UNREAL STEGANOGRAPHY:

Using a VR application as a steganography carrier

Sheffield Hallam University
Computer Security with Forensics
By Stuart Wilson

Abstract

This report focuses on the use of virtual reality as a potential steganography carrier file to avoid detection of forensic analysis applications commonly used within law enforcement. The goal is to show how a virtual reality game/environment can be made with little training, what file types can be stored within it and if the files can be extracted once the environment has been packaged and if forensic tools can analyse the files. This has been done by producing a virtual reality environment using Unreal Engine, as when comparing Unity and Unreal as mentioned within section 3.3, Unreal proved easier to use within the given time. Once the virtual reality environment was built, the steganography file needed to be created. This was done by using popular tools such as Our Secret, Deep Sound and Open Puff.

Once the steganography files had been created they were placed into the virtual reality environment and the entire application was packaged. From here, the packaged environment was placed into Encase 8 and Internet Evidence Finder for testing. After analysing the virtual reality application within the forensic analysis programs, no evidence was found and only two pieces of steganography data were recovered. By showing that virtual reality applications can be used to store data within them, it has allowed for ways to store potentially harmful data in otherwise non-conspicuous files.

Acknowledgment

If not for the support and guidance provided by my supervisor, Youcef Djerbib, this thesis would not have been possible. As such I would personally like to express my gratitude for his help in encouraging me to do my best throughout this thesis. I would also like to thank the lectures within the ACES department at Sheffield Hallam University for their support and knowledge in helping me to achieve my best while studying.

Contents

List of figures

1. Introduction

This report will cover several key aspects which digital forensic investigators face in todays' society. One of the major issues is steganography, the art of hiding information within other information such as image files, PDFs, audio files and many more. It will also investigate how the growing use of virtual reality and different forms of steganography can be used by criminals or other organisations to hide sensitive information within these digital environments with little training using free open source tools or applications.

It will also show how these techniques affect digital forensic investigators including ways on how to detect if a file has been subjected to forms of steganography and if the files are recoverable with the same or different tools used to hide them.

Within section 2 and 3 of this thesis, it will cover the history of virtual reality such as when virtual reality was first developed and the current uses, the technology of virtual reality, augmented reality and mixed reality along with various types of secondary devices used by virtual reality. Section 4 of this thesis will contain the literature used and reviewed within this thesis which allowed for research to be conducted within steganography and virtual reality. This lead on to the methodologies, which will be covered within section 5, and will outline what methodology will be used, along with the different types of methodologies. From here, research was conducted into steganography, covered within section 6, and includes the various types of steganography throughout history to modern day developments.

This thesis also includes a section dedicated to the building of the experiment, covered within section 7. This section contains information on how to create a virtual reality environment, followed by the storing of steganography files within it. The lead onto the results section, covered in section 8, which outlines the results of experiment though using dedicated forensic analysis software. Section 9 of this thesis covers the discussion, which includes the results means, what went well while conducting the research and experiment and what would be changed. Section 10 contains the conclusion, which outlines the overall research of this thesis and the impact it can have within the field of forensic analysis. From this, came the reflection and evaluation, covered in section 11 and 12, which covers what went well and what didn't, the strengths and weaknesses and potential improvements for the project. The final section covers the future works of the project, outlined in section 13. Which includes the use of different tools to both create and analyse the virtual reality environment.

1.1 Aims & Objectives

The aims and objectives of this thesis are to outline how the creation of a virtual reality environment can be used as a potential steganography file carrier to elude potential forensic investigators. The ease on how each it is to create steganography files and how to retrieve this evidence. This will be done through:

- Testing the application in various forensic tools such as Encase 8, Internet Evidence Finder (IEF), Forensic Tool Kit (FTK) and Autopsy.

- The use of and accessibility of tutorials on how to generate a virtual reality environment from video sharing sites such as YouTube
- The amount of different steganography tools which are currently available for free.
- The attempted retrieval of the placed evidence within the environment

2. History of virtual reality development

Virtual reality as we know it today started back in the early 1960s with the first head mounted display (HMD) developed by Morton Heilig, called the Telesphere Mask (see figure 1). However, he also developed the Sensorama Simulator (see figure 2), a stationary device with a seat which not only allowed the user to view a 3D film, but also had the ability to immerse the user with other senses such as sound, wind, smell, vibrating chair and touch (Brockwell, 2016). This however wasn't commercially successful due to it only being able to handle small amounts of people at a time and not being portable. According to the The Franklin Institute (2018) the term Virtual Reality was "first used in the mid-1980s when Jaron Lanier, founder of VPL Research, began to develop the gear, including goggles and gloves, needed to experience what he called "virtual reality."

From these developments, Ivan Sutherland then developed his own head mounted display called the Ultimate Display. However, due to its sheer size and weight, it later became known as The Sword of Damocles (Flores-Arredondo & Assad-Kottner, 2015) (see figure 3). The difference between this and other headsets of the time is that this was the first to use a computer to generate the images shown in the headset, whereas other devices used a camera to display a live feed or a recording. At the time, the images created by the computer and displayed on the HMD were only wireframe rooms and objects, as the technology at the time did not have enough graphical processing power to generate what we perceive today as CGI (computer generated images).

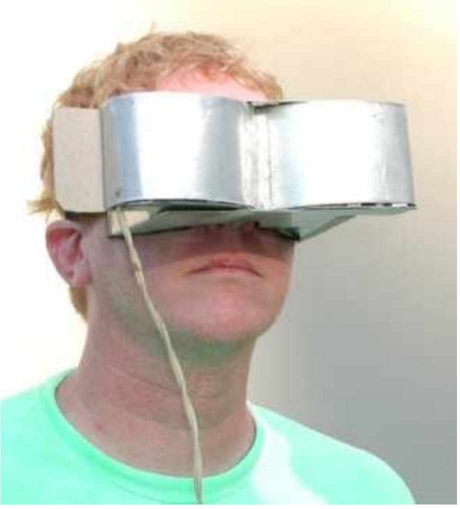


Figure 1 Telesphere Mask (Virtual Reality Society, 2015)

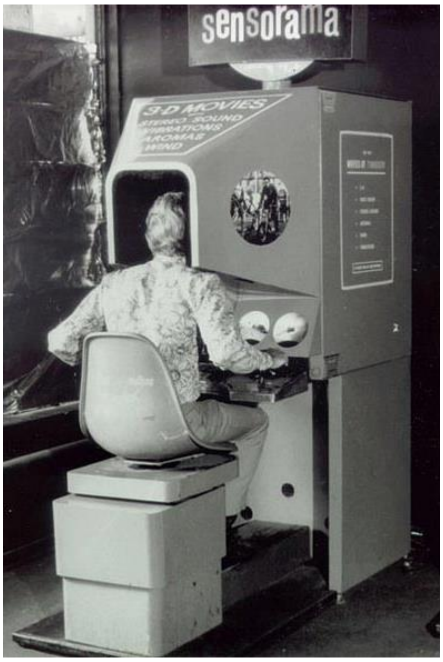


Figure 2 Sensorama Simulator (pc mag, n.d.)

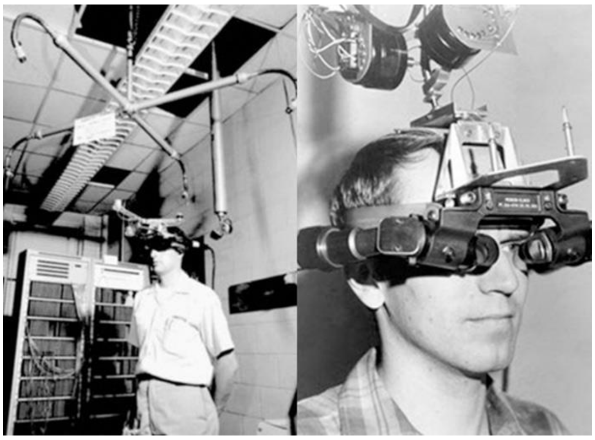


Figure 3 Sword of Damocles (Elaine, 2016)

In recent years HMD's have grown in popularity and become vastly smaller and cheaper form what they once were, take for example the Oculus Rift (see figure 4). Here we have a prime example of a popular consumer product which has allowed consumers to not only experience virtual reality created by other people and organisations, but also to create their own virtual worlds and environments. It also includes a motion tracking stand which creates the sense of realism for the users when they turn or move their heads. At the time of writing this report, the Oculus Rift costs around £399, making this the cheapest dedicated VR headset compared to other headsets such as the HTC Vive (see figure 5) costing £499. However, HTC also offer a pro edition of the Vive which offers the wearer to fully experience surround sound and higher quality images but at a cost of £561.

Figure 4 Oculus Rift (Amazon, 2018)

Figure 5 HTC Vive (VIVE VR SYSTEM, 2018)

2.1 Difference between VR, AR & MR

2.1.1 Virtual reality

Virtual reality (VR) is a computer-generated environment displayed in such a manner that the user would be immersed in that environment as a player or character, depending on the type of virtual reality used. Virtual reality works by creating a full virtual world in which the user can explore without any natural reality involved. There are several devices which have virtual reality capability as mentioned above but these devices require a computer with a good graphics card output to be able to run. There are some devices which are cordless and do not require a computer to run but instead run on battery power and use mobile phones, such as the Samsung Gear (see figure 6) or the Google Cardboard (see figure 7).

Figure 6 Samsung Gear VR (Samsung, 2015)

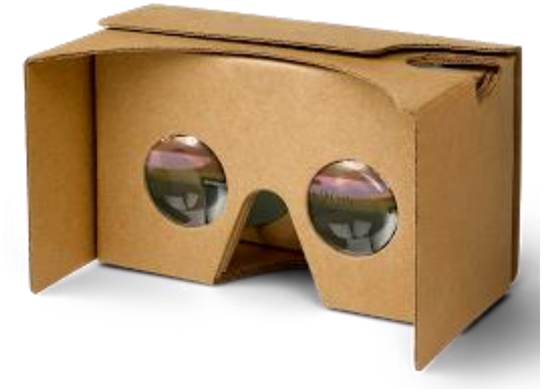


Figure 7 Google Cardboard (Google, 2018)

2.1.2 Augmented reality

Augmented reality (AR) was first coined by Thomas Caudell and David Mizell back in the 1990's to describe how the head mounted displays, which electricians used at the time, worked. In their paper, they described how the augmented reality system worked and stated that "a user looks at a workpiece and sees the exact 3D location of a drill hole is indicated by a bright green arrow, along with the drill size and depth of the hole specified in a text window floating next to the arrow. As the user changes his perspective on the workpiece, the graphical indicator appears to stay in the same physical location." (Caudell & Mizell, 1992). Moving from this to todays augmented reality technology, it has, like with all advancements, become smaller, cheaper and more efficient, and as such, this type of technology can now be found in everyday mobile phones.

There has also been the development of AR dedicated devices such as the Microsoft HoloLens, although there currently is a debate over whether it is a mixed reality or an augmented reality device. Augmented reality can work in several ways according to the University of Exeter, one being with marker locations, in which the computer-generated object will lock onto specific points and then display the computer-generated image, and the other being marker less, in where the computer-generated image locks onto a specific location and displays. They state that "this method uses a combination of an electronic devices' accelerometer, compass and location data (such as the Global Positioning System – GPS) to determine the position in the physical world, which way it is pointing and on which axis the device is operating." (University of Exeter, 2010). At present, there are several applications which stands out for using these features, such examples would be the mobile application known as Pokémon Go, Snapchat and Facebook Messenger.

2.1.3 Mixed reality

Mixed reality (MR) is like augmented reality, in that it displays computer generated images onto real surfaces, however the difference between the two is that mixed reality aims to create virtual objects, such as animals, that would be generated within the environment, and if the user walked out of the area and came back then the animal would still be in that position or location. Whereas augmented reality creates computer generated items within a local area but doesn’t bind them to that area for later use (Johnson, 2016).

When comparing virtual reality with augmented and mixed reality, the difference is obvious but at the same time each shares a similarity with the others. Virtual reality and augmented both use CGI for their surroundings and objects, yet one is obviously a complete virtual world (see figure 8) and the other only takes specific aspects from the virtual world and incorporates them into reality (see figure 9). They are also different in how they generate depth of field. Augmented reality works by producing a three-dimensional image over a specific area whereas virtual reality creates an entire three-dimensional environment and controls the view from the user’s perspective through the use of a headset and motion tracking.

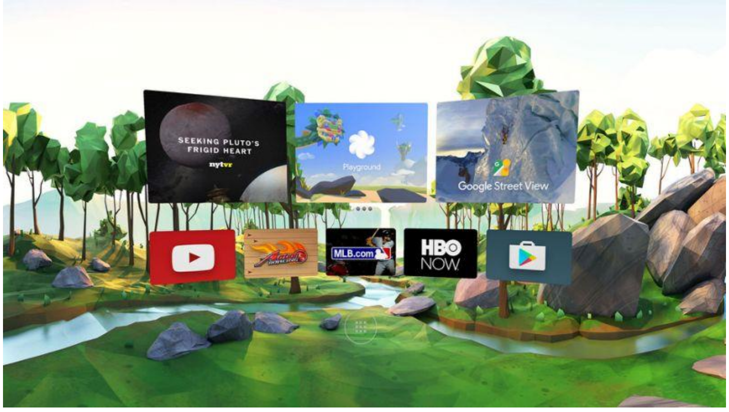


Figure 8 Virtual Reality Display (Parrish, 2016)

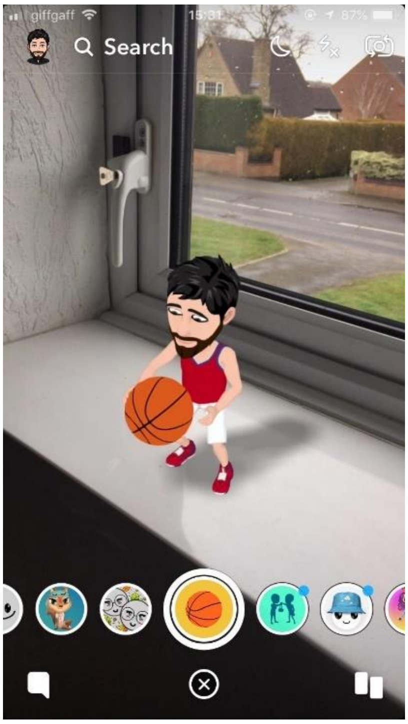


Figure 9 Snapchat AR (Wilson, 2018)

2.2 Development of sensory immersion

Sensory immersion is when the user of a virtual world feels as if they have a sense of presence within that environment, which can be accomplished by using various aspects of reality, such as touch, smell, visuals, sound and taste. By using these aspects of immersion, it gives the virtual world/environment a sense of realism and as a result, has the potential to trick the user's brain into believing the environment is real. This has many applications in todays' society, such as being able to treat people with various conditions such as social anxiety or post-traumatic stress disorder (PTSD).

There are various products which can give the sense of immersion, some come with consumer products such as the Oculus Rift, which comes with haptic feedback controllers to give the user a physical response and allows them to interact with the virtual environment. Most headsets on the market today offer three out of the five senses, being sound, visuals and touch, there are others dedicated devices such as the product offered by thinkgeek.com known as the "VR Sensory Immersion Generator" which allows the user to experience smell, touch, sounds and taste (ThinkGeek, 2018)

3. Virtual Reality Technology & Applications

What we consider as virtual reality technology has only recently been available for consumers to buy in the past few years. This is due in no small part to technology getting smaller and faster, which has allowed companies to develop virtual reality headsets for consumers at affordable prices. However, as most virtual reality headsets require a computer to run, the computers themselves need to be able to support such technology and as a result, these computers are still somewhat expensive, pricing in at over £1000 for a laptop. When it comes to virtual reality however, a custom desktop computer running a 7th generation intel i7 processor with 8GB of RAM, followed by 2 USB 3.0 ports and a HDMI 1.3 port with a dedicated graphics card output such as a Nvidia GTX 1060, is more effective and cheaper for supporting virtual reality devices.

Back when VR first started out, it began as a fixed HMD (head mounted display) but didn't track the users head movements, it only surrounded the user with a display to give the appearance of an immersive world. This device was called the Sensorama and offered the user several sensory inputs such as smell, audio, visual and touch, which for its time was revolutionary and created the first stepping stone to what we know today as virtual reality.

Modern day virtual reality headsets connect to a computer followed by a tracking device which can track the user's actions and interoperates them into the environment, such as the moving of the persons head or picking up objects. These computers need to have a capable/dedicated graphics processor for the user to see the virtual environment on the headset display, as it requires quite a lot of power to generate a three-dimensional world which can change angle when the user moves. The reason these devices require a computer to show the environment within the headset itself is to ensure that it remains portable to some aspect but also offer clear high definition graphics.

3.1 Dedicated vs Non-dedicated devices

For dedicated devices that have been created with the sole purpose of virtual reality in mind, the first device which most would say would be the Oculus rift. This device has been in development for the past few years but has since moved from development to consumer editions. In the most recent edition, the tracker which comes as standard, tracks infrared points within and around the headset itself (see figure 10). Each point represents key areas which the tracker can distinguish and then plot which way the user is facing along with the angle allowing for 360-degree tracking, into the virtual reality environment, whereas the original development edition, only had basic orientation tracking and no built-in audio.

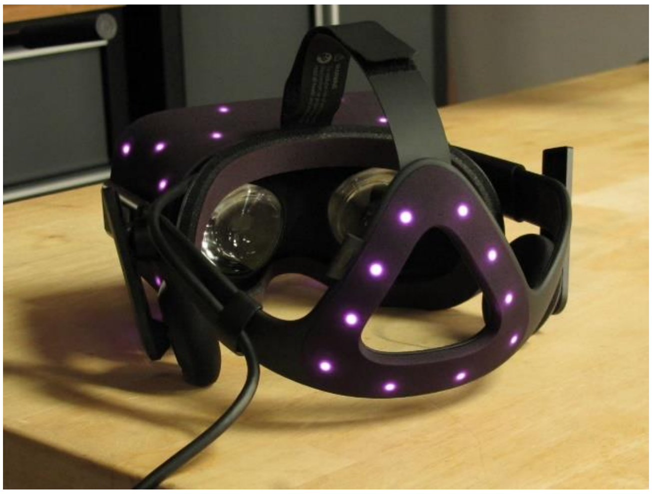


Figure 10 Oculus Rift Infrared Points (ifixit, 2016)

The HTC Vive is another dedicated device which was created with the sole purpose of supporting virtual reality. It works like the Oculus Rift in that it tracks the user's head movements and controllers but has multiple tracking devices instead of just the one. The Vive comes with what is known as haptic feedback controllers (see figure 11). These devices allow the user to manipulate and interact with the virtual reality environment, such as picking up objects or pushing virtual buttons. However, the controllers also give the user a sense of immersion as they offer a sense of feeling when touching objects like rocks (HTC, 2018).

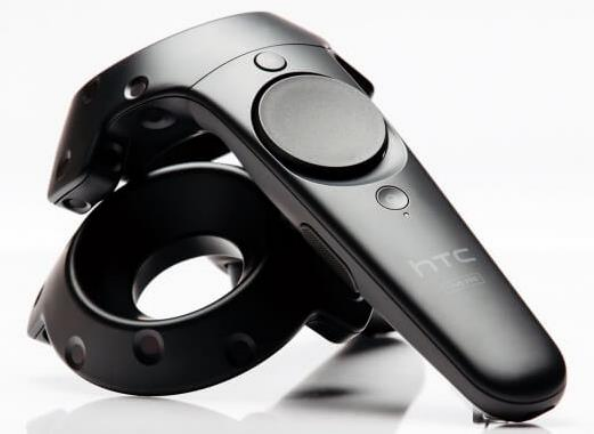


Figure 11 HTC Vive Haptic Feedback Controller (Kvist, 2016)

Both the devices as mentioned above are what is known as dedicated devices, however, there are also devices which are not dedicated but do support virtual reality, example, the Samsung Gear VR. This device works by using the users Samsung mobile device as the display and audio output which is placed within a housing which the user can then wear on their head. This has somewhat of an advantage over the dedicated devices as it has no cables attaching it to a computer, making it truly portable. However, as the display is the mobile smart phone, this will use the battery and will not have such a sharper picture when compared to the Vive or the Oculus.

Another popular non-dedicated virtual reality headset would be Cardboard created by Google. This device works like the Gear VR, in that it uses the user’s smart phone as the display and audio output, but cardboard works with both Samsung and iPhone. However, the cardboard doesn’t have straps which attach it to the user’s head, making it not fully portable and comfortable but does give a very basic view into how virtual reality works.

3.2 Input/output devices

As with nearly all forms of technology, there is what is known as peripherals. These are devices which put information into a system and get information out of a system, such as printers, scanners, keyboards and computer mice. In relation to virtual reality, these peripheral devices can be anything from the headsets to the motion trackers. The haptic feedback controllers, which most virtual reality devices use, are an example of both an input and output device, as the user puts data into the environment when using the controllers but also receives data out of the environment when touching an object. The way the haptic feedback controllers' work is through slight vibrations within the controller itself, which trigger under specific conditions set within the virtual reality environment. As mentioned previously, there are such peripheral devices which provide the user with a sense of immersion, such as immersion generators, which produce wind, sound, smell and touch.

Recently, however, there has been a development in sensory immersion, in the form of virtual reality motion chairs and haptic feedback devices. These chairs, such as the MMOne, move along multiple axis allowing the user to feel more immersed in the VR environment. The development in the haptic feedback comes in the form of gloves. These gloves work in the way haptic feedback controllers' work, in the sense that they vibrate when a specific condition has been met. However, they are more precise, in that the user can feel specific vibrations in localised areas and not just one section. There has also been a vest developed, called the Hardlight VR suit which works in the same way as the gloves mentioned previously.

3.3 Virtual Reality Software

To create a virtual reality environment, specialist software, which not only has the capacity to create an environment which can be used on a variety of devices, but also has usability which the user can understand and familiarise themselves with, are required. Currently there are several key pieces of software available to download which not only offer the user the ability to create virtual reality environments but are also known for detail and quality of how the software creates the environment. One such application, which has also been used during the experiment in this research project, is the popular software known as Unreal Engine created by Epic Games. This software allows the users to create a variety of projects such as FPS (First Person Shooters), virtual reality environments and much more. Not only does it allow for the creation of such projects, but it also has a community marketplace in which other users and developers can upload and share projects or add-ons either for free of for money. It also has provided the user with multiple ways of packaging the projects for different devices such as PlayStation, Android and IOS devices and virtual reality headsets such as Oculus Rift, Google Cardboard and more.

Not only is there Unreal Engine but there is other software such as Unity which has been created by Unity Technologies. However, when testing this application to see if it was suitable for the experiment, it appeared too complex and less user friendly than Unreal Engine, but with appropriate training and time, the application would undoubtedly be around the same level of usability. Both Unreal and Unity are the recommended choice for creating a virtual reality environment along with other types of games as they both offer support and have plenty tutorials on YouTube, but there are more and more programmes being designed and developed with the sole purpose of virtual reality and augmented reality in mind (Kraft, 2016).

3.4 Applications

When it comes to virtual reality, many would associate it with the video game industry, yet in recent years, it has been adapted to serve in other sectors outside the gaming world. There are several industries which have recently taken advantage of virtual reality; one such would be within the education industry, in which VR is used to teach students a variety of subjects, ranging from visualising history to seeing how the human body works. Ying, Jiong, Wei, Jingchun, & Xiaopeng (2017) state that “VR education can take you into a virtual scene, in which students could make real interaction and communication with foreign teachers and students”.

Not only is it being used within education, but it is also being used within theme parks to make rides more immersive (White, 2016). The virtual reality applications being used by these parks have mapped the motions of the rides to that within the VR environment, so when the ride moves in a certain way, this is replicated into the VR environment. Another use of virtual reality within other industries would be within the medical sector in which virtual reality is used to help train doctors in performing operations and diagnosing symptoms on a virtual character. From this, doctors and nurses can gain a more in-depth feel into how to perform an accurate diagnosis on a real patient in the future.

Virtual reality is also being adapted by the judiciary system in that it can be used within court rooms to show juries a reconstructed crime scene. According to Varinsky (2016), they state that “The immersive technology offers a way for members of a jury to look inside a crime scene or watch a simulation of an accident with a level of detail that photographs, and witness testimonies can’t capture”. From this, we can assume that the use of virtual reality will be playing a key role in allowing juries to view key evidence from their own perspective.

A recent development using virtual reality would be treating people with posttraumatic stress disorder (PTSD) by placing them into an immersive virtual reality environment which allows them to be rehabilitated. This is known as VRET which stands for Virtual Reality Exposure Therapy. One such project used to help treat people with PTSD was known as Bravemind. This project was developed by the University of Southern California and according to Rizzo, Hartholt, Grimani, Leeds, & Liewer (2014); they state that “Bravemind was designed specifically to support customizable options for a range of relevant traumatic experiences”. Bravemind originated from a previous VRET developed back in 2007; however, Bravemind draws upon the original data and expands upon it by creating more scenarios and increased detail.

Not only has VRET been developed to help people with PTSD but also to help treat people with phantom limb pain (PLP). According to Henriksen, et al. (2016) they hypothesize that “A VR simulation could grant the therapy a more dynamic, immersive environment, which could greatly increase the potential and possibilities of its exercises”.

Recently, virtual reality has made the jump from individuals using it to play games to multiple connected users in a virtual reality chat room, like that found in the application known as VR Chat. This type of virtual reality uses Unity SDK to build each environment as well as allowing other users to make their own custom environment. From this, players can choose a virtual avatar to represent themselves within the chosen world and can communicate with other simply by talking towards the other users’ avatar. These types of environments could allow for the development of illegal virtual reality file hosting, allowing multiple users to view and possible add to that environment, be it videos, images or other such material.

4. Literature Review

As with all forms of data, there are those who want to hide it from any unwanted eyes in a way which would seem like a simple piece of information when in truth there is far more than meets the eye. Recently however, more and more people are taking advantage of concealing digital data in attempts to send files hidden within other files so no one would truly know what is going on in the background other than the intended recipient. This is of concern to the digital forensic investigators, whose job it is to analyse these types of files in a way which not only preserves the original data but also allows them to provide evidence within a court of law about their findings relating to a case.

Back in 2012, an article was published on the BBC website by Prof Alan Woodward of the University of Surrey, in which he described the hiding of data as "the whole world can see it but only those who know where to look can see the intended message" (Woodward, 2012). Since then, many more tools and procedures have been developed with the intention of concealing data from anyone other than the intended recipient.

Kessler (2007) argues that there is a "fine line between protecting one's privacy and preventing a court-sanctioned search", but it would depend on the type of data and which way they have chosen to conceal this data, whether it is in a simple location but within several subfolders or for example, a JPEG has been renamed and had its extension changed to a system file. However, Conlan, Baggili, & Breitinger (2016) argue that there has not been enough "academic research towards what can be deemed as 'anti-digital forensics', 'anti-forensics', or 'counter-forensics'". Anti-forensics is a method used to hinder investigations and prevent evidence from being discovered, within digital forensics, this can be anything from steganography to what is known as a Zip Bomb. As the project will revolve around concealing data within a virtual reality environment using anti-forensic techniques it is possible that this will lead to furthering academic research related to anti-forensics.

Since new technologies are being developed all the time, it is inevitable that forensic investigators would face new problems and challenges. Lillis, Becker, O'Sullivan, & Scanlon (2016) state "the variety of new digital evidence sources poses new and challenging problems for the digital investigator from an identification, acquisition, storage and analysis perspective." As the development of VR has grown rapidly in the past few years it is logical to think that so to would the issues relating to forensically analysing such files.

Depending on which program is used to create a virtual reality environment or game, the file and folder structure will be different, however in the case of this project, the program used was Unreal Engine 4.17 created by Epic Games. When the project was being created, it produced a master folder relating to the project being created at that time and several subfolders and files relating to that build. Each folder was named accordingly to what it contained relating to the build, such as Config, Build & Content. These folders contain crucial information that the program needs to successfully open the build, without them the build could become corrupt. But for forensic investigators, searching these folders with conventional tools would prove ineffective. This is because if an image is placed within the virtual reality environment, the program creates its own version of that image and changes its data type to that of a uasset file, which when placed into a forensic analyser, only shows information relating to the function within the environment, not what it looks like or what it contains.

In the past few years, steganography has been an ever-increasing issue for forensic investigators due to the presence of free and easy to access programs which allow any user to perform steganography processes with ease. However, with malware such as stegoloader and Zbot going around, it is becoming clear that the need for steganalysis is vital and more research needs to be done to allow investigators to find and analyse such files. Hamid, Yahya, Ahmad, & Al-Qershi (2012) state “using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files”. Kothari, Thakkar, & Khara (2017) also state that “Information hiding is to hide some secret information in cover objects, such as an image, audios, videos, texts, etc.” Both these papers have failed to consider the possibility that a file subjected to steganography could also be hidden within another carrier such as a virtual reality environment.

As mentioned above, with the recent development of virtual reality, digital forensic investigators are now facing, the need to advance research in looking for concealed data which has been hidden using steganography and/or other means. There is an urgent need to use methods or tools which would allow forensic investigators to search and analyse all new and upcoming file formats in the event that they could be used to hide data.

5. Methodologies

5.1 Introduction

The section of this report will focus on the research methodology used, a brief description of each different type of methodology followed by the pros and cons of each along with which specific method was chosen and why. It will also include the aims and objectives of this report and the experiment to be carried out.

5.2 Qualitative

In qualitative research, the focus is more towards describing how something happened rather than focusing solely on numerical results. This usually results in using open-ended questions to gather data but can prove difficult to quantify but can provide more specific details into a person's behaviours or feelings and is often used within the social sciences. By using this, it can allow a researcher to discover more detailed information relating to a specific theory (skillsyouneed, 2018).

5.3 Quantitative

Compared to the qualitative methodology as mentioned earlier, the quantitative methodology relies on numerical data rather than open-ended questions, which allows for them to be classified and placed into a graph to order them. By using this, it can provide accurate results in an experiment such as one revolving around mathematics. However, the downside of using this is that it can sometimes lack the detail needed in some findings. (skillsyouneed, 2018)

5.4 Inductive

The inductive approach to research, also known as the "bottom up" approach, normally starts with an experiment based around current/observed trends and then the results generated from the analysis of the data allows for a hypothesis to be generated and then the creation of the theory. This type of research differentiates from other types of research as the theory doesn't drive the experiment or influence the analysis of the results, but instead generates a range of generalisations from the observed data.

5.5 Deductive

A deductive approach is based around developing a new theory or hypothesis from a current theory through testing by developing a research approach to testing this new theory or hypothesis and allows for the generalisation of specific areas. Using this methodology allows for the creation of new theories based from current ones, which can further the research within the target field of the given hypothesis depending on whether the hypothesis is supported or not by the data analysis (Research Methodology, 2018)

5.6 Mixed

A mixed methodology research method comprises of a variety of different research methods such as using inductive, quantitative and the waterfall method. This isn't just restricted to the most used methods either; it can be anything in which the author deems necessary. The positives of this method allow the author to have a wider range of methods to use by combining many different aspects which make for a good overall methodology; however, the negatives of this type of methodology bring over the negatives of the other methodologies used.

5.7 Selected Research method for this project

This project will be using a mixed approach to research as each of the mentioned methodologies above have areas which will be useful in the planning of the research, the design of the application and the analysis of the results which will help to back up the theory of this this thesis. Not only will this methodology include several aspects on how each section will be completed but it will allow for a broader spectrum in which the analysis of the results will be conducted.

The research for this thesis will be carried out through several methods, one being the review of the literature currently available within the field of steganography and virtual reality. The other will be through experimentation by using multiple forensic analysis applications such as Encase 8, Internet Evidence Finder and Forensic Tool Kit on the virtual reality application, to see if any evidence can be found while using sound procedures for forensic analysis. This will be accomplished by using a qualitative approach.

While using different tools for the analysis, other tools which are used to create virtual reality applications will be compared for their effectiveness and ease of use. Finally, the reason why virtual reality was chosen over other such realities such as augmented and mixed, is due to VR becoming increasingly used and will be shown through a deductive approach.

6. Steganography

This history of steganography dates to ancient Greece, in which the word steganography originates and combines the words known as steganos which loosely translates to covered or concealed and grafia, which means writing from ancient Greek and the first known instance was coined by Johannes Trithemius. Krishnan, Thandra, & Baba (2017) state “Steganography embeds a secret message inside an innocent looking cover medium, stealthily, without creating any attention”.

Over the next few centuries, steganography changed and adapted with the times and as such, multiple methods have been created. One popular method was when secrets were tattooed onto slaves’ heads and then dispatched when their hair grew back. According to Kour & Verma (2014) “steganography is not only the art of hiding data but also hiding the fact of transmission of secret data”. Continuing from Kour and Verma’s definition, we can see that for steganography to be effective, the data or information needs to be sent without arousing suspicion from would be snoopers or attackers.

When Steganography transitioned onto computers back in the early 21st century, it allowed for the creation of other carriers and mediums in which secret messages could be sent using the internet in various forms such as images and documents. One such case of notable use of steganography would be back in 2001, according to Zielińska, Mazurczyk, & Szczypiorski (2013) “utilization of the steganographic methods by terrorists while planning the attack on USA on 11th of September 2001”. Recently however, more and more people have been using steganography, for both non-malicious and malicious purposes, and according to the McAfee Lab Threat report of June 2017, a cyberattack tool known as stegloader (aka Gatak) started using image steganography to infect computers with malware and ransomware (McAfee, 2017).

In steganography there are two main methods which are used to conceal the information within the chosen carrier file, these are using the least significant bit (LSB) method (see figure 12) and the bit adding method. The way LSB works, is by using parts of the original file and replacing these bits with the bits from the new file which keeps the file size of the carrier close to the original which in turn reduces detection whereas bit adding, increases the size of the carrier file, increasing the likelihood of detection.

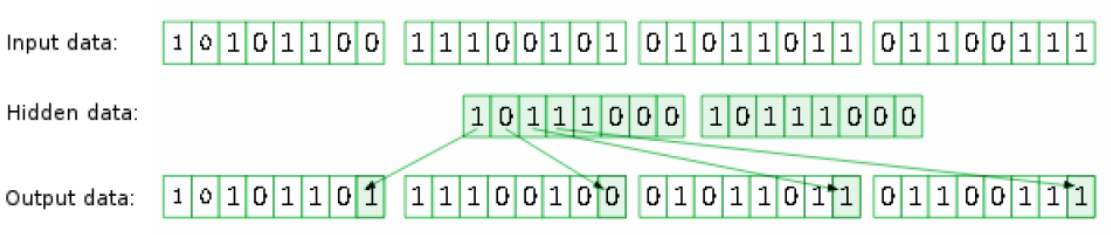


Figure 12 Least Significant Bit Diagram (Kwiatkowska & Swierczewski, 2014)

6.1 Different types of steganography

As mentioned in section 6, slaves used to have their heads tattooed with information and once their hair had regrown, they would be sent to the intended destination and upon arrival, their head would be shaved again to reveal the hidden information. Not only would slaves be used as carriers, but wood would be used as well, this is done by engraving the wood with the information and then covering it with a layer of wax, which would then be melted off by the intended recipient. This is known as physical steganography and was used all the way up until the America revolution, during which time, written information was sent using invisible ink, which was accomplished by using lemon juice and other such fluids. For the recipient to decipher these messages, they simply needed to use a form of heat or light. Not only would invisible ink be used, but also by capitalising specific letters within the information, so when the capital letters are combined, they form a new message (Mount Vernon, 2018).

Since the development of digital devices and the internet, there have been multiple different types of carriers created such as audio files, video files, Images and text documents. These types of carriers are classified under digital steganography, in which the digital information is added to the carriers' own data bits by replacing useless information of that carrier or using unused bits.

Printed steganography such as letters with specific characters capitalised which when combined created a secret message providing the receiver knew what the decipher key was. The first notable use during of printed steganography was during world war two when the Nazis created the microdot which could contain several pages of information including images. However, to see this information, the receivers would need to magnify the document up to 200 times (Woerner, 2015).

A recent development in steganography would be network steganography or protocol steganography which, according to Seo, Manoharan, & Mahanti (2016) "network steganography can be used as a real-time communication tool without raising suspicion".

Another popular method of steganography uses the last bit of information within a carrier file to conceal the hidden text data. According to Vashishtha, Dutta, & Sur (2013), "the least significant bit is modified to hide the secret message; this technique is known as the least significant bit (LSB) steganography or LSB embedding". From this, we can assume that this is steganography down to its basic form, in that it is converting the secret information such as a text messages into binary bits and then merging these binary bits into the carrier's own bits.

6.2 Steganography Software

There are currently several tools on the internet which allow anyone to perform steganography on their own files, be it commercial software or open source; they all perform similar tasks to each other. The software which has been used in this project is OurSecret and OpenPuff, as they were both open source and contained useful features for the investigation. There are several other tools which were tested as part of the experiment, but they proved to be ineffective for multiple reasons, yet they did have features which would be useful. Upon choosing tools to use, several factors were considered, such as what formats the software can use as a carrier, what security features it has and what processes it uses to encode information into the carriers.

When comparing the tools before the experiment and general testing, it was important to consider whether the tools had the ability to add passwords to the carriers to ensure that if the steganography files were to be found, the passwords would ensure that the data within wouldn't be able to be extracted. As such, the tool known as OpenPuff, was the tool of choice for one aspect of the experiment as it not only had the ability to have multiple passwords for the carrier, but it also offered the option to add a decoy file to the carrier that in the event of a password being cracked, the user would simply get a decoy file instead of the correct one. Comparing this to another tool which was used during the experiment such as OurSecret, showed that it was a capable tool, but it didn't have much in terms of features such as no ability to add passwords or decoy files and that it only had the ability to use image files as carriers whereas OpenPuff can use multiple file types and support file sizes up to 256MB. When comparing other steganography tools such as Picel and Xiao Steganography, they only support image steganography so it restricts what the user can use as their carrier file.

7. Project build

This section of the research project covers how the theorised VR carrier file was created followed by the tools used, the creation of the fake evidence, the methods used when implementing the created evidence into the VR environment and finally a way to extract the created evidence from the environment.

There are many tools currently available to consumers which allow anyone to create virtual reality environment, providing they have a computer with enough processing power and a dedicated graphics card capable of handling the high level of detail the virtual reality will inevitably create. This is a result of the fact that the software used to create the environment will require a lot of time to compile and render the landscape.

As mentioned in section 6.2, there are several steganography tools available, such as consumer products and community developed tools, designed to conceal data. Both sets of tools require several hours of teaching to allow the user to be able to successfully create a workable virtual environment which can then be transferred to a virtual reality headset. Such teaching can be through self-teaching and trial and error techniques, or through tutorial videos found on sites such as YouTube.

As mentioned in section 3.3, the tools and tutorials can easily be found online and proves that anyone can create a virtual reality environment or game, without any official training. The accessibility of the tools creates several potential issues for digital forensic investigators as there are more and more tools which are being developed with the purpose of concealing data. Such tools not only allow for the creation of a virtual reality environment but also allow for the creation of augmented reality environments, first person games and more. The tool which was used to develop the virtual reality environment on which this thesis is based upon, was the popular computer application known as Unreal Engine created by Epic Games which can be downloaded from the following site: https://www.unrealengine.com.

There were also several add-ons used to give the virtual environment a more professional looking feel. These included a form of camouflage for the evidence, so it doesn’t stand out when manually searching for it within the environment.

7.1 Creating a virtual reality environment

Prior to creating the virtual reality environment, the size and overall landscape needed to be decided along with how the evidence would be incorporated into the world. The environment’s size could be considered an open world environment, meaning that player can explore the entire environment without limitations. In the context of this thesis, an open world environment is beneficial as it creates a greater area in which to conceal potential data. As all the elements within the world can be customised, several areas were modified with the intention of storing and concealing the evidence, which will have been created later.

7.1.1 World Machine

A third-party tool, known as World Machine which can be downloaded from the following site: https://www.world-machine.com/, was used to create and customise the size of the environment. This is because World Machine can produce realistic landscapes (see figure 13) along with options to modify it, such as adding erosion effects and more. It also offers the option to use Google Maps to copy select areas of real world terrain and use them as a part of the landscape.

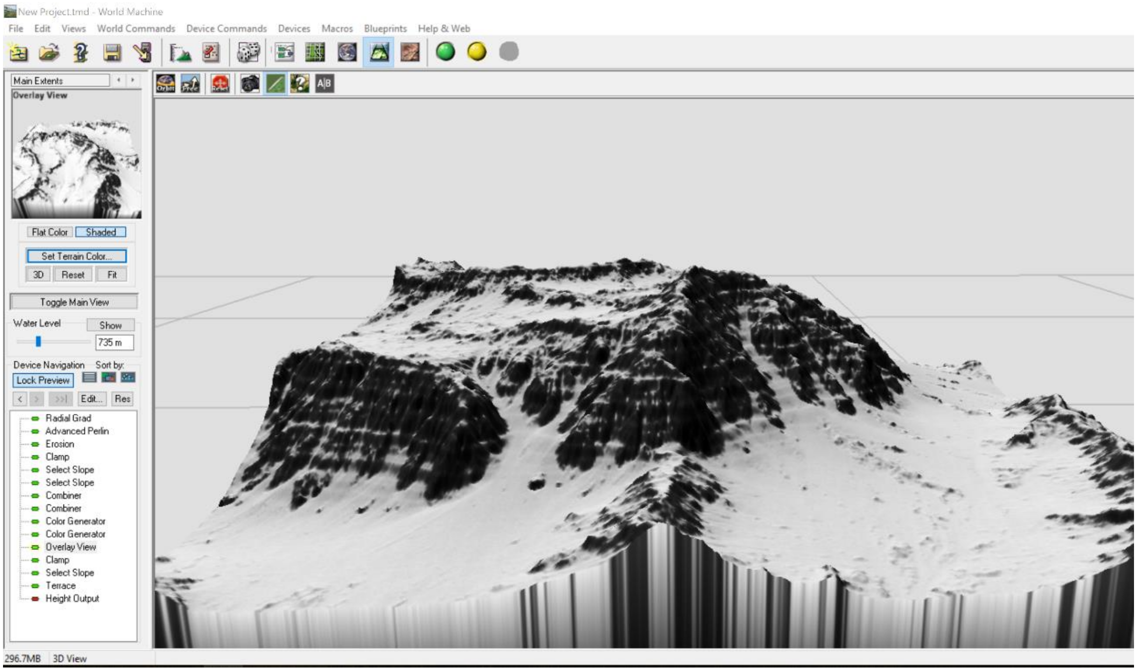
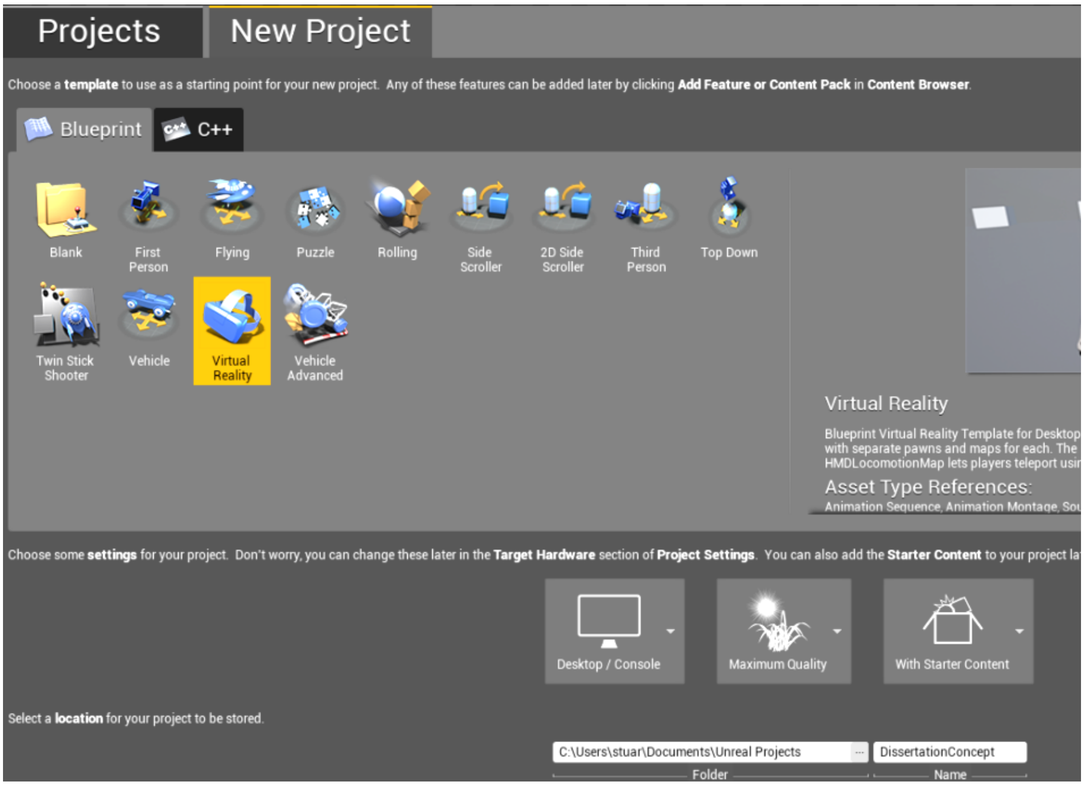


Figure 13 World Machine landscape environment

7.1.2 Unreal Engine

When the overall landscape had been created in World Machine, it was then exported out as a RAW 16 file, so it could be used within Unreal Engine as the primary landscape. However, before the created environment was imported into Unreal Engine, a basic level needed to be generated on which the virtual reality application will be based on. This was done by opening Unreal and selecting a new project, from here the option to select starter content was chosen and the desired platform was chosen as Desktop (see figure 14), this is so the environment will be able to perform correctly.



Choose a **template** to use as a starting point for your new project. Any of these features can be added later by clicking **Add Feature or Content Pack** in **Content Browser**.

Virtual Reality

Blueprint Virtual Reality Template for Desktop with separate pawns and maps for each. The HMDLocomotionMap lets players teleport usi

Asset Type References:

Animation Sequence, Animation Montage, Sou

Choose some **settings** for your project. Don't worry, you can change these later in the **Target Hardware** section of **Project Settings**. You can also add the **Starter Content** to your project la

Desktop / Console

Maximum Quality

With Starter Content

Select a **location** for your project to be stored.

Folder: C:\Users\stuar\Documents\Unreal Projects

Name: DissertationConcept

Figure 14 Unreal Engine new project selection

Once the application had created the desired output, a new VR basic level was chosen, as it provided the necessary building blocks for the virtual reality environment to work (see figure 15).

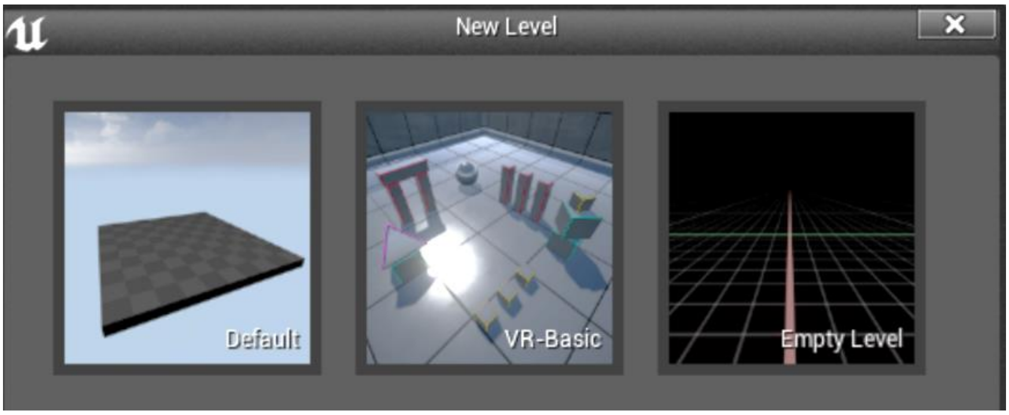
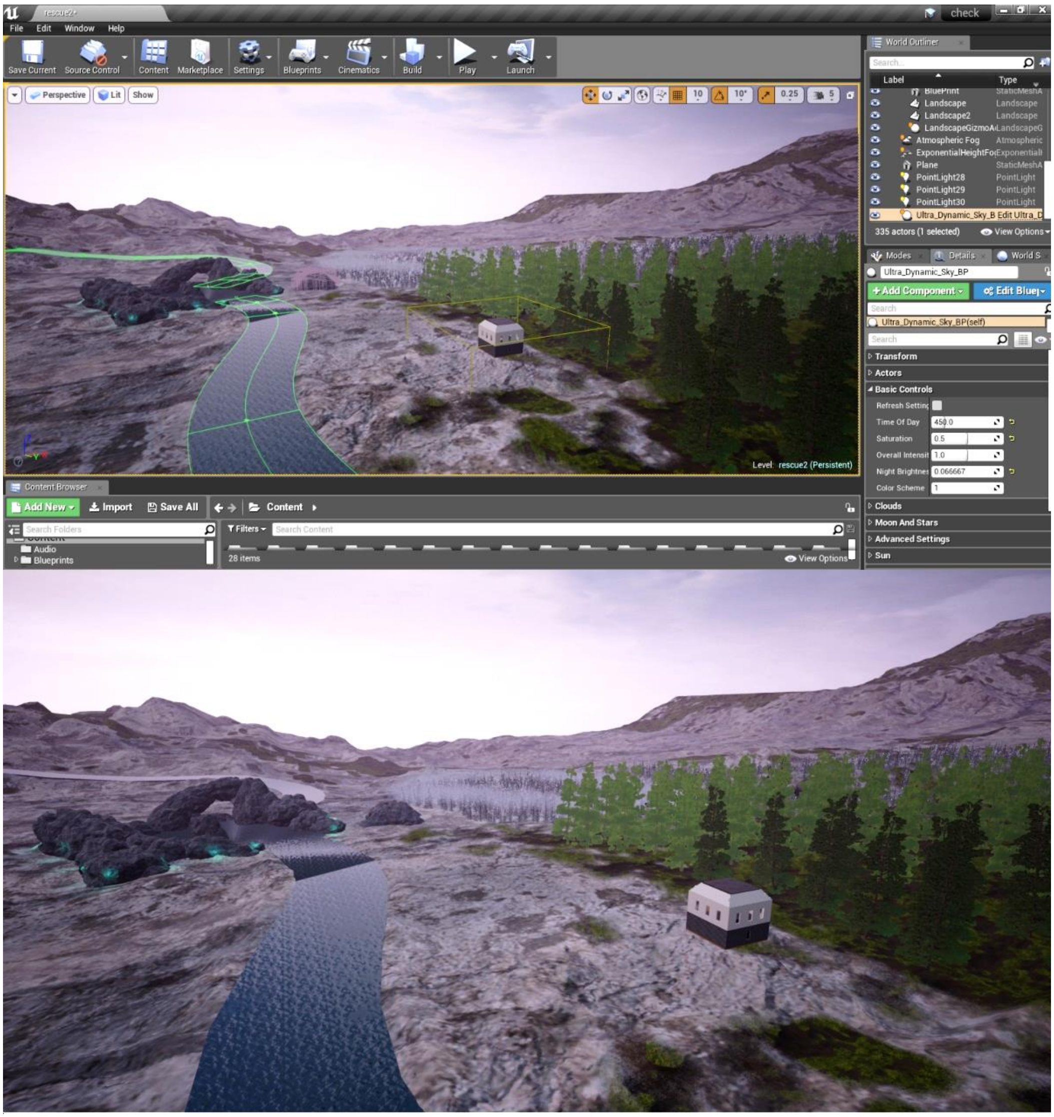


Figure 15 Unreal Engine new level selections

The environment produced previously in World Machine can now be imported and customised, so the evidence can remain securely hidden. From here, the inbuilt tools within Unreal Engine were used to modify the height and angles of several areas to allow for more precise customisation.

The textures were then added to the landscape, which helped to ensure that the world would appear more realistic instead of the standard grey pixelated texture. From here, several rock formations were introduced, and these were then modified to be hollow. The rocks were then made to appear solid, meaning that the user would not be able to pass through when approaching them however, some areas of the rock were made so that the user could pass through, allowing them to effectively enter the rock at a specific point. Such rock formations would allow for data concealment within the rocks, which would only be found if the rocks were approached at a precise angle.

To make the evidence further concealed, a weather and time system was introduced. This restricted the view of several files which were out in the open, and as such added a form of camouflage. When importing the created evidence files into the environment, a few add-ons and assets were required from the Epic Games marketplace, to not only give the environment a more professional look to it but also to allow the application to work with other headsets. An example of the camouflage used was when the video file, which had been created prior to the creation of the virtual environment, needed an in-game environment player which would play automatically on a continuous loop. By doing this, it reduced the need for a trigger which, when activated, would cause the video to play. Figure 16 shows the completed virtual reality environment both running and within Unreal Engine prior to packaging.



Label	Type
BluePrint	StaticMeshA
Landscape	Landscape
Landscape2	Landscape
LandscapeGizmoA	LandscapeG
Atmospheric Fog	Atmospheric
ExponentialHeightFo	Exponentiall
Plane	StaticMeshA
PointLight28	PointLight
PointLight29	PointLight
PointLight30	PointLight
Ultra_Dynamic_Sky_B	Edit Ultra_D

335 actors (1 selected)

Ultra_Dynamic_Sky_BP

Ultra_Dynamic_Sky_BP(self)

Transform

Actors

Basic Controls

Refresh Setting	□
Time Of Day	450.0
Saturation	0.5
Overall Intensit	1.0
Night Brightnes	0.066667
Color Scheme	1

Clouds

Moon And Stars

Advanced Settings

Sun

28 items

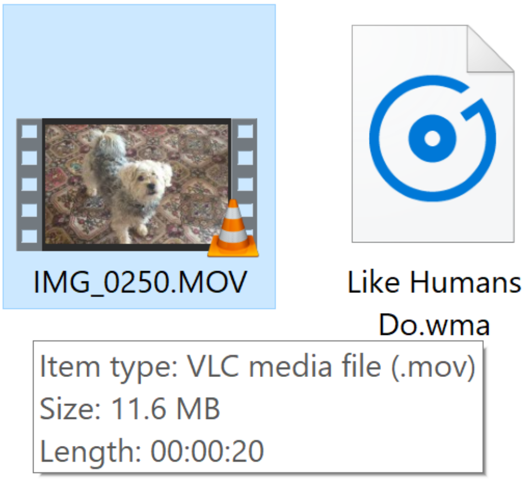
Figure 16 Virtual reality environment completion and comparison

7.2 Creating steganography files

When creating the steganography files, there were a variety of different files which could be used, not only within the created environment but also ones which would look less conspicuous if found, as such, multiple carriers were used such as audio files, video files and image files. As such, several steganography tools such as OurSecret, OpenPuff 4.0, Coagula and DeepSound were used in this experiment.

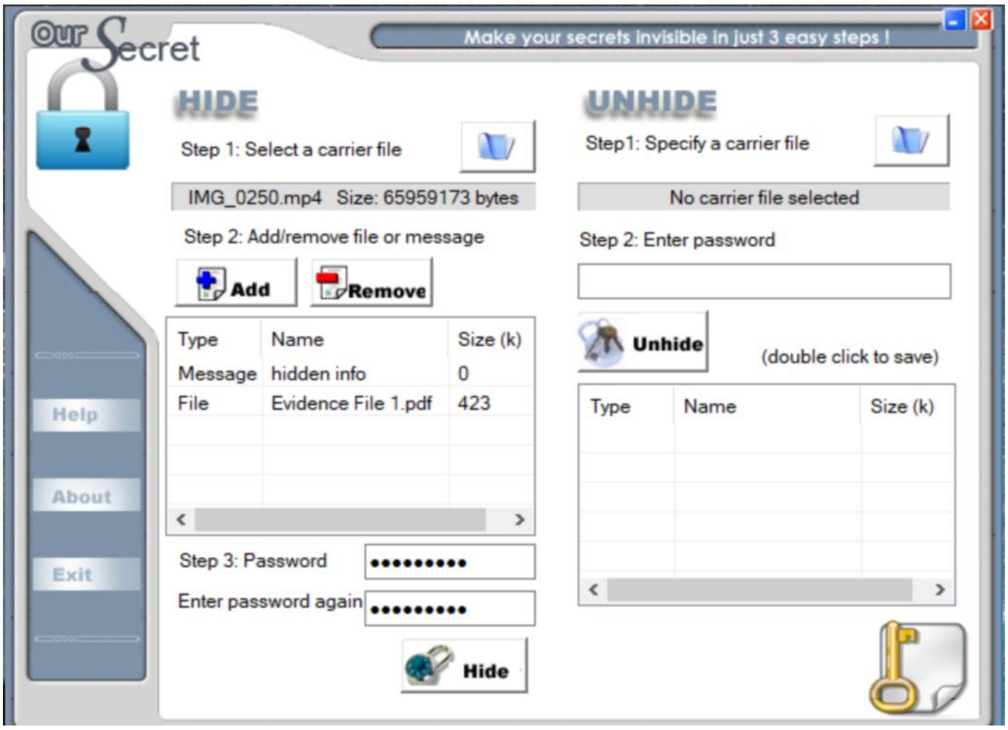
Upon creating the evidence, it was decided that several files would be picture files, taken by the author on a mobile phone, another would be a generic PDF document and the final file would be a Word document. From here, the evidence needed carrier files in which to hide in. One carrier was created by using a mobile phone to record a video, and the other 4 were taken from copyright free sources, ranging from images to music files.

Using the tools mentioned previously, each of the carrier files was subjected to steganography and the created evidence was added respectively to each file. Upon subjecting the carrier files to steganography, the tools used provided the option to add a password or several passwords during the process for added security. In the case of the video carrier file, the application allowed for the addition of text to be added as well as images. In figures 17 to 19, they show the original video file and file size, the evidence which was going to be placed within the file, the software used and the outputted steganography file and file size.



Item type: VLC media file (.mov)
Size: 11.6 MB
Length: 00:00:20

Figure 17 Video evidence and file size before steganography



Step 1: Select a carrier file

IMG_0250.mp4 Size: 65959173 bytes

Step 2: Add/remove file or message

Type	Name	Size (k)
Message	hidden info	0
File	Evidence File 1.pdf	423

Step 3: Password ••••••••••

Enter password again ••••••••••

Step1: Specify a carrier file

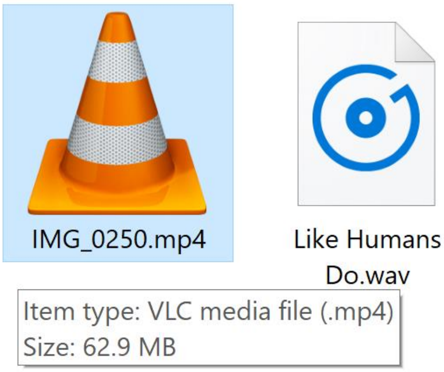
No carrier file selected

Step 2: Enter password

(double click to save)

Type	Name	Size (k)

Figure 18 Our Secret Steganography application with video carrier, PDF and Message file with password protection



Item type: VLC media file (.mp4)
Size: 62.9 MB

Figure 19 Video file size after being subjected to steganography

In one instance, one of the image evidence files was created by writing the Steganography and was saved as an image file, this file was then placed into Coagula and converted to a sound wave for later use in one of the audio carrier files. For further details and screenshots, see appendix B.

Prior to being subjected to steganography, one of the audio carrier files was modified using Audacity to insert the Coagula created file mentioned previously and was saved as a new complete file. This file was later subjected to steganography using the application DeepSound, to add the PDF evidence giving the file two different forms of steganography.

7.3 Storing files within the VRE

After the above steganography files had been created, each was placed into the virtual reality environment using several different methods. When importing the video file, an in-game video player was added and linked to the video itself from within the project folder as this would ensure that the video will remain in one place throughout the entire lifetime of the game. Once the file had been linked, the video player was moved behind a rock formation and its size adjusted accordingly. Figure 20 shows the rock formation from the outside and then from within, displaying the hidden video evidence.

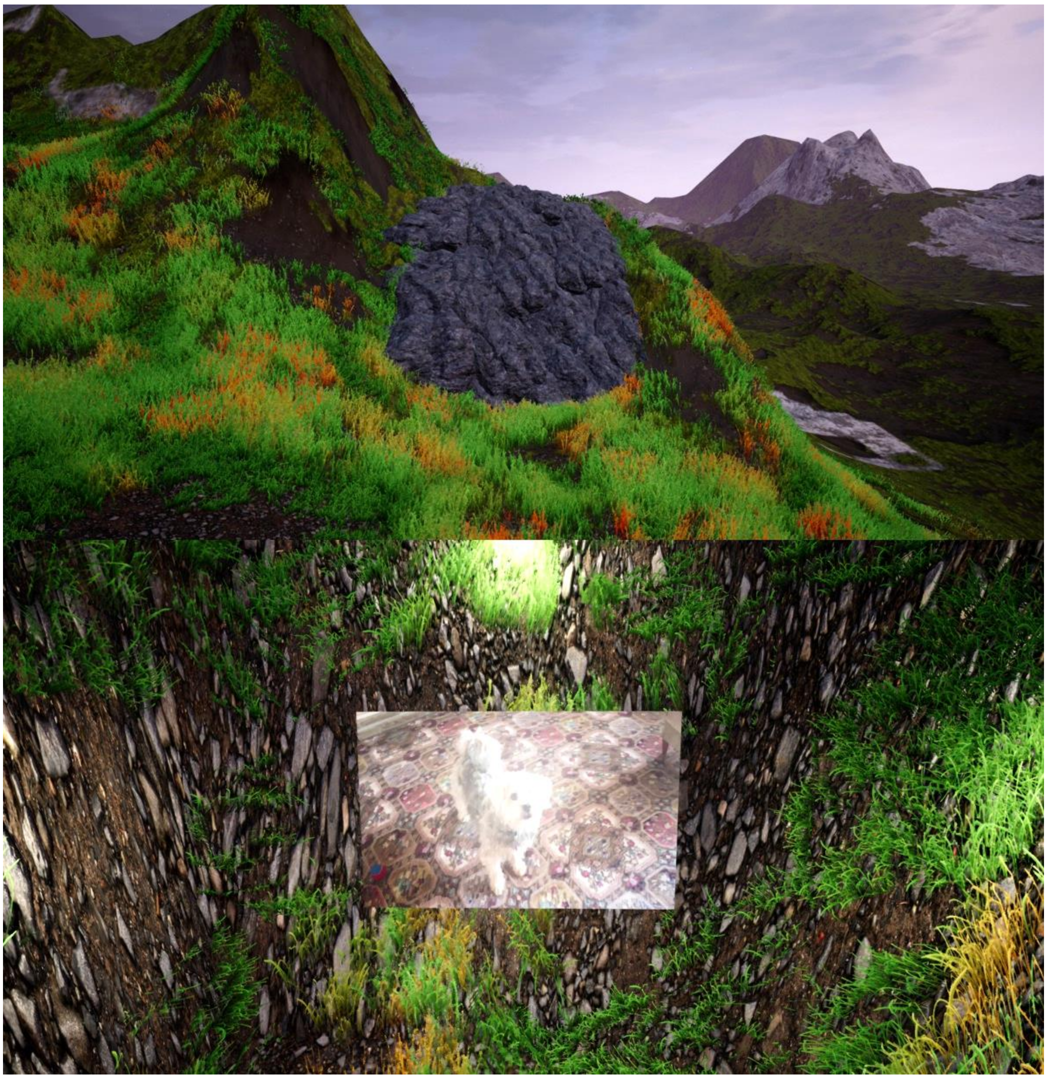


Figure 20 Rock formation within the virtual environment and the hidden video evidence inside

One of the audio carrier files was also added to this same area, however, as the sound can travel in the environment, this needed to be reduced by adjusting the attenuation for the audio file which controlled how far the audio can be heard from within the environment along with its radius.

The same had been done with the secondary audio file, which was placed into the environment, but the difference was that the second audio file had no visible icon which the user could see. Figure 21 shows the secondary audio file within the virtual reality environment with the sound attenuation field highlighted while also within the rock formation.

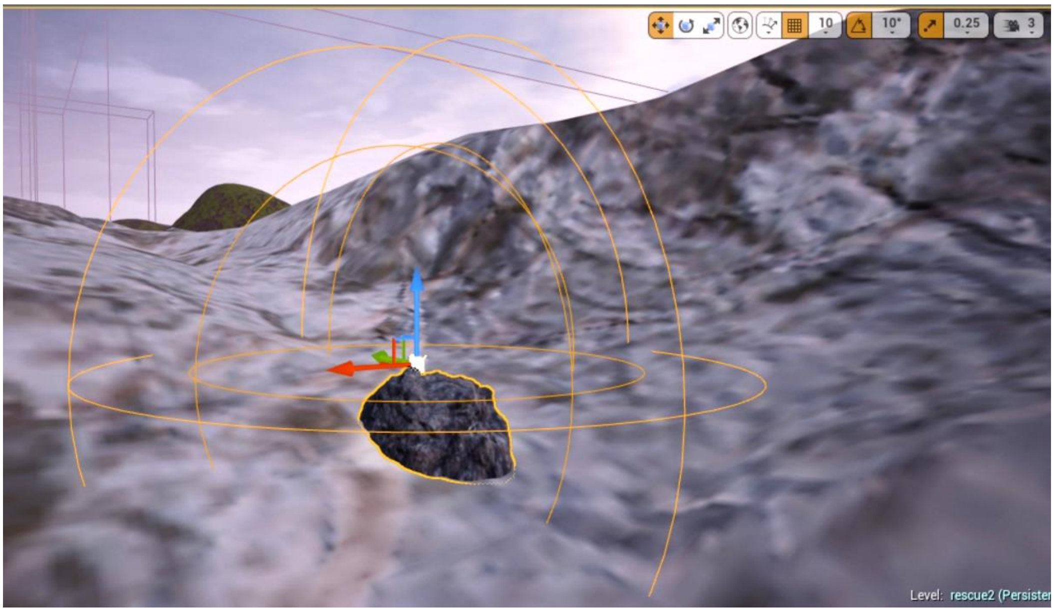


Figure 21 Secondary audio file with attenuation field within the virtual reality environment

Next came the importing of the image carriers; one image file was placed into a rock formation like the video file. However, all the rocks were adjusted so that the player could not pass through them as easily as the video one. Figure 22 shows the rock formation from the outside and the map evidence file from within the rock formation.

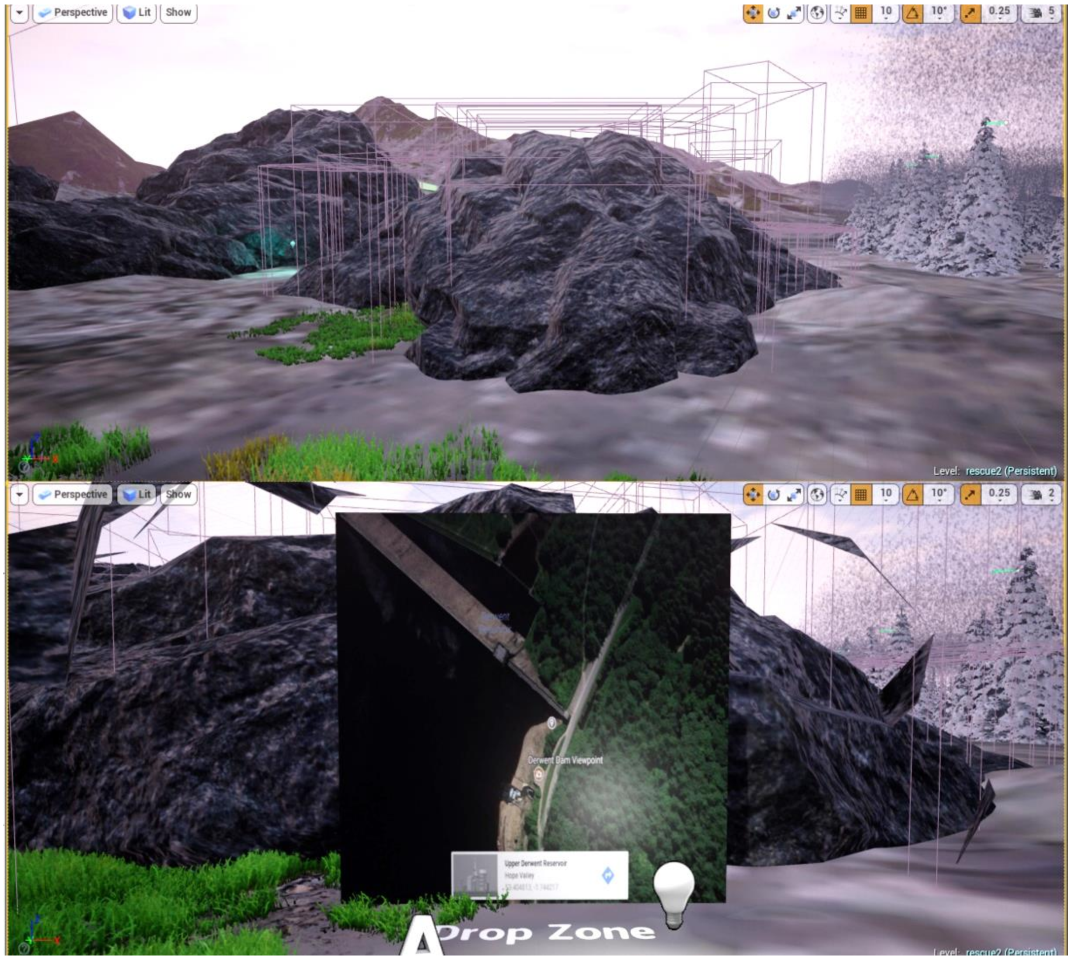
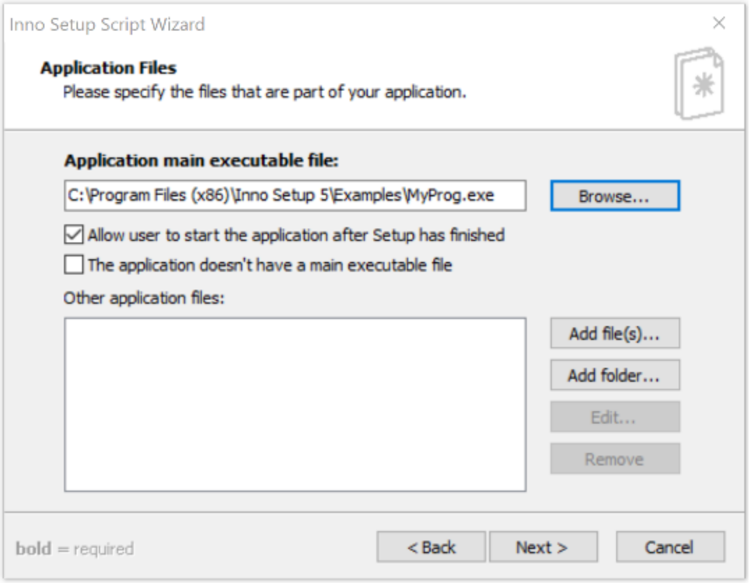


Figure 22 Rock formation from the outside and inside view with evidence

This was done by using a blocking volume. Another image carrier was placed in the open environment itself but behind a grass formation to not arouse suspicion; however, this would likely be found due to the colour of the photo and its proximity to the spawning of the player.

When the files were successfully placed within the environment, some of them such as the video file and the image files, were changed as the program created a duplicate copy of the files which can only be read within the Unreal Engine gaming platform. These files had customisable file names, but the file extension was that of a uasset file which is a file format used by Unreal to store assets relating to that specific game/level such as images, audio and animations. However, the original files remained within the content browser.

Upon completing the build of the environment, it needed to be exported in a way which would make the distribution of the program easy while also keeping the assets secure. As the Unreal Engine has pre-built options for exporting, all that was required was to select the correct option depending on what platform the environment was going to be sent to. However, before the packaging began, there was an option to add encryption to the package files, which would prevent anyone from accessing the data stored within unless the password was entered upon importing the files, this option was left unticked to allow for a non-biased experiment. After the environment had been successfully packaged, it needed to be modified for mass distribution. As such, another third-party application was used to compile the project folder as an executable installer. This program, known as Inno Setup Compiler, compressed the project folder into multiple bin folders followed by the executable. Using this software, it specified where the project would be unpackaged and installed and provided the option for a desktop launcher. Figures 23 to 28 show the process of choosing the executable file and the VR folder and modifying the script to allow for the application to be compress the VR folder into an install file.


Inno Setup Script Wizard

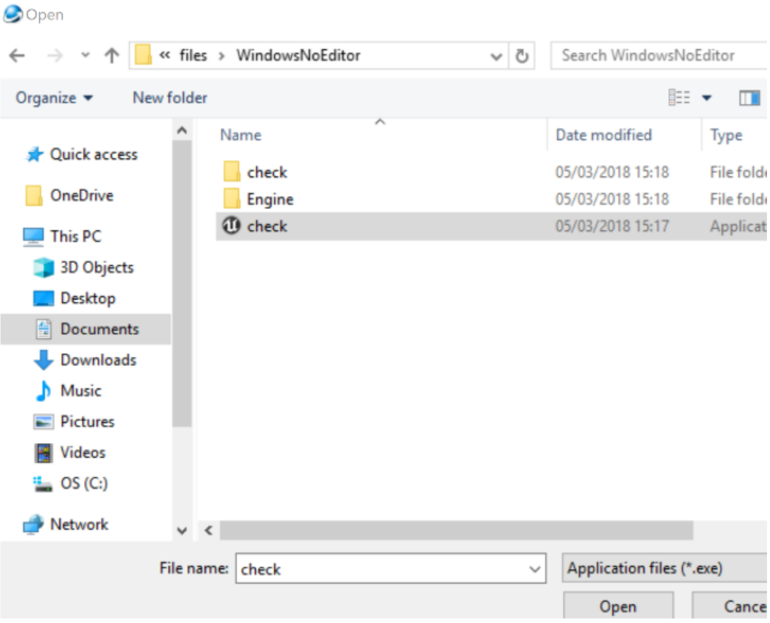
Application Files
Please specify the files that are part of your application.

Application main executable file:
C:\Program Files (x86)\Inno Setup 5\Examples\MyProg.exe

☑ Allow user to start the application after Setup has finished
☐ The application doesn't have a main executable file

Other application files:

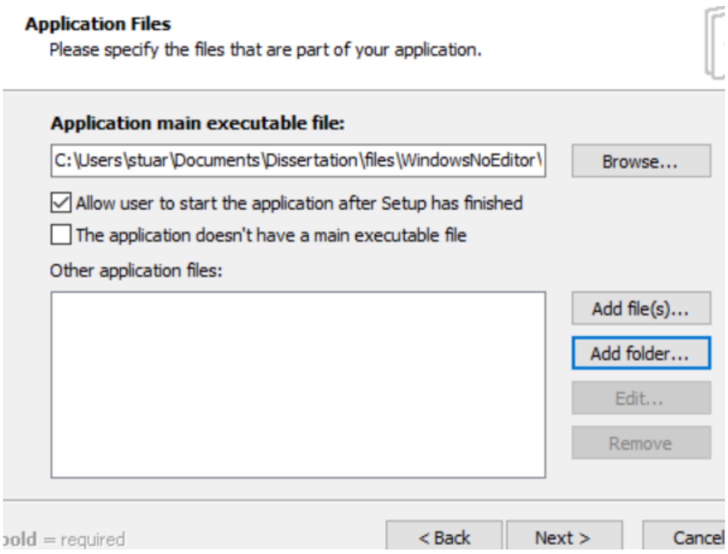
Figure 23 Inno Setup Compiler selecting executable file



File name: check

Application files (*.exe)

Figure 24 Inno Setup Compiler executable file selected



Application Files

Please specify the files that are part of your application.

Application main executable file:

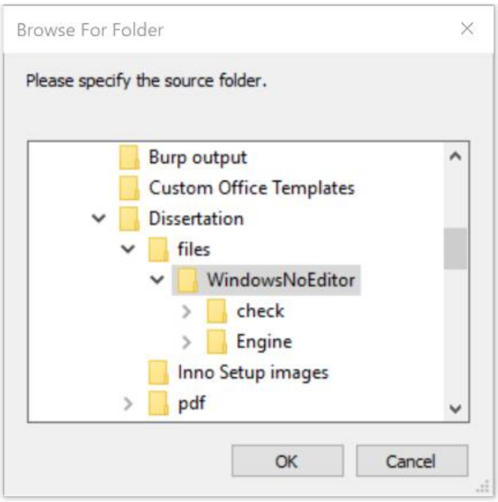
C:\Users\stuar\Documents\Dissertation\files\WindowsNoEditor\

☑ Allow user to start the application after Setup has finished

□ The application doesn't have a main executable file

Other application files:

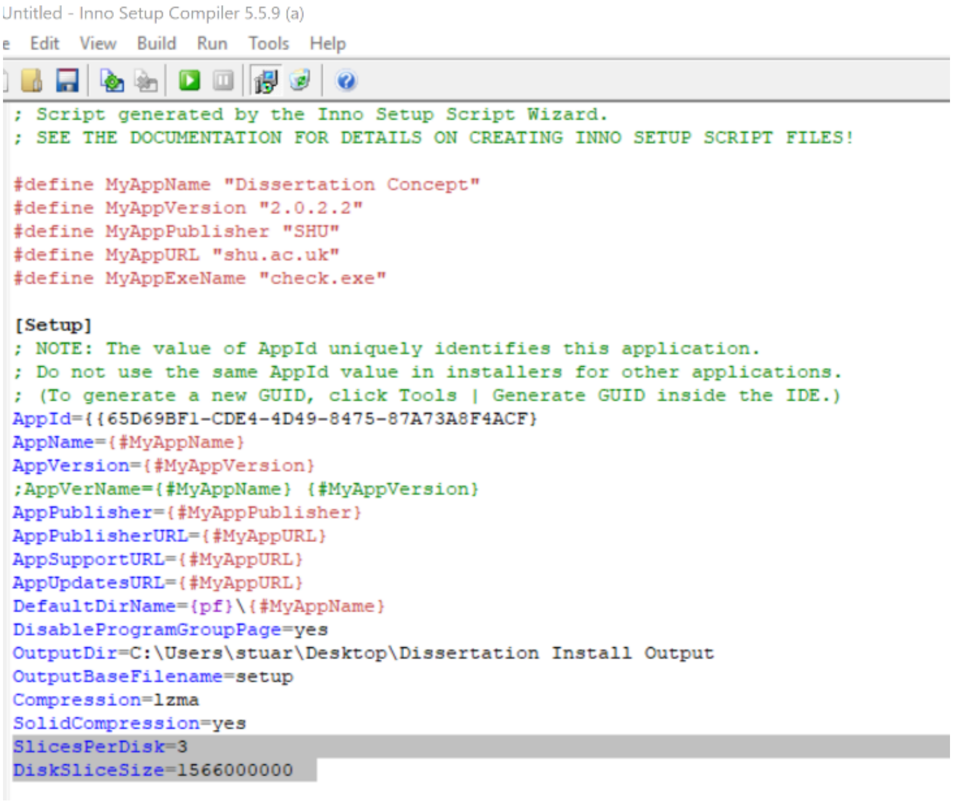
Figure 25 Inno Setup Compiler selecting packaged VR folder



Browse For Folder

Please specify the source folder.

Figure 26 Inno Setup Compiler selected packaged VR folder

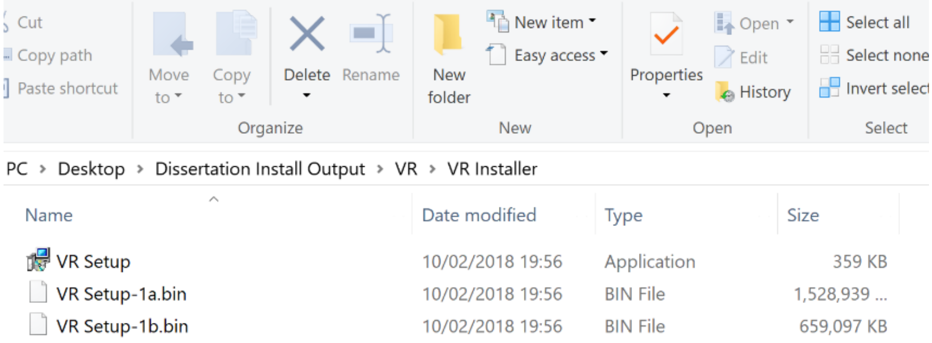

Untitled - Inno Setup Compiler 5.5.9 (a)
e Edit View Build Run Tools Help

```
; Script generated by the Inno Setup Script Wizard.
; SEE THE DOCUMENTATION FOR DETAILS ON CREATING INNO SETUP SCRIPT FILES!

#define MyAppName "Dissertation Concept"
#define MyAppVersion "2.0.2.2"
#define MyAppPublisher "SHU"
#define MyAppURL "shu.ac.uk"
#define MyAppExeName "check.exe"

[Setup]
; NOTE: The value of AppId uniquely identifies this application.
; Do not use the same AppId value in installers for other applications.
; (To generate a new GUID, click Tools | Generate GUID inside the IDE.)
AppId={{65D69BF1-CDE4-4D49-8475-87A73A8F4ACF}
AppName={#MyAppName}
AppVersion={#MyAppVersion}
;AppVerName={#MyAppName} {#MyAppVersion}
AppPublisher={#MyAppPublisher}
AppPublisherURL={#MyAppURL}
AppSupportURL={#MyAppURL}
AppUpdatesURL={#MyAppURL}
DefaultDirName={pf}\{#MyAppName}
DisableProgramGroupPage=yes
OutputDir=C:\Users\stuar\Desktop\Dissertation Install Output
OutputBaseFilename=setup
Compression=lzma
SolidCompression=yes
SlicesPerDisk=3
DiskSliceSize=1566000000
```

Figure 27 Inno Setup Compiler script with modifications



PC › Desktop › Dissertation Install Output › VR › VR Installer

Name	Date modified	Type	Size
VR Setup	10/02/2018 19:56	Application	359 KB
VR Setup-1a.bin	10/02/2018 19:56	BIN File	1,528,939 ...
VR Setup-1b.bin	10/02/2018 19:56	BIN File	659,097 KB

Figure 28 outputted installer files

7.4 Attempted access

Upon completion of the virtual reality environment with the test evidence in place, the application was executed to see if the evidence could be seen once it was in as well as to see if everything performed the way it should. Once the initialising had been completed, the environment successfully launched and allowed for user exploration. Figure 29 shows a screenshot of the finished virtual reality environment. However, due to a hardware issue, the virtual reality headset was not compatible with the computer, in the sense that the display within the headset didn't have access to the graphics card directly and as such did not display anything. However, the motion of the headset still worked within the virtual environment as the camera moved when the headset did.

Despite the headset not being completely compatible with the computer, the environment did generate the entire test evidence. Figure 30 shows an example of one of the evidence files within the virtual reality environment, specifically the map file.

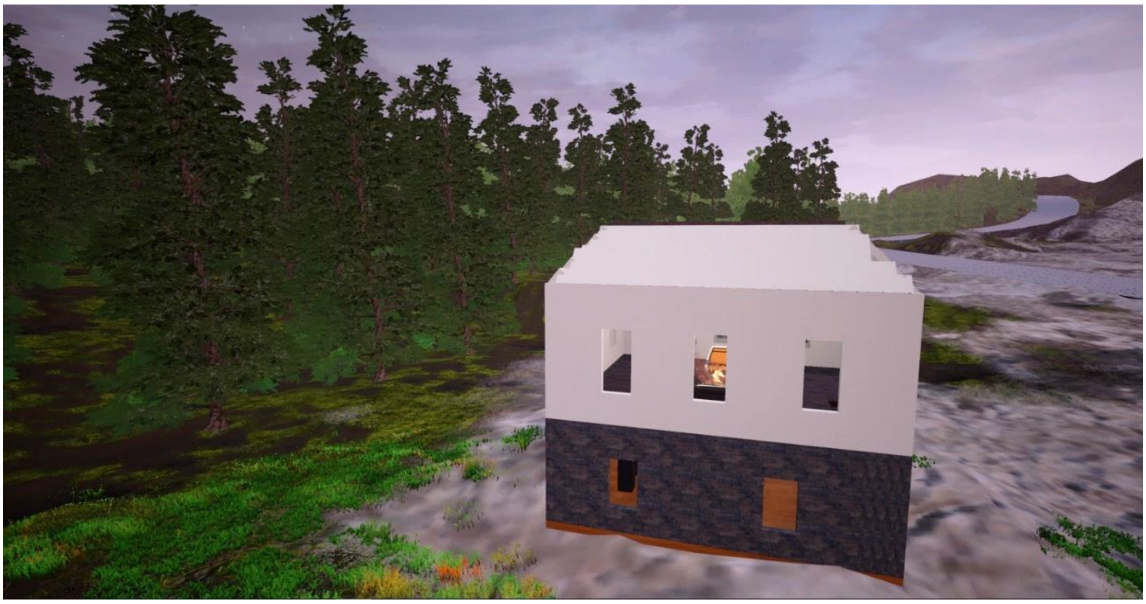


Figure 29 Virtual Reality Environment Completion

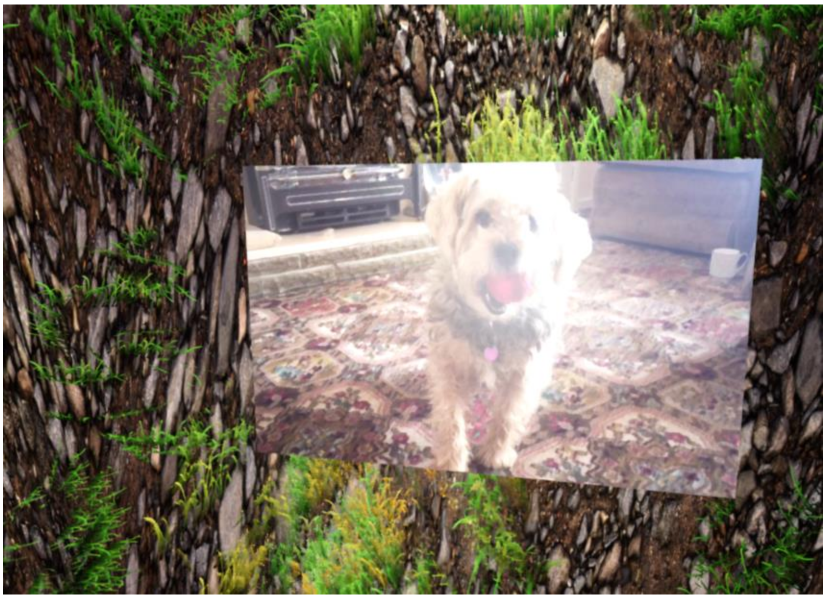


Figure 30 Virtual Reality Environment Test Evidence

Following the initial launch, the install directory was examined to see if any of the test evidence was available to the user for potential retrieval of the steganography files. However, when searching for the test evidence, only the video evidence file was found. This is due to when the video was imported into the environment, it needed to be stored within the project directory, whereas the images, audio and text evidence are stored within the PAK data file. A PAK file is an archive file type used by video games and web browsers to store information relating to the application, such as textures and sounds and can only be opened using 3rd party programs. A 3rd part program would be any application designed to extract the contents of PAK files but are not used within forensics.

Furthermore, if, during the packaging process of the application, the option to encrypt the files is selected, the data stored within the PAK files will not be accessible to anyone without the decryption key, thus preventing access to the game assets.

When trying to access the data within the PAK file, multiple third-party computer programs, such as Dragon UnPACKer 5, PAK Explorer and Umodel, were used to test not only the success rate but also what data could be viewed or retrieved. However, during testing, all but one program failed to access the data, claiming that the file type was not supported. After using the program called Umodel on the PAK file, the test evidence was successfully extracted to a designated output folder, but not before selecting the correct version of Unreal Engine used during the creation.

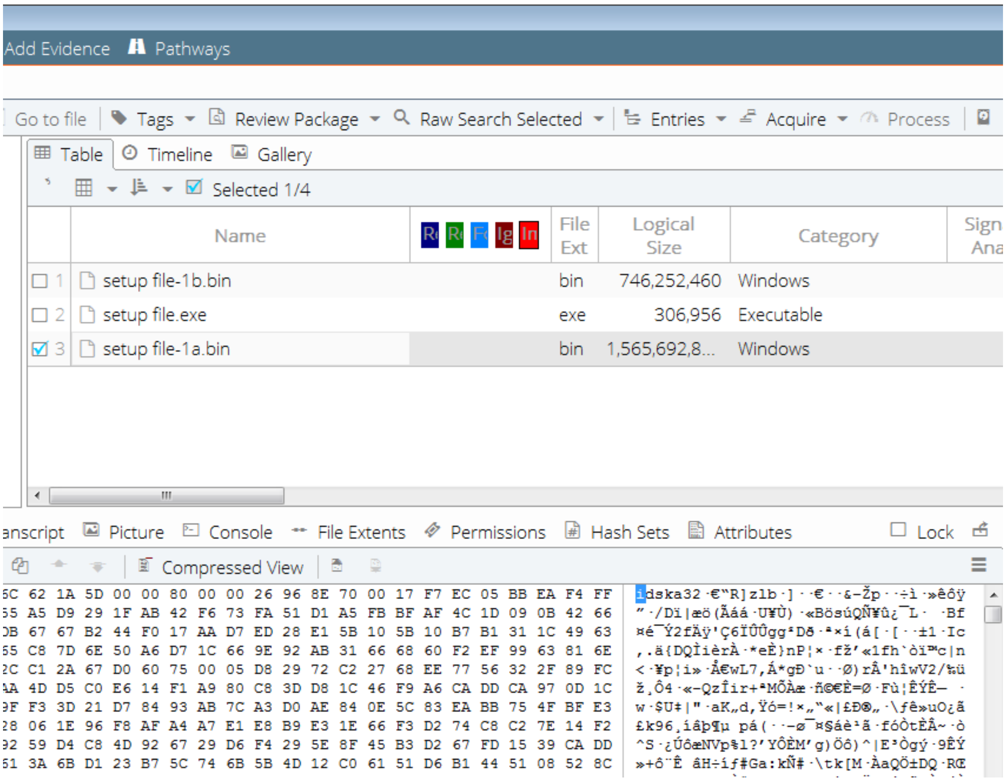
8. Results

This section covers the results of the experiment while using forensic tools such as Encase 8, Autopsy, Forensic Tool Kit 6.2 (FTK) and Internet Evidence Finder (IEF). It will also cover the processes used with each forensic program such as whether carving was selected, what file types to carve for, the relevance of the HEX data. Including what evidence was or wasn't found, what category the evidence was classified as within each tool and what the potential impact of this could be. It will also include the 3rd party application, Umodel, designed to extract the evidence if no evidence is found using the forensic tools mentioned above and if the evidence stored within the carriers can still be accessed.

8.1 Encase

After successfully creating the virtual reality environment and generating the install application from these files using Inno Setup compiler, they were subjected to several forms of testing and analysis within forensic computer programs such as Encase, IEF (Internet Evidence Finder), Autopsy and FTK (Forensic Tool Kit).

Upon analysing the application install files within Encase 8 by dragging them in as single files, none of the test evidence was found within any of the install files. The only evidence which could be considered notable would be the HEX data of each file, as each contained some form of directory structure but not much with regards to locating any viable test evidence. Figure 31 shows one of bin files belonging to the install application within Encase 8 along with the hex view of that specific file.



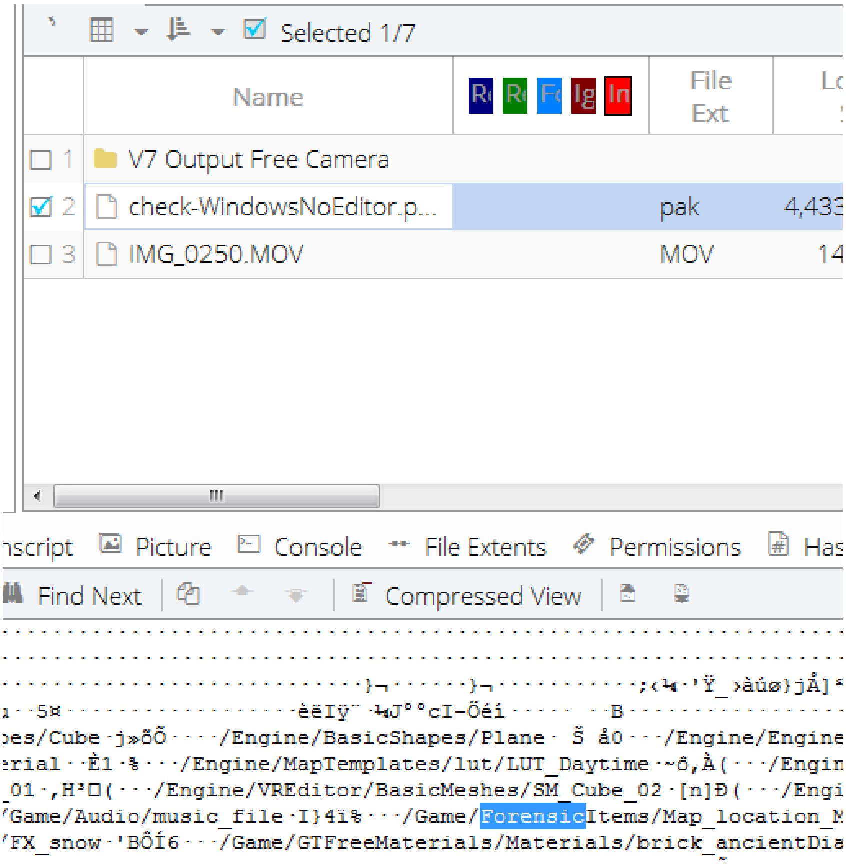
	Name	R R F Ig In	File Ext	Logical Size	Category	Sign Ana
□ 1	setup file-1b.bin		bin	746,252,460	Windows	
□ 2	setup file.exe		exe	306,956	Executable	
☑ 3	setup file-1a.bin		bin	1,565,692,8...	Windows	

```
5C 62 1A 5D 00 00 80 00 00 26 96 8E 70 00 17 F7 EC 05 BB EA F4 FF   idska32·€"R]zlb·]··€··&–Žp··÷ì·»êôÿ
55 A5 D9 29 1F AB 42 F6 73 FA 51 D1 A5 FB BF AF 4C 1D 09 0B 42 66   ”·/Dï|æö(Ãáá·U¥Ù)·«BösúQÑ¥û¿¯L·  ·Bf
DB 67 67 B2 44 F0 17 AA D7 ED 28 E1 5B 10 5B 10 B7 B1 31 1C 49 63   ¤é¯Ý2fÄÿ'Ç6ÏÛÛgg²Dð·ª×í(á[·[··±1·Ic
55 C8 7D 6E 50 A6 D7 1C 66 9E 92 AB 31 66 68 60 F2 EF 99 63 81 6E   ,.ä{DQÌièrÀ·*eÈ}nP¦×·fž’«1fh`òï™c|n
2C C1 2A 67 D0 60 75 00 05 D8 29 72 C2 27 68 EE 77 56 32 2F 89 FC   <·¥p¦i»·Å€wL7,Á*gÐ`u··Ø)rÂ'hîwV2/‰ü
AA 4D D5 C0 E6 14 F1 A9 80 C8 3D D8 1C 46 F9 A6 CA DD CA 97 0D 1C   ž¸Ô4·«–QzÎir+ªMÕÀæ·ñ©€È=Ø·Fù¦ÊÝÊ—  ·
9F F3 3D 21 D7 84 93 AB 7C A3 D0 AE 84 0E 5C 83 EA BB 75 4F BF E3   w·$U‡|"·aK„d,Ÿó=!×„“«|£Ð®„·\ƒê»uO¿ã
28 06 1E 96 F8 AF A4 A7 E1 E8 B9 E3 1E 66 F3 D2 74 C8 C2 7E 14 F2   £k96¸iâþ¶µ pá(··–ø¯¤§áè¹ã·fóÒtÈÂ~·ò
92 59 D4 C8 4D 92 67 29 D6 F4 29 5E 8F 45 B3 D2 67 FD 15 39 CA DD   ^S·¿ÚôæNVp‰l?’YÔÈM’g)Öô)^|E³Ògý·9ÊÝ
51 3A 6B D1 23 B7 5C 74 6B 5B 4D 12 C0 61 51 D6 B1 44 51 08 52 8C   »+ô¨Ê âH÷íf#Ga:kÑ#·\tk[M·ÀaQÖ±DQ·RŒ
```

Figure 31 Encase 8 Analysis of install application files

However, upon testing the root directory after installing the application within a virtual machine using the same methods as mentioned earlier, no questionable evidence was found within Encase again. Despite the video test evidence being easily located within the root directory of the install folder, EnCase failed to classify this as noteworthy evidence. This isn't to say that Encase is not capable of finding this evidence but might require additional add-ons or scripts to the program for it to successfully find this information or a user whose expertise of encase are more capable.

Upon further analysing the root directory, the PAK file which contains all the evidence for the virtual reality environment, was found manually and then placed into Encase for analysis. Despite no evidence being extracted, the directory structure within the PAK file was displayed (see figure 32) which contained the folders and the files within them. This could be considered a notable find as each of the test evidence was displayed in the hex data view, allowing for the possible option of carving the files out.



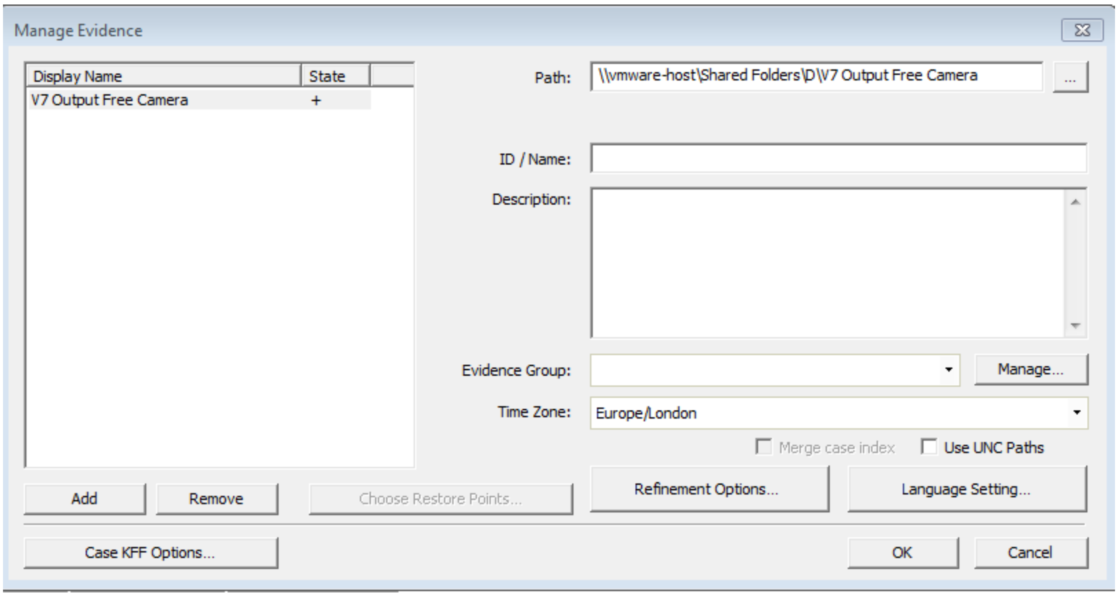
		Name	File Ext	Lo
□	1	V7 Output Free Camera		
☑	2	check-WindowsNoEditor.p...	pak	4,433
□	3	IMG_0250.MOV	MOV	14

```
··························································
··························································
··························}¬······}¬···········;‹¼·'Ÿ_›àúø}jÅ]ª
ı··5¤·················èëIÿ¨·¼J°°cI–Öéí·····  ··B················
ɔes/Cube·j»õÕ····/Engine/BasicShapes/Plane·  Š å0···/Engine/Engine
ɛrial··È1·%···/Engine/MapTemplates/lut/LUT_Daytime·~ô,À(···/Engin
_01·,H³□(···/Engine/VREditor/BasicMeshes/SM_Cube_02·[n]Ð(···/Engi
'Game/Audio/music_file·I}4ï%···/Game/ForensicItems/Map_location_M
'FX_snow·'BÔÍ6···/Game/GTFreeMaterials/Materials/brick_ancientDia
```

Figure 32 Encase 8 HEX view of PAK file

8.2 Forensic Toolkit (FTK)

To analyse the virtual reality application, install files within Forensic Took Kit 6.2 a new case was created. However, as the evidence has been hidden within other files, the processing options were customised to allow the application to search for them by using multiple methods, such as data carving. From here the evidence was added a directory which contained the 3 separate files (see figure 33) and the program began to analyse them for any potential evidence.



Display Name	State
V7 Output Free Camera	+

Path: \\vmware-host\Shared Folders\D\V7 Output Free Camera

ID / Name:

Description:

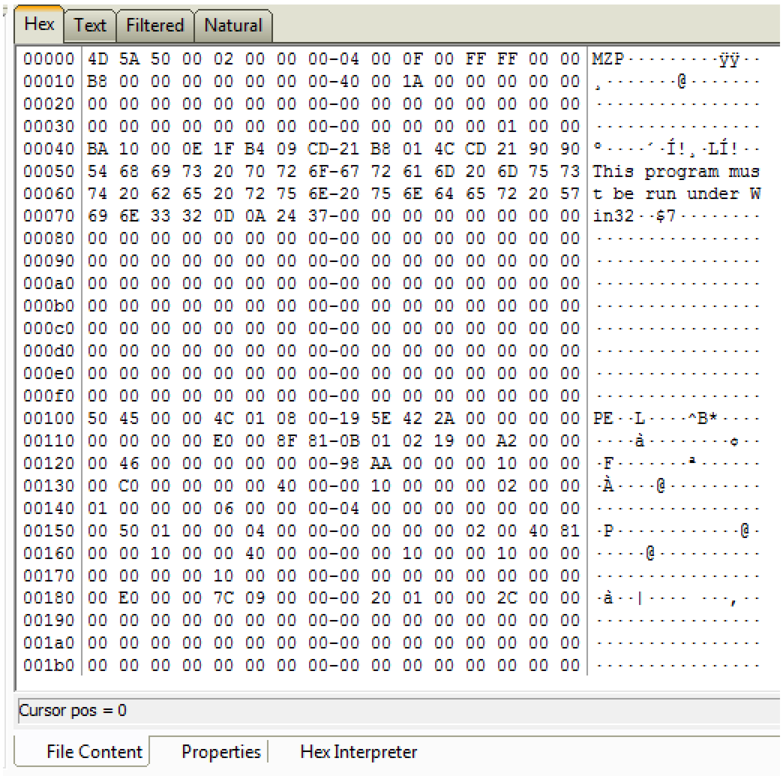
Evidence Group:

Time Zone: Europe/London

□ Merge case index □ Use UNC Paths

Figure 33 Forensic Tool Kit 6.2 Install files added for analysis

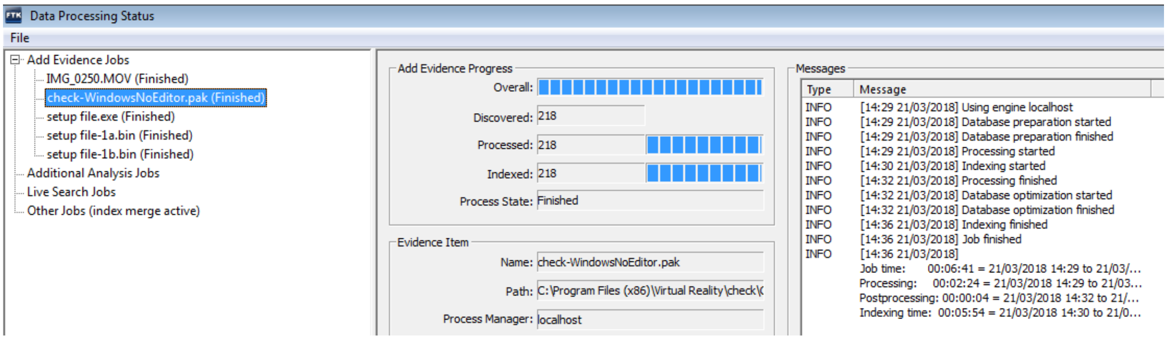
After the program, had finished analysing the files, no notable evidence was displayed relating to either file and the hex data revealed nothing of interest (see figure 34). From here the experiment was then installed onto the virtual machine and the PAK file and the video file were added as separate evidence (see figure 35). The reason behind this is the PAK file and movie files both contain the evidence but cannot be accessed without installing the application first.



```
00000 4D 5A 50 00 02 00 00 00-04 00 0F 00 FF FF 00 00 MZP·········ÿÿ··
00010 B8 00 00 00 00 00 00 00-40 00 1A 00 00 00 00 00 ¸·······@·······
00020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00030 00 00 00 00 00 00 00 00-00 00 00 00 01 00 00 00 ················
00040 BA 10 00 0E 1F B4 09 CD-21 B8 01 4C CD 21 90 90 º····´·Í!¸·LÍ!··
00050 54 68 69 73 20 70 72 6F-67 72 61 6D 20 6D 75 73 This program mus
00060 74 20 62 65 20 72 75 6E-20 75 6E 64 65 72 20 57 t be run under W
00070 69 6E 33 32 0D 0A 24 37-00 00 00 00 00 00 00 00 in32··$7········
00080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00100 50 45 00 00 4C 01 08 00-19 5E 42 2A 00 00 00 00 PE··L····^B*····
00110 00 00 00 00 E0 00 8F 81-0B 01 02 19 00 A2 00 00 ····à·········¢··
00120 00 46 00 00 00 00 00 00-98 AA 00 00 00 10 00 00 ·F········ª·····
00130 00 C0 00 00 00 00 40 00-00 10 00 00 00 02 00 00 ·À····@·········
00140 01 00 00 00 06 00 00 00-04 00 00 00 00 00 00 00 ················
00150 00 50 01 00 00 04 00 00-00 00 00 00 02 00 40 81 ·P············@·
00160 00 00 10 00 00 40 00 00-00 00 10 00 00 10 00 00 ·····@··········
00170 00 00 00 00 10 00 00 00-00 00 00 00 00 00 00 00 ················
00180 00 E0 00 00 7C 09 00 00-00 20 01 00 00 2C 00 00 ·à··|···· ···,··
00190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
001b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Cursor pos = 0

Figure 34 Forensic Tool Kit 6.2 HEX view of install files



Add Evidence Jobs
- IMG_0250.MOV (Finished)
- check-WindowsNoEditor.pak (Finished)
- setup file.exe (Finished)
- setup file-1a.bin (Finished)
- setup file-1b.bin (Finished)

Additional Analysis Jobs
Live Search Jobs
Other Jobs (index merge active)

Add Evidence Progress
Overall:
Discovered: 218
Processed: 218
Indexed: 218
Process State: Finished

Evidence Item
Name: check-WindowsNoEditor.pak
Path: C:\Program Files (x86)\Virtual Reality\check\(
Process Manager: localhost

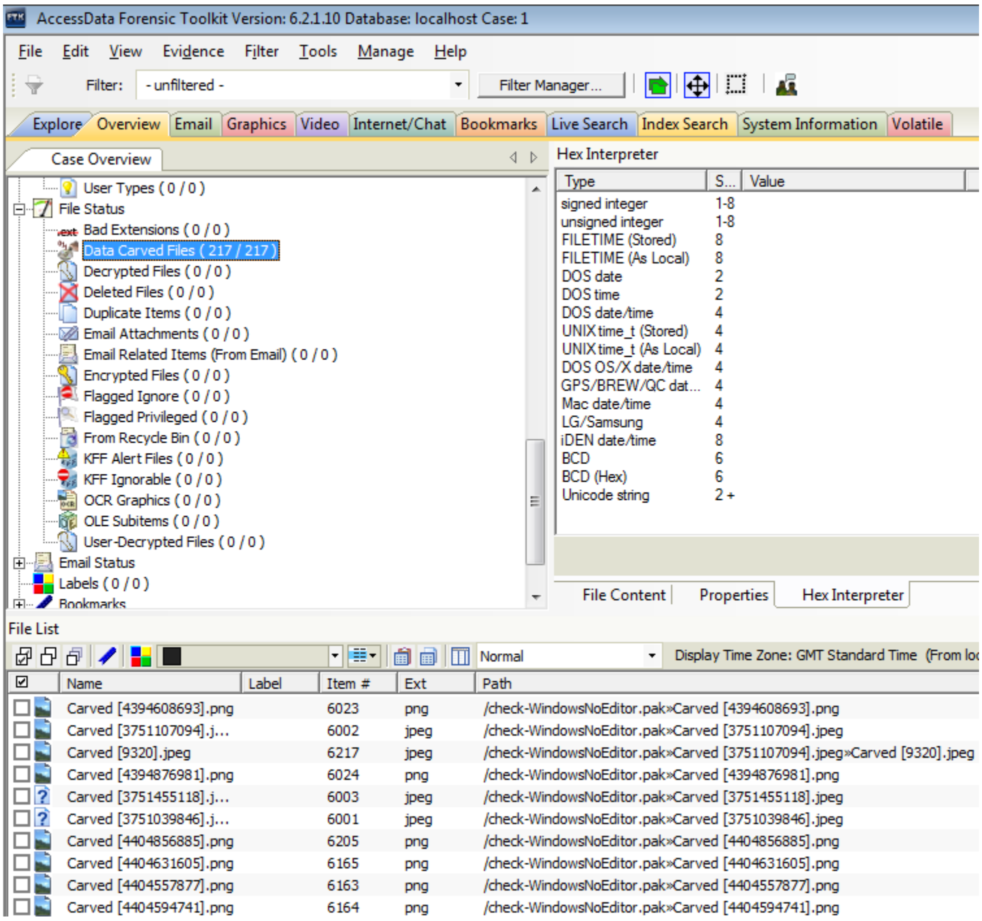
Messages

```
Type    Message
INFO    [14:29 21/03/2018] Using engine localhost
INFO    [14:29 21/03/2018] Database preparation started
INFO    [14:29 21/03/2018] Database preparation finished
INFO    [14:29 21/03/2018] Processing started
INFO    [14:30 21/03/2018] Indexing started
INFO    [14:32 21/03/2018] Processing finished
INFO    [14:32 21/03/2018] Database optimization started
INFO    [14:32 21/03/2018] Database optimization finished
INFO    [14:36 21/03/2018] Indexing finished
INFO    [14:36 21/03/2018] Job finished
INFO    [14:36 21/03/2018]
        Job time:       00:06:41 = 21/03/2018 14:29 to 21/03/...
        Processing:     00:02:24 = 21/03/2018 14:29 to 21/03...
        Postprocessing: 00:00:04 = 21/03/2018 14:32 to 21/...
        Indexing time:  00:05:54 = 21/03/2018 14:30 to 21/0...
```

Figure 35 Forensic Tool Kit 6.2 PAK file and Video file added

Once the evidence was added into FTK, it displayed 4 jpeg image files which were carved out of the PAK file; however, upon trying to view these files, no image was displayed. From here each image was placed into a hex data viewer in the attempt to extract the image and view it as a new file, this proved futile as the data was unreadable.

Upon further investigation, FTK did display approximately 217 image files, but these files were false positives, and only showed simple icon files relating to the Unreal Engine and various window icons (see figure 36).



Filter: - unfiltered -

- User Types (0 / 0)
- File Status
  - Bad Extensions (0 / 0)
  - Data Carved Files (217 / 217)
  - Decrypted Files (0 / 0)
  - Deleted Files (0 / 0)
  - Duplicate Items (0 / 0)
  - Email Attachments (0 / 0)
  - Email Related Items (From Email) (0 / 0)
  - Encrypted Files (0 / 0)
  - Flagged Ignore (0 / 0)
  - Flagged Privileged (0 / 0)
  - From Recycle Bin (0 / 0)
  - KFF Alert Files (0 / 0)
  - KFF Ignorable (0 / 0)
  - OCR Graphics (0 / 0)
  - OLE Subitems (0 / 0)
  - User-Decrypted Files (0 / 0)
- Email Status
- Labels (0 / 0)
- Bookmarks

Type	S...	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (Stored)	8	
FILETIME (As Local)	8	
DOS date	2	
DOS time	2	
DOS date/time	4	
UNIX time_t (Stored)	4	
UNIX time_t (As Local)	4	
DOS OS/X date/time	4	
GPS/BREW/QC dat...	4	
Mac date/time	4	
LG/Samsung	4	
iDEN date/time	8	
BCD	6	
BCD (Hex)	6	
Unicode string	2 +	

Normal
Display Time Zone: GMT Standard Time (From lo

☑	Name	Label	Item #	Ext	Path
☐	Carved [4394608693].png		6023	png	/check-WindowsNoEditor.pak»Carved [4394608693].png
☐	Carved [3751107094].j...		6002	jpeg	/check-WindowsNoEditor.pak»Carved [3751107094].jpeg
☐	Carved [9320].jpeg		6217	jpeg	/check-WindowsNoEditor.pak»Carved [3751107094].jpeg»Carved [9320].jpeg
☐	Carved [4394876981].png		6024	png	/check-WindowsNoEditor.pak»Carved [4394876981].png
☐	Carved [3751455118].j...		6003	jpeg	/check-WindowsNoEditor.pak»Carved [3751455118].jpeg
☐	Carved [3751039846].j...		6001	jpeg	/check-WindowsNoEditor.pak»Carved [3751039846].jpeg
☐	Carved [4404856885].png		6205	png	/check-WindowsNoEditor.pak»Carved [4404856885].png
☐	Carved [4404631605].png		6165	png	/check-WindowsNoEditor.pak»Carved [4404631605].png
☐	Carved [4404557877].png		6163	png	/check-WindowsNoEditor.pak»Carved [4404557877].png
☐	Carved [4404594741].png		6164	png	/check-WindowsNoEditor.pak»Carved [4404594741].png

Figure 36 Forensic Tool Kit 6.2 217 False Positive image files

8.3 Autopsy

When using the application known as Autopsy 4.6 to analyse the virtual reality application files, no notable evidence was displayed except for approximately 6 false positive emails, despite selecting all the ingest modules to allow for a further investigation of the files (see figure 37).

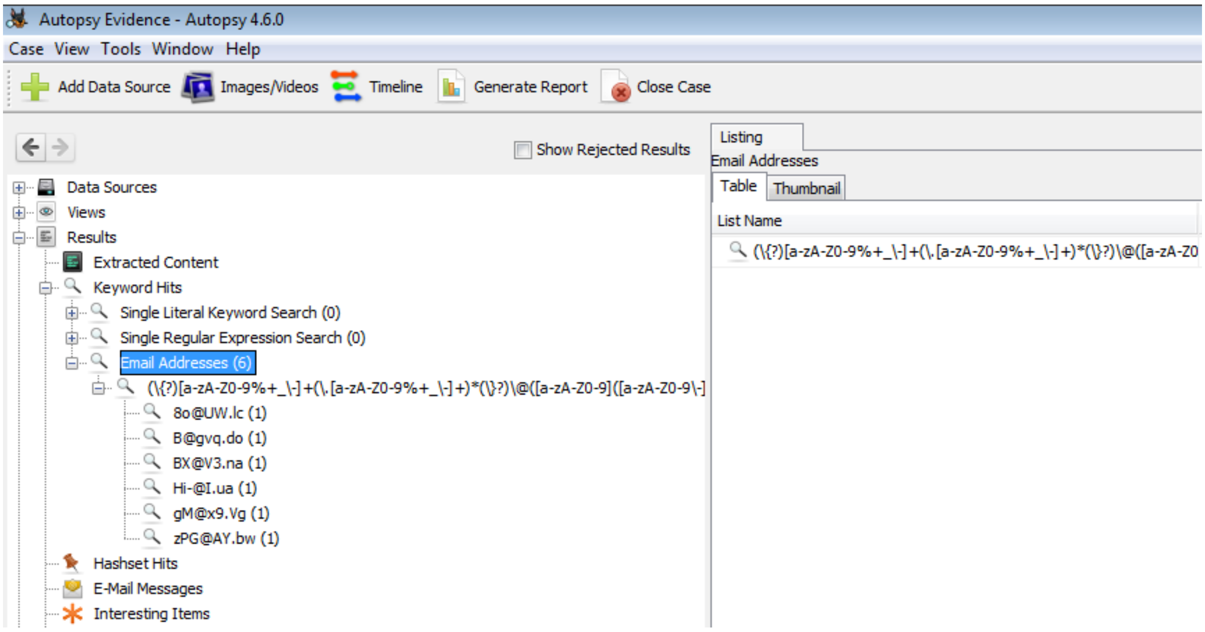


Figure 37 Autopsy 4.6 Analysis of Install files with results

From here the installed PAK file, which contain the evidence along with the movie file, were added into Autopsy under LogicalFileSet2 (see figure 38) to test if the application could search through not only the PAK file but also the steganography movie file and display any notable data. Several further false positive email addresses were found, this is because Autopsy categorises any piece of text with the @ symbol as an email (see figure 39).

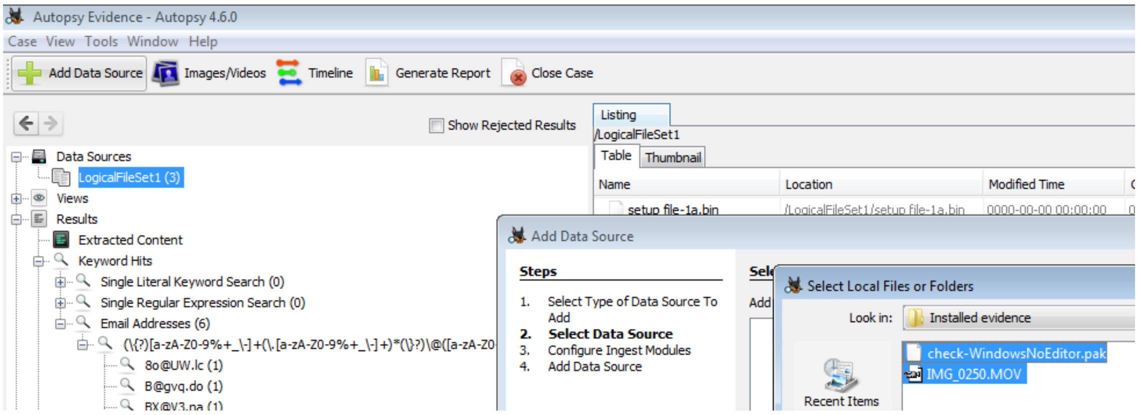
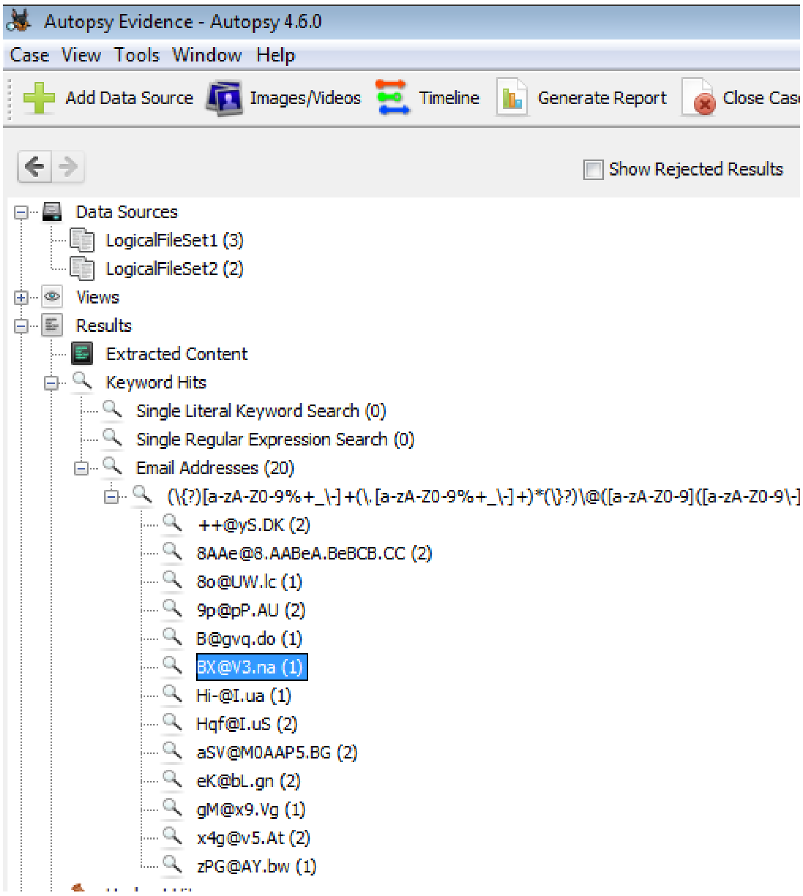


Figure 38 Autopsy 4.6 Selecting PAK file and Video file

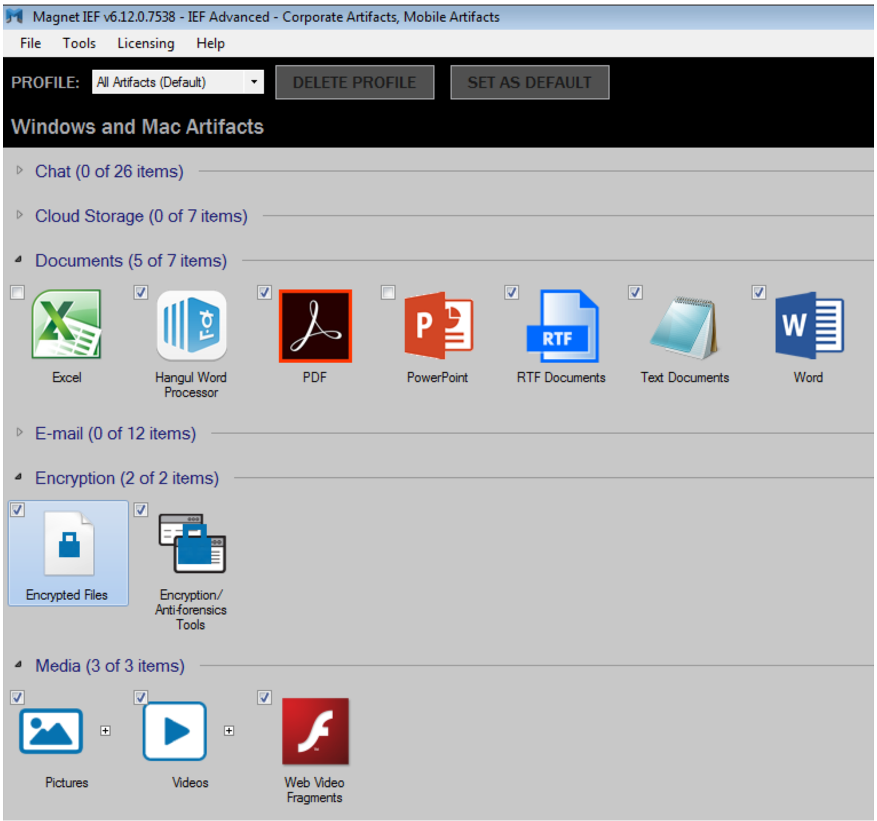


```
Data Sources
    LogicalFileSet1 (3)
    LogicalFileSet2 (2)
Views
Results
    Extracted Content
    Keyword Hits
        Single Literal Keyword Search (0)
        Single Regular Expression Search (0)
        Email Addresses (20)
            (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]
                ++@yS.DK (2)
                8AAe@8.AABeA.BeBCB.CC (2)
                8o@UW.lc (1)
                9p@pP.AU (2)
                B@gvq.do (1)
                BX@V3.na (1)
                Hi-@I.ua (1)
                Hqf@I.uS (2)
                aSV@M0AAP5.BG (2)
                eK@bL.gn (2)
                gM@x9.Vg (1)
                x4g@v5.At (2)
                zPG@AY.bw (1)
```

Figure 39 Autopsy 4.6 analysis results of PAK file and video file

8.4 Internet Evidence Finder

To process the virtual reality application, install files, the files and folder data type was selected as this allowed for the examination of the entire folder. From here the artifacts options were changed to search for any type of media file, encryption file, documents file types, followed by several operating system options (see figure 40). The reason for this is to see if any possible data from the building of the application can be found along with any evidence files.


Magnet IEF v6.12.0.7538 - IEF Advanced - Corporate Artifacts, Mobile Artifacts

File Tools Licensing Help

PROFILE: All Artifacts (Default) DELETE PROFILE SET AS DEFAULT

Windows and Mac Artifacts

Chat (0 of 26 items)

Cloud Storage (0 of 7 items)

Documents (5 of 7 items)

□ Excel ☑ Hangul Word Processor ☑ PDF □ PowerPoint ☑ RTF Documents ☑ Text Documents ☑ Word

E-mail (0 of 12 items)

Encryption (2 of 2 items)

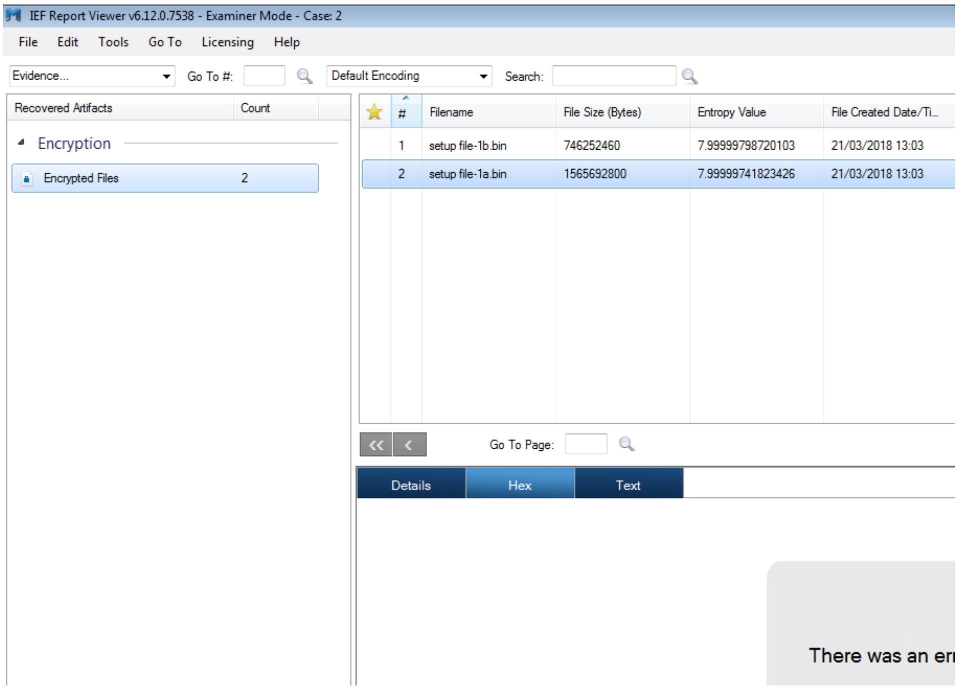
☑ Encrypted Files ☑ Encryption/ Anti-forensics Tools

Media (3 of 3 items)

☑ Pictures ☑ Videos ☑ Web Video Fragments

Figure 40 Internet Evidence Finder Artifacts selection

Once IEF had completed the analysis of the files it then displayed the results consisting of only 2 encryption files. These proved to be just the 2 bin files used for the installation of the application and did not provide any relevant information (see figure 41).


IEF Report Viewer v6.12.0.7538 - Examiner Mode - Case: 2

File Edit Tools Go To Licensing Help

Evidence... Go To #: Default Encoding Search:

Recovered Artifacts	Count
Encryption	
Encrypted Files	2

☆	#	Filename	File Size (Bytes)	Entropy Value	File Created Date/Ti...
	1	setup file-1b.bin	746252460	7.99999798720103	21/03/2018 13:03
	2	setup file-1a.bin	1565692800	7.99999741823426	21/03/2018 13:03

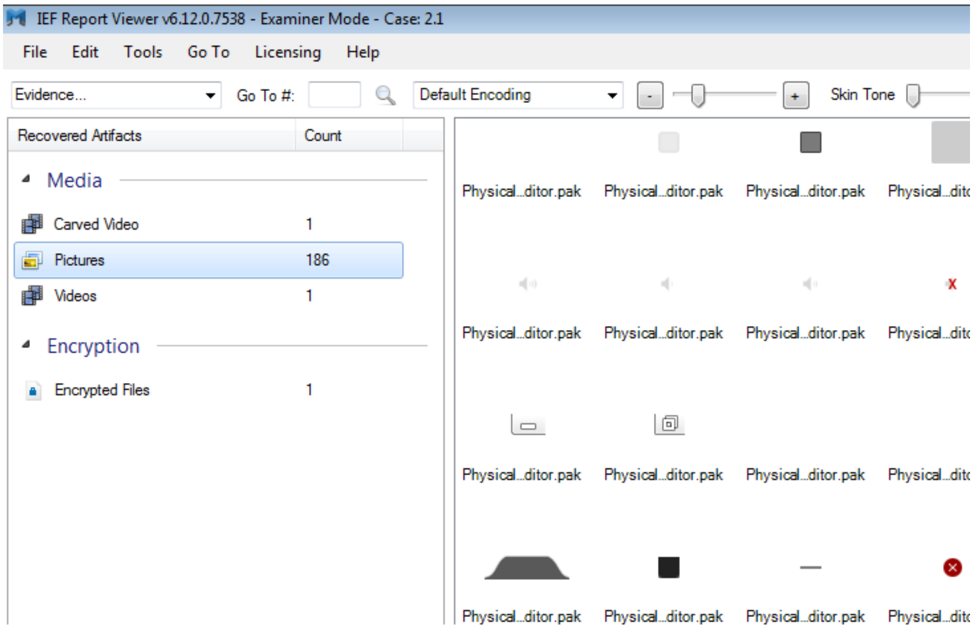
Go To Page:

Details Hex Text

There was an er

Figure 41 Internet Evidence Finder Install Analysis results

As the application install files provided no relevant information, the program was then installed to the virtual machine and the PAK file and the movie file was copied and placed into a folder on the desktop for ease of access. IEF was then restarted and this new evidence was added. The same artifacts options were selected again and IEF began to analyse these new files. Once it completed, the results shown displayed 186 images which proved to be false positives (see figure 42), 1 carved and normal video and 1 encrypted video which was the same as the other video files mentioned. This proved interesting as IEF was able to successfully identify the video file as an encrypted file due to it being subjected to steganography; however, no further information was displayed.

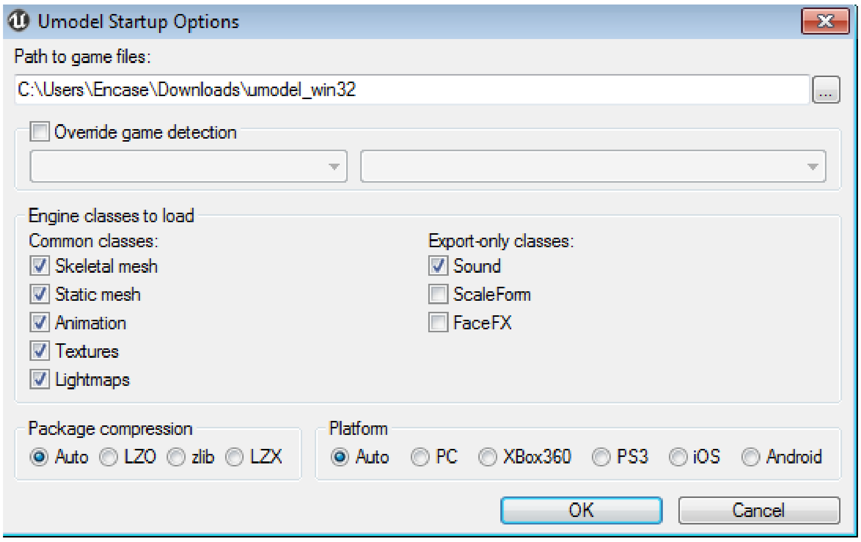


Recovered Artifacts	Count
Media	
Carved Video	1
Pictures	186
Videos	1
Encryption	
Encrypted Files	1

Figure 42 Internet Evidence Finder False Positive Image results

8.5 Umodel

As Umodel is a 3rd party application specifically designed to be able to extract information from Unreal Engine PAK files, the results gathered will be used to see if the steganography data is still intact after being added to the game. For the application to successfully extract the data, the PAK file was copied from the install directory to the application directory, from here Umodel was executed, the PAK file was chosen and the option to export sound was selected (see figure 43).



Path to game files: C:\Users\Encase\Downloads\umodel_win32

□ Override game detection

Engine classes to load

Common classes:
☑ Skeletal mesh
☑ Static mesh
☑ Animation
☑ Textures
☑ Lightmaps

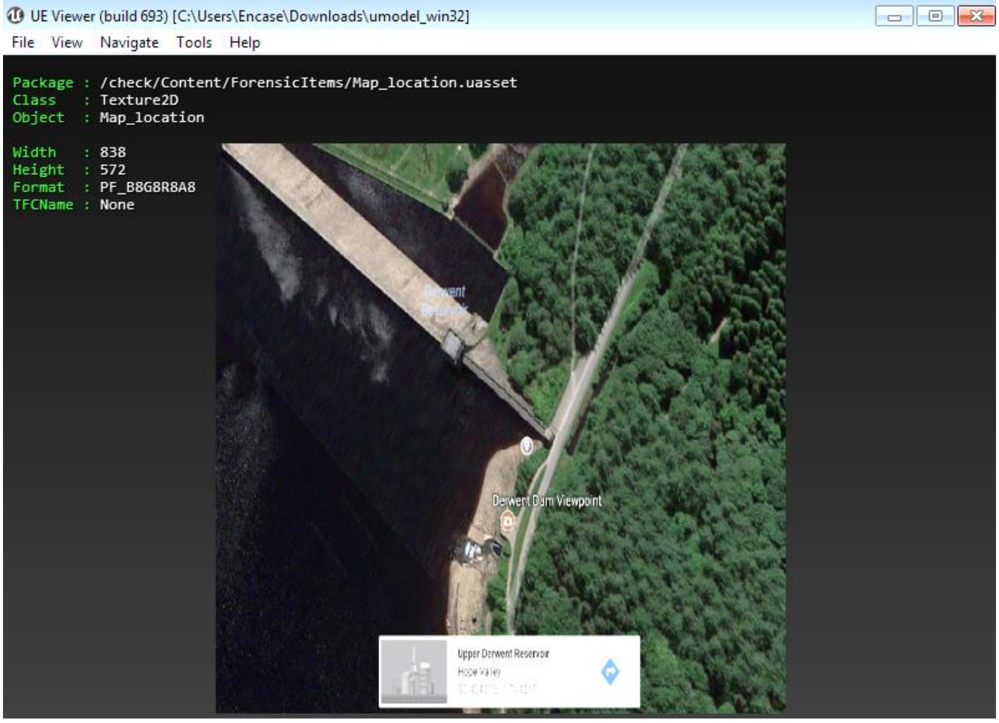
Export-only classes:
☑ Sound
□ ScaleForm
□ FaceFX

Package compression: ● Auto ○ LZO ○ zlib ○ LZX

Platform: ● Auto ○ PC ○ XBox360 ○ PS3 ○ iOS ○ Android

Figure 43 Umodel processing options

Once the PAK file was opened, the forensic folder and audio folder were located and the files within them exported. When trying to view the images, all of them displayed (see figure 44) however, the steganography data within them couldn't be recovered due to the file type changing along with the file size. When testing the audio files, each file played, however, the steganography file data within them was not recoverable due to the same issues as mentioned above.



```
Package : /check/Content/ForensicItems/Map_location.uasset
Class   : Texture2D
Object  : Map_location

Width   : 838
Height  : 572
Format  : PF_B8G8R8A8
TFCName : None
```

Figure 44 Umodel Evidence being displayed

As the video file was already accessible due to it not being stored within the PAK file, it was placed back into the application called OurSecret to see if the evidence stored was recoverable. After entering the correct password, all the files stored within were still there and intact, allowing for the extraction and viewing.

9. Discussion

When conducting the experiment with the forensic tools mentioned in the previous section, it was clear that each tool was not capable of analysing the install files or the PAK file successfully. Regarding Encase 8, a personal call was made to guidance technical support that develops Encase, for clarification to see if the tool can search through PAK files, to which they responded it couldn’t as it is unsupported at this time.

Encase was however able to get a directory structure within the text field, but no visible evidence could be neither extracted nor seen except for the file names. The same reason goes for Forensic Tool Kit, which does not fully support the file type, as it can carve images from the PAK file however these images are unreadable despite transferring the HEX data directory to a new file. Upon searching the FTK forum for potential workarounds and attempting to call AccessData, no workaround was given, confirming that FTK cannot search this file effectively.

Internet Evidence Finder however was able to classify the video file as potential evidence but only after the video was manually placed into the application. This shows that while IEF can find potential steganography files it cannot fully search PAK files for evidence without only displaying false positives or the corresponding install files. Magnet Forensics was contacted for clarification as to whether IEF can work around this issue. Upon response, they suggested that the PAK file's extension should be changed to that of a ZIP file; however, after changing the file extension to that of a ZIP one and placing it back into IEF, the same number of false positives was found.

Since all these tools do not successfully search and extract potential evidence from the PAK file or the corresponding install files, this reaffirms the hypothesis of this document in that using virtual reality as a carrier file can successfully conceal evidence from forensic tools.

When first developing the project, the application known as Unity, developed by Microsoft, was used as the original game engine. However, shortly after attempting to use this to create the virtual reality environment, it proved too complex to understand within the given timeframe and as such Unreal Engine was used instead, mainly due to there being multiple tutorials online in how to build a virtual reality environment, including multiple free add-ons and plugins. This did require time to learn how to use the tool but proved effective at creating a basic VR world.

If the experiment was to be done differently, more background research into different game engines would be conducted and encryption would be used on the PAK file to ensure all the data remains secure.

Linking back to the statement within the literature review, no one has considered that using virtual reality as a steganography carrier file could allow for hidden files to go unnoticed by forensic examiners.

10. Conclusion

While using a virtual reality environment as a potential carrier for other information in relation to steganography, it was assumed that the steganography files would be recoverable using the correct tool. However, upon testing this theory, it revealed that once the secondary carriers, such as the image and the audio files, were imported into the environment, the data within them was lost due to the file format changing and the file size shrinking. However, one of the audio files which had been subjected to Coagula, the sound wave image was still intact and viewable using Sonic Visualizer.

The video evidence was also expected to remain secure within the environment, however, due to the application used in building the virtual reality program, the video file remained outside of the virtual reality environment structure and thus the steganography data within was still intact and recoverable.

This differed from the expected results, as the file formats should have remained the same due to the application supporting them. However, it is possible that the formats changed when they were added into the application itself as application assets.

Since the video evidence remained intact and the hidden files inside were still accessible, the use of a virtual reality application as a steganography carrier file has been proven to work. Not only because the video file remained secure but also since the images and audio files within the application were undiscovered by several major forensics applications and could only be extracted using Umodel. The difference between Umodel and the forensic tools used, is that Umodel is designed to solely search through and extract files from with a PAK file whereas the forensic tools are not.

The reason this is important is that anyone with enough computing power can successfully build a virtual reality program and store potentially anything they desire within it, such as illegal images, instructions, videos and more without arousing suspicion.

11. Reflection

Upon deciding that the thesis would be based on virtual reality steganography, several tools needed to be researched and understood to use them effectively, this required searching the manuals for each tool along with tutorials on YouTube on how to do specific things. However, the original tool which was chosen to build the virtual reality application, known as Unity, proved difficult to grasp within the given timeframe and as such the secondary tool Unreal Engine needed to be learnt. This delayed the build and completion of the virtual reality environment.

When using the new tool, several issues arose when building and packaging. One such issue was the recurring crashing and corruption of the save file due to a plugin designed to add different substances, such as water and rock textures. Another issue which occurred was after the initial packaging had been completed, in which the packaged content was only several folders with an executable file and not a single executable file as thought. This required research into various software applications which could compress the directory structure into a single executable file and required time to learn the application.

Not only were there issues to be overcome but thanks to these issues, key knowledge was gained into how various types of steganography techniques work along with knowledge in how to successfully build a virtual reality environment and how to extract the files within it. Several tools which were used during the experiment development have allowed for in-depth knowledge into how these tools work and how to use them effectible.

As steganography is a common method used in anti-forensics, and with the development of using non-traditional files as carriers, such as using virtual reality, a future career in developing tools to help find hidden information for forensic investigators will be useful. This is because more and more people are using steganography to conceal their data from potential unwanted viewers.

From my project specification, I set optional deadlines of when I wanted to complete specific parts of my thesis and deliverable, however, these deadlines proved too optimistic as I underestimated the time it would take to build a virtual reality environment and the overall write up. In the end the project deliverable was completed before the deadline and to a good standard and the write up was completed and refined within the given time frame.

12. Evaluation

If the project were to be improved, more detail would be integrated into the environment, so the rocks don't stand out as much and the PAK file which stored the assets and the evidence would be encrypted. This is to prevent tools such as Umodel from accessing the data within and to test if new forensic applications can access the data. If not, then a possible decryption tool could be developed which can either bypass the encryption or find the encryption key and display the contents.

As this project did not contain any participants or have any ethical objections, alternative actions could range from simply using different material as evidence to using multiple people to test the environment. As such, if the project were to include the use of multiple people being able to access the same virtual reality environment from different locations, this would open the virtual reality application to a multiplayer environment instead of a single player one. The same could also be done to gather information about how easily people can find the evidence and how they would hide the evidence within the environment.

13. Future Work

Future work should focus on using multiple tools to build a virtual reality environment instead of using just one, as it will allow for multiple tests to be conducted into what the forensic tools can and cannot do with relation to analysing them for potential evidence. If the same tool is to be used again, the generated PAK file should be encrypted for better security against the tools which can open unencrypted PAK files and will further test how effective the tools are at finding the PAK file and if they have been updated, how effective they are at decrypting the file and extracting the files.

14. References

Amazon. (2018). *Oculus Rift*. Retrieved April 10, 2018, from Amazon: https://www.amazon.co.uk/Oculus-301-00204-01-Rift/dp/B00ZFOGHRG

Brockwell, H. (2016, April 3). *Forgotten genius: the man who made a working VR machine in 1957*. Retrieved from Techradar: https://www.techradar.com/news/wearables/forgotten-genius-the-man-who-made-a-working-vr-machine-in-1957-1318253

Caudell, T. P., & Mizell, D. W. (1992). *Augmented Reality: An Application of Heads-Up Display Technology to Manual Manufacturing Processes.* IEEE.

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *DFRWS USA 2016 - Proceedings of the 16th Annual USA Digital Forensics Research Conference*, 65.

Elaine, T. (2016, March 26). *GARP Virtual Reality*. Retrieved from etsanggarp.blogspot.co.uk: http://etsanggarp.blogspot.co.uk/2016/03/

ferragallo. (n.d.). *sensorama*. Retrieved from ferragallo: http://www.ferragallo.com/sensorama.html

Flores-Arredondo, J. H., & Assad-Kottner, C. (2015). Virtual reality: a look into the past to fuel the future. In *The Bulletin of the Royal College of Surgeons of England* (10 ed., Vol. 97, pp. 424-426). The Royal College of Surgeons of England. doi:10.1308

Gear VR (2015). (n.d.). Retrieved April 4, 2018, from Samsung: http://www.samsung.com/uk/wearables/gear-vr-r322/

Google. (2018). *Google Cardboard*. Retrieved April 10, 2018, from store.google: https://store.google.com/product/google_cardboard

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image Steganography Techniques: An Overview. *International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3)*, 1.

Henriksen, B., Nielsen, R., Szabo, L., Evers, N., Kraus, M., & Geng, B. (2016). An affordable virtual reality system for treatment of phantom limb pain. *VRIC '16 Proceedings of the 2016 Virtual Reality International Conference* (p. 1). Laval, France: Association for Computing Machinery.

HTC. (2018). *Controller*. Retrieved from HTC: https://www.vive.com/uk/accessory/controller/

ifixit. (2016, April). *Oculus Rift CV 1 Teardown*. Retrieved from ifixit: https://www.ifixit.com/Teardown/Oculus+Rift+CV1+Teardown/60612

Johnson, E. (2016, July 13). *What are the differences among virtual, augmented and mixed reality?* Retrieved from Recode:

https://www.recode.net/2015/7/27/11615046/whats-the-difference-between-virtual-augmented-and-mixed-reality

Kessler, G. C. (2007). Anti-Forensics and the Digital Investigator. *Australian Digital Forensics Conference* (p. 2). School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.

Kothari, L., Thakkar, R., & Khara, S. (2017). Data hiding on web using combination of Steganography and Cryptography. *2017 International Conference on Computer, Communications and Electronics* (p. 1). Jaipur: IEEE.

Kour, J., & Verma, D. (2014). Steganography Techniques –A Review Paper. *International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5)*, 1.

Kraft, C. (2016, March 24). *Getting Started With VR: The Best Software Tools Are Free*. Retrieved from Makezine: https://makezine.com/2016/03/24/makers-introduction-vr-best-software-tools-free/

Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017). An Overview of Text Steganography. *International Conference on Signal Processing, Communications and Networking* (p. 1). Chennai: IEEE.

Kvist, J. W. (2016, March). *HTC Vive Controller*. Retrieved from buyvrguide: https://www.buyvrguide.com/vr-controllers/htc-vive-controller/

Kwiatkowska, M., & Swierczewski, L. (2014). *Steganography - coding and intercepting the information from encoded pictures in the absence of any initial information*. Retrieved from lvee: https://lvee.org/en/abstracts/106

Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016, April 13). *Current Challenges and Future Research Areas for Digital Forensic Investigation.* Retrieved from Academia: https://www.academia.edu/21648777/Current_Challenges_and_Future_Research_Areas_for_Digital_Forensic_Investigation

McAfee. (2017). *McAfee Labs Threat Report.* McAfee. Retrieved from https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-jun-2017.pdf

Mount Vernon. (2018). *Spy Techniques of the Revolutionary War*. Retrieved from Mount Vernon: http://www.mountvernon.org/george-washington/the-revolutionary-war/spying-and-espionage/spy-techniques-of-the-revolutionary-war/

Parrish, K. (2016, May). *Google wants VR to work far better on Android phones with 'Daydream'*. Retrieved from Yahoo Finance: https://finance.yahoo.com/news/google-daydreams-better-vr-android-204514499.html pc mag. (n.d.). *Definition of: virtual reality*. Retrieved April 10, 2018, from PCMag: https://www.pcmag.com/encyclopedia/term/53945/virtual-reality

Research Methodology. (2018). *Deductive Approach*. Retrieved from Research Methodology: https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/

Rizzo, A., Hartholt, A., Grimani, M., Leeds, A., & Liewer, M. (2014). Virtual Reality Exposure Therapy for Combat-Related Posttraumatic Stress Disorder. *Computer Vol 7 Issue 7*, 35.

Samsung. (2015). *Gear VR (2015)*. Retrieved from samsung: http://www.samsung.com/uk/wearables/gear-vr-r322/

Seo, J. O., Manoharan, S., & Mahanti, A. (2016). *Network Steganography and Steganalysis - A Concise Review.* Auckland: IEEE.

skillsyouneed. (2018). *Quantitative and Qualitative Research Methods*. Retrieved from skillsyouneed: https://www.skillsyouneed.com/learn/quantitative-and-qualitative.html

The Franklin Institute. (2018, March 30). *HISTORY OF VIRTUAL REALITY*. Retrieved from The Franklin Institute: https://www.fi.edu/virtual-reality/history-of-virtual-reality

ThinkGeek. (2018). *VR Sensory Immersion Generator*. Retrieved from Think Geek: https://www.thinkgeek.com/product/ivpl/

thinkgeek. (n.d.). *VR Sensory Immersion Generator*. Retrieved from thinkgeek: https://www.thinkgeek.com/product/ivpl/

University of Exeter. (2010, September 19). *What is Augmented Reality*. Retrieved from Augmented Reality: http://blogs.exeter.ac.uk/augmentedreality/blog/2010/09/19/what-is-augmented-reality/

Varinsky, D. (2016, November 29). *Virtual reality is being used to recreate crime scenes in the courtroom*. Retrieved from Business Insider: http://uk.businessinsider.com/virtual-reality-in-the-courtroom-2016-11

Vashishtha, L. K., Dutta, T., & Sur, A. (2013). *Least Significant Bit Matching Steganalysis Based on Feature Analysis.* Guwahati: IEEE.

Virtual Reality Society. (2015, December). *History Of Virtual Reality*. Retrieved from vrs: https://www.vrs.org.uk/virtual-reality/history.html

VIVE VR SYSTEM. (2018). Retrieved April 10, 2018, from vive.com: https://www.vive.com/us/product/vive-virtual-reality-system/

White, J. (2016, March 18). *We took a ride on the world's first VR rollercoaster*. Retrieved from Wired: http://www.wired.co.uk/article/galactica-alton-towers-virtual-reality-rollercoaster-samsung-gear-vr

Woerner, M. (2015, February 11). *The Most Fascinating Spy Gear From The Spy Museum's Archives*. Retrieved from io9: https://io9.gizmodo.com/the-most-fascinating-spy-gear-from-the-spy-museums-arch-1685241601

Woodward, A. (2012, August 28). *Viewpoint: Criminals can hide data in plain sight*. Retrieved from BBC: http://www.bbc.co.uk/news/technology-19370581

Ying, L., Jiong, Z., Wei, S., Jingchun, W., & Xiaopeng, G. (2017). VREX: Virtual reality education expansion could help to improve the class experience (VREX platform and community for VR based education). *IEEE Frontiers in Education Conference (FIE),* (p. 2). Indianapolis 2017, 1-5.: IEEE. Retrieved from IEEE Xplore Digital Library.

Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2013). *Development Trends in Steganography.* Warsaw: Warsaw University of Technology, Institute of Telecommunications.

15. Appendix

15.1 Appendix A

PROJECT SPECIFICATION - CS&N

Student:	**Stuart Wilson**
Date:	**22-09-2017**
Supervisor:	**Youcef Djerbib**
Degree Course:	**BSc (Hons) Computer Security with Forensics**
Title of Project:	**How the use of Virtual Reality and Steganography can be used by criminals to hide data within a Virtual Environment**

Elaboration

The subject I will be basing my research on will be how potential criminals can take advantage of today's open source tools and tutorials to hide data in non-traditional locations. In the case of my project, I have chosen Virtual Reality while using steganography applications to conceal them more thoroughly.

As the use of computer forensics is becoming more vital in today's society, due to the use of the ever-growing issue of anti-forensics, crimes and secrecy, more and more people are trying to find ways of hiding data which cannot be found by conventional methods. In my project, I will show how it is possible to hide data within a Virtual Environment as well as using recent steganography techniques and tools to conceal the information from normal digital forensic tools such as Autopsy, EnCase and more.

I will also expose multiple images to steganography applications to see which one proves the most effective at concealing the information, which one isn't effective, including how easy it is for people to use them.

My goal for this project is to show a working virtual environment with images located in it which have been the subject to different steganography tools. I will then show how these types of files might get overlooked using traditional forensic applications and what this could mean for the forensic community.

Project Aims

- Use Steganography on test images
    1. generate test images from either own photos or taken from Google copyright free
    2. generate text/file which would be placed into said photos using steganography
    3. try to keep file size down using LSB locations in which to place hidden text
- Build a Virtual Environment
    1. Use software such as Unreal Engine and Unity to build the virtual environment.
    2. follow tutorials online in how to build a working model
    3. place test images within the environment
- Place Virtual Environment within a digital forensic analyser
    1. Try to find images using such tools as EnCase and Autopsy
    2. If images found document which method worked best
    3. If images not found, test within different tools and report on findings

Project deliverable(s)

I will produce a Virtual Reality Environment which will be based on the Windows Platform as well as a hypothesis which will contain the most likely of outcomes when testing my VRE in forensic software. The most likely outcome would be that the software detects and locates the images within the environment however as this would be a new method there is a slight chance that the software wouldn't pick up on it and as such would need to be adapted to search these types of files.

Action plan

Task	Deadline	Optional Deadlines	Meetings with supervisor
Project Specification and ethics submission	13/10/17	06/10/17	25/10/17
Complete build of virtual reality environment	-	16/10/17	01/11/17
Begin information review	-	06/10/17	01/11/17
Start and complete steganography images	-	15/10/17	-
Place Steganography images into environment and build	-	15/10/17	-
Information review submission	24/11/17	-	22/11/17
Begin analysis of environment	-	23/10/17	22/11/17
Contents page and progress review	30/01/18	-	17/01/18
Structure of report with 3-4 chapters completed	02/03/18	-	07/02/18
Critical reflection started	-	05/02/18	07/02/18
Final submission of project	16/04/18		21/02/18 07/03/18 28/03/18 04/04/17

Ethics

Ethics Checklist – CS&N 55-6699 Final Year Project

If the answer to any question is 'yes' the issue **MUST** be discussed with your project supervisor.

Question	***Yes/No***
1. Does the project involve human participants? This includes surveys, questionnaires, observing behaviour, testing etc.	No
2. Does the project involve the use of live animals?	No
3. Does the project involve an external organisation? If yes, please write the name of the organisation here:	No
4. Does the project require access to any private or otherwise sensitive material?	No
5. Does the project require the reproduction (beyond normal academic quotations) of materials authored by a source other than yourself?	No

Adherence to SHU policy & procedures

Declaration

I can confirm that:

I have read the Sheffield Hallam University Research Ethics Policy (available at http://www.shu.ac.uk/_assets/pdf/research-ethics-policy.pdf)

I agree to abide by its principles.

Signature Stuart Wilson Print Name: Stuart Allan Wilson

Date: 27/09/2017

15.2 Appendix B

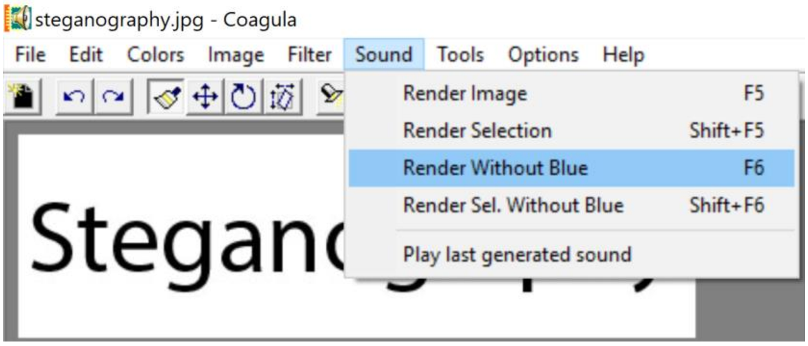

steganography.jpg - Coagula
File
Edit
Colors
Image
Filter
Sound
Tools
Options
Help
Render Image F5
Render Selection Shift+F5
Render Without Blue F6
Render Sel. Without Blue Shift+F6
Play last generated sound
Stegano

Figure 45 Image file loaded into Coagula and rendered without the colour Blue

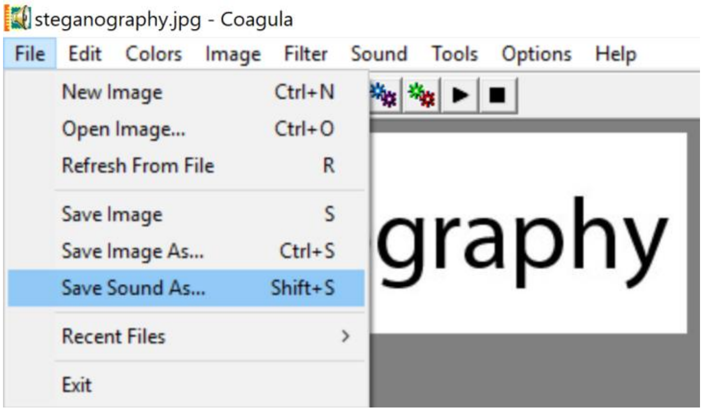


Figure 46 Image within Coagula being saved as a sound file

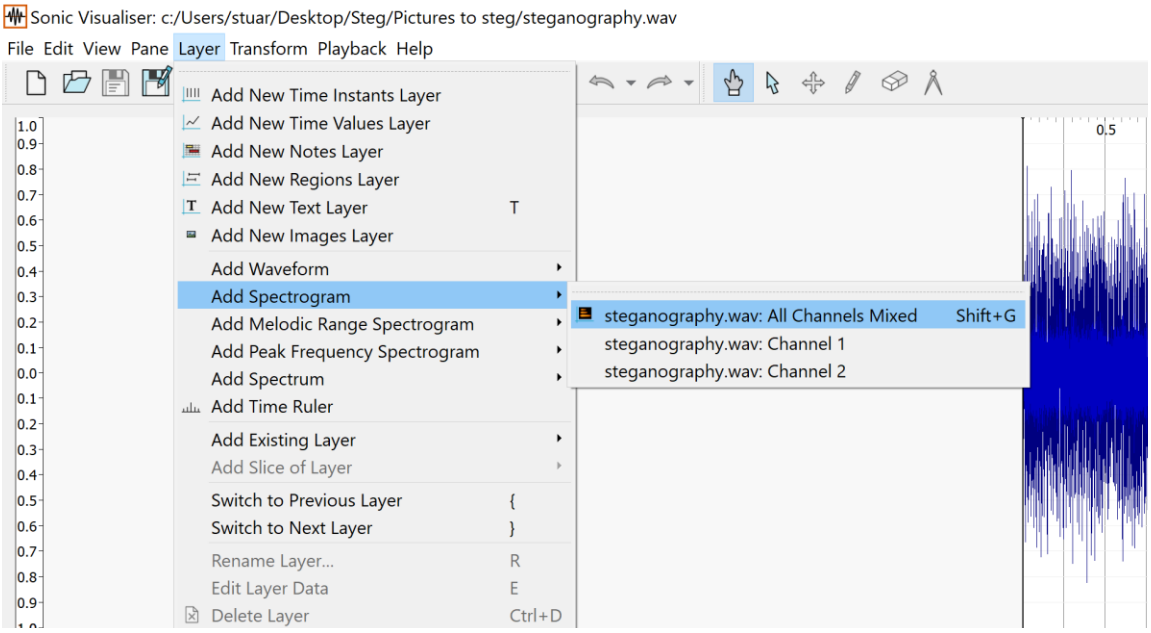


Figure 47 Coagula sound file opened within Sonic Visualiser and Spectrogram being added

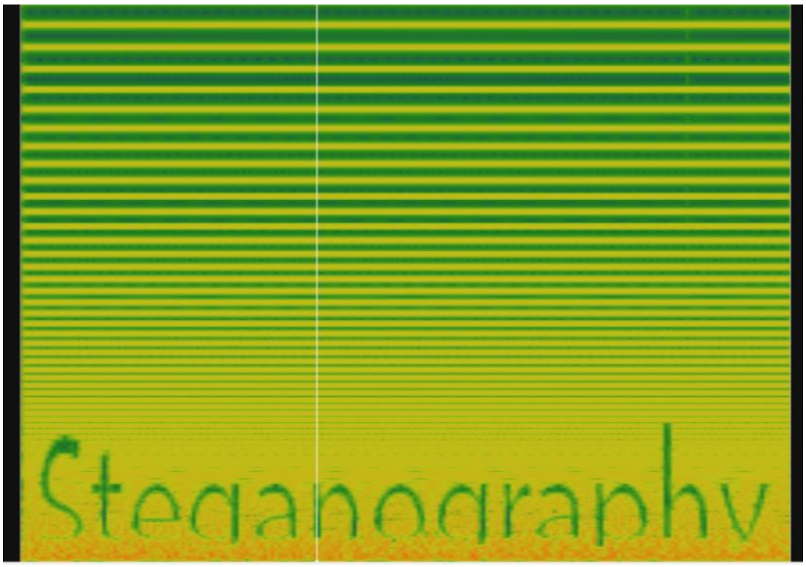


Figure 48 Sonic Visualiser displaying image from Coagula