new ISO standard to digital forensics was being introduced and police departments were struggling to integrate it into their current work, and with the time scale we had all been working for at the beginning of the project meant that I needed to jump straight into what I thought was the ISO they had been concerned about which was ISO 27037 (ISO/IEC 27037 [2]) instead of ISO 17025 (ISO/IEC 17025 [1]) so my project began looking at all the different digital forensic standards and I read more into what guidelines were currently being used by police departments within Europe.

I continued down this path until week 3 came when I had my first meeting with Gwent police who had heard I was doing work into digital forensic standards and after my meeting with them it became clear that I had been concentrating on the wrong ISO standard and so in week 3 I changed my direction and goals of the entire project to align more with what they wanted from the project because that had been my original intention to assist in helping police forces navigate an ISO standard that was causing them problems, but my misunderstanding of the ISO standard not being a “forensic” standard but one that was a general validation of laboratories meant that I partly wasted the first few weeks of the project, so this was a case of double loop learning where I got my original assumptions wrong and had to adjust accordingly to narrow my scope. In week 4 we received feedback from our initial plans and this change in focus would go on to greatly help me as most of the feedback from the moderator involved how broad a scope my project has been and my greatly exaggerated expectations for my end deliverables of the project, so I spent my entire time changing the scope of the project and its overall deliverables to focus on ISO 17025 [1] which went towards addressing the feedback from the moderator, the problem from this that I had to overcome was that I had already been doing work in the first few weeks around different forensic standards so I modified my project to still include a look at guidelines and standards that European police forces abide by but the overall scope of the project changed so that the main centre piece of the project was around ISO 17025 [1] which is why the title of my project changed to “Application of ISO 17025 [1] with Inter-Laboratory Testing”. From this change in direction I adjusted my Gantt chart and extended my research into week 5 so that I could collect more information around ISO 17025 [1] while at the same time start to plan the images I would be making and what devices the police wanted these images to be on.

When it got to week 6-7 I was on track after my research and mapping of ISO 17025 [1] to understand what the changes were with this ISO and how much of a higher standard forensic labs were expected to be held accountable for, in week 8 I had a drop in motivation trying to decide how best to implement these images either through a virtual machine or to make them on separate machines in the university laboratories and if there was any way to dynamically create these images without me needing to spend a lot of time in the labs creating each image, this mixed in with external factors made me fall behind on my work. In weeks 9-10 I spent time making the finishing touches on what the scenarios would be for each device and what content I would need to collect to populate these digital images. Weeks 11-12 were

spent making and testing the images and if I had to do this again I know I would have tried to put in a little time each week building up these images adding multiple users to the scenarios so that analysts wouldn't just have one user to look at but many and only one of them would have the explicit images they were looking for and this would help to make the images more authentic as people don't go to the length of sterilizing every computer that they have used before giving it to another family member and also from this there could have been a more realistic timeline of files without the need to use "timestomp" to alter the files MAC times, and with testing the biggest thing that drained my time was the pre-processing that needed to be done for each image and having 4 separate tools having to pre-process a 500Gb image meant that I had a lot of free time to spend trying to add notes into my report and document the process but by the third day of testing I had run out of tasks that I needed to do and testing was the only thing holding me back and I couldn't continue until it was finished and it was terribly inefficient of me to have continued in this way.

One of my regrets was starting the digital images too late out of the 15 weeks which made me abandon any work involving mobile forensics as I had so little knowledge of this type of forensics and I didn't have time to research it more, so I concentrated on the common conventional devices that I was comfortable with when making my images. If I was to do this project again I would move up my timescale of the digital images making them more of a centre piece in my project and flesh them out a lot more with work done into email artefacts, social media and cloud storage that I only touched upon when it came to testing the different images as a lot of these use an email to set up an account and I found it difficult for the main social media platforms to accept dummy emails and they needed a mobile phone which I wasn't willing to give up my number onto each of these scenarios, and also if I had known which ISO the police had their concerns about in the beginning of my project then it would have been a lot less tenuous and the best deliverables from this project are the ones that the police desired to have so I succeeded in assisting Gwent police in inter-laboratory testing to help get their accreditation for ISO17025 [1] within the allotted time frame. Visualises of my Gantt chart can be found in the appendix at the end of this report.

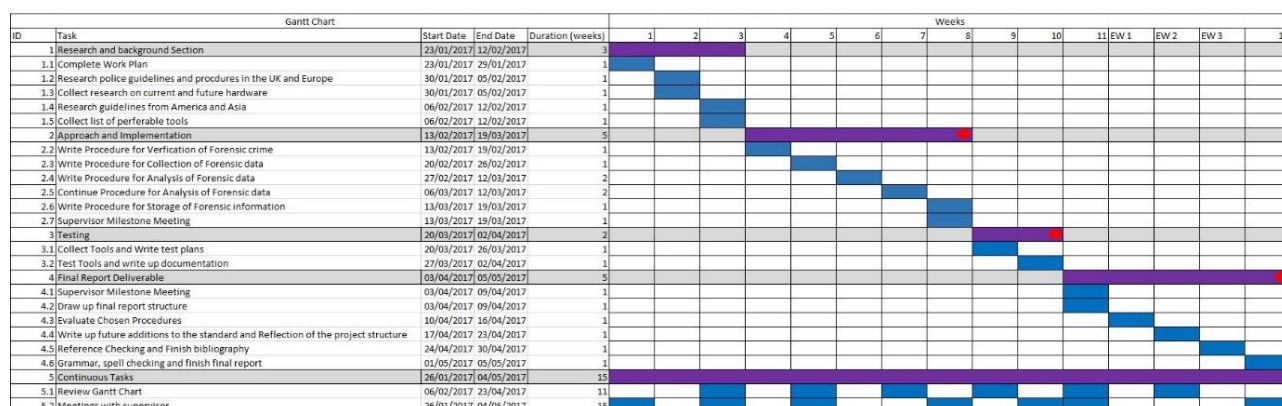
9. Glossary

- ISO– International Organization for Standardization
- IEC - International Electrotechnical commission
- ACPO - Association of Chief Police Offices
- OLAF - Office européen de lutte antifraude
- EU – European Union
- ADS – Alternate Data Stream(s)
- IEF – Internet Evidence Finder
- C4ALL – Categorise for all
- SSD – Solid State Drive
- DVD – Digital Versatile Disc
- USB – Universal Serial Bus
- HPA – Host Protected Area
- DCO – Device Configuration Overlay
- SLA – Service Level Agreement
- VM – Virtual Machine
- NTFS -New Technology File System
- ATA – Advanced Technology Attachment
- FTK – Forensic Toolkit

10. Appendix

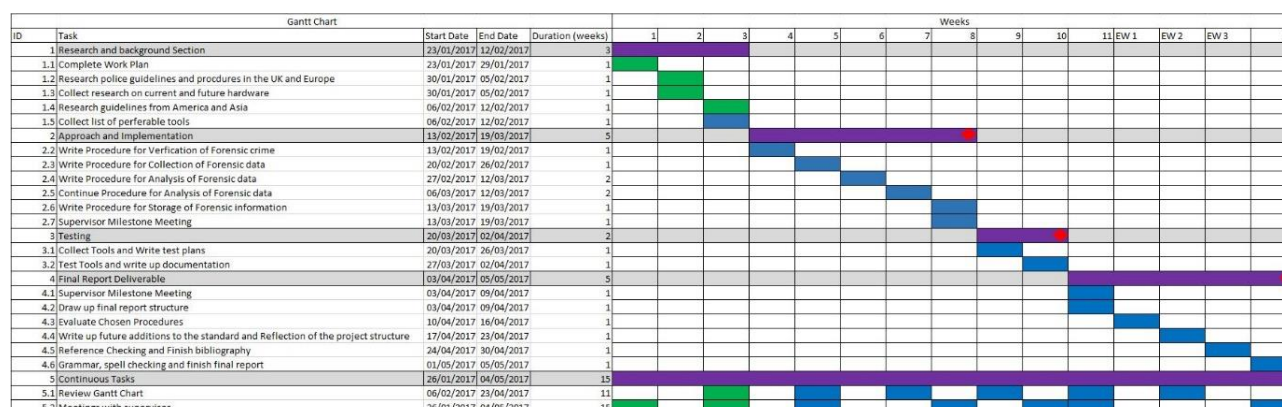
10.1 Diary of Gantt chart

Week 1:



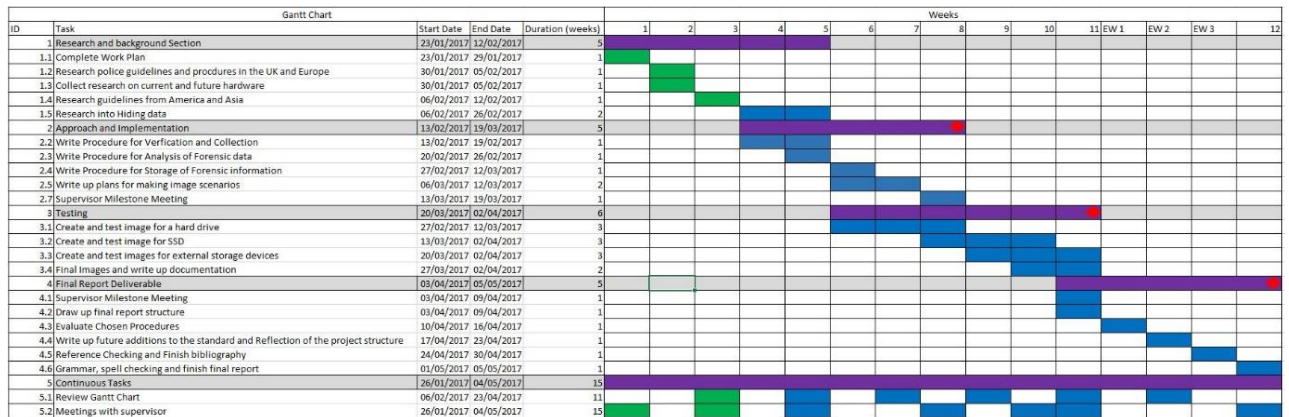
This is the initial plan for the project and what I aim to achieve over the next couple of weeks

Week 2-3:



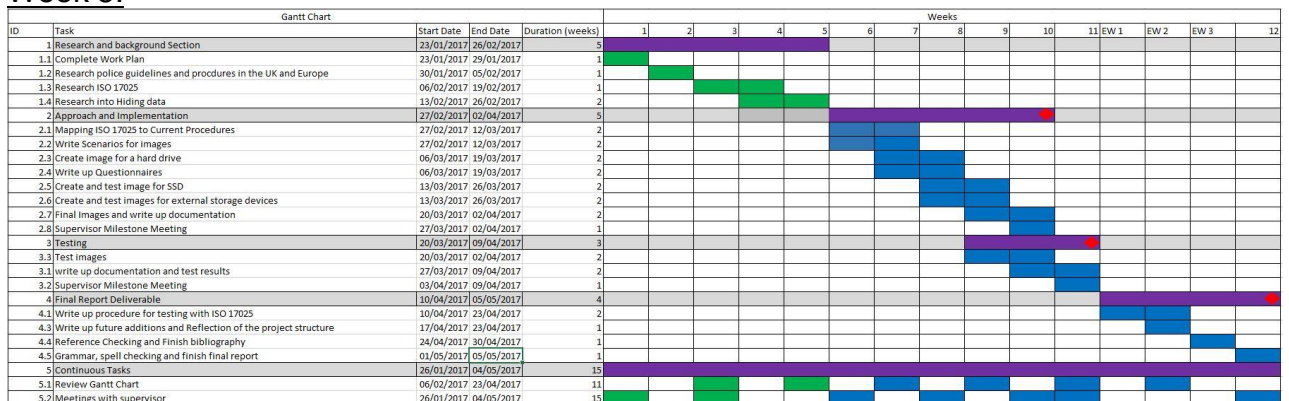
This shows that I have managed to meet most of my targets in the starting weeks, but I had a 2-hour meeting with Newport Gwent police at the end of week 3 that is making me reassess my plans and one of my primary requirements of a recommended tools list is being adjusted after my discussion with them.

Week 4:



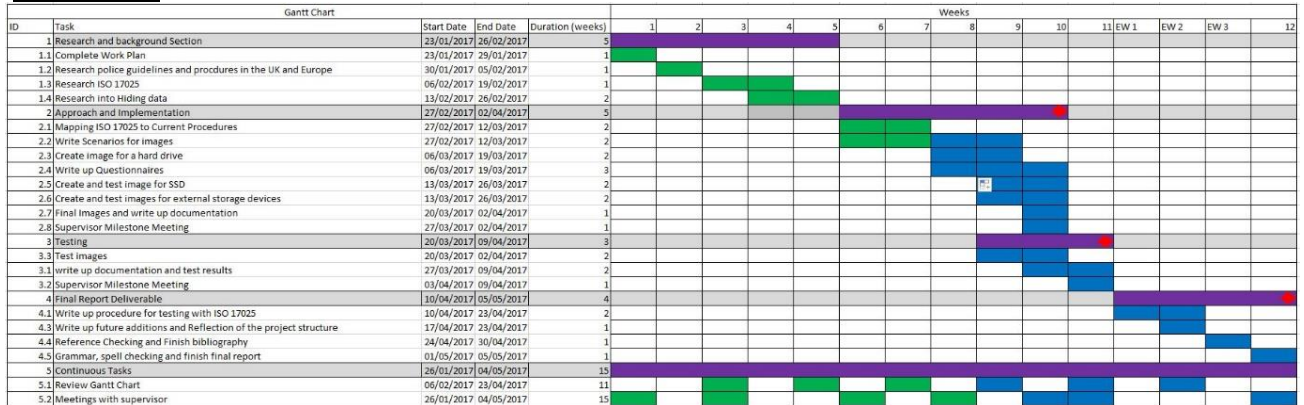
This is the new plan that I have had to adjust to meet some of the needs that real forensic analysts have identified as a problem that they need to consider which is the scientific testing of tools to prove that if someone else used the same tool that they would get the same result. I have expanded the research section to cover a bit more learning on the go for hiding the data, this will help me to write up plans for how to make these images and where best I will hide this information, through my current research I have noticed that most of the developed countries have very similar processes of how to conduct an investigation so my project has made a slight switch to cover more about the tools earlier on and to cut the writing up and updating procedures to a couple weeks less that I had originally had. The testing has been expanded extensively to meet with the needs outlined by the police.

Week 5:



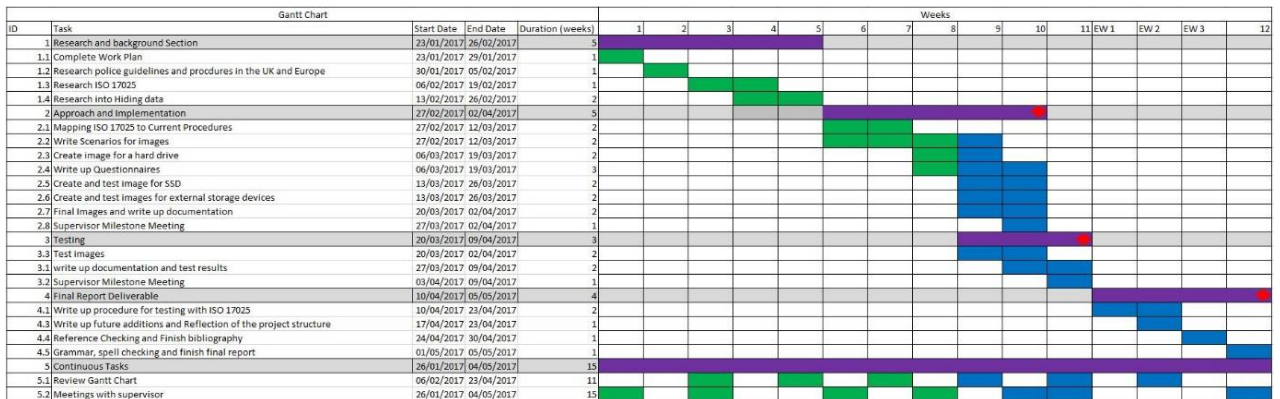
Adjusting to feedback from the initial plan of the task being to unrefined and the scope being too broad I've done a complete overall of the tasks and aims and made the changes accordingly to the project with a heavy focus on ISO 17025 [1] and a concentration around scientific Testing.

Week 6-7:



Tasks are continuing as expected nothing of relevance to report

Week 8:

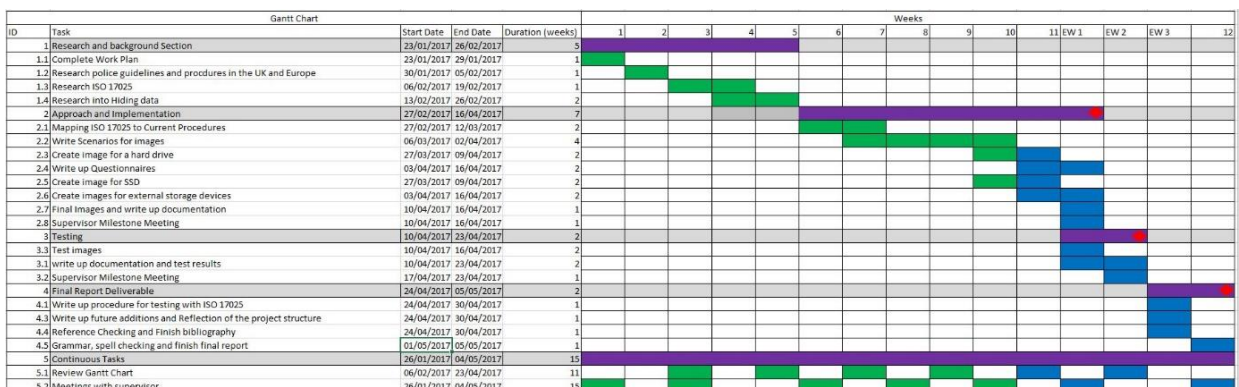


Started to fall behind on work through external factors taking up time from the dissertation have adjusted the Gantt chart to add more of work load needed through weeks 9 and 10 to catch up on work that was missed out on in week 8

Monday 20th March 2017

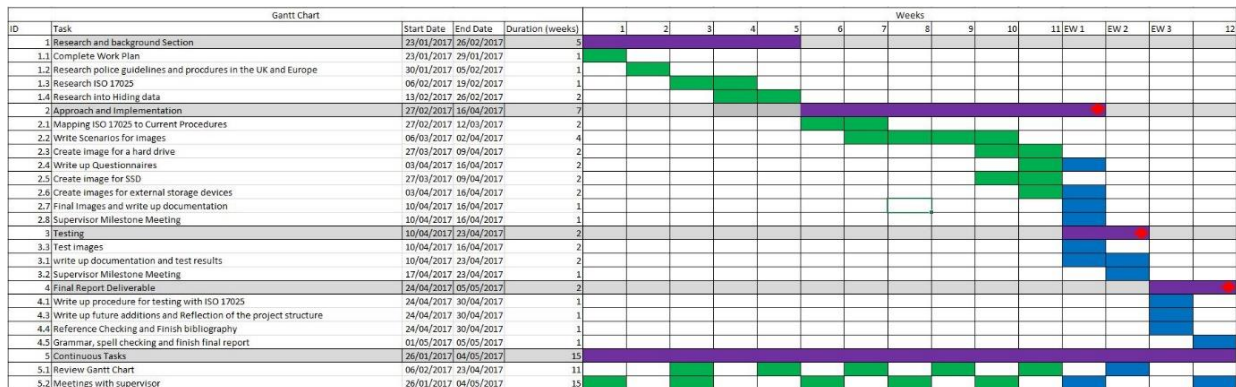
Had another meeting with police to hand out the clean devices that will be worked on and discuss some of the requirements that were outlined in the previous meeting as well as talking about how to make these images as authenticate as possible to make sure that the tools are tested in as exhaustive a manner as possible.

Week 9-10



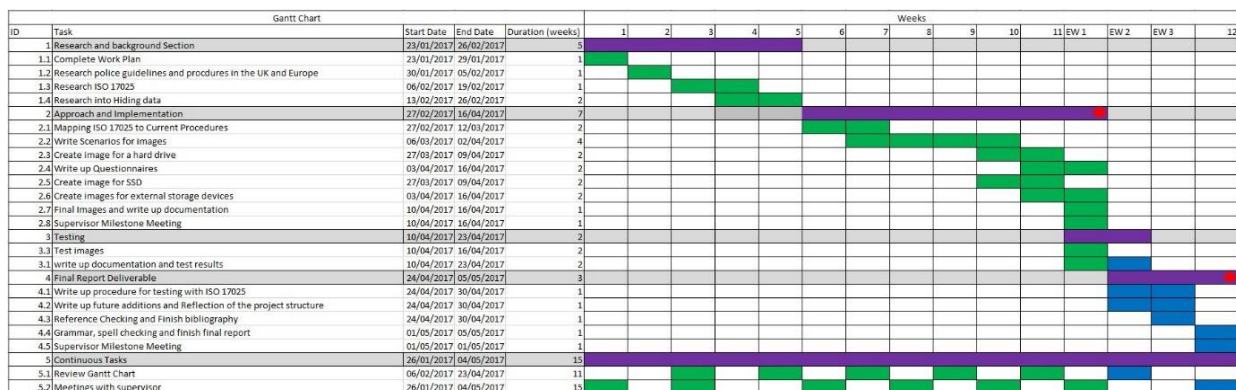
Struggled to get back to routine after week 8 derailing external factors so week 9 was less productive and then week 10 was building up to all the images and testing to come from week 11 onwards

Week 11



I hit my targets and got most of the important images ready for testing and if I can stick to this plan I should only be writing up my report for the final weeks of Easter and not need to worry about getting evidence for test plans and we were still waiting on C4ALL as it could not be accessed from within the UK so the police are getting us a licence to use.

Easter Week 1



After the set-back in week 8 I finally managed to put in enough time to get ahead of the work load that was starting to pile up quite drastically and the amount of pre-processing of the digital images allowed for me to work in parallel to write and plan more things in my report

Easter Week 2-3

Gantt Chart					Weeks														
ID	Task	Start Date	End Date	Duration (weeks)	1	2	3	4	5	6	7	8	9	10	11	EW 1	EW 2	EW 3	12
1	Research and background Section	23/01/2017	26/02/2017	5															
1.1	Complete Work Plan	23/01/2017	29/01/2017	1															
1.2	Research police guidelines and procdures in the UK and Europe	30/01/2017	05/02/2017	1															
1.3	Research ISO 17025	06/02/2017	19/02/2017	1															
1.4	Research into Hiding data	13/02/2017	26/02/2017	2															
2	Approach and Implementation	27/02/2017	16/04/2017	7															
2.1	Mapping ISO 17025 to Current Procedures	27/02/2017	12/03/2017	2															
2.2	Write Scenarios for images	06/03/2017	02/04/2017	4															
2.3	Create image for a hard drive	27/03/2017	09/04/2017	2															
2.4	Write up Questionnaires	03/04/2017	16/04/2017	2															
2.5	Create image for SSD	27/03/2017	09/04/2017	2															
2.6	Create images for external storage devices	03/04/2017	16/04/2017	2															
2.7	Final Images and write up documentation	10/04/2017	16/04/2017	1															
2.8	Supervisor Milestone Meeting	10/04/2017	16/04/2017	1															
3	Testing	10/04/2017	23/04/2017	2															
3.1	Test images	10/04/2017	16/04/2017	2															
3.1	write up documentation and test results	10/04/2017	23/04/2017	2															
4	Final Report Deliverable	24/04/2017	05/05/2017	3															
4.1	Write up procedure for testing with ISO 17025	24/04/2017	30/04/2017	1															
4.2	Write up future additions and Reflection of the project structure	24/04/2017	30/04/2017	1															
4.3	Reference Checking and Finish bibliography	24/04/2017	30/04/2017	1															
4.4	Grammar, spell checking and finish final report	01/05/2017	05/05/2017	1															
4.5	Supervisor Milestone Meeting	01/05/2017	01/05/2017	1															
5	Continuous Tasks	26/01/2017	04/05/2017	15															
5.1	Review Gantt Chart	06/02/2017	23/04/2017	11															
5.2	Meetings with supervisor	26/01/2017	04/05/2017	15															

11. References

- [1] ISO/IEC 17025: (2005), General Requirements for the competence of testing and calibration laboratories, Available at:
http://www.uobaghdad.edu.iq/uploads/pics13/q1684/iso17025_11_eng.pdf
[Online] [Accessed: 4th May 2017]
- [2] ISO/IEC 27037: (2012), Guidelines for identification, collection, acquisition and preservation of digital evidence, Available at:
<https://www.iso.org/standard/44381.html> [Online] [Accessed: 4th May 2017]
- [3] Incident Management and Forensics Working Group (2013), "Mapping the Forensic Standard ISO/IEC 27037 [2] to cloud computing", pp.10-26 [online]. Available at:
https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037_2-to-Cloud-Computing.pdf [Accessed: 4th May 2017]
- [4] DAC Janet Williams QPM, (2012), ACPO Good Practice Guide for Digital Evidence. Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
[Online] [Accessed 4th May 2017]
- [5] Giovanni Kessler, (2016), Guidelines on Digital Forensic Procedures for OLAF Staff. Available at: https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf [Online] [Accessed 4th May 2017]
- [6] ISO 27001: (2013), Information Security Management. Available at:
http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf [Online] [Accessed 4th May 2017]
- [7] Forensic Science Regulator, (2016), Codes of Practice and Conduct for forensic science providers and practitioners in the criminal justice system Issue 3. Available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/499850/2016_2_11_-_The_Codes_of_Practice_and_Conduct_-_Issue_3.pdf
[Online] [Accessed 4th May 2017]
- [8] Guidance Software, Encase. Available at:
<https://www.guidancesoftware.com/encase-forensic> [Online] [Accessed 4th May 2017]
- [9] C4All. <https://c4all.e-crime.on.ca/> [Offline] [Unavailable 4th May 2017]

- [10] Magnet Software, AXIOM. Available at:
<https://www.magnetforensics.com/magnet-axiom/> [Online] [Accessed 4th May 2017]
- [11] Griffeye, Griffeye Analyse. Available at: <https://www.griffeye.com/>
[Online] [Accessed 4th May 2017]
- [12] Hannuvisiti, ForGe Forensic test image generator. Available at:
<https://github.com/hannuvisti/forg> [Online] [Accessed 4th May 2017]
- [13] Data Protection Act 1998, Available at:
<http://www.legislation.gov.uk/ukpga/1998/29/contents> [Online] [Accessed 4th May 2017]
- [14] Benjamin Tissot, Royalty Free Music by Bensound. Available at:
<http://www.bensound.com/> [Online] [Accessed 4th May 2017]