Northumbria University NEWCASTLE

A report submitted in partial fulfilment

of the regulations governing the award of the Degree of

BSc. (Honours) Computer and digital forensics

at the University of Northumbria at Newcastle

<u>Project Report</u>

Investigation and comparison of the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform

Author: Shona Start

Supervisor: Philip Anderson

2019 / 2020

Investigative Project

Authorship Declaration

I declare the following:

(1) that the material contained in this dissertation is the end result of my own work and that due acknowledgement has been given in the bibliography and references to ALL sources be they printed, electronic or personal.

(2) the Word Count of this Dissertation is 19750

(3) that unless this dissertation has been confirmed as confidential, I agree to an entire electronic copy or sections of the dissertation to being placed on the eLearning Portal (Blackboard), if deemed appropriate, to allow future students the opportunity to see examples of past dissertations. I understand that if displayed on eLearning Portal it would be made available for no longer than five years and that students would be able to print off copies or download.

(4) I agree to my dissertation being submitted to a plagiarism detection service, where it will be stored in a database and compared against work submitted from this or any other School or from other institutions using the service.

In the event of the service detecting a high degree of similarity between content within the service this will be reported back to my supervisor and second marker, who may decide to undertake further investigation that may ultimately lead to disciplinary actions, should instances of plagiarism be detected.

(5) I have read the Northumbria University/Engineering and Environment Policy Statement on Ethics in Research and Consultancy and I confirm that ethical issues have been considered, evaluated and appropriately addressed in this research.

SIGNED: S.Start 17/05/2020

Acknowledgements

I would like to thank my supervisor for his support and guidance throughout the entirety of this project.

Abstract

This report focuses on the computer gaming applications Discord, Twitch and Steam from a digital forensics' perspective. In the first half of this paper the applications are explored and researched into how they and their features function. Research has also been conducted into the dangers they can have for minors and vulnerable peoples. The first half of this study also looks at the Windows 10 operating system and the forensics techniques that can be applied to this system, alongside the forensics techniques for other sources of data such as network forensics and volatile memory forensics.

The second half of this study focuses on the forensics investigation into these applications. It discusses how data was created on a Windows 10 computer for each application and how data was collected from the file system, volatile memory and network traffic. Digital forensics techniques were used to analyse the data from each application and these finding are presented in an understandable format. Finding include where data was found relating to messages, images, videos, video/audio calls and streaming sessions on each of the applications. Although some problems with the Steam application have impacted to quality of the results from this instigation, this study still provides a basis for forensics analysis of the applications and possibly similar applications.

Contents

Authorship Declaration 2

Acknowledgements 3

Abstract 4

Chapter 1: Introduction 6

Chapter 2: An introduction to gaming and chat applications 7

Chapter 3: The dark side of gaming applications 10

Chapter 4: An introduction to Windows 10 and Digital Forensics 13

Chapter 5: Investigation Plan 17

Chapter 6: Investigation Results 22

Hard-Drive 22

Volatile memory 40

Network Traffic 44

Chapter 7: Evaluation 51

Discussion and evaluation of findings 51

Evaluation of tools and methods 53

Comparing to other work 54

Evaluation of the project process 56

Chapter 8: Conclusion 59

Future work 60

References 61

Bibliography 68

Appendices 70

1: Terms of Reference 70

2: Table of Figures 93

3: Figures 45 – 51 95

Chapter 1: Introduction

Digital forensics is branch of forensic science that involves the investigation and recovery of data and evidence found on digital devices. There are many subsections of digital forensics which all tend to focus on a specific data source. This study will focus on three subsections: computer forensics, network forensics and volatile memory forensics. These will be used to conduct a study of the three applications Discord, Twitch and Steam on a Windows 10 computer. These applications have been chosen because of their popularity and the illicit activities that transpire on their communication channels; activities such as grooming, gambling and other abusive content. Detection of such activities on these platforms is in its infancy and this study hopes to fill that gap by not only providing a forensics analysis of each of these applications but also a comparison of the data collected for those who need to or are interested in collecting data or evidence from the applications Discord, Steam and Twitch and similar applications.

The aim of this project is to "compare the recoverable forensics artefacts from a selection of online gaming and chat applications running on a Windows 10 platform". To achieve this aim, eight objectives have been developed:

1. To research and give context to the selection of applications and their live streaming capabilities.
2. To research the illicit activities of the malicious users of these platforms.
3. To research and provide background information relating to Windows 10 and the effects this operating system will have on the investigation, exploring possible forensics techniques that could be implemented.
4. To create a thorough plan of how this investigation will be executed, including ethical issues, equipment use, investigation plan, and data analysis plan.
5. Implement the investigation plans documenting all results and collecting all relevant data.
6. Analysis of the data, comparing the data collected across each of the applications.
7. Evaluation of the findings, discussing the usefulness of the information and its implications.
8. Evaluation of the areas of this project that could be improved and further work that could be implemented in the future.

In this report the author has used the six p's of research to complete each of these objectives and present the results into the investigation into the three applications chosen. The investigation into the chosen applications involved creating data on a Windows 10 computer using each of the applications separately. Following ACPO (Association of Chief Police Officers) guidelines and the ADMF (Abstract Digital Forensic Model), this data was collected and analysed using forensic techniques and forensics software in order to determine the recoverable forensics artefacts from each of the applications. The recoverable forensics artefacts are presented and compared in this report along with an evaluation of project results and project process.

Chapter 2: An introduction to gaming and chat applications

This chapter will introduce electronic games and computer gaming applications. It will investigate the features provided by these applications, as well as give a detailed overview of the three applications chosen for this project.

Gaming is the running of electronic games (also known as video games) on electronic devices. Devices such as Xbox, PlayStation, Nintendo Switch and PCs (Personal Computers). Many types of games exist but most can be sorted into one of two categories. These categories are single player and multiplayer. Single player games are video games designed so that only one person can play the game at a time, whereas multiplayer games are games where more than one person can play at the same time, either locally (for example Overcooked), online over the internet (for example The Elder Scrolls Online), or a mixture of both (for example Diablo 3). Some games have both single and multiplayer features but mainly focus on one of the two. For example, Dragon Age Inquisition is a single player game with optional online multiplayer gameplay. On the other hand, Warframe is mainly an online multiplayer game with optional single player gameplay. As of 2019, there are more than 2.5 billion gamers across the world (newzoo, 2019).

PCs are one of the most popular platforms for playing video games. It is estimated that by 2021 there will be 1.4 billion PC gamers (statista, 2018). Most other devices commonly used for running video games are pre-built with software and features for playing games. However, PC's are not always built primarily for video games and are more customizable. This means that to play most modern video games on a PC other software and applications are recommended and sometimes required. These applications can provide many services. Examples of these applications include Steam, Origin, Uplay, Twitch, Xbox Live, TeamSpeak, Mumble, Mixer, Beam, HitBox, and Discord. Most of these applications are initially free, only requiring an email address to sign up; however, they also may have in-app purchases.

Some of these applications are primarily focused on communication features. Even if the main goal of the particular application is not communication features, most of these applications provide some communication features alongside their main feature. These features are often designed to be used alongside both single player and multiplayer games. The level of communication features provided by an application is dependent on the application itself. Most applications will at least have IM (Instant Messaging) capabilities.

IM's are real-time text transmissions sent and received over the Internet. IM can allow for the instant sharing of a range of digitally based information; including text, images, audio, video and documents. IM is usually used for one-to-one communication. It is possible for an IM communication to be sent to multiple people. However, chat rooms are another way of doing this. Chat rooms are another feature that are often available in gaming applications. Chat rooms are very similar to IM; in fact the two terms are often used interchangeably. The main difference between the two is that chat rooms often include many people that may or may not know each other, who come together to talk about a dedicated topic, whereas IM is usually designed to be used only with people of whom the user already knows, similar to email. IM usually comes with a system that allows the monitoring of other users to determine their availability, often called a Friends List or Contacts List. (Bazara, B, Fatma, T, 2009).

As stated earlier, IM and chat rooms allow for a sharing of a range of digitally based information. This can include text, images, audio, video and documents. Text refers to an electronic message generally consisting of alphanumeric characters. Some applications have a limit for how many characters a message can contain, for example, the application Discord has a limit of 2,000 characters per message. Text communications can also include URLs (Uniform Resource Locators). A URL is a unique identification address for a resource on the internet. This identification is used to distinguish any resource on the internet including web pages, images, and sound files (Network Working Group, 2005). When a URL is shared, using IM the receivers can use this to access the resource themselves. Images refers to a digital photo, drawing or graphic. File formats for digital images include PNG (Portable Network Graphics), JPEG (Joint Photographic Experts Group) and TIFF (Tagged Image File Format). As with text, applications often limit the size of images, for example Steam has a limit of 10MB. Audio refers to recorded sound. File formats for audio include WAV (Waveform Audio File), MP3 (Moving Picture Experts Group Layer-3 Audio) and FLAC (Free Lossless Audio Codec). Video refers to recorded moving visual images. File formats for video include AVI (Audio Video Interleave), MP4 (Moving Picture Expert Group-4) and WMV (Windows Media Video). Audio and video messages can be combined or separate. Like with the limits of other digitally-based information, applications limit the size of video and audio, for example Discord has a limit of 8MB per audio or video file (Chanty, 2018). Documents refer to something containing digital information, like Word Documents, Spreadsheets, PowerPoints and PDFs (Portable Document Format).

Two other features gaming applications often include are video calling and live streaming. Video calling allows users to stream live video and audio for one-to-one communication. Live streaming is similar but designed for one-to-many communication. Live streaming often also allows for the broadcasting of content from a users digital device, for example, video games and other applications. Both video calling and live streaming use VoIP. VoIP stands for Voice over Internet Protocol; it is a communication standard that allows for the conversion of audio and video into a format that can be transmitted live over the internet. One of the major users of VoIP to make phone calls over the internet instead of over analogue telephone lines. (Patel, R. et al 2013. DeSantis, M, 2006).

Another feature gaming applications sometimes have is digital distribution. Applications such as Steam, Uplay, GOG and Origin are primarily designed for distribution of video games and software. Some of the software and video games are available for free whereas others need to be purchased (Klappenbach, M. 2019). Applications also often have other financial or trading transactions. Live streaming features often have donation systems that allow for the sending of money and/or gifts to the person broadcasting. Other applications often have systems for the trading of digital goods such as video game items, cosmetics (sometimes called skins), collectables and in-game currencies (Wax io. 2017).

For this project the author has chosen three gaming applications which are commonly used alongside video games. These applications have been chosen for their popularity and the differences in the features they provide. The first of these applications is Steam.

Steam was released in 2003 by Valve (Sayer, M. Wilde, T. 2018), it has always primarily been a digital distribution service. It is one of the most popular video game distribution services with over thirty thousand video games available from the service, (Bolding, J. 2019) and roughly 90 million monthly active users (Fenlon, W. 2019). Steam has an age limit of 13, but does come with parental controls. Since its first release, many new features have been added to the application, including systems for IM, live streaming, trading of digital goods, non-game related digital distribution and many other features. One of the newest features of Steam is Remote Play Together, released November 2019, which is a system that allows local multiplayer games to be played online with others on the internet (Steam, 2019).

The second application the author has chosen is Discord. Discord was released in 2015 by Discord Inc. (originally named Hammer and Chisel). Discord has an age limit of 13, but does not have any verification methods to enforce this. The application is primarily a VoIP service designed for use with video games. Discord has IM, Chat rooms, live streaming, video calling and is one of the most popular VoIP applications as of 2018, with 130 million users (Fogel, S. 2018). Discord previously distributed games; however, this service was discontinued in October 2019. One of Discord's newest features is Go Live, this is a feature that allows live streaming of video games to up to 10 people at a time and was released August 2019 (Goslin, A. 2019).

The final application chosen is Twitch. This application was realised June 2011 by Justin.tv; it is now owned by Amazon. Twitch is primarily a live streaming service. However, it also provides features for IM and group chats. There are also features in Twitch that allow users to donate money or send a monthly payment to the people who live stream. Twitch has an age limit of 13 and users aged between 13 and 18 require a parent or guardians permission to sign up. One of Twitch's newest features is Twitch Studio, this is a new free software designed to be used alongside Twitch. This software makes it easier for anyone to livestream on Twitch, the Beta for this was released November 2019 (Twitch, 2019).

In summary, video game applications are very popular and come with many features that allow users to perform a number of activities. Some of the major features available on these applications are focused on communicating with other users, for example VOIP calling and live streaming. Furthermore, systems for digital distribution, digital trading, financial transactions and many more features are often also included within the applications. Steam, Discord and Twitch are some of the most popular applications available. So collecting digital forensics evidence from these applications will be the author's focus.

Chapter 3: The dark side of gaming applications

In this chapter the author will be discussing how on applications like Twitch, Steam and Discord, evidence of cyberbullying, malware, underage gambling, violent content, sexual content, grooming and child exploitation can be found. Exposure to these aspects can lead to mental and physical abuse; and in children may lead to growth and development issues.

Cyber bullying and emotional abuse is present in many places across the internet, including video game applications. Exposure to such abuse can cause depression and anxiety, especially in children and other vulnerable people (NSPCCa, 2019). The NSPCC (National Society for the Prevention of Cruelty to Children) rates Twitch and Discord as having a medium risk to Cyberbullying, whereas Steam has been given a high risk (Net Aware, 2019a. Net Aware, 2019b. Net Aware, 2019c). Discord reports from January to April 2019 show that the application has received 8,941 reports of harassment and 4,929 reports of threatening behaviour (Nelly, 2019).

Malware can be programs or code that are designed to be harmful to a computer or internal computer systems. There are many types of malware, including types that can delete everything they infect or flooding networks and systems,s so they are unusable, or even steal information (Malwarebytes, 2018). The term 'Malware' can include viruses, worms, Trojan horses and spyware. Malware can gain access to a device through untrusted URLs or downloading infected software and files (Webroot, 2018). An example of malware is Eskimo. In 2014, Eskimo was spread using a bot on Twitch's chat features. The bot would then invite users of Twitch to participate in a raffle to win digital items and skins for video games by clicking on a URL and entering their email address. The webpage would then bring up a popup to tell the user they were successfully entered into the raffle. However, once selected, this popup would initiate the downloading and execution of a Windows binary file. This file would target Steam and could perform a number of actions on a user's account including selling/trading digital goods, buying items, and sending and accepting friend requests. Eskimo was able to steal a user's online available currency and inventory (FSLabs, 2014). Discord also has issues with malware, between January and April 2019 the application received over 700 reports related to malware and malicious URLs (Nelly, 2019). One type of malware that targets Discord is called Spidey Bot, which was designed to steal users' personal data including passwords, usernames, email address and their IP address. The malware is also able to steal the first 50 characters stored in Windows clipboard (The storage area for text that has been copied or cut on a Windows machine) and can install a backdoor to allow for attacks from other malware. (Matyus, A. 2019).

In the UK (United Kingdom) the minimum legal age for gambling is 18 years old. In 2018, the UK Gambling Commission performed a study estimating that around 450,000 minors between the ages 11 and 16 gamble regularly. The UK Gambling Commission also estimates almost a million minors have been exposed to gambling through loot boxes (Gambling Commission, 2018). Loot boxes are present in many modern online multiplayer games. These boxes contain digital items such as in-game cosmetics and collectables, but can only be opened through gameplay or paying some form of currency. Many people would consider this to be gambling, as it often involves using real money to get items based on chance. However, the UK Gambling Commission states that loot boxes themselves do not qualify as gambling (Gambling Commission, 2017a). Nevertheless, loot boxes have led to the creation of Skin gambling, which is recognised by the UK Gambling Commission as gambling (Gambling Commission, 2017b). Skin gambling is a form of gambling where digital items such as cosmetics are used as a currency to bet on casino-style public games of chance. Counter-Strike: Global Offensive is a game developed by Valve only available for PC through Steam. In 2015, Counter-Strike: Global Offensive was linked to underage gambling. Steam allows for the linking of third-party websites to Steam accounts which has allowed for Skin Gambling sites such as “Counter-Strike: Global Offensive Lounge” and “OPSKins” to operate more easily using Steams own currency systems to aid their function. These websites often have no requirement for age verification and sometimes even encourage minors to use their sites (Morris, D, 2016). In 2016, lawsuits were initiated against Valve. One of these lawsuits involved minors as young as 12 who had become addicted to skin gambling (Assael, S, 2017). Another application with issues relating to gambling is Twitch. The application has many streams dedicated to gambling, and many of these can be accessed without any age verification. Considering the age limit of Twitch is 13, this could expose many minors to gambling. Also, in 2018 the UK Gambling Commission discovered two unlicensed casino websites were being advertised on the application (Kent, E. 2019).

Violent content can be found in many forms across the internet, including video games, images, videos and online stories. Between January and April 2019, Discord had 4,992 reports of adult and inappropriate content, which includes graphic and violent images (Nelly, 2019). It is rated as a medium risk of violent content by the NSPCC (Net Aware, 2019b) . One example of violent content on Discord is the Bianca Devins Murder. On the 14th of July 2019, Bianca Devins was stabbed to death in New York. Graphic Images of Devins’ body were shared to a group chat on Discord by the murderer. (Cooper, K. 2019). Steam also has violent content present on its application. The NSPCC rates it as a high risk for violent content (Net Aware, 2019c). The application has a subsection dedicated to violent games. These games and many other games with questionable content are allowed on the application, because Valve allows all games on the application, except those games considered illegal or trolling (Trolling is a purposeful and childish attempt to create a negative emotional reaction for the instigators own amusement) (Steam, 2018). Steam has many games rated as the most violent games, including Manhunt and Postal 2, which are both very violent games banned in several countries (Renardson, A. 2010). In 2018, Valve removed a game called Active Shooter from Steam, a game which simulated a mass shooting from the point of the shooter or the SWAT team trying to take them down. (BBC, 2018). Unlike Steam, Twitch prohibits games it deems too violent and games with an adult’s only ESRB rating, such as Manhunt (Twitch, 2017). Twitch also prohibits gore and violence in its community guidelines (Twitch, 2019). However, because most of Twitch’s content is live, enforcing this is not always feasible. For example, on the 9th October 2019, a terrorist attack was live streamed to Twitch by the attacker. The live stream includes the attacker making anti-Semitic comments and attempting to gain access to a synagogue where he intended to cause a mass shooting but could not gain entry so instead attacked those on the street. The live stream was active for 35 minutes but was only viewed by five users. However, after the live stream ended the video was kept on Twitch for another 30 minutes, where it was viewed by a further 2,200 users. (Haselton, T. Graham, M. 2019).

Another form of content that these applications can expose minors and vulnerable peoples to is sexual content. The NSPCC rates Twitch and Discord as having medium risk of sexual content, and Steam with a high risk (Net Aware, 2019a. Net Aware, 2019b. Net Aware, 2019c). Steam allows adult games for purchase, with prices ranging roughly from £0.79 up to £30. These games include sexual content and nudity and can easily be bought by a minor lying about their age. In 2019, an adult game called "Rape Day" was removed from the application after online petitions were created against it. The game reportedly contained violence, sexual assault, non-consensual sex, obscene language, necrophilia, and incest (Evans, P. 2019). Another application that allows sexual content is Discord. Discord allows sexual content on the application as long as the content is shared with consent from the individual(s) present in the material and it does not depict minors (Discord, 2017). Discord received 4,171 reports of exploitative content and 4,992 reports of NSFW (Not Safe for Work) content between January and April 2019. Discord defines exploitative content as "A user discovers their intimate photos are being shared without their consent; two minors' flirting leads to trading intimate images with each other" (Nelly, 2019).

Grooming is where a person builds a relationship with a vulnerable individual, such as a child, and gets them to trust them so they can manipulate, exploit and abuse the individual (NSPCC, 2019c).The NSPCC reported that over 200,000 minors might be victims of online grooming. The charity estimates 1 in 25 minors between the ages of 11 and 17 have sent, received or been asked to send sexual content to an adult (NSPCC, 2019b). On applications like Discord, Steam and Twitch, developing relationships with strangers is the norm; this obviously increases the chances that children will be put into contact with groomers. Live streaming features present in the applications add extra dangers to grooming. Twitch is reported as one of the most popular places for the grooming and exploitation of minors (NSPCC, 2019b). In 2019, Twitch streamer "Aaitpoes" was accused of reportedly grooming minors using his online popularity (Glaze, V. 2019). Discord has a worrying number of reports which involve it as a starting point or main application for child grooming and exploitation. For example, in January 2019 six men and one woman were arrested in Florida and charged for conspiracy to commit human tracking and sexual battery with a child under the age of 16. One of the children involved in the case was a 17 year old who came into contact with the groomers through Discord (Sederstrom, J, 2019). Another example is Timothy A. Marcinko who was arrested October 2019; and charged with 32 counts of indecent solicitation of a child, 36 Counts of possession of child pornography and 4 Counts of grooming (McHenry Police Department, 2019). Timothy A. Marcinko used Discord to communicate and groom a minor under the age of 17 (Borcia, S. 2019).

To summarise, these applications can be very dangerous especially for minors and other vulnerable peoples because of the existence of threats such as cyberbullying, malware, violent content and child exploitation. Not all users of these applications will come across the type of material and content discussed. However, the risks present with these applications are why it is vital to study collecting forensic evidence, so that cases involving these can be more easily investigated and can be more comprehensive.

Chapter 4: An introduction to Windows 10 and Digital Forensics

This chapter will discuss some fundamentals required in order to conduct a study into collecting forensics evidence from Twitch, Steam and Discord. It will detail the OS (Operating System) that has been chosen to conduct this study on and the forensics tools and techniques that will be used in order to collect and analyse forensic artefacts from the applications.

Digital forensics is the preservation, identification, extraction, and documentation of evidence found on digital devices such as computers, laptops, smartphones, digital cameras, networks and storage devices (Houses of Parliament, 2016). In this study the digital device in question is a computer running the OS (Operating System) Windows 10. An OS is software that manages a computer's memory, processes, hardware and software. An OS is the most user-friendly way to communicate with a computer. An OS will provide many features which are required to run applications such as Twitch, Steam and Discord; for example program execution, memory management, resources allocation I/O (Input/Output) operations, file systems and error detection (Bitesize, 2017). Windows 10 is the newest OS in the Windows NT series created by Microsoft. Windows 10 was released in 2015 (Myerson, T, 2015) since then it has become the most used OS for desktop PC's in the world, recently overtaking one of its predecessors and the previous most popular OS in the world for Desktop; Windows 7 (Warren, T., 2019). The Windows NT series of operating systems has been the most popular for many years and as of December 2019 over 60% of desktop market shares worldwide are controlled by Microsoft (Statcounter, 2019). Windows 10's popularity is one of the major reasons this Desktop OS was chosen over others for this study. This is important because it is likely most users of Steam, Twitch and Discord are using Windows 10. In fact data shows that over 70% of Steam users run the desktop application on Windows 10 (Gough, C, 2019). The Discord and Twitch desktop applications run on Windows and MacOS. However, as of December 2019 MacOS only holds roughly 16% of desktop market shares (Statcounter, 2019) so it can be reasonably be assumed that the majority of the applications users are using Windows 10.

Windows 10 provides many forensic artefacts that could be collected. Forensics artefacts are the data left behind by a user's activities. Artefacts are valuable in digital forensics because they can contain data that not even the user may realise exists, and are often difficult to access and manipulate so provide more validity. For example in 2006 Kari Baker committed suicide by overdose this was initially confirmed by a suicide note. However, further investigations into her husband, Matt Bakers, workplace server revealed incrementing search terms which helped prove he had murdered his wife. In this example the artefacts may have included search terms, websites accessed, URLs visited, how many times these had been visited, the date and times of these activities and the web browser used to access them (Baker v. State, 2011). In this study the author will determine the useful artefacts that can be gathered from Steam, Discord and Twitch and where these can be found on a Windows 10 OS.

On a Windows 10 machine data can be collected from a number of locations including, Windows registry, prefetch files, MRU's (Most Recently Used), jump list, thumbcache and SRUM (System Resource Usage Monitor).

The Windows registry is a database containing data required for the configuration of user accounts, applications and hardware devices on a Windows machine. The registry consists of 4 main files, these are SAM (Security Account Manager), System, Security and Software (Microsoft, 2019). The SAM registry contains data on user accounts including passwords, groups and domains. System is a registry dedicated to data relating to system settings such as the boot profile, system name, hardware profile and configurations. The security registry stores security settings like policies for users and groups. The software registry contains data on all the software and applications on the machine including settings, directories, paths and any licensing (Alwis, C 2019. Farmer, D 2006). Prefetch files provide pre-loaded code for applications created by Windows 10 when an application is running for the first time on a machine. Prefetch files can contain data on how many times the application has been run, timestamps for when the application was first and last run (McQuaid, J. 2014). MRU's are files that store data corresponding to recent user activity on a machine. Examples of MRU's include OpenSaveMRU, LastVisitedMRU and RunMRU. The OpenSaveMRU stores data on files that have been opened or saved within a dialog box. LastVisitedMRU stores data executables that were used to open files listed in the OpenSaveMRU. The RunMRU tracks programs and applications that have been launched from the Run command app (Peterson, G. Et al. 2009). The jump list is another indicator of recent user activity on Windows 10. It contains a list of media files that have recently been accessed by applications. However, this function can be turned off by the user in the Windows 10 settings, so is not always reliable (BlackBag, 2017). The thumbcache is a database containing thumbnails of pictures and videos. Thumbnails are reduced-size versions of the original content created by Windows for organizational purposes. Thumbnails often remain on a system even when the original image is deleted or removed (Quick, D. et al. 2014). The SRUM tracks system performance. It will contain data on the applications run and the bytes sent/received per application per hour in the last 30 to 60 days (Lee, R. 2015).

To collect and analyse artefacts the author will use a forensics toolkit. Some examples of forensics toolkits include FTK (Forensic Toolkit), EnCase, SANS SIFT, Magnet Axiom Examine and The Sleuth Kit. For this project the author has chosen to mainly use EnCase Version 8. This software has been chosen because it is a multipurpose forensic toolkit; this means it can be used to perform a number of tasks without needing additional software. The author also has more familiarity with EnCase so will find using this software less of a challenge then other forensics software. The toolkit Magnet Axiom Examine will also be used to validate the results from encase and ensure reliable results.

Other sources of forensics evidence will be analysed during this study, for example volatile memory. Volatile memory is computer data that is only maintained while a machine is powered, so once a machine is powered down this data is lost. In a real life situation volatile memory is not always collectable (Infosec, 2018). However, as this study will take place in a controlled environment volatile memory will be collected for analysis. Volatile memory can provide data on current processes including hidden processes and terminated processes. It can also provide information on network connections, open files, passwords, encrypted content and malicious code (Amari, K. 2009). The author will use Magnet RAM Capture to collect volatile memory and Magnet Axiom Examine to analyse this data.

Another source of forensics evidence that will be analysed during this study is network traffic. Network traffic is the data that moves across a network, and usually contained in network packets. There are many different types of packets that can provide a lot of information. Session data can reveal details of conversations between two network entities such as who was communicating, when and for how long this communication continued for (European Union Agency for Cybersecurity, 2019). It is important to analyse network traffic because all three applications use internet connection constantly for most of their features and will automatically attempt to connect to a network when starting up. The author will use Wireshark to collect and analyse network traffic.

Throughout this study, the author will follow ACPO (Association of Chief Police Officers) Good Practice Guide for Computer Based Electronic Evidence where feasible (Williams, J. 2012). This is the current guideline for investigating cyber security incidents and crime followed by British law enforcement, so it is important the author follows it. One of the ways the author will comply with this is by ensuring evidence produced is un-changed from when it was first collected at the point of seizure. To do this a full copy, sometimes called an image, will be taken of the digital device. This image is how the digital data will be viewed and collected, without any data being altered or changed at all.

The author will also follow ADFM (Abstract Digital Forensic Model). There are nine phases in ADFM, these can be seen in appendices figure 45. In the first phase, Identification, the type of incident is determined. However, this step is not required as this study will not involve a real incident. The second phase is preparation, this is where tools, techniques and other requirements are planned and prepared. The tools and techniques to be used in this study have already been planned and prepared as discussed earlier. The next phase is approach strategy, this involves developing a procedure to maximise the collection of evidence while minimizing the impact of this collection on victims. As with the first phase this is not required as this study will not involve a real incident. The fourth phase is preservation, which is the isolation, securing and containment of both physical and digital evidence. This study only focuses on digital evidence; to preserve this interaction with the device in question will be limited to data creation and the planned actions for data recovery. Preservation is followed by collection, in this phase a duplication of the digital evidence present on the hard drive will be created. Phase six is examination, this phase is the search of evidence relating to the suspected crime. For this study this phase will be the search of data relating the applications which could possibly be used as evidence in a real case. Phase seven is the analysis of the evidence collected, including determination of the significance of the evidence. The second to last phase is presentation, which is a summary and explanation of all the evidence in an appropriate format. The last phase is the returning of the physical and digital property to its owner. In this study not all of these phases will be necessary, however ADFM will still be used as a guide throughout (Rukayat, A. 2016).

The six “P’s” of research are also a guide for the process of research. The “P’s” are categorised as; Purpose, Products, Process, Participants, Paradigm and Presentation. Throughout this study, all aspects of the 6 “P’s” of research were considered. “Purpose” is defined as the reason for conducting the research and why it is important or useful to research this topic. The “purpose” of this research is to investigate and provide a detailed report on the artefacts and content that can and cannot be collected from Steam, Twitch and Discord. The author believes this research is important because of the dangers these platforms can pose to vulnerable peoples; as detailed in chapter 2. “Products” are the expected outcomes of the research. The outcome of this research is this report, which details the author’s findings. It is the authors hope that this report will be able to assist any peoples who come across these platforms in their investigations. “Process” is defined as how the research is to be conducted; including collection methods, data analysis and the limitations of these methods. The “Process” of this study can be simplified and compressed into four parts; research into to subject and applications, creation of the data onto the device to be studied, collection of this data using appropriate software (EnCase, Wireshark, Magnet RAM) and analysis of this data using Encase and Wireshark. “Participants” involve those both directly and indirectly involved in the research and the legal and ethical implications of these people being involved. This study does not involve anyone directly or indirectly except for the author themselves, their supervisor and second marker. “Paradigm” is defined as a shared way of thinking that is commonly believed; there are four main factors of a research paradigm; Ontology, Epistemology, Methods, and Methodology. Ontology is the study of beliefs about reality and existence. On the other hand, Epistemology is the study of the nature of knowledge, including how knowledge is acquired and validated. Method is the use of specific means for collecting data, for example, through questionnaires and interviews. Methodology is the study and critical analysis of data production techniques. This is the factor of the research paradigm that the author will be focusing on. “Presentation” is how the research will be delivered and explained to others. The presentation method for this research is this report (Oates, B. 2006).

In summary, this study will use digital forensics to determine the forensic artefacts that can be gathered relating to the applications on a computer running Windows 10 using the forensics software Encase. Windows 10 has been chosen as the OS for this investigation due to its popularity among users of Steam, Discord and Twitch. This study will also examine volatile memory and network traffic created by these applications. This data will be collected using Magnet RAM capture and Wireshark. Throughout this study ACPO, ADFM and the six P’s will be followed as close as is reasonable.

Chapter 5: Investigation Plan

In order to create a balanced and fair study the data creation process will need to be planned in advance. This chapter will detail the approaches planned to be taken and why these approaches have been chosen.

All data will be created and collected using a computer running a clean install of Windows 10 version 1903. This computer will be referred to as Main-Device throughout this report. The IP address for this device is 192.168.3.161. A clean install is required for this device to maintain data integrity, as data that has been previously created on Main-Device could affect the study results. A device running Windows 10 version 1803, which will be referred to as Secondary-Device, will have no data collected directly from the device; it will act only as a way of communicating with Main-Device. This address will have the IP address 192.168.56.1. Secondary-Device has both a camera and microphone inbuilt; Main-Device will have an audio and video a camera and microphone connected to it. These will be used in the creation of audio and video data.

It will be essential to have certain software and applications on Main-Device. Essential software and applications that will be present on Main-Device are detailed below

- Software that is included with Windows 10 such as Internet Explorer.
- Wireshark version 3.2.0 which is necessary to capture network traffic during data creation
- Magnet RAM Capture version 1.2.0 which is necessary to capture volatile memory after investigation is complete
- Steam application version 1581460722, this is necessary to create data for collection. The most up-to-date version of the application has been chosen to ensure the latest features are available and the application is stable.
- The most up-to-date Twitch application version (as of 03/04/2020) with Twitch Studio beta version 0.85.8 which is necessary to create data for collection. As with Steam the most up-to-date version of the applications has been chosen for stability.
- Discord application stable version 55041 this app is necessary to create data for collection. This version was chosen as it is the current most up-to-date.
- The video game “Rubi The Wayward Mira” , this game was chosen because it is a low power game , available for free and can be live streamed on all of the applications

Secondary-Device will also have Steam application version 1581460722, the most up-to-date Twitch application version (as of 03/04/2020) with Twitch Studio beta version 0.85.8 and Discord application version 55041; in order to effectively communicate with Main-Device without risk of version incompatibility. Accounts for these applications have been created in advance for both Main-Device and Secondary-Device. These accounts were created using throwaway email addresses, “icp.maindevice2020@gmail.com” for Main-Device and “icp.seconddevice2020@gmail.com” for Secondary-Device. Details for these accounts can be found in appendix figure 48.

The aim is to conduct a balanced study across the platforms; therefore, not all sources of evidence will be studied. For example, the Steam application allows users to create public status posts, however, the author will not investigate this feature as neither Twitch or

Discord have a similar feature. A prior investigation has been conducted into the features of the applications; this can be seen in appendix figure 47. Taking these limits into account, a detailed plan can be created. An example of the plan for Steam can be seen below (Table 1). A full plan for data creation including comments throughout the process is included in appendix figure 49.

Figure 1 -– Steam Data Creation Plan

Device	**Activity**
Main-Device	Turn on device
Main-Device	Open Wireshark
Main-Device	Start capturing data using Wireshark
Main-Device	Open Steam application
Main-Device	Enter login details and login
Main-Device	Use the add game feature to add “Rubi The Wayward Mira” to account game library
Secondary-Device	Send icp.maindevice2020 a friend request
Main-Device	Accept friend request
Main-Device	Using Steam chat send message “Steam 1 Ad astra per aspera” to icp.seconddevice2020
Secondary-Device	Reply to message with “Steam 2 Acta deos numquam mortalia fallunt”
Main-Device	Reply to message with http://www.google.co.uk
Main-Device	Send voice chat request to icp.seconddevice2020
Secondary-Device	Accept voice chat request
Main-Device and Secondary-Device	Keep voice chat active for 1 minute
Secondary-Device	Send icp.maindevice2020 ImageSteam.png
Secondary-Device	Send icp.maindevice2020 VideoSteam.mov
Main-Device	open “Rubi The Wayward Mira” from Steams game library
Main-Device	Send icp.seconddevice2020 an invite to watch

Secondary-Device	Accept invite to watch
Main-Device and Secondary-Device	Keep Steam Broadcast active for 15 minutes
Main-Device	Go into Steam broadcast settings and enable “Record video from all applications on this machine”, “Record audio from all applications on this machine” and “Record my microphone”
Main-Device	Using Steam broadcast chat send message “Steam 3 Carpe vinum”
Secondary-Device	Using Steam broadcast chat send message “Steam 4 Alea iacta est”
Main-Device	Open Internet explorer and search for “cute cat videos”
Main-Device	Play a random video with the sound enabled
Main-Device	Close “Rubi The Wayward Mira”
Main-Device	Insert external storage device into device
Main-Device	Stop Wireshark from capturing data, save data captured onto external storage device
Main-Device	Close Wireshark
Main-Device	Open Magnet RAM capture
Main-Device	Save data collected by Magnet RAM capture onto external storage device
Main-Device	Switch off device

In most official investigations an investigator will not have prior knowledge of the data present on a device. However, as this is a research study, this is an advantage the author will have. This is important as this study aims to distinguish the recoverable data from non-recoverable data; and this will not be possible without prior knowledge of the content on the computer.

Three timed uses of Main-Device will be conducted; one for each application. This is so that each application will have its own collection of network traffic and volatile memory, ensuring limited interference from the other applications. After these uses are completed, an external computer will be used to capture the data from the devices hard drive using Encase. This may cause some interference between applications. It would be more robust and reliable to collect data after each timed use and then perform a full factory reset on Main-Device. However, this is not possible due to resource limitations. Secondary-Device will be prepared in advance, as no data will be collected directly from the device.

The first step will always be to turn on the machine and enable Wireshark to start capturing network traffic. Wireshark will continue to run in the background throughout the timed use of Main-Device. Once this is confirmed to be running, the application (Twitch, Steam, or Discord) will be opened and logged into using a username and password. The accounts for each application have had limited activity prior to this to reduce the irrelevant data being present.

In order to perform a number of the tasks planned for the timed use of Main-Device and Secondary-Device will be required to communicate with each other. On these applications enabling communication requires the users to be online "friends". Therefore for each application, Secondary-Device will send a friend request to Main-Device which will then be accepted. This will enable IM, both devices will send one message containing the platform name, a number corresponding to the order of the message, and a unique Latin phrase. This format is followed to differentiate between messages sent on the platforms. A URL (Uniform Resource Locator) will also be shared using IM, for all applications. This will be the URL "www.google.co.uk" , this URL has been chosen because it is a simple URL that is unlikely to be blocked by the applications as suspicious activity.

IM will also be used to share images and videos. Sharing of such content is only available on Steam and Discord. Images and videos will be sent from Secondary-Device so that they are not stored on Main-Device except for on the applications. These images and videos will be named by media type and platform they will be shared through, for example ImageSteam.jpg and VideoDiscord.mov. This has been done so that the images and videos can be identified even if corrupted. The two images that will be sent across Discord and Steam will both be 187KB and 1280px in length and width and these images can be seen in appendix figure 46. The two videos will both contain the same sound and video, which lasts for approximately 5 seconds. These files are 3.59MB. The images and videos have been designed to be extremely small to comply with Discord and Steams upload limits and to avoid complications with possible corruption or long upload times.

Audio and video calling will be conducted on Discord, whereas calling will be limited to audio on Steam as video is not supported on this application. These calls will last for a timed 1 minute. During this 1 minute period audio will be recorded using a microphone and video with a webcam. Live streaming will also be conducted on all applications. This will consist of Main-Device broadcasting to Secondary-Device for 15 minutes. During this timed period the screen will broadcast the video game "Rubi the Wayward Mira" for a period of time before switching to broadcasting all content on the computer. During the 15 minutes audio will be live recorded using a microphone and for Twitch and Discord video will be live recorded using a webcam. During the broadcast of all content Main-Device will open Internet Explorer and search for a cute animal video, this video will then be played with the sound on to demonstrate sound from other applications on the live stream that can be picked up by live streaming. Both Twitch and Steam have group chat features that become active during a live stream, both Main-Device and Secondary-Device will use these chat systems to send one unique message following the same format that will be used to send IM messages.

After all planned activities have been completed within an application, to preserve data, the application will no longer be interacted with. The Wireshark capture of network traffic will be immediately stopped and Magnet RAM capture will be used to gather volatile memory from Main-Device. An external storage device will be used to store data collated such as volatile memory, network traffic and any clones of Main-Device. This storage device will only be accessible by the author to ensure data cannot be tampered with.

In summary, to create data for this project three separate uses of the computer named Main-Device will be conducted, and in each one of either Discord, Twitch or Steam will be heavily used. Accounts on these applications have already been created and full plans for the data have been made. During the creation of data Wireshark and will be Magnet RAM capture used to collect network traffic and volatile memory. After the three planed uses have been completed a clone of the Main-Device hard drive will be created and stored on a secure storage device.

Chapter 6: Investigation Results

In this chapter the author will review the data collected from the captures of the hard drive, network traffic and volatile memory. The data that can be collected from each application will be discussed and compared. The author will also discuss some of the problems that occurred during the creation of data that may affect the data that can be collected.

Hard-Drive

A duplication of the Main-Device hard drive was successfully created. Data was analysed using Encase and validated using Magnet Axiom Examine. From this analysis the author has established all three applications create files and directories when they are installed on a machine. These files are often stored on a user profile in order to separate one user's activities from another. The hidden folder AppData contains a lot of information relating to applications on a user profile. The full path for AppData is \Users\[NAME]\AppData\. Within this folder are 3 directories called Roaming, Local and LocalLow. The Roaming folder stores information that can be moved with a user profile from computer to computer. For example, in many large organisations user profiles are synced to a server; including data in the roaming folder, this allows their employees to log into their profile from any computer connected to the server. On the other hand the Local folder contains information that is specific to the computer it is stored on. It is also often used to store files determined too big to be stored in the Roaming folder. The folders and files that are stored in the Local folder are designated by the creator of an application; this means that when looking for data relating to applications both the Roaming and Local files should be analysed as data storage will completely differ depending on the application. For example, on Main-Device, files relating to the Discord application can be found in both the Roaming and Local folder, whereas files relating to Twitch can be found in the Roaming folder and files relating to Steam can be found in the Local folder. The LocalLow folder is very similar to the Local folder; however, it is only used by applications with more strict security settings who do not have access to the Local folder. None of the three applications are restricted so this file is not of interest in the analysis of Main-Device (Hoffman, 2017).

As stated earlier the file systems within AppData relating to the Discord application are split between Local and Roaming. The paths for these directories are \Users\[NAME]\AppData\ Local\Discord and \Users\[NAME]\AppData\Roaming\Discord. On Main-Device the Local folder contains files that support Discord in its functioning, for example, the executable to start the application, language packs, update information and resources. On the other hand the Roaming folder contains more information relating to usage of the application. Files and Folders in AppData relating to Twitch are stored in two directories, the paths for these are Users\[NAME]\AppData\Roaming\Twitch Studio and Users\[NAME]\AppData\ Roaming\Twitch Studio. This is because Twitch Studio is an add-on for Twitch that is not required for the main Twitch application to function. However, this was required in this study as Video Streaming is only available with Twitch Studio present. Files and folders in AppData relating to the Steam application are in the path Users\[NAME]\AppData\ Local\Steam. On Main-Device there are two folders inside of this directory, these are widevine and htmlcache. The file widevine contains licencing and data files for the program Widevine. Widevine is used by many applications and devices to enforce digital copyright protection. The htmlcache folder contains a lot of information of interest when investigating Steam.

The file systems with in AppData for Discord, Twitch and Steam differ in many ways but do follow some similar structures for example the files Blob_storage, Code Cache, Cache, GPUCache, Local storage, Logs and VideoDecodeStats are all names of files that are common within the application directories. The Blob_storage folder is named this way because it stores BLOBs (Binary Large OBjects), these are collections of binary data. Storing binary data this way allows it to be uploaded onto the cloud. On main_device empty folders named using long string of hexadecimal characters are found in the Blob_storage folders for each application. This data is not readable as it corresponds with a cloud database the author does not has access to (Myers, T. et al. 2020).

The Cache folder is the location where applications store recently used data so that it can be accessed quickly if it is needed again. Cache files are temporary and therefore the cache file may be missing information. However, a cache can store a lot of different information including images, videos, audio and web pages. Each of the applications has at least one Cache folder.

The Discord Cache folder is located in the path \Users\[NAME]\AppData\Roaming \Discord\Cache\. On Main-Device this cache has a total of 58 items. Many of these items relate to the general function of Discord and do not provide much information outside of this. However, files of value can be found. For example on Main-Device evidence of the files ImageDiscord.png and VideoDiscord.mov can be found. During creation of data ImageDiscord.png was sent from Secondary-Device to Main-Device on the 25/02/20 at approximately 17:28. Two data files were found on Main-Device relating to this image (See figures 3 and 4). Both files are dated as being created on the 25/02/20, however, the first file, f_00002f, is timed at 17:28:51 and the second, f_000033, at 17:29:28. Both files provide an almost accurate timestamp for when ImageDiscord.png was downloaded onto Main-Device. The file f_000030 (Figure 5) contains data relating to VideoDiscord.mov. This video clip was sent from Secondary-Device to Main-Device on the 25/02/20 17:29. As with image file the creation timestamp for f_000030 corresponds with the actual creation date.

Figure 2 - Activity: ImageDiscord.png and VideoDiscord.mov

Discord		
Device	**Activity**	**Date/Time**
Secondary-Device	Send icp.maindevice2020 ImageDiscord.png	25/02/2020 17:28
Secondary-Device	Send icp.maindevice2020 VideoDiscord.mov	17:29

Figure 3 - f_00002f

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord\Cache \f_00002f
File Created	25/02/20 17:28:51
Last Written	25/02/20 17:28:51
Last Accessed	25/02/20 17:28:51

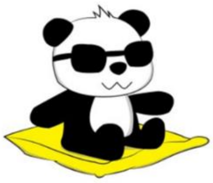


Figure 4 - f_000033

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord\Cache \f_000033
File Created	25/02/20 17:29:28
Last Written	25/02/20 17:29:28
Last Accessed	25/02/20 17:29:28

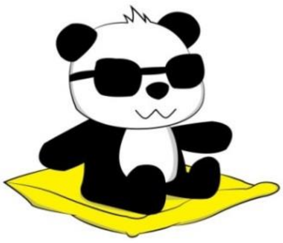
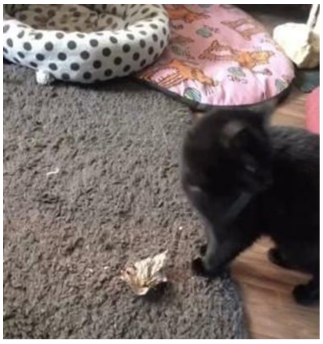


Figure 5 - f_000030

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord\Cache \f_000030
File Created	25/02/20 17:29:24
Last Written	25/02/20 17:29:24
Last Accessed	25/02/20 17:29:24



The Twitch Cache folder is located in the path \Users\[NAME]\AppData\Roaming \Twitch\Electron3\Cache\. During creation of data no images or videos were uploaded, as Twitch does not support this. However, other files can be found in the Cache folder. For example during creating of data Main-Device watched a Steam broadcast from Secondary-Device. In the Cache folder 22 files can be found relating to this stream. Each of these files contain a video clip with audio that lasts between 1 or 2 seconds. This may not seem like much but fragments of sentences can be heard throughout the clips. The first and last clips can be seen in Figures 7 and 8. These clips are logged as being created on the 03/03/20 at 17:51:05 and 17:51:52, the other 20 files have time stamps between these two. These timestamps match the time the streaming took place; between 17:51 and 17:52.

Figure 6 - Activity: Twitch Secondary-Device Stream

Twitch Application		
Device	**Activity**	**Date/Time**
Secondary-Device	Using Twitch Studio start streaming (With audio and video enabled)	03/03/2020 17:51-17:52
Main-Device	Go to seconddevice2020 profile and view stream	17:51-17:52
Secondary-Device	Keep Steam active 1 minute	17:51-17:52

Figure 7 – f_00006a

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Twitch\Electron3\Cache\f_00006a
File Created	03/03/20 17:51:05
Last Written	03/03/20 17:51:05
Last Accessed	03/03/20 17:51:05

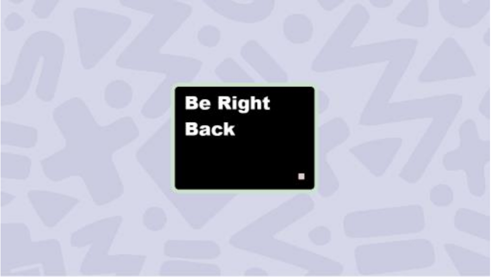
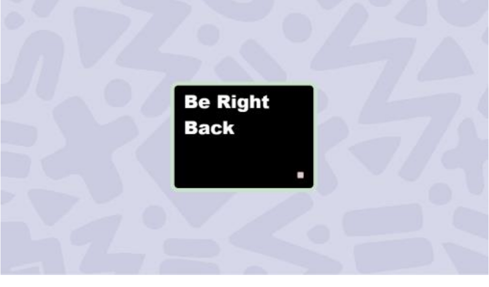


Figure 8 – f_000082

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Twitch\Electron3\Cache\f_000082
File Created	03/03/20 17:51:52
Last Written	03/03/20 17:51:52
Last Accessed	03/03/20 17:51:52



The Steam Cache folder is located in the path \Users\[NAME]\Appdata\Local \Steam\htmlcache\Cache\. One of the problems faced during the creation of data was the uploading of VideoSteam.mov, this was unsuccessful and therefore no data will exist relating to this video. However, Secondary-Device was able to send ImageSteam.png to Main-Device. A file relating to this image was found in the cache folder. This file is f_000043 and can be seen in figure 10. As with Discord the time stamp for this image is accurate to the upload time of the image.

Figure 9 – Activity: ImageSteam.png and VideoSteam.mov

Steam Application (Attempt Three)			
Device	**Activity**	**Date/Time**	**Other notes**
Secondary -Device	Send icp.maindevice2020 ImageSteam.png	10/03/2020 18:06	
Secondary -Device	Send icp.maindevice2020 VideoSteam.mov	N/A	File type now not supported, attempt to change file type also not supported.

Figure 10 – f_000043

Item Path	SS_FYP\D\Users\student\AppData\Local\Steam\htmlcache\Cache\f_000043
File Created	10/03/20 18:06:08
Last Written	10/03/20 18:06:08
Last Accessed	10/03/20 18:06:08

Another issue faced during the creation of data on the Steam application was that many of the features of Steam required to create this data were locked unless a certain amount of money is spent on an account. This led to 3 attempts at creating data which can be seen in appendix figure 49. During the first attempt, on the 03/03/2020, this feature was discovered and the attempt was halted as neither Secondary-Device nor Main-Device could send friend requests to each other. On the Second attempt the plan was changed so that a “Steam Wallet Code” would be used to add the required funds to the account so that the features required would be unlocked. However, this code was repeatedly brought back as invalid and eventually a timed lockout was issued on the account, so the attempt had to be stopped. On the third attempt once again, the code was repeatedly brought back as invalid and another timed lockout was put in place. Due to these repeat events the author attempted to input the code in the Secondary-Device, this was successful. This allowed Main and Secondary-Device to perform many of the activities however some were not possible. For instance, part of the lock stops accounts from streaming or interacting with streams. Therefore Main-Device could not stream as planned so Secondary-Device was used in its place. This means that no data on Streaming from Main-Device has been created and that messages that were to take place during streaming were limited (See Table 11).

Data was found in the Cache file relating to the message Secondary-Device was able to send during the streaming. This data was found in the file Data_1 and can be seen in Figure 12. Data_1 is a block file, block files are used to store Cached data that is small so doesn't need its own file. This is done by storing the data in fixed-size "blocks" (Slo.Sleuth, 2013). In the Steam files on Main-Device there are a total of 4 block files; named data_0, data_1, data_2, data_4. In Data_1 one of the "Blocks" within this file contains data that shows that the Steam account icp.seconddevice2020 sent the message "Steam 4 Alea iacta est" on Steam Broadcast Chat, which matches the data that was input. Data files also exist in Discord and Twitch's Cache files on Main-Device although nothing in relation to the test data was found, however this does not rule out that these may store similar data to Steam data_1 in other situations.

Figure 11 – Activity: Steam Broadcast Chat

Steam Application (Attempt Three)			
Device	**Activity**	**Date/Time**	**Other notes**
Main-Device	Using Steam broadcast chat send message "Steam 3 Carpe vinum"	N/A	Account cannot comment without money in account
Secondary-Device	Using Steam broadcast chat send message "Steam 4 Alea iacta est"	10/03/2020 18:15	

Figure 12 - data_1

Item Path	SS_FYP\D\Users\student\AppData\Local\Steam\htmlcache\Cache\data_1
File Created	03/03/20 16:57:22
Last Written	10/03/20 18:29:27
Last Accessed	10/03/20 18:29:27
Start Sector	60,591,346
Sector offset	351
File Offset	267,615
Length	361

```
•https://Steambroadcastchat.akamaized.net/chat/16872462649606435778/messages/
195313?chat_o
rigin=bc1-tuk1.chat.Steamcontent.com:8071                    { "messages": [ {"s
teamid":"76561199018202816", "instance_id":900071565,
"persona_name":"icp.seconddevice2020
", "flair":"", "in_game":false, "msg":"Steam 4 Alea iacta est"} ], "next_request": 196006
}
```

A type of file that can be found throughout AppData folders relating to Discord, Twitch and Steam is the log files. Log files are used to keep track of events that happen on a software, application or operating system (Fisher, T, 2020).
Discord has 3 log files within \Users\[NAME]\AppData \Roaming\Discord, these files are modules.log, VideoDecodeStats\ 000003.log and Local Storage\leveldb\000003.log. The logs file modules.log is a record of the installation of Discord, updates and update checks. This file does not include timestamps or any user specific information. The file VideoDecodeStats\ 000003.log also does not provide much information within. However, the Last Written and Last Accessed timestamps for these files can give the approximate time for when the application was last opened (See figures 13 and 14).

Figure 13 - modules.log

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord\modules.log
File Created	24/02/20 17:56:58
Last Written	25/02/20 17:21:37
Last Accessed	25/02/20 17:21:37

Figure 14- \VideoDecodeStats\000003.log

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord \VideoDecodeStats\000003.log
File Created	24/02/20 17:58:40
Last Written	25/02/20 17:21:35
Last Accessed	25/02/20 17:21:35

The log file Local Storage\leveldb\000003.log, which can be seen in Figure 17, is a record of Voice channels. Voice channels are how Discord transmits sound from one user to another; each voice channel has its own unique ID. In log file the one voice channel ID is present this is because both the 1 minute (Table 15) and 15 minute (Table 16) calls used the same voice channel. Timestamps are present in the file, and are stored as Unix time but can be converted into a human-readable format (Epoch Converter, 2020). The first "lastConnectedTime" in the file is 1582651551903 this converts to 25 February 2020 17:25:51.903. This timestamp matches the start time of the 1 minute call. The next 2 "lastConnectedTime" timestamps are at 17:26:51.904 and 17:27:34.506, these two timestamps would have been taken during the 1 minute call. However, the time stamp after this is 1582652057261 which converts to 17:34:17.261, this timestamp matches the start of the 15 minute call. There is an obstacle with differentiating between the calls; this is due to the fact that nothing unique separates the entries these timestamps are located in. If the calls had been in different voice channels the ID would have identified this as a separate call however this is not the case on Main-Device. The last "lastConnectedTime" timestamp in Local Storage\leveldb\000003.log converts to the 25 February 2020 17:48:36.070. This timestamp correctly records the time the 15 minute voice channel was closed. Local Storage\leveldb\000003.log also contains partial messages that was sent from Main-Device during the stream, this message has been saved under "draft" and time stamped as 1582652115037, which converts to the 25 February 2020 17:35:15.037. The partial message only contains "Discord 4" which is the start of the message shown in table 16.

Figure 15 - Activity: Discord Video Call

Discord Application		
Device	**Activity**	**Date/Time**
Main-Device	Send voice call request to icp.seconddevice2020	25/02/2020 17:25
Secondary-Device	Accept video call request	17:26
Main-Device and Secondary-Device	Keep video chat active for 1 minute (video and audio)	17:27

Figure 16 - Activity: Discord Streaming

Discord Application			
Device	**Activity**	**Date/Time**	**Other notes**
Main-Device	Send video call request to icp.seconddevice2020	25/02/2020 17:34	
Secondary-Device	Accept video call request	17:34	
Main-Device and Secondary-Device	Keep Discord call active for 10 minutes (video and audio)	17:34-17:48	Extended to 15 minutes
Main-Device	In the video settings turn on screen share (Also make sure both camera and microphone are enabled)	17:34	Screen share disables webcam
Main-Device	In Discord direct message send message "Discord 4 Audentes	17:35	

	fortuna iuvat”		

Figure 17 - \Local Storage\leveldb\000003.log

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Discord\Local Storage\leveldb\000003.log
File Created	24/02/20 17:58:30
Last Written	25/02/20 17:49:14
Last Accessed	25/02/20 17:49:14
File Offset	6,193
Length	5,549

```
/Discordapp.com DraftStore {"_state":{},"_version":0} ,_https://Discordapp.com
scientist:triggered {"v":1,"e":{"user|2020-
01_hide_nitro_tab":{"time":1582651296828,"hash":3695065393},"user|2020-
01_in_app_reporting":{"time":1582651466081,"hash":3695065393}}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826515519
03
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826516119
04
,"selectedChannelIds":{"null":"681913905785995271"}} ajp META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStoreu
{"selectedVoiceChannelId":null,"lastConnectedTime":1582651654506,"selectedChanne
lIds":{"null":"681913905785995271"}}• K1~ META:https://Discordapp.com *_https://
Discordapp.com PopoutWindowStore {"_state":{},"_version":0} RQ META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826519972
62
,"selectedChannelIds":{"null":"681913905785995271"}} qMl META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826520572
61
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com )_https://Discordapp.com MediaEngineStore
{"default":{"permission":true,"mode":"VOICE_ACTIVITY","modeOptions":{"threshold"
:-
40,"autoThreshold":true,"vadLeading":5,"vadTrailing":25,"delay":20,"shortcut":[]
},"mute":false,"deaf":false,"echoCancellation":true,"noiseSuppression":true,"aut
omaticGainControl":true,"noiseCancellation":false,"experimentalEncoders":false,"
silenceWarning":true,"attenuation":0,"attenuateWhileSpeakingSelf":false,"attenua
teWhileSpeakingOthers":true,"localMutes":{},"localVolumes":{},"localPans":{},"in
putVolume":100,"outputVolume":100,"inputDeviceId":"default","outputDeviceId":"de
fault","videoDeviceId":"default","qos":true,"soundshareSettingsVersion":2,"sound
shareVolume":20,"soundshareDucking":80,"videoHook":true,"experimentalSoundshare"
:true,"openH264":true}} META:https://Discordapp.com #_https://Discordapp.com
DraftStore`
```

```
{"_state":{"681913905785995271":{"timestamp":1582652115037,"draft":"Discord 4
"}},"_version":0}3 META:https://Discordapp.com -_https://Discordapp.com
SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826521172
71
,"selectedChannelIds":{"null":"681913905785995271"}}"j META:https://
Discordapp.com #_https://Discordapp.com DraftStore {"_state":{},"_version":0}O?
META:https://Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826521772
70
,"selectedChannelIds":{"null":"681913905785995271"}} <E@ META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826522373
51
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826522972
79
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826523572
61
,"selectedChannelIds":{"null":"681913905785995271"}}!{? META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826524174
06
,"selectedChannelIds":{"null":"681913905785995271"}}f META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826524773
55
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com *_https://Discordapp.com StreamerModeStore
{"disableSounds":false} META:https://Discordapp.com -_https://Discordapp.com
SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826525375
40
,"selectedChannelIds":{"null":"681913905785995271"}} *_https://Discordapp.com
StreamerModeStore5 {"disableSounds":false,"disableNotifications":false}
META:https://Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826525975
51
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826526572
74
,"selectedChannelIds":{"null":"681913905785995271"}}% META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
```

```
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826527172
72
,"selectedChannelIds":{"null":"681913905785995271"}}Q META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826527777
10
,"selectedChannelIds":{"null":"681913905785995271"}} META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStore
{"selectedVoiceChannelId":"681913905785995271","lastConnectedTime":15826528375
36
,"selectedChannelIds":{"null":"681913905785995271"}}o1 META:https://
Discordapp.com -_https://Discordapp.com SelectedChannelStoreu
{"selectedVoiceChannelId":null,"lastConnectedTime":1582652916070,"selectedChanne
lIds":{"null":"681913905785995271"}
```

Twitch has the highest amount of log files compared to Discord and Twitch. On Main-Device there are 7 log files within \Users\[NAME]\AppData\Roaming\Twitch\Electron3\ and 5 log files within \Users\[NAME]\AppData\Roaming\Twitch Studio\Electron3\. Most of these files do not provide useful timestamps or any user specific information. On Main-Device some of these files are completely empty including the file 000005.log (See Figure 18). This files Last Written and Last Accessed timestamps could give approximate time for when the application was last opened. However, as this is the only log file which provides this timestamp and many of the other log files created by Twitch have widely varying timestamps this may be a fluke.

Figure 18 - 000005.log

Item Path	SS_FYP\D\Users\student\AppData\Roaming\Twitch\Electron3\000005.log
File Created	03/03/20 17:42:56
Last Written	03/03/20 17:42:56
Last Accessed	03/03/20 17:42:56

The application Steam has 4 log files within \Users\[NAME]\AppData\Local\Steam\htmlcache\. These files are 000003, Local Storage/leveldb/000003, Session Storage/000003 and VideoDecodeStats/000003. These files do not contain any useful user specific information; this may be because of the issues the author had with creating data using the Steam application. Data relating to streaming could have been stored in these files but main-service could not stream as planned no data will have been created.

Although the issues with data creation on the Steam application have limited the amount of data available for study, sources of data can still be found. For example, in the path D\Program Files (x86)\Steam\ many files relating to the function of the Steam application including many Valve Data Files are stored. VDF's (Valve Data Files) are a unique file type that is only used by the Steam application (Fileinfo, 2020). loginusers.vdf can be seen in Figure 20, it contains information relating to user details of accounts used on Steam on Main-Device. Details of only one account are present in this file because only one account was used on Main-Device. The correct Account name and Display name for Main-Devices

Steam account can be found in this file with a timestamp of 1583862634 which converts to 10 March 2020 17:50:34 (Epoch Converter, 2020). This timestamp corresponds with the time Steam was last logged into (See table 19). The "RememberPassword" is set to 0; This means that Steam has not been set to store the users password. If the password is stored this will be set to 1. Similarly the value "MostRecent" is set to 1, meaning that this account was the last account accessed. If further accounts had been used on Main-Device these would be set to 0.

Another VDF file, localconfig.vdf, can be seen in Figure 21. This file stores data relating to users currently logged into Steam, it exists so that users can still access their account details and games even if no internet connection is available. On Main-Device localconfig.vdf is contained within a folder named 1057569060, this folder is named after the Steam user ID of the account the data is connected to. If multiple Steam accounts existed on Main-Device these would each have their own localconfig.vdf file. This file can contain many details on an account including streaming details and the account name including any previous account names used. It can also provide the same information for friends of the account. However, on Main-Device the file does not provide much; a snippet of Secondary-Devices version of this file has been provided in Figure 22 to show the type of information that might have been included of Main-device if not for the issues the author had with data creation on Steam.

Figure 19 – Activity: Login to Steam

Steam Application (Attempt Three)		
Device	**Activity**	**Date/Time**
Main-Device	Open Steam application	10/03/2020 17:49
Main-Device	Enter login details and login	17:50

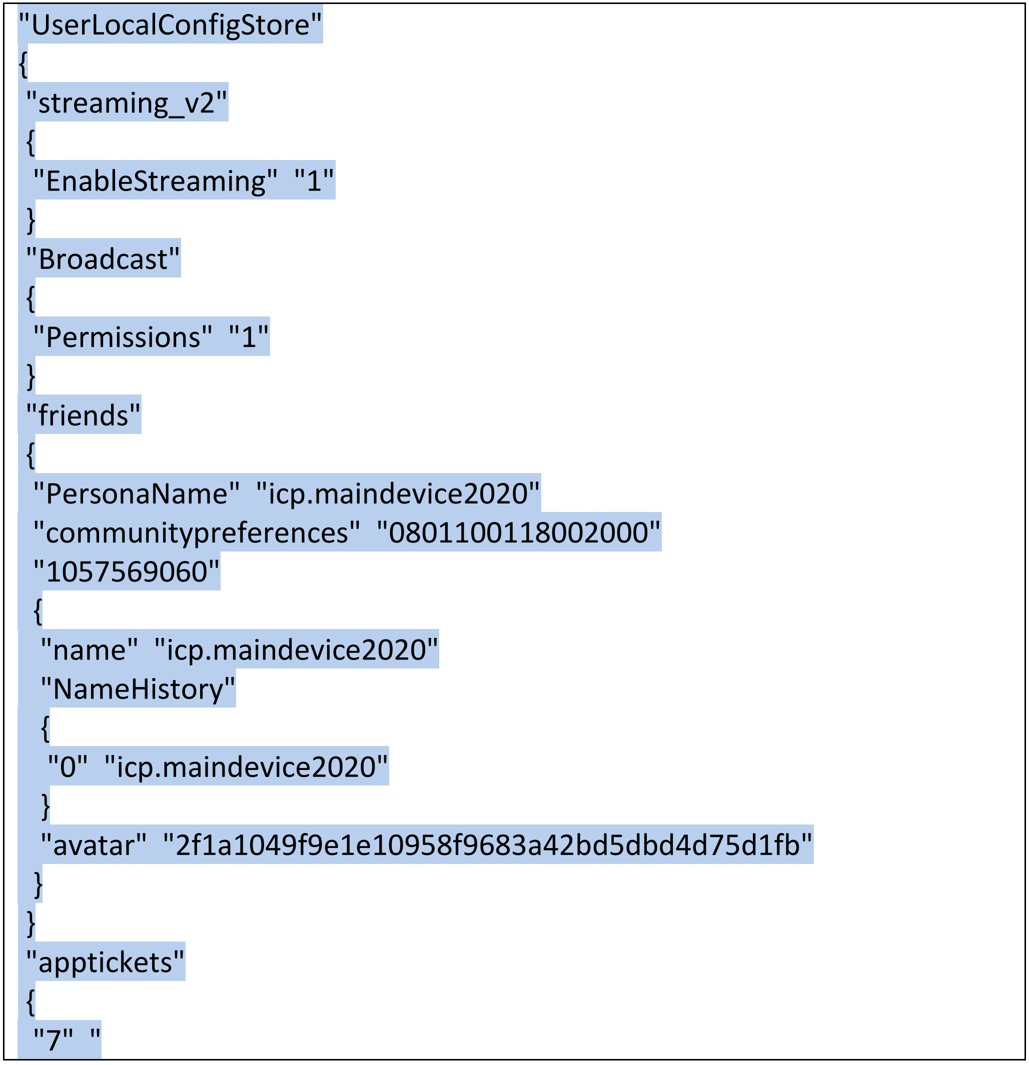
Figure 20 - loginusers.vdf

Item Path	SS_FYP\D\Program Files (x86)\Steam\config\loginusers.vdf
File Created	03/03/20 16:57:06
Last Written	10/03/20 17:50:34
Last Accessed	10/03/20 17:50:34
Start Sector	45,388,412
Sector offset	416
Length	184

```
"users"
{
 "76561199017834788"
 {
  "AccountName"  "maindevice2020"
  "PersonaName"  "icp.maindevice2020"
  "RememberPassword"  "0"
  "MostRecent"  "1"
  "Timestamp"  "1583862634"
}
```

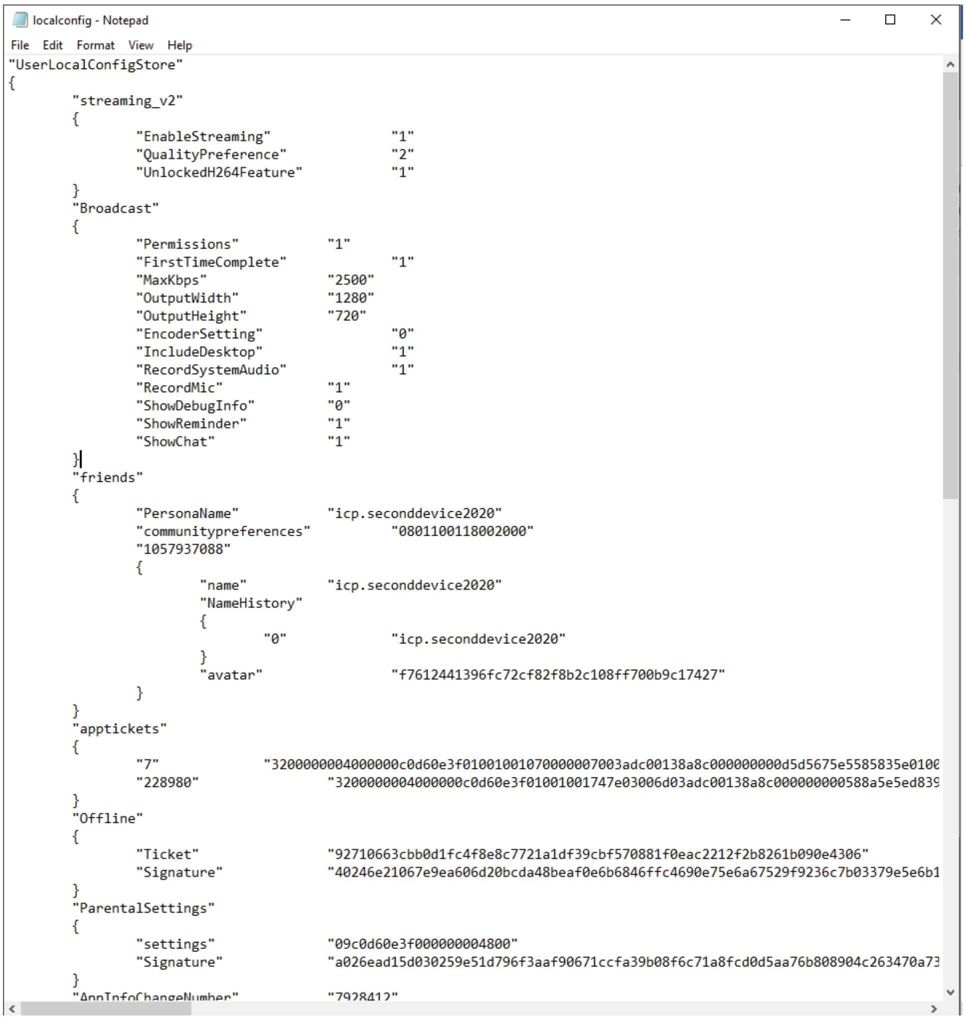
Figure 21 - localconfig.vdf

Item Path	SS_FYP\D\Program Files (x86)\Steam\userdata\1057569060\config\localconfig.vdf
File Created	10/03/20 18:20:28
Last Written	10/03/20 18:20:28
Last Accessed	10/03/20 18:20:28
MD5	
Start Sector	4,431,856
Length	405



```
"UserLocalConfigStore"
{
 "streaming_v2"
 {
  "EnableStreaming"  "1"
 }
 "Broadcast"
 {
  "Permissions"  "1"
 }
 "friends"
 {
  "PersonaName"  "icp.maindevice2020"
  "communitypreferences"  "0801100118002000"
  "1057569060"
  {
   "name"  "icp.maindevice2020"
   "NameHistory"
   {
    "0"  "icp.maindevice2020"
   }
   "avatar"  "2f1a1049f9e1e10958f9683a42bd5dbd4d75d1fb"
  }
 }
 "apptickets"
 {
  "7"  "
```

Figure 22– Secondary-Device: localconfig.vdf



```
"UserLocalConfigStore"
{
        "streaming_v2"
        {
                "EnableStreaming"               "1"
                "QualityPreference"             "2"
                "UnlockedH264Feature"           "1"
        }
        "Broadcast"
        {
                "Permissions"           "1"
                "FirstTimeComplete"             "1"
                "MaxKbps"               "2500"
                "OutputWidth"           "1280"
                "OutputHeight"          "720"
                "EncoderSetting"                "0"
                "IncludeDesktop"                "1"
                "RecordSystemAudio"             "1"
                "RecordMic"             "1"
                "ShowDebugInfo"         "0"
                "ShowReminder"          "1"
                "ShowChat"              "1"
        }
        "friends"
        {
                "PersonaName"           "icp.seconddevice2020"
                "communitypreferences"          "0801100118002000"
                "1057937088"
                {
                        "name"          "icp.seconddevice2020"
                        "NameHistory"
                        {
                                "0"             "icp.seconddevice2020"
                        }
                        "avatar"                "f7612441396fc72cf82f8b2c108ff700b9c17427"
                }
        }
        "apptickets"
        {
                "7"             "3200000004000000c0d60e3f01001001070000007003adc00138a8c000000000d5d5675e5585835e0100
                "228980"                "3200000004000000c0d60e3f01001001747e03006d03adc00138a8c000000000588a5e5ed839
        }
        "Offline"
        {
                "Ticket"                "92710663cbb0d1fc4f8e8c7721a1df39cbf570881f0eac2212f2b8261b090e4306"
                "Signature"             "40246e21067e9ea606d20bcda48beaf0e6b6846ffc4690e75e6a67529f9236c7b03379e5e6b1
        }
        "ParentalSettings"
        {
                "settings"              "09c0d60e3f000000004800"
                "Signature"             "a026ead15d030259e51d796f3aaf90671ccfa39b08f6c71a8fcd0d5aa76b808904c263470a73
        }
        "AppInfoChangeNumber"           "7928412"
```

Metadata is data that gives information about other data. It is usually used to summarize basic information about data. On a Windows computer all metadata changes to the file system are logged in a file called $LogFile. This file can be found in the root directory of the file system it collects data from (Suhanov, M. 2019). In the case of Main-Device this is the Directory \D\$LogFile. This file is largely unreadable to a human however it is possible to find readable data within. At two points in Main-Device $LogFile the account name and display name for the Steam account are stated, these can be seen in figure 23. Although data is not provided on where the metadata for these two entries has been collected from, the data shown closely resembles the data found in the loginusers.vdf file (See figure 20). It is likely the two instances in $LogFile are previous iterations. The major difference between the main file and the previous iterations is the timestamps. In loginusers.vdf the timestamp is 1583862634 which converts to the 10th of March 2020 17:50:34, this date and time matches the date and time of the Steam login during the third attempt (see table 24). The two entries in $LogFile are dated at 1583859317 and 1583254626. The first converts to the 10th Math 2020 16:55:17 which is the date and time of the login during the second Steam attempt. The second converts to the 3rd March 2020 16:57:06 which is the date and time of the login during the first attempt (Epoch Converter, 2020).

Figure 23 - $LogFile

Item Path	SS_FYP\D\$LogFile
File Created	10/02/20 17:45:15
Last Written	10/02/20 17:45:15
Last Accessed	10/02/20 17:45:15

Entry 1

Start Sector	7,362,881
Sector offset	480
File Offset	12,375,008
Length	180

```
"users"
{
 "76561199017834788">D{
  "AccountName"  "maindevice2020"
  "PersonaName"  "icp.maindevice2020"
  "RememberPassword"  "0"
  "MostRecent"  "1"
  "Timestamp"  "1583859317"
```

Entry 2

Start Sector	7,426,489
Sector offset	264
File Offset	44,942,088
Length	180

```
"users"
{
 "76561199017834788"
 {
  "AccountName"  "maindevice2020"
  "PersonaName"  "icp.maindevice2020"
  "RememberPassword"  "0"
  "MostRecent"  "1"
  "Timestamp"  "1583254626"
```

Figure 24– Activity Steam: Login

Device	Activity	Date/Time
Steam Application (Attempt One)		
Main-Device	Enter login details and login	03/03/2020 16:57
Steam Application (Attempt Two)		
Main-Device	Enter login details and login	10/03/2020 16:55
Steam Application (Attempt Three)		
Main-Device	Enter login details and login	10/03/2020 17:50

The system file pagefile.sys is another source of data found in the root directory of the file system. System files are used on Windows operating systems to store system settings. The pagefile.sys file contains data that would usually be stored in RAM (Random access memory) but cannot be stored there due to issues such as overcapacity of RAM. When data is moved from RAM into the pagefile.sys file, the least used data is moved first (Martin, C 2018). Similarly to $LogFile the data contained in pagefile.sys is largely unreadable to a human however it is possible to find readable data within. Data relating to Discord, Twitch and Steam was found in the file examples can be seen in Figure 25. The first three entries sampled from pagefile.sys provide the display names used on Secondary-Device for each of the applications. However, this data would be extremely hard to find within pagefile.sys without prior knowledge of the display name. The fourth entry contains data almost exact to that found in the file localconfig.vdf (See Figure 21). The fifth entry contains the first message sent from Main-Device to Secondary-Device and the time this message was sent (See table 26) but not the date. As with the first three entries this data would extremely hard to find without some prior knowledge of what to search for.

Figure 25- pagefile.sys

Item Path	SS_FYP\D\pagefile.sys
File Created	10/02/20 09:56:25
Last Written	10/03/20 18:29:31
Last Accessed	10/03/20 18:29:31

Entry 1

Start Sector	22,717,026
Sector offset	364
File Offset	1,331,213,676
Length	61

```
@icp.seconddevice2020 - Discord
```

Entry 2

Start Sector	21,721,201
Sector offset	8
File Offset	821,350,920
Length	582

```
"MESSAGE","data":{"topic":"presence.484889514","message":"{\"type\":\"presence\",\
"data\":
{\"user_id\":485278114,\"availability\":\"online\",\"activity\":{\"type\":\"broadcasting\
"
,\"channel_id\":\"485278114\",\"stream_id\":\"764496129\",\"channel_login\":\"secon
ddevice
2020\",\"channel_display_name\":\"seconddevice2020\"},\"index\":4,\"updated_at\":1
58325785
8,\"user_login\":\"seconddevice2020\",\"activities\":[{\"type\":\"broadcasting\",\"chan
nel
_id\":\"485278114\",\"stream_id\":\"764496129\",\"channel_login\":\"seconddevice20
20\",\"c
hannel_display_name\":\"seconddevice2020\"
```

Entry 3

Start Sector	21,720,676
Sector offset	368
File Offset	821,082,480
Length	39

```
https://www.Twitch.tv/seconddevice2020
```

Entry 4

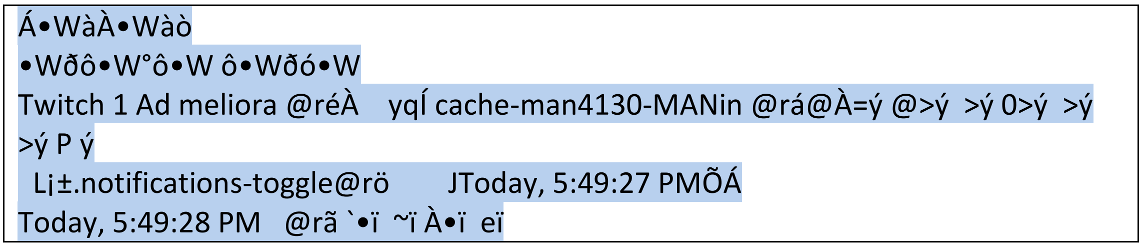
Start Sector	63,390,478
Sector offset	5
File Offset	2,236,754,949
Length	368

```
LocalConfigStore"
{
 "streaming_v2"
 {
  "EnableStreaming"  "1"
 }
 "Broadcast"
 {
  "Permissions"  "1"
 }
 "friends"
 {
  "PersonaName"  "icp.maindevice2020"
  "communitypreferences"  "0801100118002000"
  "1057569060"
  {
   "name"  "icp.maindevice2020"
   "NameHistory"
   {
    "0"  "icp.maindevice2020"
   }
   "avatar"  "2f1a1049f9e1e10958f9683a42bd5dbd4d75d1fb"
```

Entry 5

Start Sector	21,584,049
Sector offset	40
File Offset	751,129,128
Length	684

```
Twitch 1 Ad meliora @rÙ     QjóNB37B544FE8F784A0.net
=RljErrorNotAvailable‰9 @rÖ  Å
•W@Æ•WÀÆ•W°Æ•W Æ•W•Æ•W€Æ•W@rÉÀ    Î¥× cache-man4149-MAN   @rá`à-
ý € ý 07ý À0ý P ý €7ý p ý
                                  JwhisperDoNotDisturb @rï€    È/^Npublic, max-ag
e=300t@rå`°Ø^W€Ø^WpØ^W É^W?É^W`É^WĐÈ^W@rò €Ç•WàÆ•W`Ç•WPÇ•W@Ç•
W0Ç•W Ç•W       Ìš™ ?   Y  €?
          @rá ð<ý P=ý p=ý €=ý  =ý @=ý ð=ý X 3@ UC)pSC) TC)`TC)          @rÉ
```



```
Á•WàÀ•Wàò
•Wðô•W°ô•W ô•Wðó•W
Twitch 1 Ad meliora @réÀ    yqÍ cache-man4130-MANin @rá@À=ý @>ý  >ý 0>ý  >ý
>ý P ý
  L¡±.notifications-toggle@rö       JToday, 5:49:27 PMÕÁ
Today, 5:49:28 PM   @rã `•ï  ~ï À•ï  eï
```

Figure 26– Activity: Twitch message 1

Twitch Application		
Device	**Activity**	**Date/Time**
Main-Device	Using Twitch whisper send message “Twitch 1 Ad meliora” to seconddevice2020	03/03/2020 17:49

To summarise, a duplication of the hard drive was created and analysed using Encase and Magnet Axiom Examine. Most of the important information was found within the AppData folder, with the Local and Roaming folders splitting the content. Each application has a cache which holds various files that relate to recent history of the use of the application. Images, Videos and some messages where found within these cache files. Log files were also found throughout the AppData; these that are used to track events that happen while the user is browsing the application. The log files can contain information such as when the application was last updated; last opened or even when voice channels are used. These can be used to tell how active the user was on that specific application. There were also some unique file types only seen on these applications, for example VDF's (Valve Data Files). VDF's can contain metadata information about certain accounts and can display specific information about them, such as settings they have manipulated, whether they have microphones enabled, or even if they have changed their name. Finally, system files have been found that are used to store information about windows account details. These kept track of some of the information that is usually stored in RAM, and is moved into a text file when RAM is full. There were even some display names kept in these files, although they are hard to find.

Table 1 – Data retrieved from hard-drive

Key	
Not retrieved	🟥
Partially retrieved	🟧
Retrieved	🟩

Application	**Login**	**Text based messages**	**URL message**	**Image message**	**Video message**	**1 min VOIP**	**10 min VOIP**
Discord	🟥	🟧	🟥	🟩	🟩	🟧	🟧
Twitch	🟥	🟧	🟥	N/A	N/A	🟩	🟥
Steam	🟩	🟧	🟥	🟩	N/A	🟥	🟥

Volatile memory

Volatile memory was successfully captured for all applications. Only data from the third attempt at creating data for Steam will be analysed as this was the most successful attempt. All volatile memory was captured using Magnet RAM Capture and examined using Magnet Axiom Examine. Data on many types of files can be collected from volatile memory including operating system files and media files.

One type of operating system file that can be found on a Windows computer is LNK files. LNK files are shortcut files that are linked applications and files. They can give an indication of the last time the object they are linked to was accessed, even if this item has been deleted or removed from the system (McQuaid, J. 2014b). From the three captures taken of Main-Device, LNK files for each of the applications executable files can be found. These LNK files can be seen in Figures 27, 29, 30 and 32. Each come with a date and time for the creation, last written and last accessed times for the application in which they are linked. However, these dates and times are not entirely correct. For example, in Figure 27 the LNK file is connected to the Discord executable, Update.exe; the last written date provided for this file is given as 07/03/2019 which is roughly 11 months before the author even installed Discord on Main-Device so is extremely incorrect. The last accessed date and time for this file is also incorrect, the correct time is shown in table 28. Similarly, the dates for the LNK files in Figure 29 and 30, for Twitch, are incorrect. The only LNK file which has partially correct dates and times is the Steam.exe LNK shown in figure 32. The last accessed time provided for this file matches the dates and times for the first attempt at creating data for the steam application (as seen in table 33). However, this is still incorrect as the last accessed date time should match the most recent access to this application; which would be the date and time Steam was opened during the third application.

Figure 27– LNK Update.exe

Linked Path	C:\Users\student\AppData\Local\Discord\Update.exe
Target File Created	24/02/2020 17:56:27
Target File Last Written	07/03/2019 15:22:18
Target File Last Accessed	24/02/2020 17:56:27
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Target File Size (Bytes)	1523544

Figure 28 – Activity: Open Discord

Discord Application		
Device	**Activity**	**Date/Time**
Main-Device	Open Discord application	25/02/2020 17:20

Figure 29 – LNK Twitch.exe

Linked Path	C:\Users\student\AppData\Roaming\Twitch \Bin\Twitch.exe
Target File Created	24/02/2020 18:01:25
Target File Last Written	24/02/2020 18:01:25
Target File Last Accessed	24/02/2020 18:01:25
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Target File Size (Bytes)	1246096

Figure 30 – LNK TwitchStudio.exe

Linked Path	C:\Users\student\AppData\Roaming\Twitch Studio\Bin\TwitchStudio.exe
Target File Created	24/02/2020 18:03:08
Target File Last Written	24/02/2020 18:03:08
Target File Last Accessed	24/02/2020 18:03:08
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Target File Size (Bytes)	1308512

Figure 31 – Activity: Open Twitch

Twitch Application		
Device	**Activity**	**Date/Time**
Main-Device	Open Twitch and Twitch Studio	03/03/2020 17:42

Figure 32– LNK Steam.exe

Linked Path	C:\Program Files (x86)\Steam\Steam.exe
Target File Created	22/05/2018 00:30:20
Target File Last Written	11/02/2020 19:48:00
Target File Last Accessed	03/03/2020 16:53:53
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Target File Size (Bytes)	3365840

Figure 33– Activity: Open Steam

Device	**Activity**	**Date/Time**
Steam Application (Attempt One)		
Main-Device	Open Steam application	03/03/2020 16:53 – 16:56
Steam Application (Attempt Two)		
Main-Device	Open Steam application	10/03/2020 16:54
Steam Application (Attempt Three)		
Main-Device	Open Steam application	10/03/2020 17:49

A further type of operating system file that can be found on a Windows computer is prefetch files. Prefetch files provide pre-loaded code for applications created by Windows 10 when an application is running for the first time on a machine. Prefetch files can contain data on how many times the application has been run and timestamps for when the application was first and last run (McQuaid, J. 2014a). Throughout the volatile memory collected one prefetch file with a clear link to one of the applications can be found (Figure 34). This prefetch file is for the application Steam Client WebHelper. The application is required for the Steam application to fully function. Prefect files can store up to 8 last run dates and time, this file provides 2 which match up with the dates and time for the first two times Steam was opened on Main-Device (See table 33).

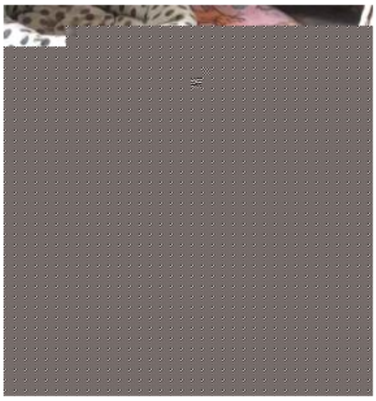
Figure 34 -– STEAMWEBHELPER.EXE

Application Name	STEAMWEBHELPER.EXE
Application Run Count	0
Last Run Date/Time	10/03/2020 16:54:34
File Hash	33109D6F
2nd Last Run Date/Time	03/03/2020 16:56:11

The media files that can be collected from volatile memory include video files, audio files and pictures. The video and audio files that where collected on Main-Device were too corrupted to determine anything from. Many of the images were the same despite that some images relating to the application where recovered. These images are mostly just logos and content that is standard within the applications. However, copies of VideoDiscord.mov and ImageDiscord.png, these images are largely corrupted and would be extremely hard to locate unless prior knowledge of the content of the image or video was known.

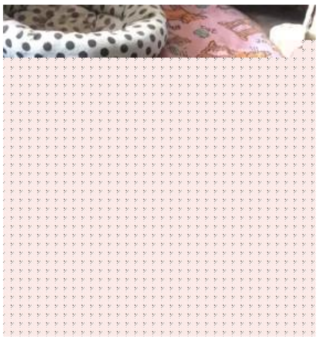
Figure 35– Volatile memory pictures

VideoDiscord.mov		ImageDiscord.png	
Size (Bytes)	20203	Size (Bytes)	111329
Original Width	284	Original Width	300
Original Height	301	Original Height	300



VideoDiscord.mov 2

Size (Bytes)	84069
Original Width	284
Original Height	301



In summary, during each session of testing the application, Magnet AXIPOM Examine was used to capture the volatile memory from the computer. These files are normally non-permanent, therefore they can very useful to capture as early as possible. One of the first files found were the LNK files, which store information about when applications are last accessed and which application they are linked to, even if the application is destroyed. Each application had an LNK file that was found; however, these displayed the incorrect timestamps. Prefetch files were also found on the computer. These files are used to store pre-loaded code for Windows 10 applications. One prefetch file found was directly linked to the Steam WebHelper, which is required by Steam to function properly. Perhaps most importantly, media files were also found in volatile memory. Most of these were basic images used by each application such as logos and content that would be used regardless of user, there were also user images and videos found from Discord that were very corrupted, so they would be quite difficult to determine anything from.

Table 2 – Data retrieved from volatile memory

Key	
Not retrieved	🟥
Partially retrieved	🟧
Retrieved	🟩

Application	**App use**	**Text based messages**	**URL message**	**Image message**	**Video message**	**1 min VOIP**	**10 min VOIP**
Discord	🟥	🟥	🟥	🟧	🟧	🟥	🟥
Twitch	🟥	🟥	🟥	N/A	N/A	🟥	🟥
Steam	🟧	🟥	🟥	🟥	N/A	🟥	🟥

Network Traffic

The software Wireshark was successfully used to collect network traffic during each of the planned sessions. As with the volatile memory capture only data gathered from the third attempt at creating data for Steam as this was the most successful attempt. The data collected has been analysed using Wireshark.

Network traffic is made up of small units of data called packets. Packets are how information is sent across networks and the internet. For example, when the video VideoDiscord.mp4 was sent from Secondary-Device to Main-Device this video will have been broken down into smaller pieces each containing a part of the video. The part of the packet that stores the fragment of data is called the payload. Each payload is given a header and a trailer. The header contains a protocol, destination address, source address and indentation number. The protocol defies what type of packet it is; videos, webpages, emails etc. all use different protocols. The source address specifies where the packet is coming from (Secondary-Device) and the destination address indicates where to packet is being sent to (Main-Device). The identification number is so that Main-Device will be able to reassemble the parts back into the video once it receives them all. The contents of a trailer are different depending on the type of network but they usually contain some sort of error checking. The full structure of a packet can be seen in figure 36. Data is shared using packets because their small size allows them to quickly transmit over many network links, each packet finding its fastest route (Live Action, 2018).

Figure 36 - Network Packet

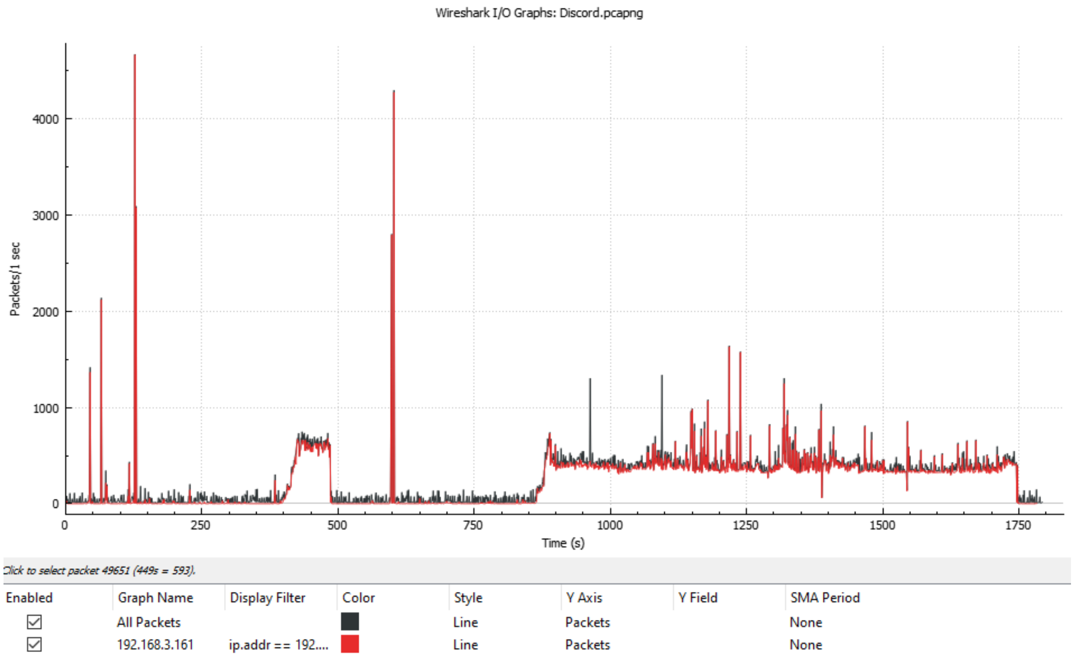
[-------------------------Header--------------------------][-----------Payload-----------][---Trailer---]

Destination Address	Source Address	Protocol	Identification number	Data	Error checking

During each data creation section Wireshark captured packets when they reached Main-Device. A total of 741,777 packets where collected however, not all of these packets relate to the applications, Main-Device or Secondary-Device as other network traffic will have been collected too. Figures 37, 39 and 41 the details provided by Wireshark for each collection can be seen.

Figure 37 - Discord Statistics

First packet:	2020/02/25 17:19:28
Last packet:	2020/02/25 17:49:21
Elapsed:	00:29:53
Packets:	469501
Time span, s:	1793.503
Average pps:	261.8
Average packet size:	871
Bytes:	409078633
Average bytes/s:	228 k
Average bits/s:	1824 k

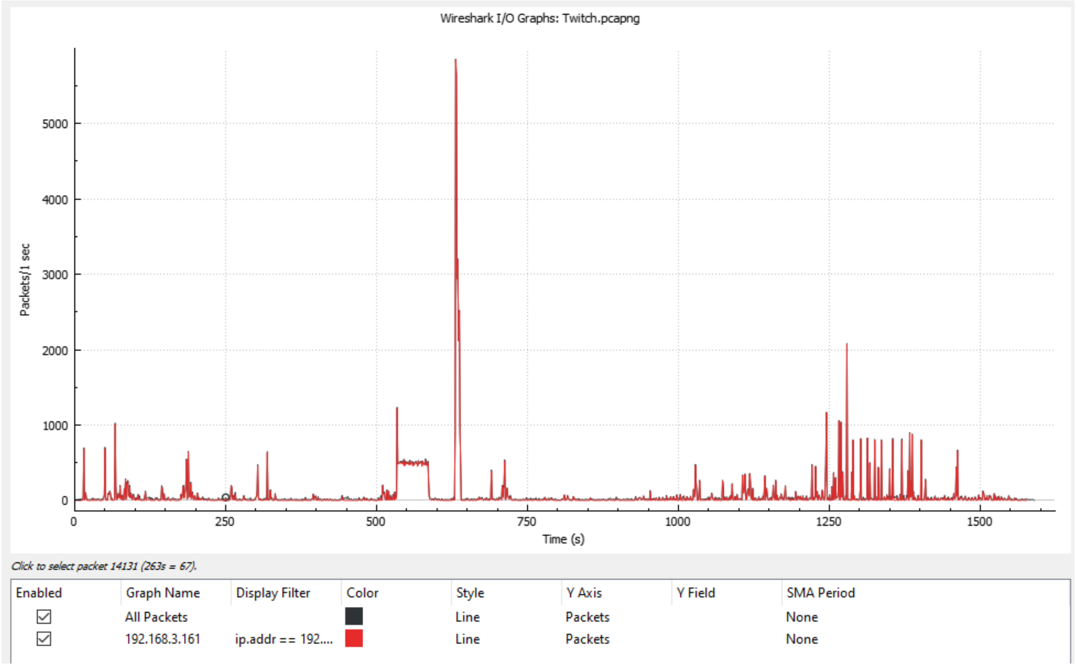


Click to select packet 49651 (449s = 593).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		⬛	Line	Packets		None
☑	192.168.3.161	ip.addr == 192....	🟥	Line	Packets		None

Figure 38- Twitch Statistics

First packet:	2020/03/03 17:42:05
Last packet:	2020/03/03 18:08:34
Elapsed:	00:26:29
Packets:	127126
Time span, s:	1589.186
Average pps:	80.0
Average packet size:	892
Bytes:	113343458
Average bytes/s:	71 k
Average bits/s:	570 k

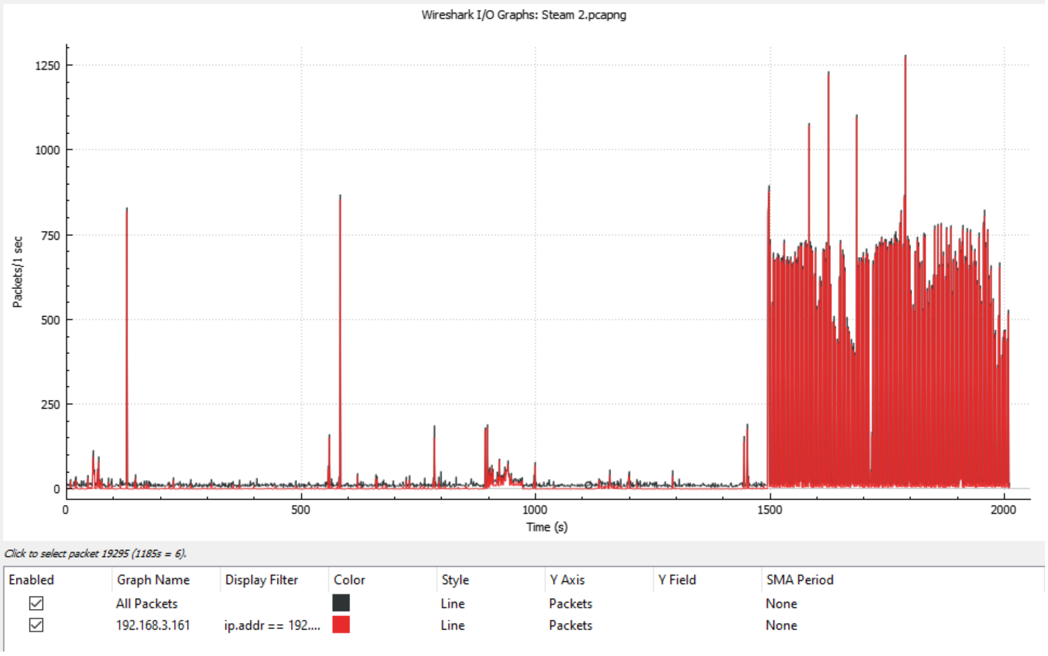


Click to select packet 14131 (263s = 67).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		⬛	Line	Packets		None
☑	192.168.3.161	ip.addr == 192....	🟥	Line	Packets		None

Figure 39 - Steam Statistics

First packet:	2020/03/10 17:49:29
Last packet:	2020/03/10 18:23:00
Elapsed:	00:33:31
Packets:	145120
Time span, s:	2011.434
Average pps:	72.1
Average packet size:	1055
Bytes:	153113912
Average bytes/s:	76 k
Average bits/s:	608 k



Click to select packet 19295 (1185s = 6).

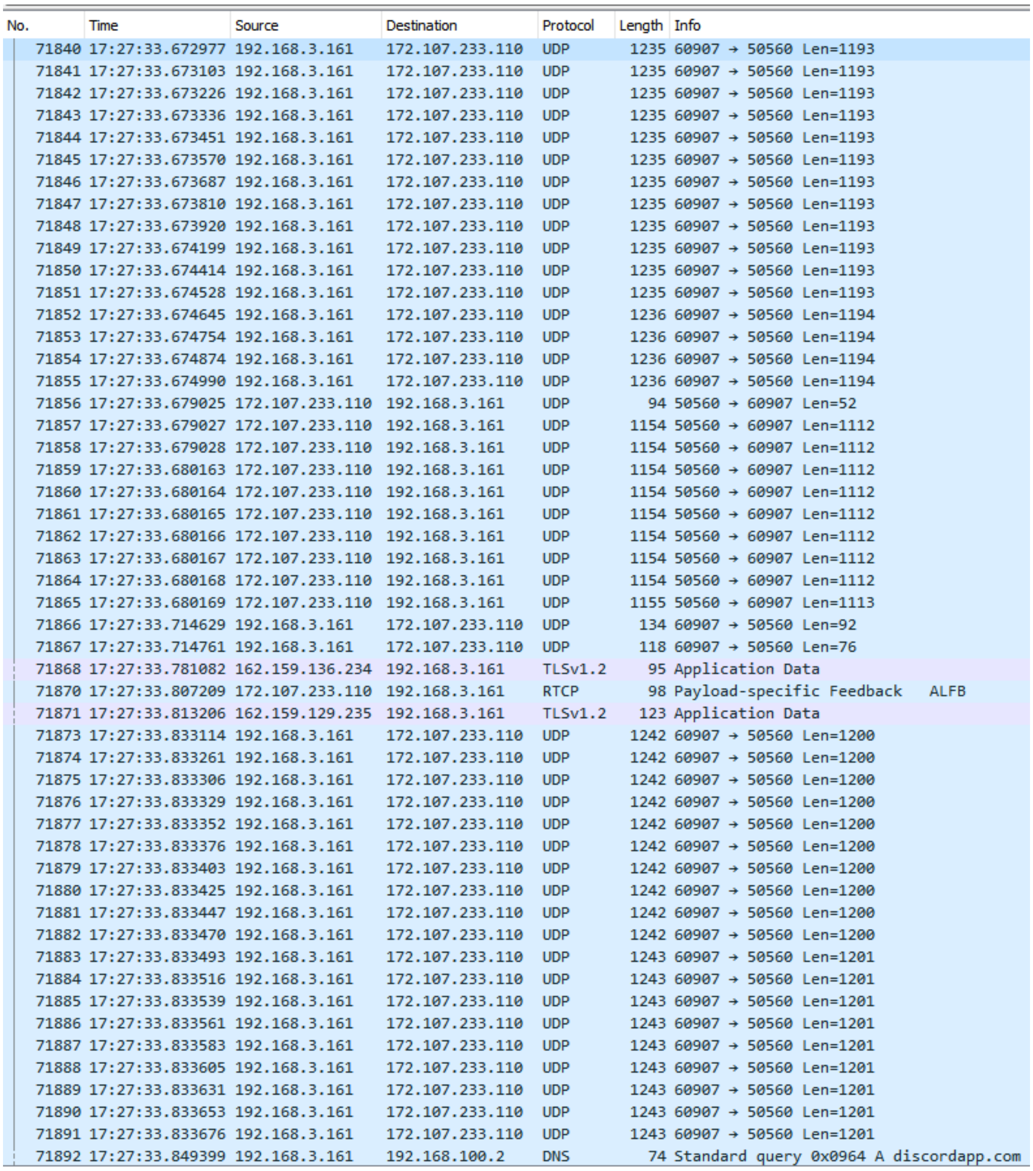
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
☑	192.168.3.161	ip.addr == 192....	🟥	Line	Packets		None

Because of the amount of packets captures it would be impossible for the author to go through every packet collected however by analysing the packets between different time frames the author has established which protocol each application uses for streaming. This can be determined by the massive increase in the packet type during VoIP (Voice over IP), samples of this traffic can be seen in tables 40, 41, and 42. During both the voice call and streaming discord used UDP (User Datagram Protocol) packets to share information. Throughout both the streaming sessions on Twitch TCP (Transmission Control Protocol) was used to transmit information. On steam UDP was used to share data during the voice call between Main-Device and Secondary-Device. However, while watching the stream from Secondary-device, Main-Device received many TCP packets. Both TCP and UDP are the two most common video streaming protocols (Sahraoui, Y. et al. 2018).

Figure 40 - Activity: Discord VoIP

Discord		
Device	**Activity**	**Date/Time**
Main-Device	Send voice call request to icp.seconddevice2020	17:25
Main-Device and Secondary-Device	Keep video chat active for 1 minute (video and audio)	17:27
˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅	˅ ˅	˅ ˅ ˅ ˅ ˅ ˅ ˅˅ ˅
Main-Device	Send video call request to icp.seconddevice2020	17:34
Secondary-Device	Accept video call request	17:34
Main-Device and Secondary-Device	Keep Discord call active for 15 minutes (video and audio)	17:34-17:48

A small sample of the UDP packets sent/receved during the the voice call:

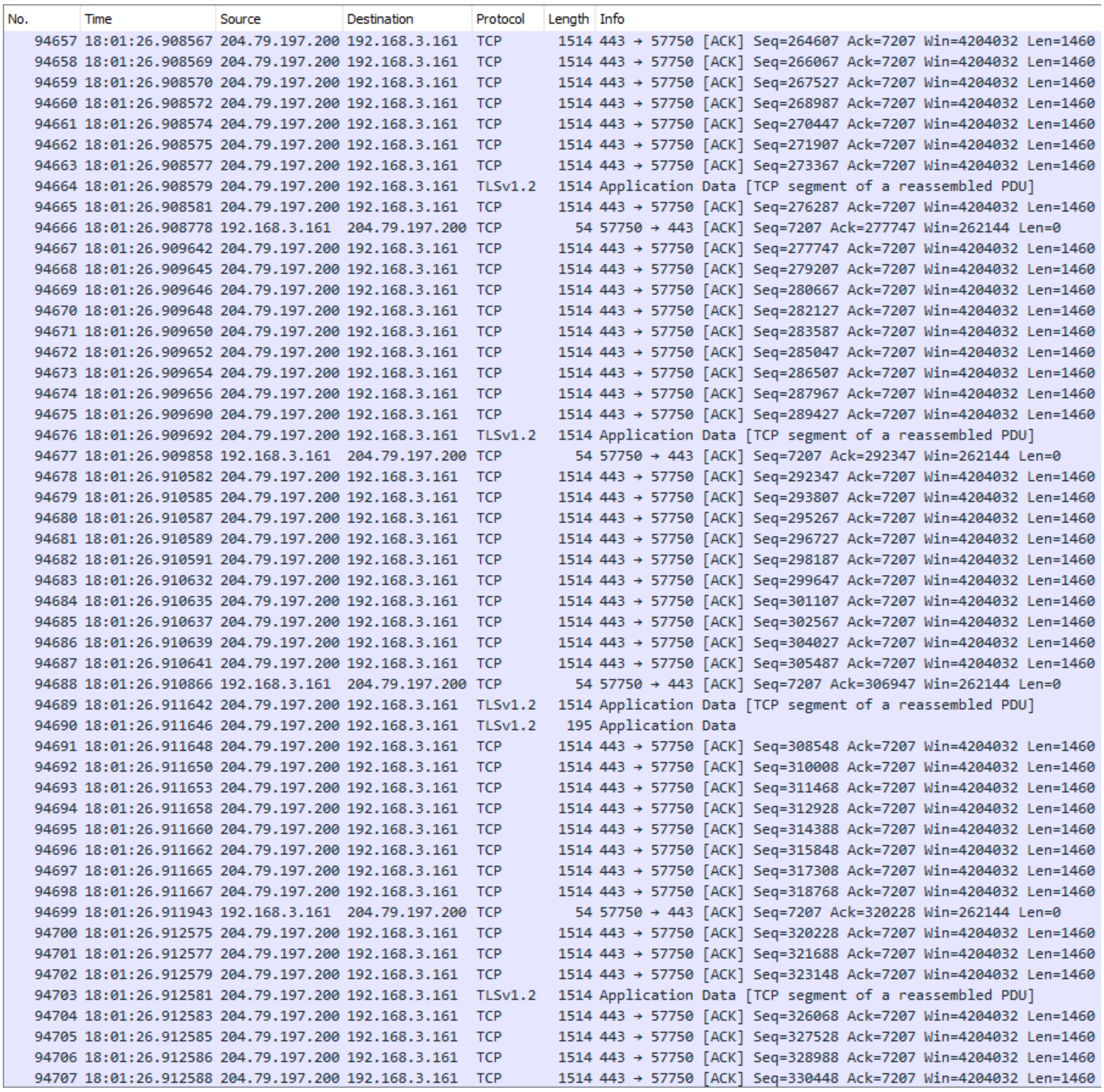


```
No.   Time            Source          Destination     Protocol Length Info
71840 17:27:33.672977 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71841 17:27:33.673103 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71842 17:27:33.673226 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71843 17:27:33.673336 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71844 17:27:33.673451 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71845 17:27:33.673570 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71846 17:27:33.673687 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71847 17:27:33.673810 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71848 17:27:33.673920 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71849 17:27:33.674199 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71850 17:27:33.674414 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71851 17:27:33.674528 192.168.3.161   172.107.233.110 UDP      1235 60907 → 50560 Len=1193
71852 17:27:33.674645 192.168.3.161   172.107.233.110 UDP      1236 60907 → 50560 Len=1194
71853 17:27:33.674754 192.168.3.161   172.107.233.110 UDP      1236 60907 → 50560 Len=1194
71854 17:27:33.674874 192.168.3.161   172.107.233.110 UDP      1236 60907 → 50560 Len=1194
71855 17:27:33.674990 192.168.3.161   172.107.233.110 UDP      1236 60907 → 50560 Len=1194
71856 17:27:33.679025 172.107.233.110 192.168.3.161   UDP        94 50560 → 60907 Len=52
71857 17:27:33.679027 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71858 17:27:33.679028 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71859 17:27:33.680163 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71860 17:27:33.680164 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71861 17:27:33.680165 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71862 17:27:33.680166 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71863 17:27:33.680167 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71864 17:27:33.680168 172.107.233.110 192.168.3.161   UDP      1154 50560 → 60907 Len=1112
71865 17:27:33.680169 172.107.233.110 192.168.3.161   UDP      1155 50560 → 60907 Len=1113
71866 17:27:33.714629 192.168.3.161   172.107.233.110 UDP       134 60907 → 50560 Len=92
71867 17:27:33.714761 192.168.3.161   172.107.233.110 UDP       118 60907 → 50560 Len=76
71868 17:27:33.781082 162.159.136.234 192.168.3.161   TLSv1.2    95 Application Data
71870 17:27:33.807209 172.107.233.110 192.168.3.161   RTCP       98 Payload-specific Feedback   ALFB
71871 17:27:33.813206 162.159.129.235 192.168.3.161   TLSv1.2   123 Application Data
71873 17:27:33.833114 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71874 17:27:33.833261 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71875 17:27:33.833306 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71876 17:27:33.833329 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71877 17:27:33.833352 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71878 17:27:33.833376 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71879 17:27:33.833403 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71880 17:27:33.833425 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71881 17:27:33.833447 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71882 17:27:33.833470 192.168.3.161   172.107.233.110 UDP      1242 60907 → 50560 Len=1200
71883 17:27:33.833493 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71884 17:27:33.833516 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71885 17:27:33.833539 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71886 17:27:33.833561 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71887 17:27:33.833583 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71888 17:27:33.833605 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71889 17:27:33.833631 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71890 17:27:33.833653 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71891 17:27:33.833676 192.168.3.161   172.107.233.110 UDP      1243 60907 → 50560 Len=1201
71892 17:27:33.849399 192.168.3.161   192.168.100.2   DNS        74 Standard query 0x0964 A discordapp.com
```

Figure 41 – Activity: Twitch VoIP

Twitch		
Device	**Activity**	**Date/Time**
Secondary-Device	Using Twitch Studio start streaming (With audio and video enabled)	17:51-17:52
Main-Device	Go to seconddevice2020 profile and view stream	17:51-17:52
Secondary-Device	Keep Steam active 1 minute	17:51-17:52
ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ	ˇ ˇ	ˇ ˇ ˇ ˇ ˇ ˇ ˇ ˇ
Main-Device	Set-up and start streaming “Entire Screen” using Twitch Studio (With audio and video enabled)	17:57
Main-Device	Keep Stream active for 10 minutes	17:57-18:07

A small sample of the TCP packets sent/receved during the the Stream from Main-Device:

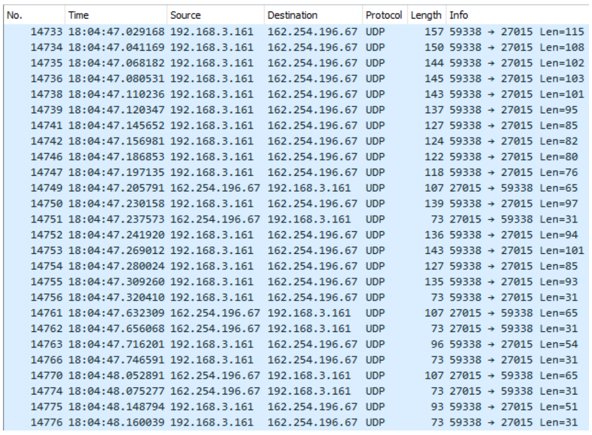


```
No.     Time            Source         Destination    Protocol Length Info
  94657 18:01:26.908567 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=264607 Ack=7207 Win=4204032 Len=1460
  94658 18:01:26.908569 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=266067 Ack=7207 Win=4204032 Len=1460
  94659 18:01:26.908570 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=267527 Ack=7207 Win=4204032 Len=1460
  94660 18:01:26.908572 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=268987 Ack=7207 Win=4204032 Len=1460
  94661 18:01:26.908574 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=270447 Ack=7207 Win=4204032 Len=1460
  94662 18:01:26.908575 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=271907 Ack=7207 Win=4204032 Len=1460
  94663 18:01:26.908577 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=273367 Ack=7207 Win=4204032 Len=1460
  94664 18:01:26.908579 204.79.197.200 192.168.3.161  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
  94665 18:01:26.908581 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=276287 Ack=7207 Win=4204032 Len=1460
  94666 18:01:26.908778 192.168.3.161  204.79.197.200 TCP        54 57750 → 443 [ACK] Seq=7207 Ack=277747 Win=262144 Len=0
  94667 18:01:26.909642 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=277747 Ack=7207 Win=4204032 Len=1460
  94668 18:01:26.909645 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=279207 Ack=7207 Win=4204032 Len=1460
  94669 18:01:26.909646 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=280667 Ack=7207 Win=4204032 Len=1460
  94670 18:01:26.909648 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=282127 Ack=7207 Win=4204032 Len=1460
  94671 18:01:26.909650 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=283587 Ack=7207 Win=4204032 Len=1460
  94672 18:01:26.909652 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=285047 Ack=7207 Win=4204032 Len=1460
  94673 18:01:26.909654 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=286507 Ack=7207 Win=4204032 Len=1460
  94674 18:01:26.909656 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=287967 Ack=7207 Win=4204032 Len=1460
  94675 18:01:26.909690 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=289427 Ack=7207 Win=4204032 Len=1460
  94676 18:01:26.909692 204.79.197.200 192.168.3.161  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
  94677 18:01:26.909858 192.168.3.161  204.79.197.200 TCP        54 57750 → 443 [ACK] Seq=7207 Ack=292347 Win=262144 Len=0
  94678 18:01:26.910582 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=292347 Ack=7207 Win=4204032 Len=1460
  94679 18:01:26.910585 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=293807 Ack=7207 Win=4204032 Len=1460
  94680 18:01:26.910587 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=295267 Ack=7207 Win=4204032 Len=1460
  94681 18:01:26.910589 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=296727 Ack=7207 Win=4204032 Len=1460
  94682 18:01:26.910591 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=298187 Ack=7207 Win=4204032 Len=1460
  94683 18:01:26.910632 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=299647 Ack=7207 Win=4204032 Len=1460
  94684 18:01:26.910635 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=301107 Ack=7207 Win=4204032 Len=1460
  94685 18:01:26.910637 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=302567 Ack=7207 Win=4204032 Len=1460
  94686 18:01:26.910639 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=304027 Ack=7207 Win=4204032 Len=1460
  94687 18:01:26.910641 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=305487 Ack=7207 Win=4204032 Len=1460
  94688 18:01:26.910866 192.168.3.161  204.79.197.200 TCP        54 57750 → 443 [ACK] Seq=7207 Ack=306947 Win=262144 Len=0
  94689 18:01:26.911642 204.79.197.200 192.168.3.161  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
  94690 18:01:26.911646 204.79.197.200 192.168.3.161  TLSv1.2   195 Application Data
  94691 18:01:26.911648 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=308548 Ack=7207 Win=4204032 Len=1460
  94692 18:01:26.911650 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=310008 Ack=7207 Win=4204032 Len=1460
  94693 18:01:26.911653 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=311468 Ack=7207 Win=4204032 Len=1460
  94694 18:01:26.911658 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=312928 Ack=7207 Win=4204032 Len=1460
  94695 18:01:26.911660 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=314388 Ack=7207 Win=4204032 Len=1460
  94696 18:01:26.911662 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=315848 Ack=7207 Win=4204032 Len=1460
  94697 18:01:26.911665 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=317308 Ack=7207 Win=4204032 Len=1460
  94698 18:01:26.911667 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=318768 Ack=7207 Win=4204032 Len=1460
  94699 18:01:26.911943 192.168.3.161  204.79.197.200 TCP        54 57750 → 443 [ACK] Seq=7207 Ack=320228 Win=262144 Len=0
  94700 18:01:26.912575 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=320228 Ack=7207 Win=4204032 Len=1460
  94701 18:01:26.912577 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=321688 Ack=7207 Win=4204032 Len=1460
  94702 18:01:26.912579 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=323148 Ack=7207 Win=4204032 Len=1460
  94703 18:01:26.912581 204.79.197.200 192.168.3.161  TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
  94704 18:01:26.912583 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=326068 Ack=7207 Win=4204032 Len=1460
  94705 18:01:26.912585 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=327528 Ack=7207 Win=4204032 Len=1460
  94706 18:01:26.912586 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=328988 Ack=7207 Win=4204032 Len=1460
  94707 18:01:26.912588 204.79.197.200 192.168.3.161  TCP      1514 443 → 57750 [ACK] Seq=330448 Ack=7207 Win=4204032 Len=1460
```

Figure 42– Activity: Steam VoIP

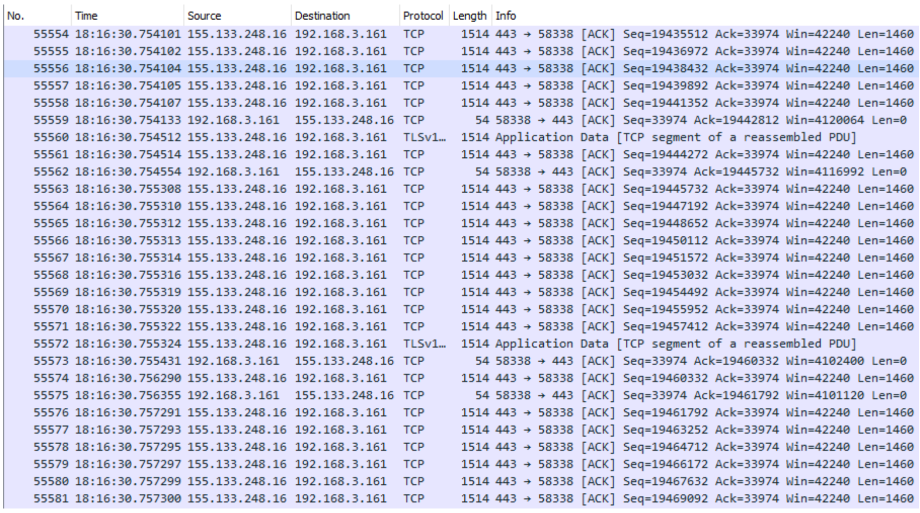
Steam (Attempt 3)		
Device	**Activity**	**Date/Time**
Main-Device	Send voice chat request to icp.seconddevice2020	18:04
Secondary-Device	Accept voice chat request	18:04
Main-Device and Secondary-Device	Keep voice chat active for 1 minute	18:05
˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅	˅ ˅	˅ ˅ ˅ ˅ ˅ ˅ ˅ ˅
Main-Device	Open “Rubi The Wayward Mira” from Steams game library	18:08
Main-Device	Send icp.seconddevice2020 an invite to watch	18:08
Secondary-Device	Open “Rubi The Wayward Mira” from Steams game library and send icp.maindevice2020 an invite to watch	18:13
Main-Device	Accept invite to watch	18:13
Main-Device and Secondary-Device	Keep Steam Broadcast active for 10 minutes	18:13-18:23

A small sample of the UDP packets sent/receved during the voice call:



```
No.   Time            Source          Destination     Protocol Length Info
14733 18:04:47.029168 192.168.3.161   162.254.196.67  UDP      157 59338 → 27015 Len=115
14734 18:04:47.041169 192.168.3.161   162.254.196.67  UDP      150 59338 → 27015 Len=108
14735 18:04:47.068182 192.168.3.161   162.254.196.67  UDP      144 59338 → 27015 Len=102
14736 18:04:47.080531 192.168.3.161   162.254.196.67  UDP      145 59338 → 27015 Len=103
14738 18:04:47.110236 192.168.3.161   162.254.196.67  UDP      143 59338 → 27015 Len=101
14739 18:04:47.120347 192.168.3.161   162.254.196.67  UDP      137 59338 → 27015 Len=95
14741 18:04:47.145652 192.168.3.161   162.254.196.67  UDP      127 59338 → 27015 Len=85
14742 18:04:47.156981 192.168.3.161   162.254.196.67  UDP      124 59338 → 27015 Len=82
14746 18:04:47.186853 192.168.3.161   162.254.196.67  UDP      122 59338 → 27015 Len=80
14747 18:04:47.197135 192.168.3.161   162.254.196.67  UDP      118 59338 → 27015 Len=76
14749 18:04:47.205791 162.254.196.67  192.168.3.161   UDP      107 27015 → 59338 Len=65
14750 18:04:47.230158 192.168.3.161   162.254.196.67  UDP      139 59338 → 27015 Len=97
14751 18:04:47.237573 162.254.196.67  192.168.3.161   UDP       73 27015 → 59338 Len=31
14752 18:04:47.241920 192.168.3.161   162.254.196.67  UDP      136 59338 → 27015 Len=94
14753 18:04:47.269012 192.168.3.161   162.254.196.67  UDP      143 59338 → 27015 Len=101
14754 18:04:47.280024 192.168.3.161   162.254.196.67  UDP      127 59338 → 27015 Len=85
14755 18:04:47.309260 192.168.3.161   162.254.196.67  UDP      135 59338 → 27015 Len=93
14756 18:04:47.320410 192.168.3.161   162.254.196.67  UDP       73 59338 → 27015 Len=31
14761 18:04:47.632309 162.254.196.67  192.168.3.161   UDP      107 27015 → 59338 Len=65
14762 18:04:47.656068 162.254.196.67  192.168.3.161   UDP       73 27015 → 59338 Len=31
14763 18:04:47.716201 192.168.3.161   162.254.196.67  UDP       96 59338 → 27015 Len=54
14766 18:04:47.746591 192.168.3.161   162.254.196.67  UDP       73 59338 → 27015 Len=31
14770 18:04:48.052891 162.254.196.67  192.168.3.161   UDP      107 27015 → 59338 Len=65
14774 18:04:48.075277 162.254.196.67  192.168.3.161   UDP       73 27015 → 59338 Len=31
14775 18:04:48.148794 192.168.3.161   162.254.196.67  UDP       93 59338 → 27015 Len=51
14776 18:04:48.160039 192.168.3.161   162.254.196.67  UDP       73 59338 → 27015 Len=31
```

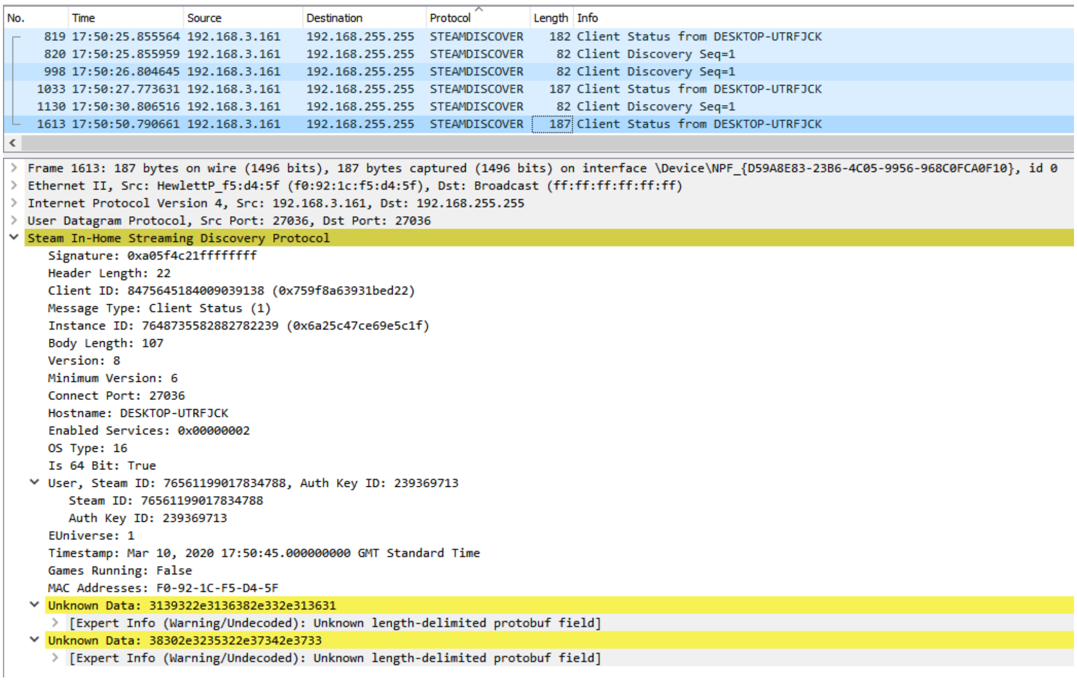
A small sample of the TCP packets sent/receved during the Streaming of Secondar-Device:



```
No.   Time            Source          Destination     Protocol Length Info
55554 18:16:30.754101 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19435512 Ack=33974 Win=42240 Len=1460
55555 18:16:30.754102 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19436972 Ack=33974 Win=42240 Len=1460
55556 18:16:30.754104 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19438432 Ack=33974 Win=42240 Len=1460
55557 18:16:30.754105 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19439892 Ack=33974 Win=42240 Len=1460
55558 18:16:30.754107 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19441352 Ack=33974 Win=42240 Len=1460
55559 18:16:30.754133 192.168.3.161   155.133.248.16  TCP        54 58338 → 443 [ACK] Seq=33974 Ack=19442812 Win=4120064 Len=0
55560 18:16:30.754512 155.133.248.16  192.168.3.161   TLSv1…   1514 Application Data [TCP segment of a reassembled PDU]
55561 18:16:30.754514 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19444272 Ack=33974 Win=42240 Len=1460
55562 18:16:30.754554 192.168.3.161   155.133.248.16  TCP        54 58338 → 443 [ACK] Seq=33974 Ack=19445732 Win=4116992 Len=0
55563 18:16:30.755308 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19445732 Ack=33974 Win=42240 Len=1460
55564 18:16:30.755310 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19447192 Ack=33974 Win=42240 Len=1460
55565 18:16:30.755312 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19448652 Ack=33974 Win=42240 Len=1460
55566 18:16:30.755313 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19450112 Ack=33974 Win=42240 Len=1460
55567 18:16:30.755314 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19451572 Ack=33974 Win=42240 Len=1460
55568 18:16:30.755316 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19453032 Ack=33974 Win=42240 Len=1460
55569 18:16:30.755319 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19454492 Ack=33974 Win=42240 Len=1460
55570 18:16:30.755320 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19455952 Ack=33974 Win=42240 Len=1460
55571 18:16:30.755322 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19457412 Ack=33974 Win=42240 Len=1460
55572 18:16:30.755324 155.133.248.16  192.168.3.161   TLSv1…   1514 Application Data [TCP segment of a reassembled PDU]
55573 18:16:30.755431 192.168.3.161   155.133.248.16  TCP        54 58338 → 443 [ACK] Seq=33974 Ack=19460332 Win=4102400 Len=0
55574 18:16:30.756290 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19460332 Ack=33974 Win=42240 Len=1460
55575 18:16:30.756355 192.168.3.161   155.133.248.16  TCP        54 58338 → 443 [ACK] Seq=33974 Ack=19461792 Win=4101120 Len=0
55576 18:16:30.757291 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19461792 Ack=33974 Win=42240 Len=1460
55577 18:16:30.757293 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19463252 Ack=33974 Win=42240 Len=1460
55578 18:16:30.757295 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19464712 Ack=33974 Win=42240 Len=1460
55579 18:16:30.757297 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19466172 Ack=33974 Win=42240 Len=1460
55580 18:16:30.757299 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19467632 Ack=33974 Win=42240 Len=1460
55581 18:16:30.757300 155.133.248.16  192.168.3.161   TCP      1514 443 → 58338 [ACK] Seq=19469092 Ack=33974 Win=42240 Len=1460
```

During the Steam capture of network traffic a usual packet was captures, the STEAMDISCOVER protocol. Not much information about this protocol is available but the packets contain details into Main-device and its Steam account, seen in figure 43 (Onsongo, N. et al. 2018).

Figure 43 - STEAMDISCOVER protocol



```
No.   Time            Source         Destination     Protocol       Length Info
  819 17:50:25.855564 192.168.3.161  192.168.255.255 STEAMDISCOVER     182 Client Status from DESKTOP-UTRFJCK
  820 17:50:25.855959 192.168.3.161  192.168.255.255 STEAMDISCOVER      82 Client Discovery Seq=1
  998 17:50:26.804645 192.168.3.161  192.168.255.255 STEAMDISCOVER      82 Client Discovery Seq=1
 1033 17:50:27.773631 192.168.3.161  192.168.255.255 STEAMDISCOVER     187 Client Status from DESKTOP-UTRFJCK
 1130 17:50:30.806516 192.168.3.161  192.168.255.255 STEAMDISCOVER      82 Client Discovery Seq=1
 1613 17:50:50.790661 192.168.3.161  192.168.255.255 STEAMDISCOVER     187 Client Status from DESKTOP-UTRFJCK

> Frame 1613: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface \Device\NPF_{D59A8E83-23B6-4C05-9956-968C0FCA0F10}, id 0
> Ethernet II, Src: HewlettP_f5:d4:5f (f0:92:1c:f5:d4:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.3.161, Dst: 192.168.255.255
> User Datagram Protocol, Src Port: 27036, Dst Port: 27036
v Steam In-Home Streaming Discovery Protocol
    Signature: 0xa05f4c21ffffffff
    Header Length: 22
    Client ID: 8475645184009039138 (0x759f8a63931bed22)
    Message Type: Client Status (1)
    Instance ID: 7648735582882782239 (0x6a25c47ce69e5c1f)
    Body Length: 107
    Version: 8
    Minimum Version: 6
    Connect Port: 27036
    Hostname: DESKTOP-UTRFJCK
    Enabled Services: 0x00000002
    OS Type: 16
    Is 64 Bit: True
  v User, Steam ID: 76561199017834788, Auth Key ID: 239369713
      Steam ID: 76561199017834788
      Auth Key ID: 239369713
    EUniverse: 1
    Timestamp: Mar 10, 2020 17:50:45.000000000 GMT Standard Time
    Games Running: False
    MAC Addresses: F0-92-1C-F5-D4-5F
  v Unknown Data: 3139322e3136382e332e313631
    > [Expert Info (Warning/Undecoded): Unknown length-delimited protobuf field]
  v Unknown Data: 38302e3235322e37342e3733
    > [Expert Info (Warning/Undecoded): Unknown length-delimited protobuf field]
```

To summarise, Wireshark was used to capture all of the network traffic while the applications were running. Wireshark was set up before each session was started, and then used to transfer all network traffic to the external hard drive after the session. All the network traffic was comprised of network packets, which are small units that contain certain information. There were over 740,000 packets transferred during the sessions, so exhaustive searching was required to find relevant packets. Of these packets, 469501 were from the Discord session, 127126 were from Twitch and 145120 were from Steam. The main types of packets sent throughout the streaming and video calls for Discord were UDP (User Datagram Protocol), for Twitch where TCP (Transmission Control Protocol) and for Steam were a mix of both.

Table 3 – Data retrieved from network traffic

Key	
Not retrieved	🟥
Partially retrieved	🟧
Retrieved	🟩

Application	Login	Text based messages	URL message	Image message	Video message	1 min VOIP	10 min VOIP
Discord	🟥	🟥	🟥	🟥	🟥	🟧	🟧
Twitch	🟥	🟥	🟥	N/A	N/A	🟧	🟧
Steam	🟥	🟥	🟥	🟥	N/A	🟧	🟧

Chapter 7: Evaluation

Discussion and evaluation of findings

The aim of this project was to investigate and compare the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform. As expected, most of the forensics artefacts collected from the applications were found on the clone of the hard-drive. Artefacts were also collected from volatile memory, however, this sources collected did not provide as much data as the author had expected. The least useful source of data was the network traffic captures as the author could not find much information relating to the applications in the data collected.

However, the artefacts found do allow the author to establish a basis for the recoverable forensic artefacts from the three applications. The data creation process (see figure 49) created artefacts relating to each application that can be sorted into 3 subsections; messages, media and video calls/streaming.

Not all messages were recoverable using hard drive cloning. Of the 14 messages successfully sent between Main-Device and Secondary-Device during data creation on the hard-drive none of the messages containing URLs were recovered and only data related to one text-based message on each application was found; in most cases this recovered data only contained a partial message. For example, in the message "Twitch 1 Ad meliora" sent from Main-Device to Secondary-Device over Twitch whisper only the first part of the message was recovered in the pagefile.sys file (figure 25). The same issue was found with data relating to Discord messages, in the message "Discord 4 Audentes fortuna iuvat" sent from Main-Device to Secondary-Device, once again only the first part of the message was recovered; this time in a log file (see figure 17). In fact, Steam is the only application where a message was fully recovered; this message was found in the applications cache file and is the only message sent from Secondary-Device that was recovered. No data relating to any of the text based or URL messages were found in the volatile memory or network traffic captures. It is clear that on all three applications recovery of data relating to text based and URL messages is difficult and not always possible. In the authors opinion the most difficult application to recover this data from is Twitch as the pagefile.sys file is extremely large and hard to read as it contains many forms of data from different sources.

In the data creation plan messages containing images and videos were to be sent from Secondary-Device to Main-Device over Steam and Discord. Twitch was not included in this comparison as the application does not currently support this type of message. The video message on Steam failed, meaning that although artefacts relating to the video message on Discord were found in both the data collected from the hard-drive (figure 5) and the volatile memory (figure 35) a comparison on the recoverable forensic artefacts relating to this type of message cannot be made. On the other hand, both messages containing images were successful and good quality copies of these images were found in both of the applications corresponding cache files (figures 3, 4 and 10). A version of the image shared over discord was also found in the volatile memory capture, however, this version was heavily corrupted (figure 35). However, no data relating to the image shared over steam was found in its volatile memory capture.

The data collected regarding video calls, audio calls and streaming sessions conducted on the applications was extremely limited. The issues with Steam which meant that a stream was not possible from Main-Device, resulting in a balanced comparison on this application compared to Twitch and Discord not being possible. On the cloned hard drive, the only application that provided solid data relating to streaming activity was Twitch. The 22 files found in the Twitch cache files relating to the streaming session from secondary-device (figures 7 and 6) together are a solid source for establishing what Main-Device was viewing and hearing during the stream. The largest source of data seems to be the network traffic captures for each application. However, the author does not have the experience or resources to analyse this data further so a comparison cannot be made from this.

Although the volatile memory and network traffic analysis did not provide as much data as the hard-drive analysis; the overall analysis has allowed the author to establish many of recoverable forensic artefacts from Discord, Twitch and Steam. This has therefore allowed them to create a comparison of the artefacts across the applications. Of all the applications, Steam left the greatest mark across all of the data sources collected from the cloned hard drive, even with the issues the author faced with creating data on this application. On the Hard-drive it was clear Steam has the most complex file structure of the three applications and left more sources for data to be found such as the applications unique VDF (Valve Data File) format (figures 20, 21 and 22). The application also left a clear mark of its presence on the volatile memory and network traffic analysis with the STEAMWEBHELPER.EXE file (figure 34) and STEAMDISCOVER protocol (figure 43). On the other hand, the Discord application created the most data with the most substance in the volatile memory with the data from images and video still being present even with corruption (figure 35).

The artefacts gathered from Main-Device are as accurate as they can be for this study. No changes were made by the author to the data collected, however, other issues can cause data to be changed or removed. To combat against this, data found on Encase was cross referenced using AXIOM to validate it. However, volatile memory and network traffic were not validated. The volatile memory should have been validated using forensics software such as Autopsy or Encase and the network traffic should have been validated using another packet analyser such as Cloudshark. The only reason this wasn't done was due to the authors inexperience with these types of forensics analysis methods and software. Gaining familiarization of further systems would have been too time consuming for this project.

The issues the author encountered with the Steam application has decreased the reliability of the findings. Because less data was able to be created for the application, there are areas of each application that could not be fully analysed and compared; these being video messages, live streaming and sending messages during live streaming. There was a similar issue with the Twitch application as while conducting research for the data creation plan the author discovered this application had less features than originally thought. For example, the application does not have support for video or image messages and does not have a video or voice calling system. This meant that although Discord and Steam have those features a comparison could not be made against the Twitch application. There is no solution to the features on the Twitch application however; the data creation for the Steam application could have been re-done although this was not possible for this study as it would have meant erasing the data created for Discord and

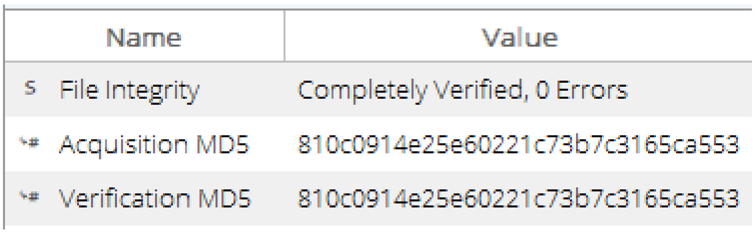
Twitch and re-doing these applications which would have severely impacted the time scale of the entire project.

Another issue that could affect the reliably of the results is that data was only created and analysed on one computer. There is a strong possibility that the data created by the applications can contrast in different situations and different systems even when computers are using the same operating system. For example, the files pagefile.sys (Figure25) and $LogFile (Figure 23). The best solution to this problem would be to run multiple tests on multiple devices and comparing the recoverable artefacts from each application across all the devices but this would be time consuming. However, a further issue is that on Main-Device the three applications studied were the only software downloaded and used. This significantly decreased the amount of overlapping data from other applications. In everyday use, a computer would be used for a multitude of things which could change or remove files and folders, meaning that the usability of some sources of data found in this study may differ with normal use.

Evaluation of tools and methods

The forensics platform Encase v8 was used to process and analyse all of the physical data collected from the hard-drive. This software performed very well and allowed the author to efficiently gather and report data in a comprehensible format. Encase v8 comes with many tools which were used to support this investigation including a report generation tool, bookmarking system and many tools for extracting and sorting data. Encase v8 allowed the author to verify the data files collected from Main-Device to ensure they had not been changed in any way. This verification created a MD5 hash which can be compared to the acquisition MD5 hash to ensure successful verification (See figure 44).

Figure 44– Encase Verification



Name	Value
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	810c0914e25e60221c73b7c3165ca553
Verification MD5	810c0914e25e60221c73b7c3165ca553

Magnet RAM Capture was used to collect all the volatile memory from Main-Device at the end of each data creation session. This software was extremely efficient at collecting the volatile memory. Magnet RAM Capture is portable software which means that it was loaded from an external Hard-drive. This limits contamination of the files on Main-Device.

Once the volatile memory data was collected, AXIOM Examine was used to process and analyse this data. This software proved to be well equipped for analysis of volatile memory. It has a user-friendly interface which assisted the authors inexperience with volatile memory knowledge prior to this study. AXIOM Examine provides a timeline generation tool, a summary of artefacts tool, and a keyword search tool which greatly allowed for efficient gathering of evidence. The software also allowed all three collections of volatile memory to be loaded onto one case and allowed comparisons between the applications within one instance of AXIOM Examine, creating a more productive analysis. AXIOM Examine was also used to verify the data collected from Encase v8, and no irregularities were found in the data.

The open source software Wireshark was used to both collect and analyse the Network Traffic. As with Magnet RAM Capture, Wireshark is a portable software enabling it to be loaded from an external hard-drive, reducing its impact on the files on Main-Device. The software was initialised at the start of each data creation and continued to run in the background with minimal disruption. Although the author has prior experience using Wireshark, they struggled to utilise the software for a forensics analysis, this software may be more appropriate for a person more experienced in network traffic forensics.

The ACPO (Association of Chief Police Officers) Good Practice Guide for Digital Evidence was successfully followed where possible throughout this project; although not all the principles defined in the guidelines were appropriate for this study as they were developed for real life cases. It is important to use this guideline as it is the current guide followed by United Kingdom digital forensics police. The guideline "That no action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court" (Williams, J. 2012) was followed during data creation to ensure the data collected was reliable and has integrity.

The ADFM (Abstract Digital Forensic Model) was also followed throughout this project. Each phase of this model which the author identified as required was completed. Following this model provided the author with a structured process for each step of the analysis and ensured the order of analysis was correct. As this model is designed for real forensics cases many of the phases were not applicable in this study so these were excluded.

Comparing to other work

Although not much research is available into forensics analysis of these applications, comparisons can be made against two papers which are somewhat related to this study. The first is "Forensics Analysis of an On-line Game over Steam Platform" by Tabuyo-Benito, R et al. This report contains a forensics analysis of a video game running on the Steam platform with a focus on recovering data relating to the "chatting features" within the video game. Similar to this study, Tabuyo-Benito, R et al. collected data from the hard-drive, volatile memory and network of a computer.

Their analysis of the hard drive revealed "configuration and log files that provide information such as the Steam UserID, the Steam ID of the game" which included the files config.vdf, loginusers.vdf and localconfig.vdf. The loginusers.vdf and localconfig.vdf files are both discovered on Main-Device that hold data relating to the Steam account (Figures 20 and 21) and the data found within these files on Main-Device seems to match up with the data found within by the Tabuyo-Benito, R et al.. The file config.vdf was present on Main-Device, however, this file was largely unreadable and didn't contain data of reliance, whereas the authors of "Forensics Analysis of an On-line Game over Steam Platform" found this file contained the userID and the username of their Steam account. This suggests the content of this file and possibly other files can differ which will mean their usability could vary wildly on a case-to -case basis. Another file that Tabuyo-Benito, R et al. found is connections.txt, this file was found in the \Program Files (x86)\Steam\logs\ path and apparently "contains all the remote connections with the user's PC" including host names and IP addresses. On Main-Device this file could not be found, again suggesting files can differ on a case to case basis (Tabuyo-Benito , R. et al. 2019).

The network forensics analysis conducted by Tabuyo-Benito, R et al. discovered two cookies sent over HTTP, called sessionid and steamLogin. These cookies are apparently used “for user identification” and assign identification purposes. However, these were not found in the analysis of the Network traffic gathered from Main-Device (Tabuyo-Benito , R. et al. 2019).

The second study which is somewhat related to this study is “Investigating whether any forensics artefacts can be retrieved from a selection of social gaming applications on different mobile devices” by McStraw, M. This study contains a forensics analysis of the Discord and Twitch application on a mobile device. As this analysis was conducted on the mobile application for Discord, much of the data found by McStraw will not correspond to the data found on Main-Device. On the Android phone analysed by McStraw, items were found in the cache folder for Discord and Twitch, including images. This is similar to the data found in the Discord cache folder on Main-Device, as both images and videos were recovered here (figures 3, 4 and 5). However, as images are not sharable on the Twitch application for computers this cannot be compared to the application for mobile phones. Another file that McStraw found in the Discord cache is Store_messages_cache_V17. This file was found to contain partial text based messages with timestamp. This file was not found on Main-Device, so it is possible it is only used to store data on mobile devices (McStraw, M. 2018).

Evaluation of the project process

In order to succeed in the aim of this project a lot of planning and organising had be put in both before and during the process.

One of the planning phases that occurred in advance was the creation of the Terms of Reference. This was created to define the purpose and structure of the project and the research it entails; and can be seen in the appendices. As part of the Terms of Reference, eight objectives were established in order to ensure that the goal of the project was fully completed.

The first object was to research and give context to the selection of applications and their live streaming capabilities. This objective was completed in chapter 2 of this report; the author researched the applications and the features they have. Each of the features were considered for use during the data creation so that a fair comparison could be made across all three applications.

The next objective was to research the illicit activities of the malicious users of these platforms. In chapter 3, the reach into the illicit activities on the applications is explained including the evidence of cyberbullying, malware, underage gambling, violent content, sexual content, grooming and child exploitation found on the applications. This object gave context to the importance of this research and provided some of the benefits the results will proved.

The third object was to research and provide background information relating to Windows 10 and the effects this operating system will have on the investigation, exploring possible forensics techniques that could be implemented. This objective was explored in chapter 4 where forensics techniques on a Windows 10 operating system were explored in detail.

This objective followed onto the fourth objective which was to create a thorough plan of how the investigation will be executed, including ethical issues, equipment use, investigation plan, and data analysis plan. Some of the planning included guidelines, methods and tools that would be used where established and explained in chapter 4. However, this objective continued into chapter 5 where the author established a detailed strategy for the execution of data creation and the software and tools that would be required to carry this out.

The fifth objective was to implement the investigation plans, documenting all results and collecting all relevant data. The documentation for carrying out of the plans can be seen in Figure 49, including issues that were faced during this implementation. Data was collected successfully during this time using Wireshark and Magnet RAM Capture as planned.

The next objective was to analyse the data collected and compare the data collected across each of the applications. This objective was completed in chapter 6 where all of the data found through the analysis is detailed and explained. The chapter also provides a comparison of the data found on each application. The seventh objective was to evaluate the findings, discussing the usefulness of the information and its real world implications. This objective was partially completed in the first half of the evaluation and will be continued into the conclusion. The last objective will also be completed in the conclusion;

the objective being to evaluate the areas of the project that could be improved and further work that could be implemented in the future.

Early in the project it was established that weekly meeting would be held between the author and their supervisor. These meetings were tracked using a project logbook which can be seen in appendices Figure 51. During each meeting it would be established what section of the research or report would be focused on for that week and often also plan for that project as a whole. The author made sure to always set aside some time every week to work on this project and balance the project and other work by setting personal weekly goals.

One of the ways the author ensured the study was carried out in a methodical manner was to ensure the six p's of research were considered throughout the project. The first P is "purpose", which is the reason for conducting the research and why it is important or useful to research this topic. As stated earlier the author believes this research is important because of the dangers these platforms can pose to vulnerable peoples; this is further detailed in chapter 2. The next P is "products"; this is the expected outcomes of the research; which in this project is this report, which details the author's findings. The third P is "Process" which is planning how the research is to be conducted. As started earlier, the process of this study can be simplified and compressed into four parts; these being research into to subject and applications, creation of the data onto the device to be studied, collection of this data using appropriate software and then analysis of this data. The fourth P is "participants" but, as this study does not involve anyone directly or indirectly except for the author and their supervisor, this was considered but deemed not required. The next P is "paradigm"; the paradigm the author has used is methodology. The last P is "presentation" which is how the research will be delivered and explained to others. However, in this project the "presentation" and "products" are one and the same (Oates, B. 2006).

Another important aspect that was established in the Terms of Reference was a project schedule. This project schedule is in the form of a Gantt chart which planned the weekly aims for the project between the week of the 28th October 2019 and week of the 27th of April 2020. Following this schedule would ensure the project was completed on time. The plan left roughly three weeks at the end to make up for any delays in other sections of the project and for proof reading and final changes. The Analysis and research chapters were completed and the Synthesis chapters started on schedule according to this plan. However, due to the issues with Steam the implementation of the data creation plan took longer than planned for. The author should have conducted more research into this application during the planning stage. Discovery of the financial requirements would have allowed more preparation and decreased the impact on the projects results as three attempts at data creation for Steam and the features that were unusable did have an impact in the overall results produced. Covid-19 also impacted the decision making process during this time as it was imperative a clone of Main-Device was taken prior to quarantine restrictions as this would cut off access all access to the device and make completing the project impossible.

The possibility was also established that quarantine restrictions would impact the authors access to the software required for analysis of the data created (Encase v8 and AXIOM examine). Time was taken out of the project plan to establish alternatives for the software. One of the alternatives was explored was AXIOM Examine portable cases. This method would have allowed the author to access some of AXIOM Examines features without requiring the full software; allowing the volatile memory analysis to continue and the hard-drive analysis to be completed on AXIOM Examine in place of Encase. However, the portable feature lacked many features, including direct access to the file structure of Main-Device which would be required to complete the hard-drive analysis. Another alternative researched was the forensics software Autopsy. Autopsy is a free multipurpose forensic toolkit that would have been used in place of Encase for analysis of the cloned data. Autopsy would have allowed access to the file system unlike AXIOM Examine. However, it was found that the type of clone taken from Main-Device was not currently supported on Autopsy so this software was not an option. Eventually, temporary software licences were provided for both Encase v8 and AXIOM examine so that they could be used from home.

The quarantine restrictions also resulted in a submission date changed for the project to the 14th May 2020 and then a further 10 working day extension was given to the author for personal circumstances. This provided more time than initially planned in the project schedule so the plan was changed to reflect this (see Figure 50). However, even with this extra time the author feels they should have set aside more time for researching and familiarizing themselves with Network forensics.

Prior to this study the author limited experience with volatile memory forensics and network forensics but throughout this study they have gained more knowledge into these fields. The author has also gained more competence with forensic software such as AXIOM Examine and Autopsy; which the author had limited familiarity with prior to this study.

Chapter 8: Conclusion

The overall purpose of this study was to investigate and compare the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform. The initial research for this investigation focused on the three applications, Discord, Twitch and Steam, and the many features they have. The author found many features for communication, like VoIP (Voice over IP) calling and live streaming; and also features for digital distribution, digital trading and financial transactions. It was important to study these features early on in order to determine which would be most beneficial to the study. Research was also conducted into the dangers of these application in order to highlight the importance of this study. The author found that threats such as cyberbullying, malware, violent content and child exploitation are present on each of these applications.

For this study, the operating system Windows 10 was chosen due to its popularity among users of Steam, Discord and Twitch. Research was conducted into the operating system and forensics techniques that could be used on this. It was also important to research volatile memory and network traffic forensic techniques as these are other sources of data that can be collected from a computer.

In order to procced with the investigation, a data creation plan was established. This defined that three separate uses of the computer would be conducted, each use focusing on a different application. During these sessions, Wireshark and Magnet RAM capture were used to collect network traffic and volatile memory. After the data creation plan was complete, a clone of the computer was taken so that the results could not be tampered with. The sessions were mostly successful, however, there were some issues with Steam that affected some of the planned activities on the platform.

The data collected from the computer was then analysed. On the clone the author found that most of the important information was found within the AppData folder, with the Local and Roaming folders splitting the content. Each application had a cache folder which contained images, videos and some messages. They also found LOG files, which track events that happen while the user is browsing the application, and unique file types such as VDF's (Valve Data Files); which can contain metadata information on the account for the Steam application.

Volatile memory did not provide as much useful data as the clone. The author found LNK (link) files, which store information about when applications are last accessed and which application they are linked to. Each application had an LNK file that was found; however, these displayed the incorrect timestamps. Media files were also found in volatile memory including the image and video sent over Discord. However, these were heavily corrupted.

Even less information was collected from the network traffic. However, this was mostly due to the authors inexperience with network forensics. Over 740,000 network packets were transferred during the sessions; 469,501 from the Discord session, 127,126 from the Twitch session and 145,120 from the Steam session. The author determined that the main type of packet sent during Discord calls/Steaming was UDP (User Datagram Protocol), whereas on Twitch was TCP (Transmission Control Protocol) and on Steam was a mix of both.

Future work

Within this project, the issues with the Steam application impacted the overall reliability of the results. The author believes a second attempt of this application would have greatly assisted the results produced. The author also believes more data could be gathered from the network traffic captures. However, at the current experience level this would require a lot more personal study into this form of forensics.

The applications, Discord, Twitch and Steam are capable of a lot more then just the features explored in this study. These applications are also typically used for a longer time frame than used in this study. The results collected from a study where these applications were used multiple times and with full use of all features for longer times would create results more accurate to real life investigations.

This study also only focused on the applications running on a Windows 10 computer, however, these applications also run on other operating systems and devices. An investigation and comparison into these applications across other operating systems and devices would be extremely beneficial.

Discord, Twitch and Steam may be three of the most popular video game applications, however, many more similar applications exist that were not discussed in this study. These could include the Xbox Live messaging service, Epic Games, and TeamSpeak. Investigating and comparing these applications with the data found in this report would help establish a better understanding of this data and possibly extend its usability.

References

Alwis, C. (2019). Windows Registry Analysis 101. [online] Forensic Focus. Available at: https://articles.forensicfocus.com/2019/04/05/windows-registry-analysis-101/ [Accessed January 2019].

Amari, K. (2009). Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. [online] SANS Institute, Pages 8-15. Available at: https://www.sans.org/reading-room/whitepapers/forensics/paper/33049 [Accessed January 2019].

Assael, S. (2017). Skin in the Game. ESPN, [online] Available at: http://www.espn.com/espn/feature/story/_/id/18510975/how-counter-strike-turned-teenager-compulsive-gambler [Accessed December 2019].

Baker v. State. (2011). [PDF] Texas: District Court McLennan County, pages 5-8. Available at: https://cases.justia.com/texas/tenth-court-of-appeals/10-10-00049-cr.pdf?ts=1370478213 [Accessed January 2020].

Bazara, B, Fatma, T. (Year published). Instant messaging: standards, protocols, applications, and research directions. [online] Nova Science Publishers Inc., Pages 1-2. Available at: https://www.researchgate.net/publication/280307922_Instant_Messaging_Standards_Protocols_Applications_and_Research_Directions [Accessed December 2019].

BBC. (2018). School shooting game Active Shooter pulled by Steam. BBC News, [online] Available at: https://www.bbc.co.uk/news/uk-44302146 [Accessed December 2019].

BitDegree, (2020). What Is JavaScript Used For And Why You Should Learn It. [online] Available at: https://www.bitdegree.org/tutorials/what-is-javascript-used-for/#What_Is_JavaScript_Used_For [Accessed March 2020].

Bitesize, (2017). Operating systems. [online] Available at: https://www.bbc.co.uk/bitesize/guides/ztcdtfr/revision/1 [Accessed January 2019].

BlagBag. (2017). Windows 10 Jump List Forensics. [Blog] Available at: https://www.blackbagtech.com/blog/windows-10-jump-list-forensics/ [Accessed January 2019].

Bolding, J (2019). Steam now has 30,000 games. [online] PC gamer. Available at: https://www.pcgamer.com/uk/Steam-now-has-30000-games/ [Accessed December 2019].

Borcia, S. (2019). McHenry man charged with soliciting child, possessing child porn. Lake McHenry Scanner, [online] Available at: https://www.lakemchenryscanner.com/2019/11/01/mchenry-man-charged-with-soliciting-child-possessing-child-porn/ [Accessed December 2019].

Cooper, K. (2019). Bianca Devins: The teenager whose murder was exploited for clicks. BBC News, [online] Available at: https://www.bbc.co.uk/news/world-us-canada-49002486 [Accessed December 2019].

DeSantis, M. (2006). Understanding Voice over Internet Protocol. [PDF] US-CERT, pages 1-2. Available at: https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf [Accessed December 2019].

Discord (2017). Discord Community Guidelines. [online] Available at: https://Discordapp.com/guidelines [Accessed December 2019].

BitDegree, (2020). What Is JavaScript Used For And Why You Should Learn It. [online] Available at: https://www.bitdegree.org/tutorials/what-is-javascript-used-for/#What_Is_JavaScript_Used_For [Accessed March 2020].

European Union Agency for Cybersecurity. (2019). Introduction to Network Forensics. Version 1.1. [PDF] pages 13-15. Available at: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf [Accessed January 2020].

Evans, P. (2019). Rape Day game pulled by Steam platform after outcry. BBC, [online] Available at: https://www.bbc.co.uk/news/blogs-trending-47484397 [Accessed December 2019].

Farmer, D. (2006). A Windows Registry Quick Reference: For the Everyday Examiner. [PDF] Vermont: Forensics Focus. Available at: https://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf [Accessed April 2020].

Fenlon, W. (2019). Steam now has 90 million monthly users. Pc gamer, [online]. Available at: https://www.pcgamer.com/uk/Steam-now-has-90-million-monthly-users/ [Accessed December 2019].

Fileinfo, (2020). VDF File Extension. [online] Available at: https://fileinfo.com/extension/vdf [Accessed April 2020].
Fisher, T (2020). What Is a LOG File?. [online] Lifewire. Available at: https://www.lifewire.com/what-is-an-log-file-2622770 [Accessed April 2020].

Fogel, S. (2018). Discord Turns Three, Hits 130 Million User Milestone. Variety, [online] Available at: https://variety.com/2018/gaming/news/Discord-turns-three-1202810983/ [Accessed December 2019].

FSLabs. (2014). A Twitch of Fate: Gamers Shamelessly Wiped Clean. [Blog] F-Secure Labs. Available at: https://archive.f-secure.com/weblog/archives/00002742.html [Accessed December 2019].

Gambling Commission. (2017a). Loot boxes within video games [online] pages. Available at: https://www.gamblingcommission.gov.uk/news-action-and-statistics/News/loot-boxes-within-video-games [Accessed December 2019].

Gambling Commission. (2017b). Virtual currencies, eSports and social casino gaming – position paper. [PDF] Available at: https://www.gamblingcommission.gov.uk/PDF/Virtual-currencies-eSports-and-social-casino-gaming.pdf [Accessed December 2019].

Gambling Commission. (2018). Young People & Gambling 2018. [PDF], Available at: https://www.gamblingcommission.gov.uk/PDF/survey-data/Young-People-and-Gambling-2018-Report.pdf [Accessed December 2019].

Glaze, V. (2019). Fortnite streamer banned after allegedly grooming children on Twitch. Dexerto, [online] Available at: https://www.dexerto.com/entertainment/fortnite-streamer-banned-allegedly-grooming-children-Twitch-763209 [Accessed December 2019].

Goslin, A. (2019). Discord's new Go Live feature will let users stream games to up to 10 friends. Polygon, [online] Available at: https://www.polygon.com/2019/8/9/20798559/Discord-go-live-private-stream-voice-channel [Accessed December 2019].

Gough, C (2018). Number of active PC gamers worldwide from 2014 to 2021. [online] Statista. Available at: https://www.statista.com/statistics/748072/number-pc-gamers-world-platform/ [Accessed December 2019].

Gough, C (2019). Share of Steam (gaming platform) users in October 2019, by operating system used. [online] Statista. Available at: https://www.statista.com/statistics/265033/proportion-of-operating-systems-used-on-the-online-gaming-platform-Steam/ [Accessed January 2020].

Haselton, T. Graham, M. (2019). About 2,200 people watched the German synagogue shooting on Amazon's Twitch. CNBC, [online] Available at: https://www.cnbc.com/2019/10/09/the-german-synagogue-shooting-was-streamed-on-Twitch.html [Accessed December 2019].

Hoffman, C (2017). What is the AppData Folder in Windows? [online] How-To Geek. Available at: https://www.howtogeek.com/318177/what-is-the-appdata-folder-in-windows/ [Accessed March 2020].

Houses of Parliament. (2016). Digital Forensics and Crime. [PDF] London: The Parliamentary Office of Science and Technology, page 1. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=13&ved=2ahUKEwi3vZSxy9noAhWNTxUIHWVuA9EQFjAMegQIBhAB&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FPOST-PN-0520%2FPOST-PN-0520.pdf&usg=AOvVaw1BmLjrNdtV1pAP-tN-XWpM [Accessed April 2020].

Infosec, (2018). What is Memory Forensics?. [online] Available at: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/memory-forensics/ [Accessed April 2020].

Kent, E. (2018). Unlicensed casino websites are being streamed on Twitch, UK gambling watchdog confirms. Eurogamer, [online] Available at: https://www.eurogamer.net/articles/2018-12-04-uk-gambling-watchdog-in-talks-with-Twitch-over-unlicensed-casino-site-streams [Accessed December 2019].

Klappenbach, M. (2019). Top 7 PC Game Digital Download Services. Lifewire, [online] Available at: https://www.lifewire.com/top-pc-game-digital-download-services-813065 [Accessed December 2019].

Lee, R. (2015). Windows Forensic Analysis Poster. Version 4.6. [PDF] DFIR Available at: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download [Accessed January 2019].

Live Action (2018). What Is a Network Packet? [Online]Available at: https://www.liveaction.com/blog/network-packet/ [Accessed April 2020].

Malwarebytes (2018). All about malware. [online]. Available at: https://www.malwarebytes.com/malware/ [Accessed December 2019].

Martin, C (2018). What is pagefile.sys? [Online] Available at: https://www.techadvisor.co.uk/how-to/windows/what-is-pagefilesys-3608749/ [Accessed April 2020]

Matyus, A (2019). Discord 'Spidey Bot' malware is stealing users' data, including passwords. [online] Digital Trends. Available at: https://www.digitaltrends.com/news/Discord-malware-spidey-bot-is-stealing-data-passwords-phone-numbers/ [Accessed December 2019].

McHenry Police Department. (2019). McHenry police arrest adult male in connection solicitaiton of a minor. [PDF] Available at: https://cityofmchenry.org/vertical/sites/%7B32BA702A-197A-429A-BC8D-0F4D5E307CAD%7D/uploads/PRESS_RELEASE_-_Marcinko_Arrest_110119.pdf [Accessed December 2019].

McQuaid, J. (2014a). Forensic Analysis of Prefetch files in Windows. [online] Magnet Forensics. Available at: https://www.magnetforensics.com/blog/forensic-analysis-of-prefetch-files-in-windows/ [Accessed January 2019].

McQuaid, J. (2014b). Forensic Analysis of LNK files. [online] Magnet Forensics. Available at: https://www.magnetforensics.com/blog/forensic-analysis-of-lnk-files/ [Accessed April 2020].

McStraw, M. (2018). Investigating whether any forensics artefacts can be retrieved from a selection of social gaming applications on different mobile devices. Northumbria University. [Accessed April 2020]

Microsoft, (2019). Windows registry information for advanced users. [online] Available at: https://support.microsoft.com/en-gb/help/256986/windows-registry-information-for-advanced-users [Accessed April 2020].

Morris, D. (2016). Player Sues Valve Software for Enabling Underage Gambling on Counter-Strike. Fortune, [online] Available at: https://fortune.com/2016/06/25/valve-software-underage-gambling/ [Accessed December 2019].

Myers, T. et al. (2020). Introduction to Azure Blob storage. [online] Microsoft Azure. Available at: https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction [Accessed March 2020].

Myerson, T (2015). Hello World: Windows 10 Available on July 29. [Blog] Windows Blog. Available at: https://blogs.windows.com/windowsexperience/2015/06/01/hello-world-windows-10-available-on-july-29/ [Accessed January 2020].

Mykhoparkina, O (2018). Discord vs Slack – Gaming, Working or Both? (Our Team's Feedback). [online] Chanty. Available at: https://www.chanty.com/blog/Discord-vs-slack/ [Accessed December 2019].

Nelly. (2019). Discord Transparency Report: Jan 1 — April 1. [Blog] Medium. Available at: https://blog.Discordapp.com/Discord-transparency-report-jan-1-april-1-4f288bf952c9 [Accessed December 2019].

Net Aware, (2019a). Twitch: A guide for parents. [online] Available at: https://www.net-aware.org.uk/networks/Twitch/ [Accessed December 2019].

Net Aware, (2019b). Discord: A guide for parents. [online] Available at: https://www.net-aware.org.uk/networks/Discord/ [Accessed December 2019].

Net Aware, (2019c). Steam: A guide for parents. [online] Available at: https://www.net-aware.org.uk/networks/Steam/ [Accessed December 2019].

Network Working Group (2005). Uniform Resource Identifier (URI): Generic Syntax. [online] The Internet Society, Pages 1-4. Available at: https://tools.ietf.org/html/rfc3986 [Accessed December 2019].

Newzoo (2019). Newzoo Global Games Market Report 2019 | Light Version. [online] Available at: https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2019-light-version/ [Accessed December 2019].

Onsongo, N. et al. (2018). Security Analysis Of Valve's Steam Platform. [PDF] pages 10-11. Available at: https://courses.csail.mit.edu/6.857/2018/project/Onsongo-Sanabria-Comas-Herold-Steam.pdf [Accessed April 2020].

NSPCC (2019a). Online abuse. [online]. Available at: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/ [Accessed December 2019].

NSPCC. (2019b). 200,000 young people may have been groomed on social networks. [online] Available at: https://www.nspcc.org.uk/what-we-do/news-opinion/200000-young-people-groomed-on-social-networks/ [Accessed December 2019].

NSPCC. (2019c). Grooming. [online] Available at: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/#what-is [Accessed December 2019].

Oates, B. (2006). Researching Information Systems and Computing. [EBook] London: SAGE Publications, pages 11-13. Available at: https://books.google.co.uk/books?hl=en&lr=&id=VyYmkaTtRKcC&oi=fnd&pg=PR11&dq=Researching+Information+Systems+and+Computing+2006&ots=w9ZACXPJZA&sig=pSD1vpxSGuM3YaYunNZ2epV_uKs#v=onepage&q=Researching%20Information%20Systems%20and%20Computing%202006&f=false [Accessed February 2020].

Patel, R. Sinha, A (2013). Analysis of VoIP Forensics with Digital Evidence Procedure. [online] International Journal for Scientific Research & Development, Pages 1. Available at: https://www.academia.edu/6803044/Analysis_of_VoIP_Forensics_with_Digital_Evidence_Procedure [Accessed December 2019].

Peterson, G. Et al. (2009). Advances in Digital Forensics. Fifth Edition. [Ebook] Orlando: Springer, Pages 83-84. Available at: https://link.springer.com/book/10.1007%2F978-3-642-04155-6 [Accessed January 2019].

Quick, D. et al. (2014). Title. [online] City published: Publisher, Pages used. Available at: https://pdfs.semanticscholar.org/97a4/a135acf7ef534992e18f643f577a6749cb3e.pdf [Accessed January 2019].

Renardson, A. (2010). Top 10 banned video games. Silicon Republic, [online] Available at: https://www.siliconrepublic.com/play/top-10-banned-video-games [Accessed December 2019].

Rukayat, A. (2016). A Survey and Critique of Digital Forensic Investigative Models. [PDF] University of Lagos: Department of Computer Sciences, pages 498-500. Available at: https://www.academia.edu/31243408/A_Survey_and_Critique_of_Digital_Forensic_investigative_Models?auto=download [February 2020].

Sahraoui, Y. et al. (2018). Performance evaluation of TCP and UDP based video streaming in vehicular ad-hoc networks. [PDF] 2018 International Conference on Smart Communications in Network Technologies, Available at: https://www.researchgate.net/publication/329902382_Performance_evaluation_of_TCP_and_UDP_based_video_streaming_in_vehicular_ad-hoc_networks [Accessed April 2020].

Sayer, M. Wilde, T (2018). The 15-year evolution of Steam. [online] PC gamer. Available at: https://www.pcgamer.com/uk/Steam-versions/ [Accessed December 2019].

Sederstrom, J. (2019). 7 Arrested In Florida After Allegedly Using Gaming App To Lure Teen Boy Into Sex Slavery. Oxygen, [online] Available at: https://www.oxygen.com/crime-time/agaming-app-Discord-allegedly-used-to-lure-teen-boys-into-human-trafficking-florida [Accessed December 2019].

Slo.Sleuth. (2013). Cashing in on the Google Chrome Cache. [Blog] BlogSpot. Available at: https://linuxsleuthing.blogspot.com/2013/02/cashing-in-on-google-chrome-cache.html [Accessed April 2020].

Suhanov, M. (2019). How the $LogFile works? [Blog] My DFIR Blog. Available at: https://dfir.ru/2019/02/16/how-the-logfile-works/ [Accessed April 2020].

Statcounter (2019). Desktop Operating System Market Share Worldwide. [online] Available at: https://gs.statcounter.com/os-market-share/desktop/worldwide/2019 [Accessed January 2020].

Steam (2019). Introducing Steam Remote Play Together. [online] Steam Community. Available at: https://Steamcommunity.com/games/593110/announcements/detail/3032537193879549687 [Accessed December 2019].

Steam (2018). Who Gets To Be On The Steam Store?. [Blog] Steam Community. Available at: https://Steamcommunity.com/games/593110/announcements/detail/1666776116200553082 [Accessed December 2019].

Tabuyo-Benito , R. et al. (2019) Forensics Analysis of an On-line Game over Steam Platform. [PDF] Tallinn University of Technology Available at: https://www.researchgate.net/publication/329997709_Forensics_Analysis_of_an_On-line_Game_over_Steam_Platform_10th_International_EAI_Conference_ICDF2C_2018_New_Orleans_LA_USA_September_10-12_2018_Proceedings [Accessed April 2020]

Twitch. (2017). List of Prohibited Games. [Online] Available at: https://help.Twitch.tv/s/article/list-of-prohibited-games?language=en_US [Accessed December 2019].

Twitch. (2019) Community Guidelines. [Online] Available at: https://www.Twitch.tv/p/en-gb/legal/community-guidelines/ [Accessed December 2019].

Twitch. (Year published). The Twitch Studio Beta: now available to everyone. Twitch.tv, [online] Available at: https://blog.Twitch.tv/en/2019/11/12/the-Twitch-studio-beta-now-available-to-everyone/ [Accessed December 2019].

Warren, T. (2019). Windows 10 is now more popular than Windows 7. The Verge, [online] Available at: https://www.theverge.com/2019/1/2/18164916/microsoft-windows-10-market-share-passes-windows-7-statistics [Accessed January 2020].

Wax io. (2017). How on earth is trading virtual items in video games a $50 billion industry?. Medium, [online] Available at: https://medium.com/wax-io/how-on-earth-is-trading-virtual-items-in-video-games-a-50-billion-industry-5972c211d621 [Accessed December 2019].

Webroot (2018). What is a Computer Virus and What Does It Do?. [online] Available at: https://www.webroot.com/au/en/resources/tips-articles/computer-security-threats-computer-viruses [Accessed December 2019].

Williams, J. (2012). ACPO Good Practice Guide for Digital Evidence. Version 5.0. [PDF] Metropolitan Police Service. Available at: https://www.dataclinic.co.uk/wp-content/uploads/2018/09/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf [Accessed February 2020].

Bibliography

Farrington, D. Muesch, N. (2015). Analysis of the Characteristics and content of Twitch live-streaming [PDF] Worcester Polytechnic Institute. Available at: https://web.wpi.edu/Pubs/E-project/Available/E-project-031915-220004/unrestricted/Analysis_of_the_Characteristics_and_Content_of_Twitch.tv_Live-streaming.pdf

Francois, J. et al. (2011) Digital Forensics in VoIP networks. Version 1 [PDF] University of Luxembourg: Interdisciplinary Center for Security, Reliability and Trust. Available at: https://www.researchgate.net/publication/224218273_Digital_Forensics_in_VoIP_networks

Horsman, G (2018). Reconstructing streamed video content: A case study on YouTube and Facebook Live stream content in the Chrome web browser cache. [PDF] University of Teesside. Available at: https://www.journals.elsevier.com/digital-investigation

Irwin, D. et al. (2011). Extraction of Electronic Evidence from VoIP: Forensic Analysis of a Virtual Hard Disk vs RAM. Volume 6. [PDF] The Journal of Digital Forensics, Security and Law. Available at: https://commons.erau.edu/jdfsl/vol6/iss1/2/

Leahy Center for Digital Investigations. (2017). Application Analysis. [PDF] Champlain College. Available at: https://www.champlain.edu/Documents/LCDI/**ApplicationAnalysis**_S17.pdf

Lokesh, K. et al. (2019). Comparative study on data extraction and acquisition tools for Facebook messages. [PDF] Ahmedabad: National Institute of Occupational Health. Available at: https://www.researchgate.net/publication/333679909_Comparative_study_on_data_extraction_and_acquisition_tools_for_Facebook_messages

Rukayat, A. et al. (2016). A Survey and Critique of Digital Forensic Investigative Models. Volume 14. [PDF] Nigeria: International Journal of Computer Science and Information Security. Available at: https://www.academia.edu/31243408/A_Survey_and_Critique_of_Digital_Forensic_investigative_Models

Rehman, A. Alharthi, K. (2016) An Introduction to Research Paradigms. [PDF] King Abdualziz University. Available at: https://www.researchgate.net/publication/325022648_An_introduction_to_research_paradigms

Sansurooah, K. (2006) Taxonomy of computer forensics methodologies and procedures for digital evidence seizure. [PDF] Edith Cowan University Perth. Available at: https://www.researchgate.net/publication/49279342_Taxonomy_of_computer_forensics_methodologies_and_procedures_for_digital_evidence_seizure

Sha, M. et al. (2016) VoIP Forensic Analyzer. Volume 6. [PDF] Prince Sattam Bin Abdulaziz University Available at: https://www.researchgate.net/publication/292642237_VoIP_Forensic_Analyzer

Sgaras , C. et al. (2016).Forensics Acquisition and Analysis of instant messaging and VoIP applications. [PDF] University College Dublin Belfield. Available at: https://arxiv.org/abs/1612.00204

Sonnekus, M. (2014). A comparison of open source and proprietary digital forensic software. Edition. [PDF] Grahamstown, South Africa: Rhodes University, pages 35-42, 60-63, 130-135. Available at: https://core.ac.uk/download/pdf/145046345.pdf

Appendices

1: Terms of Reference

Terms of Reference

Module:

KV6003: Individual Computing Project

Name:

Shona Start

ID:

w17019752

Course:

Computer and Digital Forensics

Project Title:

Investigation and comparison of the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform.

Supervisor:

Philip Anderson

Second Marker:

Petia Sice

Title

Investigation and comparison of the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform

Background to project

This project aims to compare the recoverable forensics artefacts from a selection of online gaming and chat applications running on a Windows 10 platform. These applications are developing constantly with new technologies and adding new or updating old communication services. For example Discord recently added a feature called "Go Live" (Waterloo 2019); Steam is currently running public live testing for a new feature called Remote Play Together (Steam 2019). Most gaming applications now provide VoIP services and live streaming capabilities. Of course this brings new dangers to users of the applications. These platforms are an increasing target for illicit activities such as grooming, gambling and other abusive content (National Online Safety What parents need to know about Discord 2018, Steam Parent's Guide 2018, Twitch Online Safety Guide for Parents 2019). Malicious users consider these platforms as safer methods of communication, due to detection of such activities on these platforms being in their infancy stages. The idea for this project came from my familiarity with these types of platforms and my interest in digital forensics. This project is important for minors and other vulnerable peoples who use these applications as well as victims of the crimes that were aided by these platforms. The three gaming applications this project will focus on have been specifically chosen for their popularity, differing live streaming capabilities and history of criminal activities on their platforms.

The first, Twitch, is a platform designed purely for watching and streaming live video content currently owned by Amazon. It was founded in 2011 and originally was mainly focused on the live streaming of video games. However, it has now been developed to include other types of streams. More than 17,000 of Twitch's user base gain money through the platform; through paid subscriptions, donations and ad placements (Lifewire, 2019). Twitch is a hotbed for illicit activities. For instance, In July 2019, the NSPCC (National Society for the Prevention of Cruelty to Children) reported that Twitch was one of the most popular places for the grooming and exploitation of minors (NSPCC, 2019). Additionally, In October 2019, a shooting was broadcast live over Twitch for over 35 minutes before being shut down (Dot Esports, 2019).

Another application is Discord, which is a voice, video and chat platform designed for use alongside video games. Discord only released live streaming capabilities on the 15th August 2019 (Polygon, 2019), and there are no public statistics regarding use of the new service as of yet. However, Discord already has a record of illicit users. For example, within a period of about four months (1st January 2019 – 1st April 2019), Discord received 8,941 reports of harassment, 4,929 reports of threatening behaviour, 4,171 reports of exploitative content, 3,121 reports of doxing (The releasing of private personal records). There were also many other reports of spamming, adult content, hacking, malware, self-harm and other violations of Discord's Terms of Service. During these four months, Discord banned 10,642 accounts and 714 servers for exploitative content. The examples given of exploitative content include "A user discovers their intimate photos are being shared without their consent" and "two minors flirting leads to trading intimate images with each other" (Discord, 2019). These are worrying statistics, due to the age limit of Discord being only thirteen years old, and there are no verification methods in place to enforce this, so theoretically minors of any age can access this platform.

The third application, Steam, is one of the biggest digital distribution platforms for video games on PC (Video Game Stats, 2019). It also provides social networking and video streaming services. In recent years, Valve, the company that owns Steam has been under scrutiny for its involvement with skin gambling. Skin gambling is the use of digital items in video games as a virtual currency for betting purposes. The Steam platform allows trading, buying and selling of these digital items. Evidence of underage gambling was discovered in 2016 and lawsuits were initiated against Valve. One of these lawsuits focused on minors as young as 12 who had become addicted to skin gambling. (ESPN, 2017)

There are some difficulties that will come with using these applications. For instance, Discord's newer live streaming features will make it harder to find trustworthy research on the newer system. However, the author is familiar with the platform and can navigate it well; they are also familiar with the Steam platform. On the other hand, the author is not very familiar with Twitch but as the platform was launched over 8 years ago there should be some reliable data available for research.

The platforms will be analysed from a computer running Windows 10. This operating system has been chosen because it is the currently the most popular in the world running on more than 800 million devices (The Verge, 2019). Over 70% of Steam users run the application on Windows 10 (Statista, 2019). No data is accessible for the other platforms but it's safe to assume that the majority of their computer users are also running Windows 10.

Conducting a forensic analysis on a Windows 10 machine differs in some ways from previous versions of Windows. For example, some file paths for certain artefacts will differ. Several types of software will be used to analyse the data from this machine including Encase, Magnet RAM Capture, Wireshark and Magnet Axiom. The author has some familiarity with using Encase and Wireshark, but has never conducted a forensics analysis on the data collected by Wireshark. The author has also never used Magnet RAM Capture or Magnet Axiom. This should be a challenge but the author should be able to find sufficient resources to assist them.

This project should challenge the author in many ways. The author is inexperienced in gathering and analysing some types of forensics artefacts, for example VoIP (Voice Over IP) which is used in both live streaming and video calling. Alongside this, the research this project will focus on is a newer issue for digital forensics. This will mean that it will be a challenge for the author to find academic literature from credible sources, making it more difficult to perform research into the area of study.

Proposed Work

This project will focus on comparing each of the applications from a forensics perspective. It will investigate the difficulty, speed, and complexity of retrieving artefacts for each. It will be important to research the applications including their file systems and analyse how each store and manage data; paying particular attention to data which could be potentially presented in a court of law as evidence in a real case.

The investigation will include creating digital data for analysis. The process for this creation will be thoroughly planned out before execution. However, it will likely consist of running each application on a computer, with a Windows 10 operating system, for a timed period. This could be for periods of 1 minute, 2.5 minutes and 5 minutes each. During these periods a number of activities will be performed on the applications. These activities will be depended on the abilities of each application (see Figure1). Some examples of activities would be:

- Sharing of text messages, images, sound clips and other files.
- Live streaming of a video game and if possible outside of the game.
- Communicating with another user on the platform either via text communications or/and voice combinations.

While these activities are being carried out, the software Wireshark will be used on the Windows 10 machine to capture network traffic for analysis. After the timed period is completed, all activity on the Windows 10 machine will immediately cease and magnet RAM Capture will be used to collect volatile memory from the computer for analysis. A forensics image will then be taken of the machine, and this image will be analysed using Encase, Magnet Axiom and other forensics software.

What can applications can / cannot do:	Discord	Twitch	Steam (Steam communications are removed after roughly 2 weeks)
Text communications	Yes	Yes	Yes
Live streaming of video game content	Yes (Max 10 people)	Yes	Yes
Live streaming of other software on a computer	No	Yes	Yes
Live video and audio calling	Yes	No	Only voice Calling
Image sharing	Yes (limit of 8mb)	No	Yes (limit of 10mb)
Recorded video sharing	Yes (limit of 8mb)	No	Yes
URL sharing	Yes	Yes	Yes
Recorded Audio sharing	Yes (limit of 8mb)	No	Yes
File sharing	Yes (limit of 8mb)	No	No
Financial/Trading transactions	No	Yes (Donations can be sent to approved Twitch accounts)	Yes (Trading of Steam items)

Figure1

Aims

To investigate and compare the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform.

Objectives

1. To research and give context to the selection of applications and their live streaming capabilities.
2. To research the illicit activities of the malicious users of these platforms.
3. To research and provide background information relating to Windows 10 and the effects this operating system will have on the investigation, exploring possible forensics techniques that could be implemented.
4. To create a thorough plan of how this investigation will be executed, including ethical issues, equipment use, investigation plan, and data analysis plan.
5. Implement the investigation plans documenting all results and collecting all relevant data.
6. Analysis of the data, comparing the data collected across each of the applications.
7. Evaluation of the findings, discussing the usefulness of the information and its real world implications.

8. Evaluation of the areas of this project that could be improved and further work that could be implemented in the future.

Skills

Skills	How it was acquired
Computer and digital forensics	Throughout the modules KF4001 (Introduction to Computer Security and Forensics), KF5005 (Principles of Digital Security and Forensics), KF6002 (Legal and Evidentiary Aspects of Digital Forensics) and KF6000 (Fundamentals of Digital Forensics Investigations). Alongside my own personal research.
Computer networking	During my time studying for a BTEC diploma and throughout the modules KF4002 (Network Technology 1) and KF5003 (Network Technology 2).
Specialist software	Throughout studying for my BTEC diploma and at university I have used a number of specialist software, some of which will be used in this project.
Research	Throughout my entire education as well as during volunteer work.
Interpersonal	Throughout my entire education as well as during volunteer work, my time with the scout association, and the NCS (National Citizen Service).
Self-directive	Throughout my entire education as well as during volunteer work and my time with the scout association.
Industrious	Throughout my entire education as well as during volunteer work, my time with the scout association, the RLSS, and the NCS.
Time management	Throughout my entire education as well as during volunteer work and the NCS.

Skills I will acquire	How I will acquire these skills
Network Forensics	Through my own personal research into academic papers.
Volatile Memory Forensics	Through my own research as well as in my current module KF6000.
VoIP (Voice over IP) Forensics	Through my own personal research into academic papers.

References

NSPCC. (2019). 200,000 young people may have been groomed on social networks. NSPCC, [online] pages 1. Available at: https://www.nspcc.org.uk/what-we-do/news-opinion/200000-young-people-groomed-on-social-networks/ [12/10/2019].

Richardson, L. (2019). German synagogue shooting was broadcast on Twitch. Dot Esports, [online] pages 1. Avalable at: https://dotesports.com/streaming/news/german-synagogue-shooting-was-broadcast-on-Twitch [12/10/2019].

Nelly. (2019). Discord Transparency Report: Jan 1 — April 1. [Blog] Discord. Available at: https://blog.Discordapp.com/Discord-transparency-report-jan-1-april-1-4f288bf952c9 [12/10/2019].

Goslin, A. (2019). Discord's new Go Live feature will let users stream games to up to 10 friends. Polygon, [online] pages 1. Available at: https://www.polygon.com/2019/8/9/20798559/Discord-go-live-private-stream-voice-channel [12/10/2019].

Grayson, N. (2016). The Counter-Strike Gambling Scandal, Explained. Kotaku, [online] pages 1. Available at: https://kotaku.com/why-people-are-flipping-out-over-the-counter-strike-gam-1783369102 [12/10/2019].

Warren, T. (2019). Windows 10 is now more popular than Windows 7. The Verge, [online] 1. Available at: https://www.theverge.com/2019/1/2/18164916/microsoft-windows-10-market-share-passes-windows-7-statistics [12/10/2019].

Gough, C (2019). Share of Steam (gaming platform) users in June 2019, by operating system used. [online] Statista. Available at: https://www.statista.com/statistics/265033/proportion-of-operating-systems-used-on-the-online-gaming-platform-Steam/ [12/10/2019].

Stephenson, B. (2019). All about Twitch. Lifewire, [online] page 1. Available at: https://www.lifewire.com/what-is-Twitch-4143337 [18/10/2019].

Assael, S. (2017). Skin in the Game. ESPN, [online] pages 1 Available at: http://www.espn.com/espn/feature/story/_/id/18510975/how-counter-strike-turned-teenager-compulsive-gambler [19/10/2019].

Smith, Craig. (2019). 30 Interesting Steam Stats and Facts (2019) | By the Numbers. Video Game Stats, [online] pages 1. Available at : https://videogamesstats.com/Steam-stats-facts/ [01/11/2018].

Waterloo (2019). Go Live FAQ. [online] Discord. Available at: https://support.Discordapp.com/hc/en-us/articles/360030714312-Go-Live-FAQ [07/11/2019].

Steam, (2019). Introducing Steam Remote Play Together. [online] Available at: https://Steamcommunity.com/games/593110/announcements/detail/3032537193879549687 [07/11/2019].

National Online Safety, (2019). What parents need to know about Discord. [online] Available at: https://nationalonlinesafety.com/resources/wake-up-wednesday/Discord/ [08/11/2019].

National Online Safety, (2018). Steam Parent’s Guide. [online] Available at: https://nationalonlinesafety.com/resources/wake-up-wednesday/Steam-parents-guide/ [08/11/2019].

National Online Safety, (2018). Twitch Online Safety Guide for Parents. [online] Available at: https://nationalonlinesafety.com/resources/wake-up-wednesday/Twitch-online-safety-guide-for-parents/ [08/11/2019].

Bibliography

I, Lin. Y, Yen. B, Wu. H, Wang. (2010). VoIP network forensic analysis with digital evidence procedure. The 6th International Conference on Networked Computing and Advanced Information Management, [online] pages 236-241. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5572499&isnumber=5572041 [28/09/2019].

Farrington, D. Muesch, N. (2015). Analysis of the characteristics and content of Twitch live-streaming. [PDF] Worcester Polytechnic Institution. Available at: https://web.wpi.edu/Pubs/E-project/Available/E-project-031915-220004/unrestricted/Analysis_of_the_Characteristics_and_Content_of_Twitch.tv_Live-streaming.pdf [16/09/2019].

J, François. R, State. T, Engel. O, Festor. (2010). Digital forensics in VoIP networks. IEEE International Workshop on Information Forensics and Security, [online] Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5711450&isnumber=5711434 [26/09/2019].

Irwin, D. Slay, J. Dadej, A. Shore, M. (2011). Extraction of Electronic Evidence from VoIP: Forensic Analysis of a Virtual Hard Disk vs. RAM. The Journal of Digital Forensics, Security and Law, [online] Volume6. Available at: https://commons.erau.edu/jdfsl/vol6/iss1/2/ [01/10/2019].

Sgaras, C. Kechadi, M. N, Le-Khac. (2016). Forensics Acquisition and Analysis of instant messaging and VoIP applications. [PDF] Dublin: University College Dublin Belfield. Available at: https://arxiv.org/ftp/arxiv/papers/1612/1612.00204.pdf [01/10/2019].

Last name, First initial. (2018). Forensics Analysis of an On-line Game over Steam Platform. 10th International EAI Conference, [online]. Available at: https://www.researchgate.net/publication/329997709_Forensics_Analysis_of_an_On-line_Game_over_Steam_Platform_10th_International_EAI_Conference_ICDF2C_2018_New_Orleans_LA_USA_September_10-12_2018_Proceedings [26/09/2019].

Horsman, G. (2018). Reconstructing Streamed Video Content: A Case Study on YouTube and Facebook Live Stream Content in the Chrome Web Browser Cache. Digital Investigation, [online] Volume 26, pages 30-37. Available at: https://www.sciencedirect.com/science/article/pii/S1742287618301932 [09/10/2019].

Sha, M. Manesh T. El-atty, S. (2016). VoIP Forensic Analyzer. International Journal of Advanced Computer Science and Applications, [online] Volume 7 Available at: https://www.researchgate.net/publication/292642237_VoIP_Forensic_Analyzer [26/09/2019].

Leahy Center for Digital Investigations. (2017). Application Analysis. [PDF]. Available at: https://lcdiblog.champlain.edu/research/ [19/10/2019].

Brignoni, A (2018). Finding Discord app chats in Windows. [online] Blogspot. Available at: https://abrignoni.blogspot.com/2018/03/finding-Discord-app-chats-in-windows.html [19/10/2019].

Penguin Powered Infosec Blog (2014). Steam Browser Forensics. [online] Github. Available at: http://aoighost.github.io/penguinpoweredinfosec/#!dfir/browserforensics/Steam/Steam_browserforensics.md [19/10/2019].

Resources

- Hardware:
  - Computer or laptop running Windows 10 operating system - This is one of the most crucial resources needed in the research as it will be the machine used for all of the practical research.
  - Webcam - will be vital in order to produce video artefacts. This will be provided by the loans office.
  - Microphone - will be vital in order to produce sound artefacts. This will be provided by loans office.
- Software:
  - Steam, Twitch and Discord Platform – This is important as these are the platforms to be analysed in the project. These are all free platforms easily available online.
  - EnCase – Will be used for analysis of the majority of the data captured from the computer. This software is available in the off-campus network labs.
  - Magnet Axiom – Will be used to carve evidence from the data collected. This software is provided in the computers in the off-campus network labs.
  - Wireshark – Will be used for capture and analysis of network traffic. This is a free software and also provided in the computers in the off-campus network labs.
  - Magnet RAM capture - Will be used for capture and analysis of volatile memory. This is software available free online.

Report Structure

Abstract & Introduction

- Title Page
  - Title of project and personal details.
- Abstract
  - A summary of the contents of the report (Background, Objective, Methods, Results, Conclusion).
- Chapter 1: Introduction
  - An explanation of the background of the project. Including what I will be attempting to do and why it is important

Analysis

- Chapter 2: An introduction to online gaming and chat applications
  - Objective 1
  - This chapter will give context to the selection of applications and their live streaming capabilities.
- Chapter 3: The dark side of gaming applications
  - Objective 2
  - Will present my research about the real life malicious activities that occur on these platforms.
- Chapter 4: An introduction to Windows 10
  - Objective 3
  - Will provide background information relating to Windows 10 and the effects this operating system will have on the investigation. I will also discuss possible forensics techniques that could be implemented on this operating system.

Synthesis

- Chapter 5: Investigation plan
  - Objectives 4
  - Detailed explanation of how the investigation will be executed. Including ethical issues, equipment use, investigation plan, and data analysis plan.
- Chapter 6: Investigation Results
  - Objective 5
  - Present the data collected in a understandable format
- Chapter 7: An analysis of the data collected
  - Objective 6
  - A comparison of the data collected across each of the applications.

Evaluation, Conclusions & Recommendations

- Evaluation
  - Objective 7
  - Will discuss the usefulness of the information analysed and its real world implications.
- Conclusions and Recommendations
  - Objective 8
  - Will discuss the areas of this project that could be improved and further work that could be implemented in the future.

Marking Scheme

Project Type: Investigative Project

Report & Practical Work	90%
Viva	10%

Report:

Abstract & Introduction	5%
Analysis	20%
Synthesis: Discussion	20%
Synthesis: Practical Work	30%
Evaluation & Conclusions	20%
Presentation	5%
Total	100%

Quality of Practical Work

- Compliance with any relevant ethical and safety guidelines.
- Appropriate research methodologies will be used throughout this project. These will mainly be quantitative methodologies.
- Software required to be NIST (National Institute of Standards and Technology) certified. This means the software has been tested to make sure it is accurate and reliable.
- Adherence to the ACPO (Association of Chief Police Officers) guidelines for Digital Evidence at all times. To ensure this, the data captured during the investigation will not be changed or edited in anyway and a record of processes applied to the digital data will be taken throughout the investigation. This will ensure the investigation can be repeated again with the same results.
- To the best of my abilities test data for each application will be equal, appropriate and detailed. To do this each application will have identical testing and the machine will be wiped after each collection of data

Project Plan

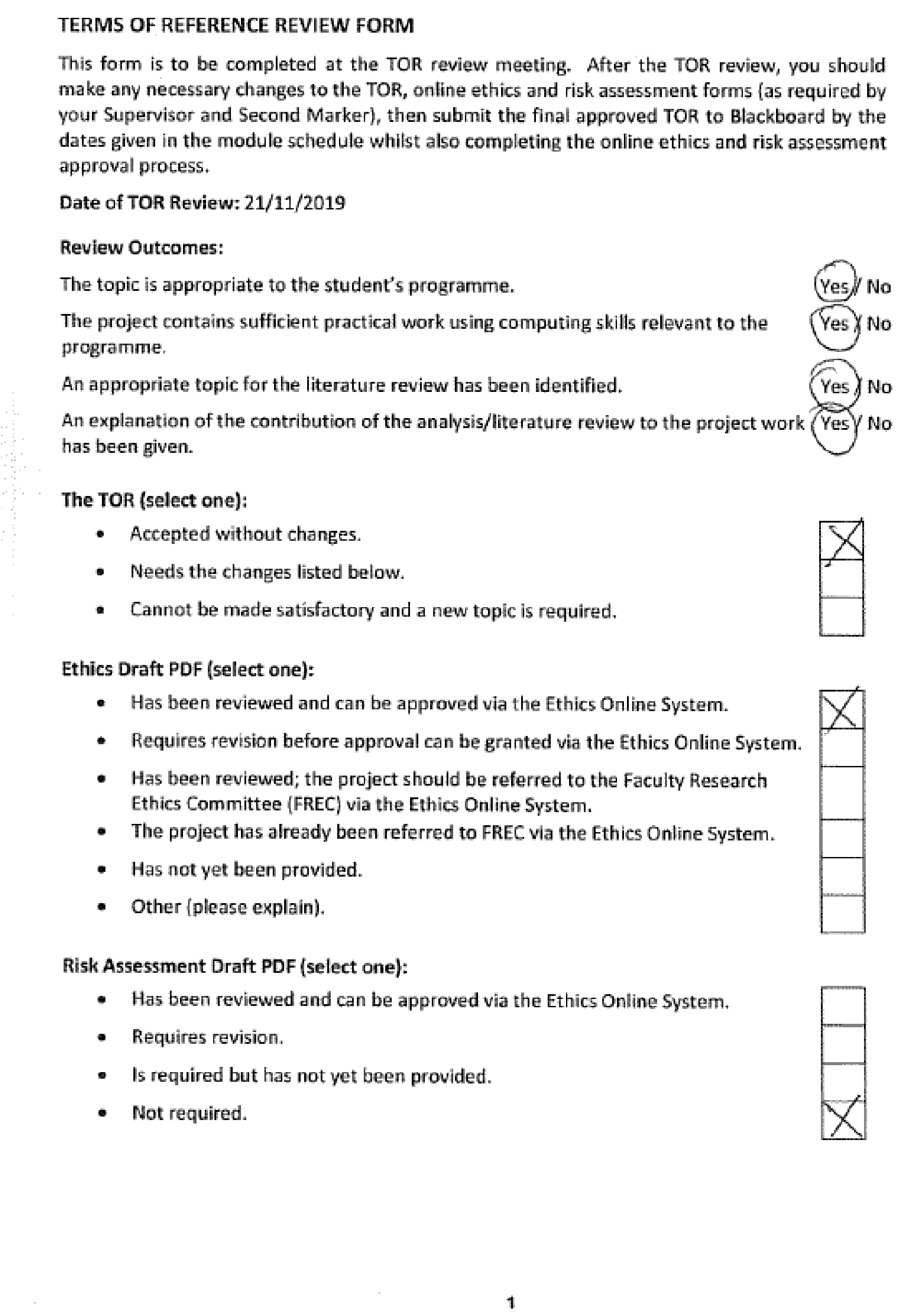
Semester 1

Title	Week of 28/10/19	Week of 04/11/19	Week of 11/11/19	Week of 18/11/19	Week of 25/11/19	Week of 02/12/19	Week of 09/12/19	Week of 16/12/19	Week of 23/12/19	Week of 06/01/20	Week of 13/01/20	Week of 20/01/20
Deadlines	TOR Draft			TOR Final		Draft Analysis Chapters			Christmas			
Proof reading and final changes												
Abstract and Introduction												
Title Page	🟦											
Abstract												
Introduction												
Analysis												
Objective 1: Research		🟦										
Chapter 1			🟦									
Objective 2: Research				🟦								
Chapter 2					🟦							
Objective 3: Research						🟦						
Chapter 3							🟦					
Synthesis												
Chapter 4/Objective 4								🟦		🟦		
Objective 5: Implement Plan											🟦	🟦
Chapter 5												
Chapter 6/ Objective 6												
Evaluation and conclusion												
Objective 7: Evaluation												
Objective 8: Future Work												

Semester 2

Week of 27/01/20	Week of 03/02/20	Week of 10/02/20	Week of 17/02/20	Week of 24/02/20	Week of 02/03/20	Week of 09/03/20	Week of 16/03/20	Week of 23/03/20	Week of 30/03/20	Week of 06/04/20	Week of 13/04/20	Week of 20/04/20	Week of 27/04/20
					Project review				Easter Holidays			Project Review 2	Project Report and USB/CD/DVD
											🟦	🟦	🟦
Abstract and Introduction													
										🟦			
								🟦		🟦			
Analysis													
Synthesis													
🟦	🟦												
		🟦	🟦										
Evaluation and conclusion													
				🟦	🟦								
						🟦	🟦						

TOR Review



TERMS OF REFERENCE REVIEW FORM

This form is to be completed at the TOR review meeting. After the TOR review, you should make any necessary changes to the TOR, online ethics and risk assessment forms (as required by your Supervisor and Second Marker), then submit the final approved TOR to Blackboard by the dates given in the module schedule whilst also completing the online ethics and risk assessment approval process.

Date of TOR Review: 21/11/2019

Review Outcomes:

The topic is appropriate to the student's programme.	[✓ Yes] / No
The project contains sufficient practical work using computing skills relevant to the programme.	[✓ Yes] / No
An appropriate topic for the literature review has been identified.	[✓ Yes] / No
An explanation of the contribution of the analysis/literature review to the project work has been given.	[✓ Yes] / No

The TOR (select one):

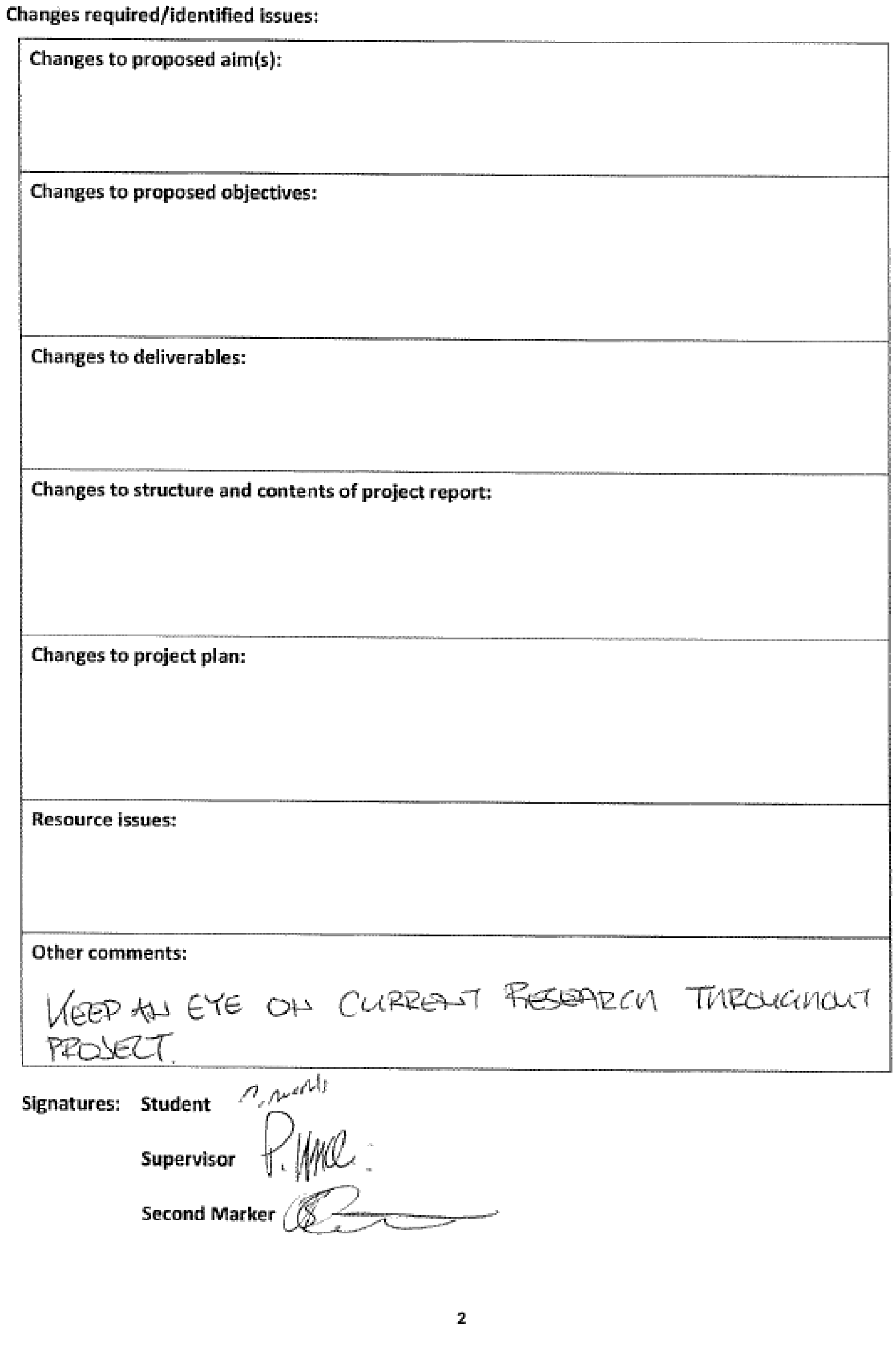
- Accepted without changes. ☒
- Needs the changes listed below. □
- Cannot be made satisfactory and a new topic is required. □

Ethics Draft PDF (select one):

- Has been reviewed and can be approved via the Ethics Online System. ☒
- Requires revision before approval can be granted via the Ethics Online System. □
- Has been reviewed; the project should be referred to the Faculty Research Ethics Committee (FREC) via the Ethics Online System. □
- The project has already been referred to FREC via the Ethics Online System. □
- Has not yet been provided. □
- Other (please explain). □

Risk Assessment Draft PDF (select one):

- Has been reviewed and can be approved via the Ethics Online System. □
- Requires revision. □
- Is required but has not yet been provided. □
- Not required. ☒



Changes required/identified issues:

Changes to proposed aim(s):
Changes to proposed objectives:
Changes to deliverables:
Changes to structure and contents of project report:
Changes to project plan:
Resource issues:
Other comments: KEEP AN EYE ON CURRENT RESEARCH THROUGHOUT PROJECT.

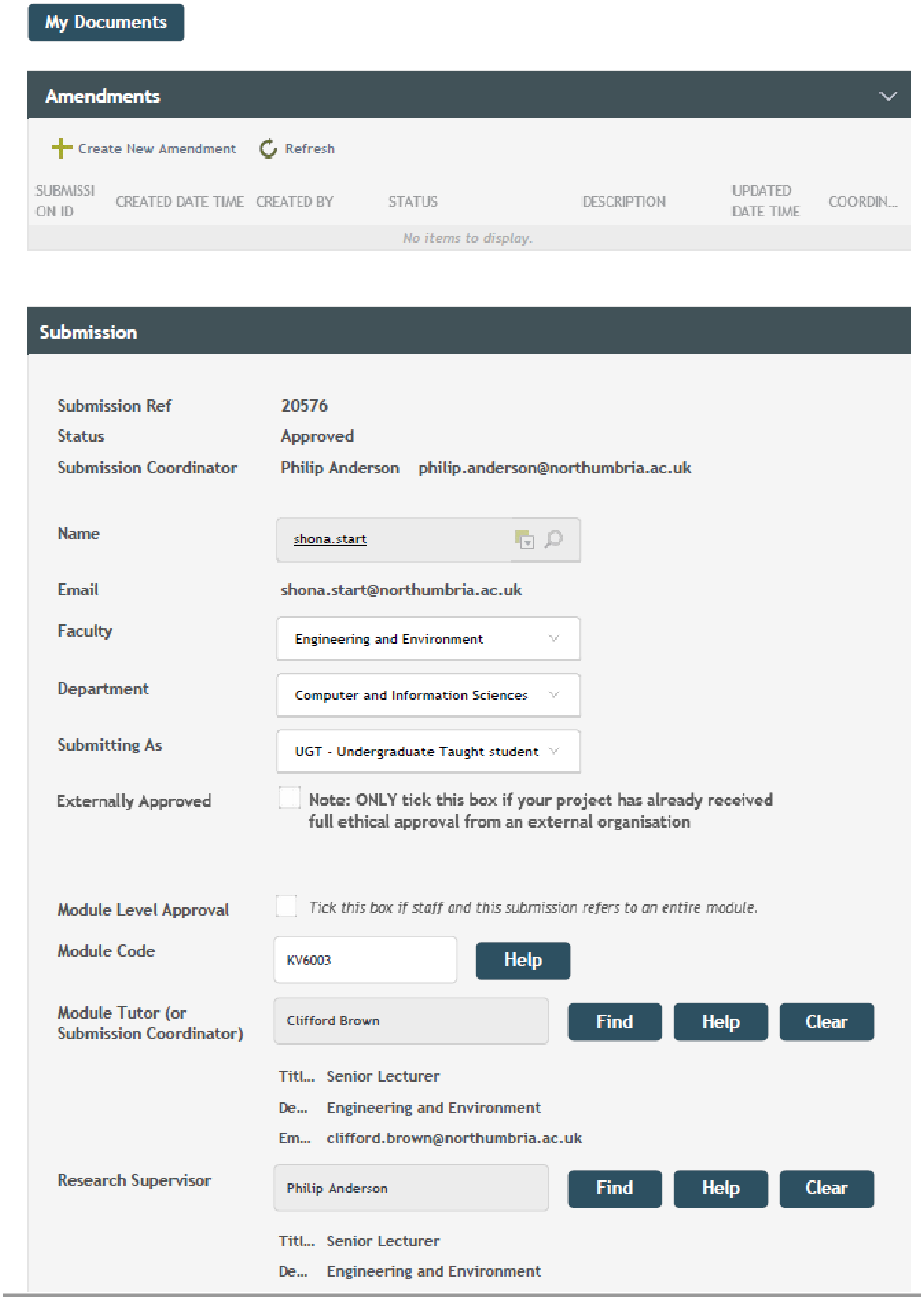
Signatures: **Student**

Supervisor

Second Marker

2

Ethics form



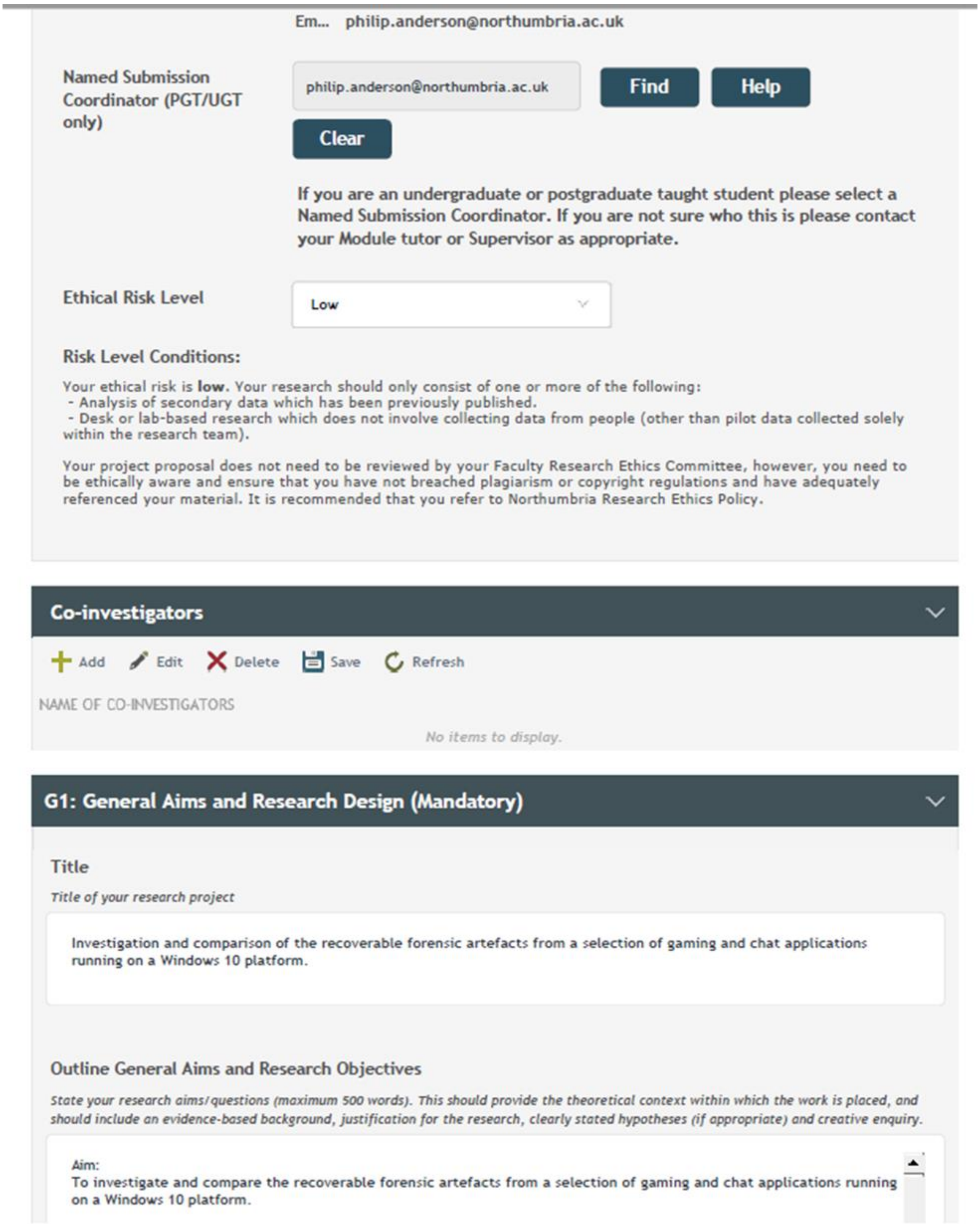
Amendments

SUBMISSION ID	CREATED DATE TIME	CREATED BY	STATUS	DESCRIPTION	UPDATED DATE TIME	COORDIN...

No items to display.

Submission

Submission Ref	20576
Status	Approved
Submission Coordinator	Philip Anderson philip.anderson@northumbria.ac.uk
Name	shona.start
Email	shona.start@northumbria.ac.uk
Faculty	Engineering and Environment
Department	Computer and Information Sciences
Submitting As	UGT - Undergraduate Taught student
Externally Approved	□ Note: ONLY tick this box if your project has already received full ethical approval from an external organisation
Module Level Approval	□ *Tick this box if staff and this submission refers to an entire module.*
Module Code	KV6003
Module Tutor (or Submission Coordinator)	Clifford Brown Titl... Senior Lecturer De... Engineering and Environment Em... clifford.brown@northumbria.ac.uk
Research Supervisor	Philip Anderson Titl... Senior Lecturer De... Engineering and Environment



Em... philip.anderson@northumbria.ac.uk

Named Submission Coordinator (PGT/UGT only)

philip.anderson@northumbria.ac.uk

If you are an undergraduate or postgraduate taught student please select a Named Submission Coordinator. If you are not sure who this is please contact your Module tutor or Supervisor as appropriate.

Ethical Risk Level: Low

Risk Level Conditions:

Your ethical risk is **low**. Your research should only consist of one or more of the following:
- Analysis of secondary data which has been previously published.
- Desk or lab-based research which does not involve collecting data from people (other than pilot data collected solely within the research team).

Your project proposal does not need to be reviewed by your Faculty Research Ethics Committee, however, you need to be ethically aware and ensure that you have not breached plagiarism or copyright regulations and have adequately referenced your material. It is recommended that you refer to Northumbria Research Ethics Policy.

Co-investigators

NAME OF CO-INVESTIGATORS

No items to display.

G1: General Aims and Research Design (Mandatory)

Title

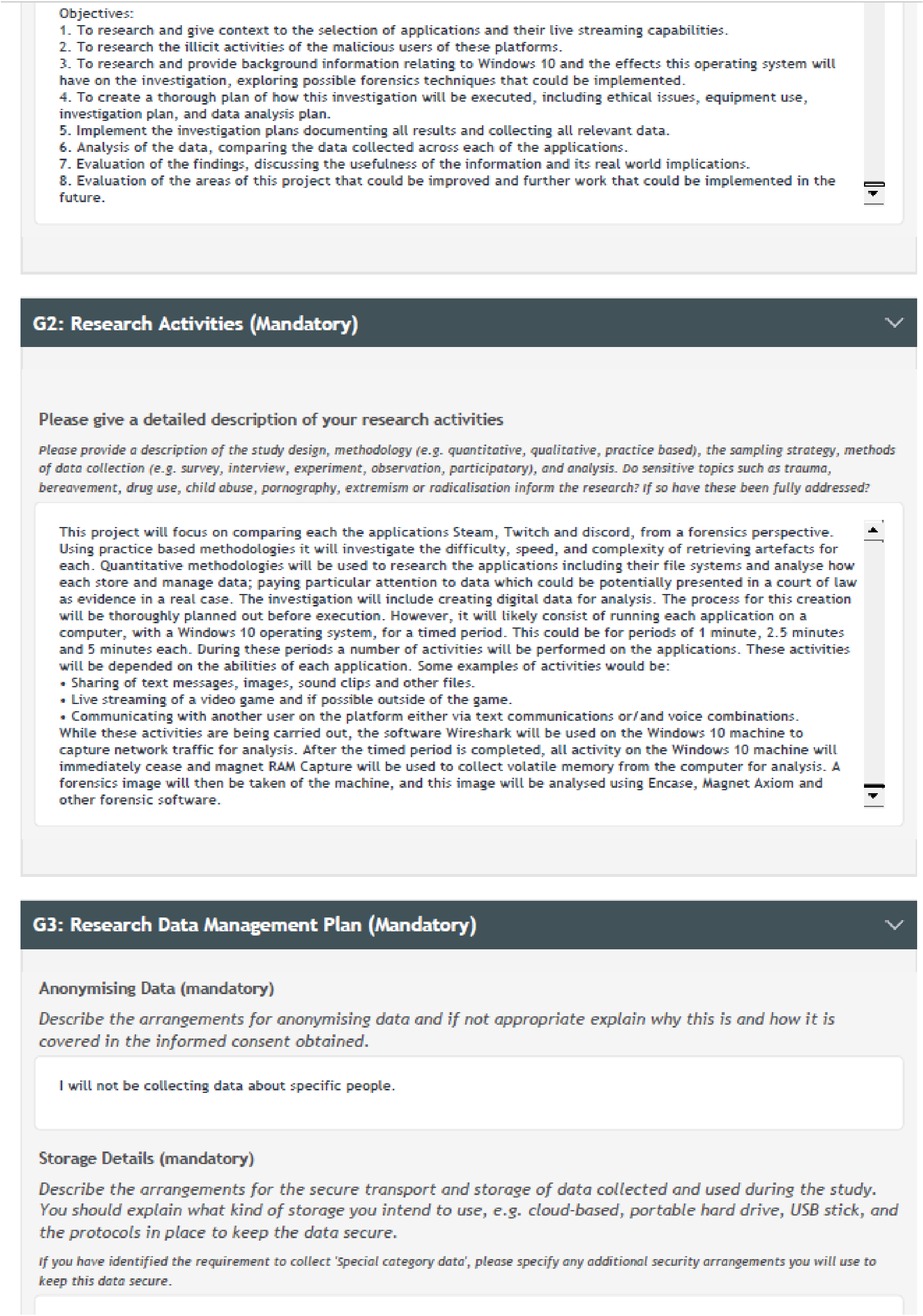
Title of your research project

Investigation and comparison of the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform.

Outline General Aims and Research Objectives

State your research aims/questions (maximum 500 words). This should provide the theoretical context within which the work is placed, and should include an evidence-based background, justification for the research, clearly stated hypotheses (if appropriate) and creative enquiry.

Aim:
To investigate and compare the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform.



Objectives:
1. To research and give context to the selection of applications and their live streaming capabilities.
2. To research the illicit activities of the malicious users of these platforms.
3. To research and provide background information relating to Windows 10 and the effects this operating system will have on the investigation, exploring possible forensics techniques that could be implemented.
4. To create a thorough plan of how this investigation will be executed, including ethical issues, equipment use, investigation plan, and data analysis plan.
5. Implement the investigation plans documenting all results and collecting all relevant data.
6. Analysis of the data, comparing the data collected across each of the applications.
7. Evaluation of the findings, discussing the usefulness of the information and its real world implications.
8. Evaluation of the areas of this project that could be improved and further work that could be implemented in the future.

G2: Research Activities (Mandatory)

Please give a detailed description of your research activities

Please provide a description of the study design, methodology (e.g. quantitative, qualitative, practice based), the sampling strategy, methods of data collection (e.g. survey, interview, experiment, observation, participatory), and analysis. Do sensitive topics such as trauma, bereavement, drug use, child abuse, pornography, extremism or radicalisation inform the research? If so have these been fully addressed?

This project will focus on comparing each the applications Steam, Twitch and discord, from a forensics perspective. Using practice based methodologies it will investigate the difficulty, speed, and complexity of retrieving artefacts for each. Quantitative methodologies will be used to research the applications including their file systems and analyse how each store and manage data; paying particular attention to data which could be potentially presented in a court of law as evidence in a real case. The investigation will include creating digital data for analysis. The process for this creation will be thoroughly planned out before execution. However, it will likely consist of running each application on a computer, with a Windows 10 operating system, for a timed period. This could be for periods of 1 minute, 2.5 minutes and 5 minutes each. During these periods a number of activities will be performed on the applications. These activities will be depended on the abilities of each application. Some examples of activities would be:
- Sharing of text messages, images, sound clips and other files.
- Live streaming of a video game and if possible outside of the game.
- Communicating with another user on the platform either via text communications or/and voice combinations.

While these activities are being carried out, the software Wireshark will be used on the Windows 10 machine to capture network traffic for analysis. After the timed period is completed, all activity on the Windows 10 machine will immediately cease and magnet RAM Capture will be used to collect volatile memory from the computer for analysis. A forensics image will then be taken of the machine, and this image will be analysed using Encase, Magnet Axiom and other forensic software.

G3: Research Data Management Plan (Mandatory)

Anonymising Data (mandatory)

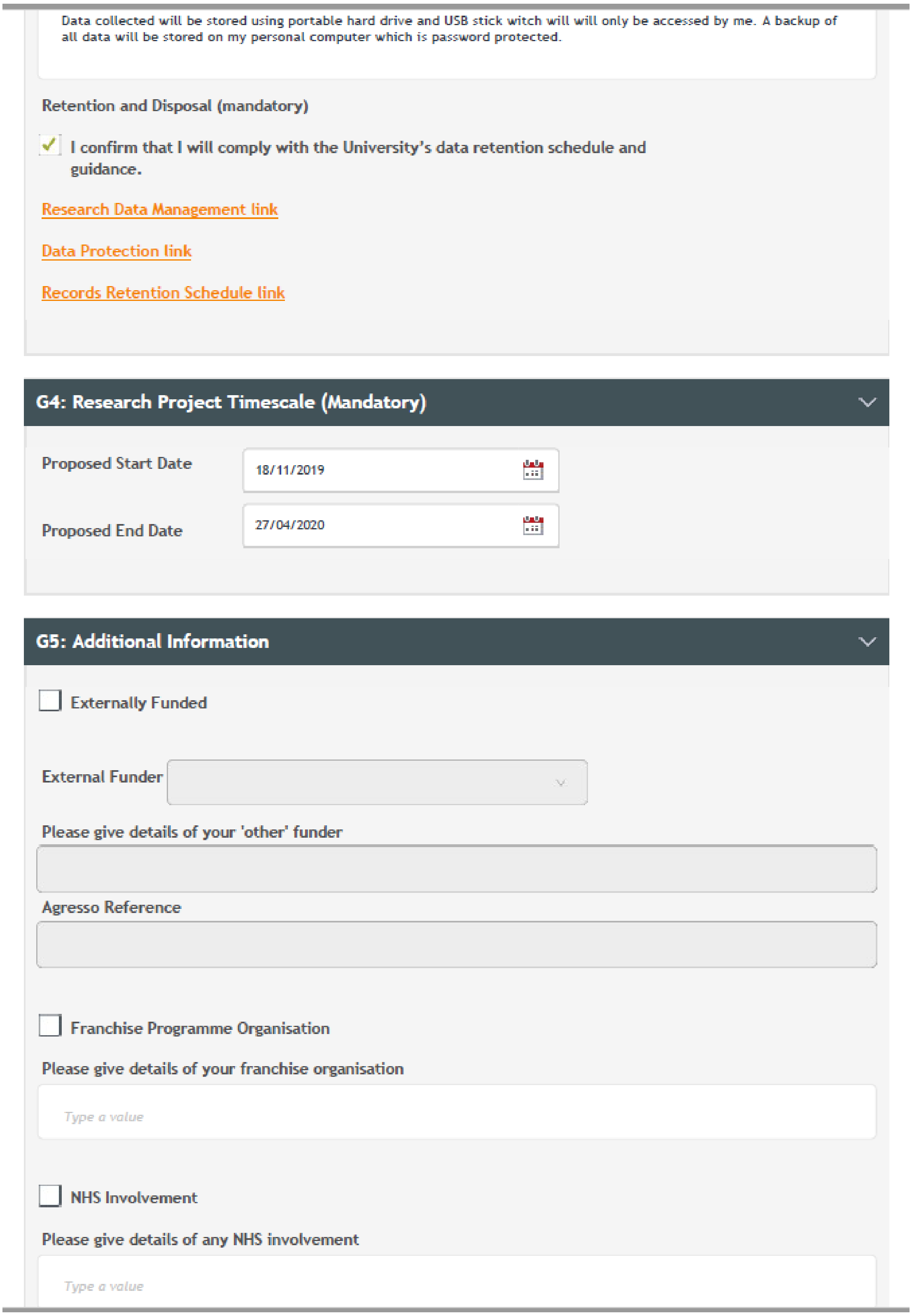
Describe the arrangements for anonymising data and if not appropriate explain why this is and how it is covered in the informed consent obtained.

I will not be collecting data about specific people.

Storage Details (mandatory)

Describe the arrangements for the secure transport and storage of data collected and used during the study. You should explain what kind of storage you intend to use, e.g. cloud-based, portable hard drive, USB stick, and the protocols in place to keep the data secure.

If you have identified the requirement to collect 'Special category data', please specify any additional security arrangements you will use to keep this data secure.



Data collected will be stored using portable hard drive and USB stick witch will will only be accessed by me. A backup of all data will be stored on my personal computer which is password protected.

Retention and Disposal (mandatory)

☑ I confirm that I will comply with the University's data retention schedule and guidance.

Research Data Management link

Data Protection link

Records Retention Schedule link

G4: Research Project Timescale (Mandatory)

Proposed Start Date 18/11/2019

Proposed End Date 27/04/2020

G5: Additional Information

□ Externally Funded

External Funder

Please give details of your 'other' funder

Agresso Reference

□ Franchise Programme Organisation

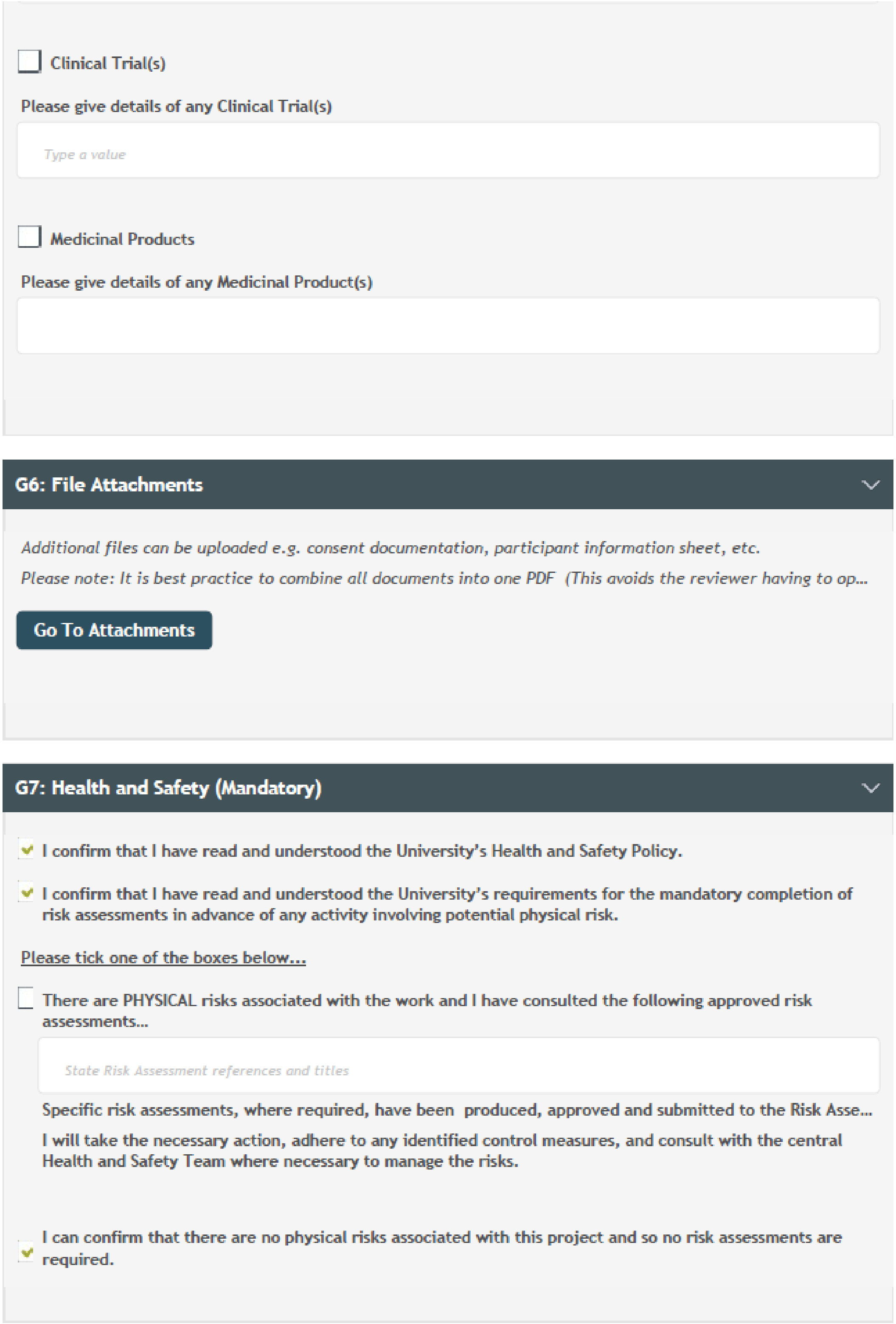
Please give details of your franchise organisation

Type a value

□ NHS Involvement

Please give details of any NHS involvement

Type a value



□ Clinical Trial(s)

Please give details of any Clinical Trial(s)

□ Medicinal Products

Please give details of any Medicinal Product(s)

G6: File Attachments

Additional files can be uploaded e.g. consent documentation, participant information sheet, etc.

Please note: It is best practice to combine all documents into one PDF (This avoids the reviewer having to op...

G7: Health and Safety (Mandatory)

☑ I confirm that I have read and understood the University's Health and Safety Policy.

☑ I confirm that I have read and understood the University's requirements for the mandatory completion of risk assessments in advance of any activity involving potential physical risk.

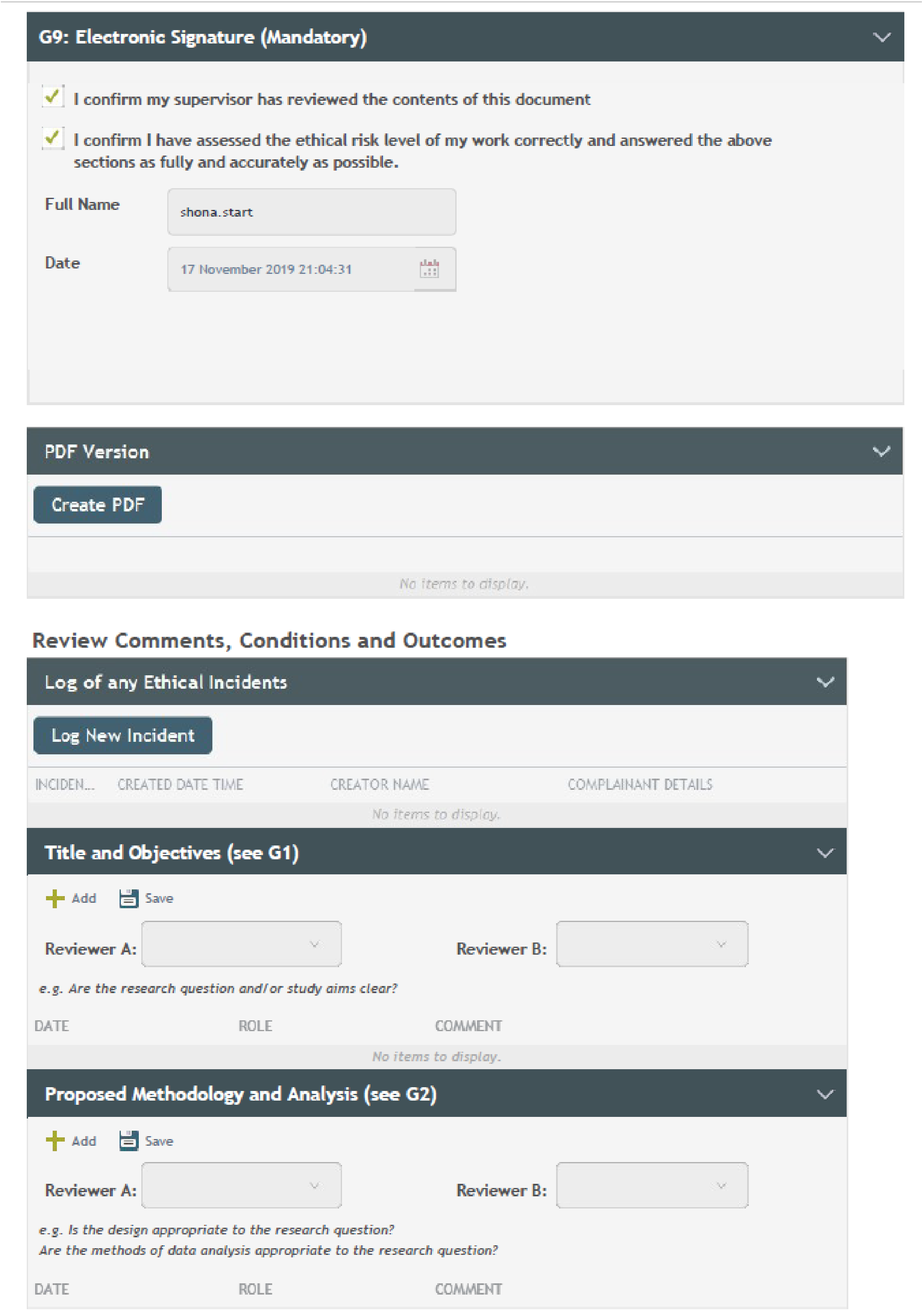
Please tick one of the boxes below...

□ There are PHYSICAL risks associated with the work and I have consulted the following approved risk assessments...

Specific risk assessments, where required, have been produced, approved and submitted to the Risk Asse...

I will take the necessary action, adhere to any identified control measures, and consult with the central Health and Safety Team where necessary to manage the risks.

☑ I can confirm that there are no physical risks associated with this project and so no risk assessments are required.



G9: Electronic Signature (Mandatory)

☑ I confirm my supervisor has reviewed the contents of this document

☑ I confirm I have assessed the ethical risk level of my work correctly and answered the above sections as fully and accurately as possible.

Full Name: shona.start

Date: 17 November 2019 21:04:31

PDF Version

No items to display.

Review Comments, Conditions and Outcomes

Log of any Ethical Incidents

INCIDEN...	CREATED DATE TIME	CREATOR NAME	COMPLAINANT DETAILS

No items to display.

Title and Objectives (see G1)

Reviewer A: Reviewer B:

e.g. Are the research question and/or study aims clear?

DATE	ROLE	COMMENT

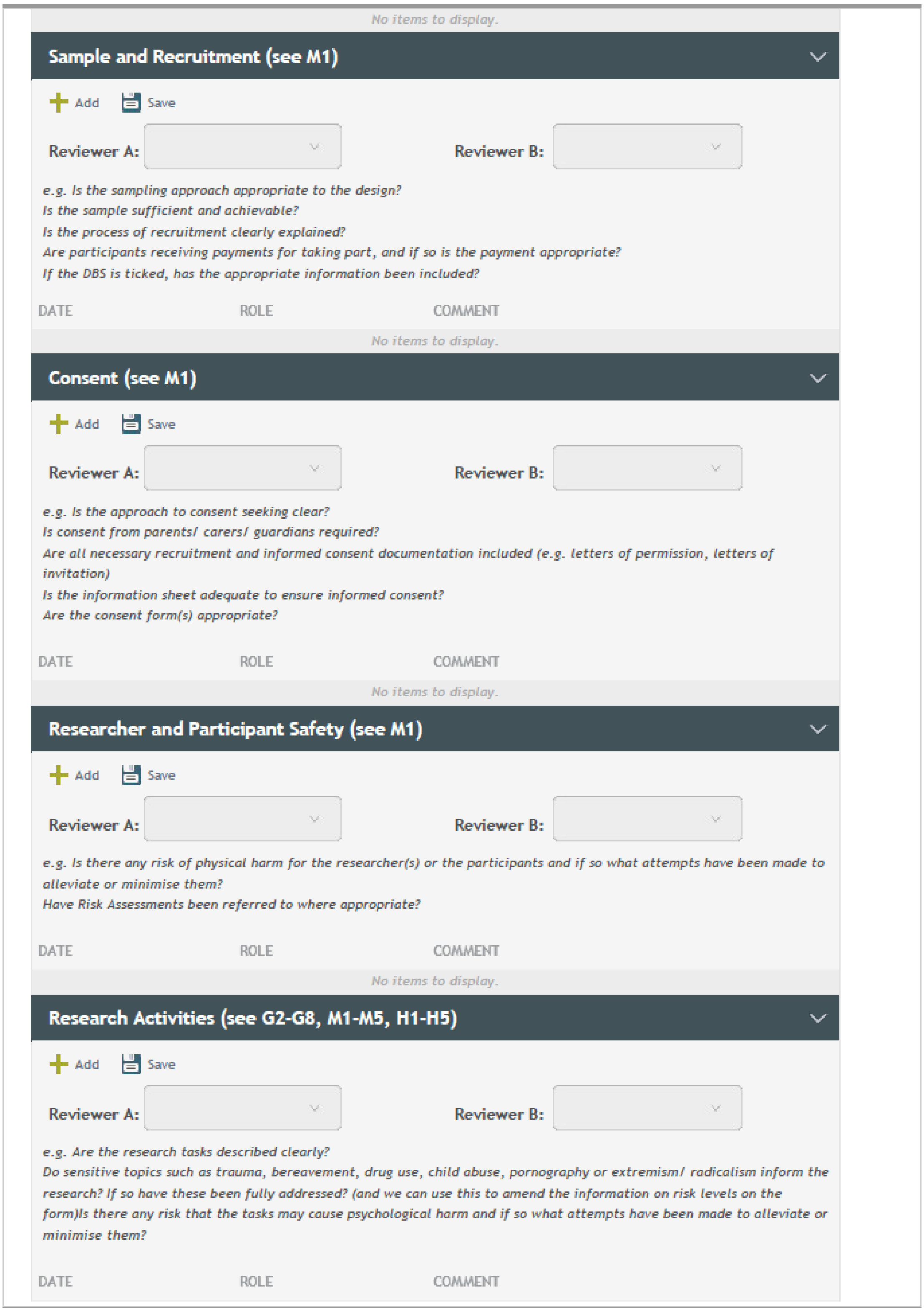
No items to display.

Proposed Methodology and Analysis (see G2)

Reviewer A: Reviewer B:

e.g. Is the design appropriate to the research question?
Are the methods of data analysis appropriate to the research question?

DATE	ROLE	COMMENT



No items to display.

Sample and Recruitment (see M1)

Reviewer A: | Reviewer B:

e.g. Is the sampling approach appropriate to the design?
Is the sample sufficient and achievable?
Is the process of recruitment clearly explained?
Are participants receiving payments for taking part, and if so is the payment appropriate?
If the DBS is ticked, has the appropriate information been included?

DATE	ROLE	COMMENT

No items to display.

Consent (see M1)

Reviewer A: | Reviewer B:

e.g. Is the approach to consent seeking clear?
Is consent from parents/ carers/ guardians required?
Are all necessary recruitment and informed consent documentation included (e.g. letters of permission, letters of invitation)
Is the information sheet adequate to ensure informed consent?
Are the consent form(s) appropriate?

DATE	ROLE	COMMENT

No items to display.

Researcher and Participant Safety (see M1)

Reviewer A: | Reviewer B:

e.g. Is there any risk of physical harm for the researcher(s) or the participants and if so what attempts have been made to alleviate or minimise them?
Have Risk Assessments been referred to where appropriate?

DATE	ROLE	COMMENT

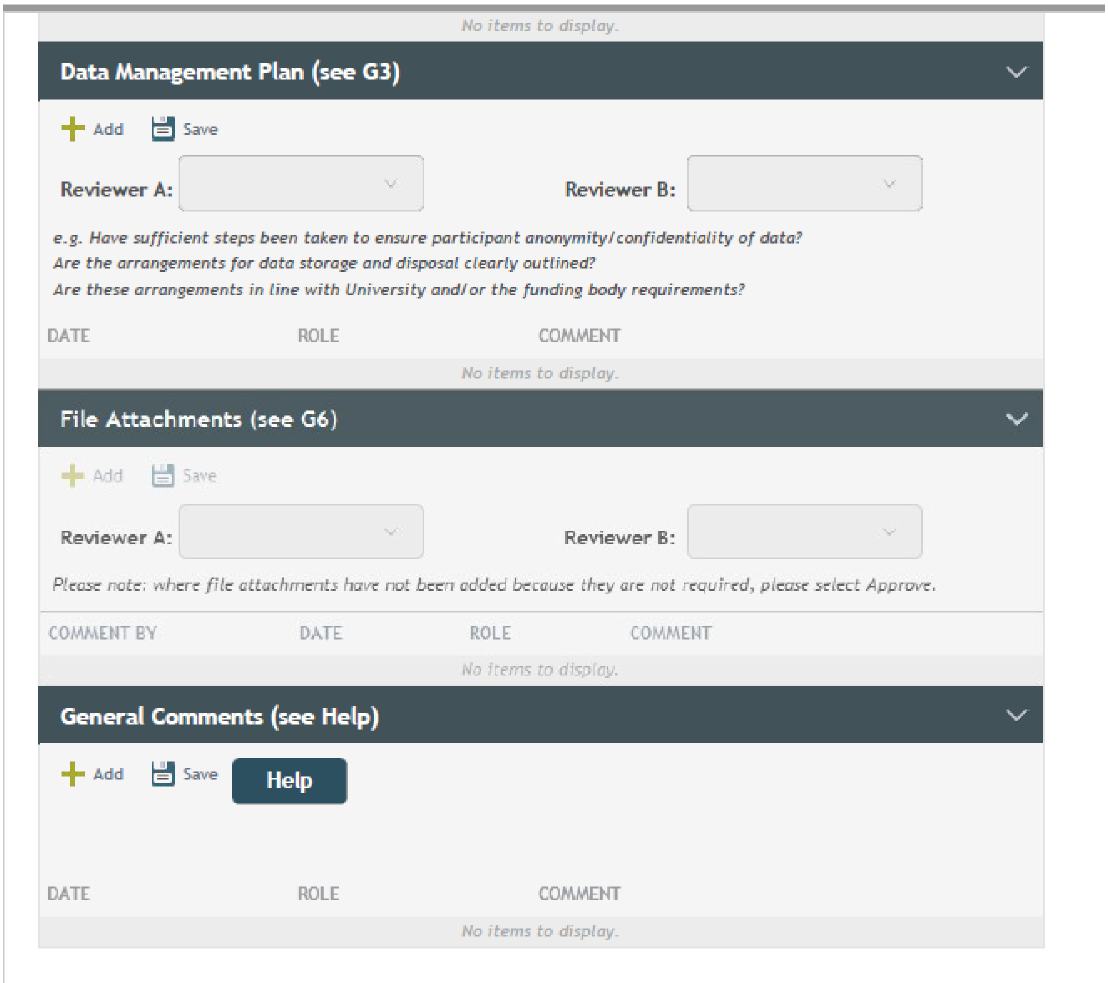
No items to display.

Research Activities (see G2-G8, M1-M5, H1-H5)

Reviewer A: | Reviewer B:

e.g. Are the research tasks described clearly?
Do sensitive topics such as trauma, bereavement, drug use, child abuse, pornography or extremism/ radicalism inform the research? If so have these been fully addressed? (and we can use this to amend the information on risk levels on the form)Is there any risk that the tasks may cause psychological harm and if so what attempts have been made to alleviate or minimise them?

DATE	ROLE	COMMENT



No items to display.

Data Management Plan (see G3)

e.g. Have sufficient steps been taken to ensure participant anonymity/confidentiality of data?
Are the arrangements for data storage and disposal clearly outlined?
Are these arrangements in line with University and/or the funding body requirements?

DATE	ROLE	COMMENT
No items to display.		

File Attachments (see G6)

Please note: where file attachments have not been added because they are not required, please select Approve.

COMMENT BY	DATE	ROLE	COMMENT
No items to display.			

General Comments (see Help)

DATE	ROLE	COMMENT
No items to display.		

2: Table of Figures

Figure 1 -– Steam Data Creation Plan 18
Figure 2 - Activity: ImageDiscord.png and VideoDiscord.mov 23
Figure 3 - f_00002f 24
Figure 4 - f_000033 24
Figure 5 - f_000030 24
Figure 6 - Activity: Twitch Secondary-Device Stream 25
Figure 7 – f_00006a 25
Figure 8 – f_000082 25
Figure 9 – Activity: ImageSteam.png and VideoSteam.mov 26
Figure 10 – f_000043 26
Figure 11 – Activity: Steam Broadcast Chat 27
Figure 12 - data_1 28
Figure 13 - modules.log 28
Figure 14- \VideoDecodeStats\000003.log 28
Figure 15 - Activity: Discord Video Call 29
Figure 16 - Activity: Discord Streaming 29
Figure 17 - \Local Storage\leveldb\000003.log 30
Figure 18 - 000005.log 32
Figure 19 – Activity: Login to Steam 33
Figure 20 - loginusers.vdf 33
Figure 21 - localconfig.vdf 34
Figure 22– Secondary-Device: localconfig.vdf 35
Figure 23 - $LogFile 36
Figure 24– Activity Steam: Login 36
Figure 25- pagefile.sys 37
Figure 26– Activity: Twitch message 1 39
Figure 27– LNK Update.exe 40
Figure 28 – Activity: Open Discord 40
Figure 29 – LNK Twitch.exe 41
Figure 30 – LNK TwitchStudio.exe 41
Figure 31 – Activity: Open Twitch 41
Figure 32– LNK Steam.exe 41
Figure 33– Activity: Open Steam 41
Figure 34 -– STEAMWEBHELPER.EXE 42
Figure 35– Volatile memory pictures 42
Figure 36 - Network Packet 44
Figure 37 - Discord Statistics 44
Figure 38- Twitch Statistics 45

Figure 39 - Steam Statistics *46*
Figure 40 - Activity: Discord VoIP *47*
Figure 41 – Activity: Twitch VoIP *48*
Figure 42– Activity: Steam VoIP *49*
Figure 43 - STEAMDISCOVER protocol *50*
Figure 44– Encase Verification *53*
Figure 45- Abstract Digital Forensic Model *95*
Figure 46 - ImageDiscord.png and ImageSteam.png *96*
Figure 47– Application Limits and Features *97*
Figure 48 - Account Details *98*
Figure 49 – Plan of Action *99*
Figure 50 - Project Plan Amended *110*
Figure 51– Project Logbook 111

3: Figures 45 – 51

Figure 45- Abstract Digital Forensic Model

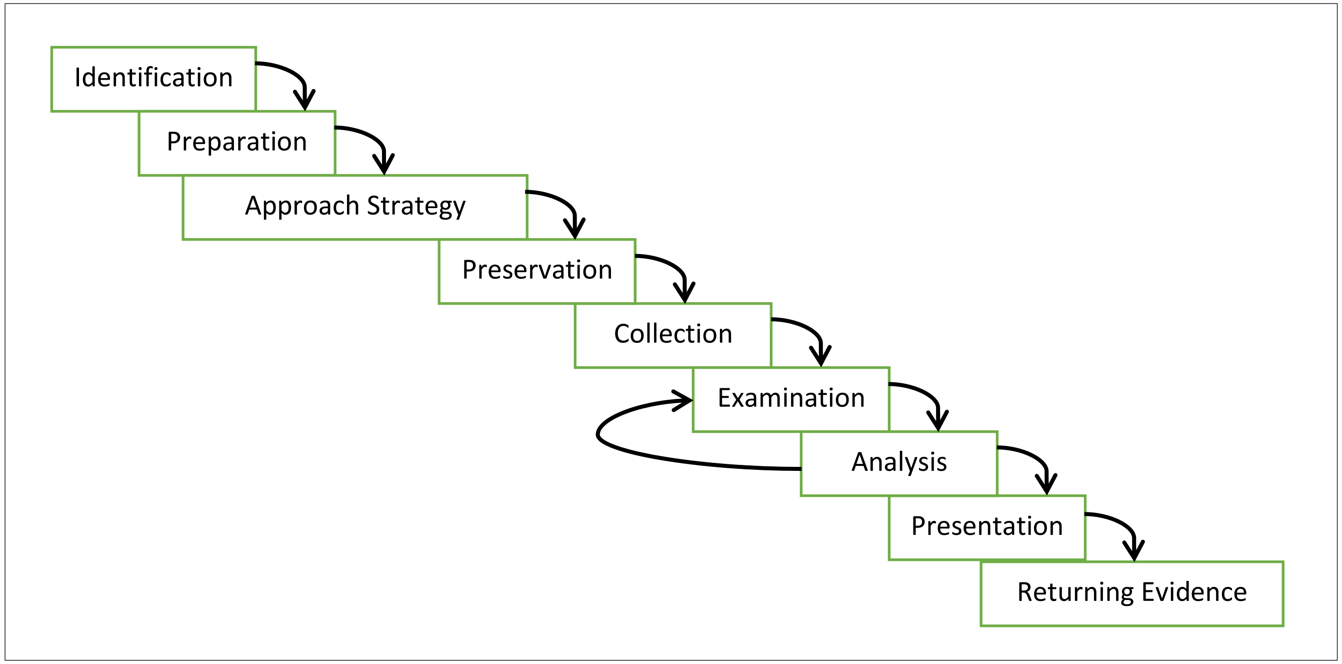


Figure 46 - ImageDiscord.png and ImageSteam.png

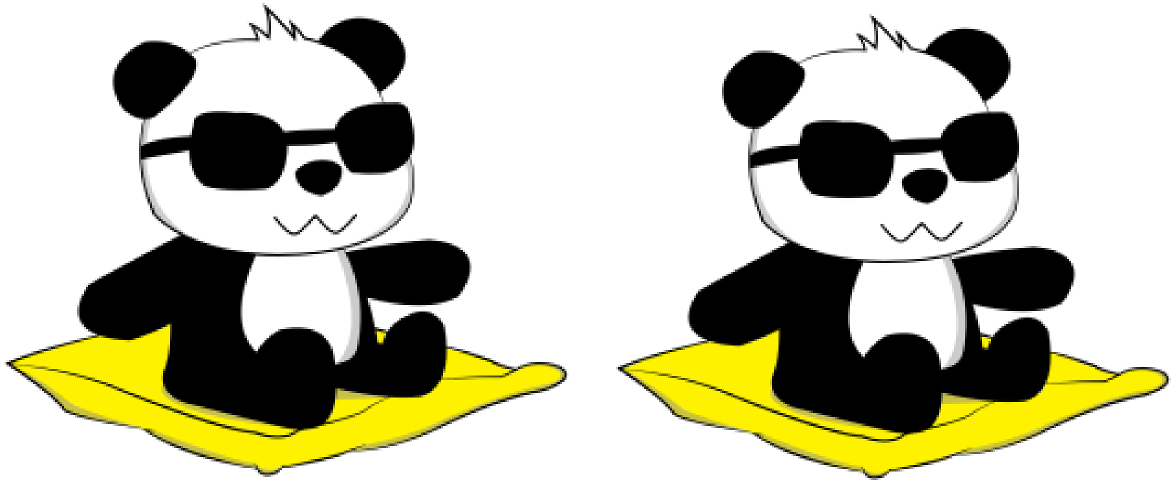


Figure 47– Application Limits and Features

Application Features	Discord	Twitch	Steam
Profile with login requirements	Yes	Yes	Yes
IM (Instant messaging) communications	Yes	Yes	Yes
Group Chat communications	Yes	Yes	Yes
Public status posts	No	No	Yes
Live streaming of video game content	Yes (To a maximum of 10 other accounts)	Yes	Yes
Live streaming of full screen	Yes (To a maximum of 10 other accounts)	Yes	Yes
Live video and audio calling	Yes	No	Only Voice
Image sharing	Yes (limit of 8mb)	No	Yes (limit of 10mb)
Recorded video/audio sharing	Yes (limit of 8mb)	No	Yes (limit of 10mb)
URL sharing	Yes	Yes	Yes
File sharing	Yes (limit of 8mb)	No	No
Friend system	Yes	Yes	Yes
Following system	No	Yes	No

Figure 48 - Account Details

Main-Device			
Application	**Account name**	**ID**	**Display name**
Discord	icp.maindevice2020@gmail.com	#3796	icp.maindevice2020
Twitch	maindevice2020	n/a	maindevice2020
Steam	maindevice2020	n/a	icp.maindevice2020
Secondary-Device			
Application	**Account name**	**ID**	**Display name**
Discord	icp.seconddevice2020@gmail.com	#9830	icp.seconddevice2020
Twitch	seconddevice2020	n/a	seconddevice2020
Steam	seconddevice2020	n/a	icp.seconddevice2020

Figure 49 – Plan of Action

Discord Application				
Device	**Activity**	**Date/Time**	**Successful**	**Other notes**
Main-Device	Turn on device	25/02/2020 17:15	Yes	
Main-Device	Open Wireshark	17:16	Yes	
Main-Device	Start capturing data using Wireshark	17:19	Yes	
Main-Device	Open Discord application	17:20	Yes	
Main-Device	Enter login details and login	17:21	Yes	
Secondary-Device	Send icp.maindevice2020 a friend request	17:21	Yes	
Main-Device	Accept friend request	17:22	Yes	
Main-Device	Using Discord direct message send message “Discord One Dulce periculum ” to icp.seconddevice2020	17:23	Yes	
Secondary-Device	Reply to message with “Discord 2 Acta non verba ”	17:23	Yes	
Main-Device	Reply to message with http://www.google.co.uk	17:24	Yes	
Main-Device	Send voice call request to icp.seconddevice2020	17:25	Yes	

Secondary-Device	Accept video call request	17:26	Yes	
Main-Device and Secondary-Device	Keep video chat active for 1 minute (video and audio)	17:27	Yes	
Secondary-Device	Send icp.maindevice2020 ImageDiscord.png	17:28	Yes	
Secondary-Device	Send icp.maindevice2020 VideoDiscord.mov	17:29	Yes	
Main-Device	open “Rubi The Wayward Mira”	17:30	Yes	Windows tried to block opening the game. Selected “Run Anyway”
Main-Device	Send video call request to icp.seconddevice2020	17:34	Yes	
Secondary-Device	Accept video call request	17:34	Yes	
Main-Device and Secondary-Device	Keep Discord call active for 10 minutes (video and audio)	17:34-17:48	Yes	Extended to 15 minutes
While streaming				
Main-Device	In the video settings turn on screen share (Also make sure both camera and microphone are enabled)	17:34	Yes	Screen share disables webcam Game and desktop sounds not detected by stream

Main-Device	In Discord direct message send message “Discord 4 Audentes fortuna iuvat”	17:35	Yes	
Secondary-Device	In Discord direct message send message “Discord 5 Condemnant quo non intellegunt”	17:35	Yes	
Main-Device	Open Internet explorer and search for “cute dog videos”	17:37	Yes	
Main-Device	Play a random video with the sound on	17:38	Yes	Live stream does no pick up on sound from video
After streaming				
Main-Device	Close “Rubi The Wayward Mira”	17:48	Yes	
Main-Device	Insert external storage device into device	17:48	Yes	
Main-Device	Stop Wireshark from capturing data, save data captured onto external storage device	17:49	Yes	
Main-Device	Close Wireshark	17:50	Yes	
Main-Device	Open Magnet RAM capture	17:51	Yes	
Main-Device	Save data collected by Magnet RAM capture onto external storage device	17:58	Yes	
Main-Device	Switch off device	17:58	Yes	
Twitch Application				
Device	**Activity**	**Date/Time**	**Successful**	**Other notes**

Main-Device	Turn on device	03/03/2020 17:38	Yes	
Main-Device	Open Wireshark	17:40	Yes	
Main-Device	Start capturing data using Wireshark	17:42	Yes	
Main-Device	Open Twitch application and Twitch studio	17:42	Yes	
Main-Device	Enter login details and login	17:44 - 17:46	Yes	
Secondary-Device	Send maindevice2020 a friend request	17:48	Yes	
Main-Device	Accept friend request	17:48	Yes	
Main-Device	Using Twitch whisper send message "Twitch 1 Ad meliora" to seconddevice2020	17:49	Yes	
Secondary-Device	Reply to message with "Twitch 2 Natura non constristatur"	17:50	Yes	
Main-Device	Reply to message with http://www.google.co.uk	17:50	Yes	
Secondary-Device	Using Twitch Studio start streaming (With audio and video enabled)	17:51-17:52	Yes	
Main-Device	Go to seconddevice2020 profile and view stream	17:51-17:52	Yes	
Secondary-Device	Keep Steam active 1 minute	17:51-17:52	Yes	

Main-Device	Open “Rubi The Wayward Mira”	17:53-17:55	Yes	
Main-Device	Set-up and start streaming “Entire Screen” using Twitch Studio (With audio and video enabled)	17:57	Yes	
Main-Device	Keep Stream active for 10 minutes	17:57-18:07	Yes	
While Streaming				
Secondary-Device	Go to maindevice2020 profile and view stream	17:58	Yes	
Main-Device	Send message “Twitch 3 Non ducor duco” in the stream chat	17:59	Yes	
Secondary-Device	Send message “Twitch 4 Amore et melle et felle es fecundissimus” in the stream chat	17:59	Yes	
Main-Device	Open Internet explorer and search for “cute raccoon videos”	18:05	Yes	
Main-Device	Play a random video with the sound on	18:05	Yes	
After streaming				
Main-Device	Close “Rubi The Wayward Mira”	18:08	Yes	
Main-Device	Insert external storage device into device	18:08	Yes	
Main-Device	Stop Wireshark from capturing data, save data captured onto external storage device	18:08	Yes	
Main-Device	Close Wireshark	18:09	Yes	

Main-Device	Open Magnet RAM capture	18:10	Yes	
Main-Device	Save data collected by Magnet RAM capture onto external storage device	18:15	Yes	
Main-Device	Switch off device	18:16	Yes	
Steam Application (Attempt One)				
Device	**Activity**	**Date/Time**	**Successful**	**Other notes**
Main-Device	Turn on device	03/03/2020 16:48	Yes	
Main-Device	Open Wireshark	16:50	Yes	
Main-Device	Start capturing data using Wireshark	16:52	Yes	
Main-Device	Open Steam application	16:53 – 16:56	Yes	Steam updated on startup
Main-Device	Enter login details and login	16:57	Yes	
Main-Device	Use the add game feature to add “Rubi The Wayward Mira” to account game library	16:58	Yes	
Secondary-Device	Send icp.maindevice2020 a friend request	N/A	No	Unable to send friend request due to “Limited account”. Attempted to send friend request from icp.maindevice2020 to icp.seconddevice2020 concluded in same

				result.
Main-Device	Stop Wireshark from capturing data, save data captured onto external storage device	17:03	Yes	Attempt ended early due to friend request issues.

Steam Application (Attempt Two)

Device	Activity	Date/Time	Successful	Other notes
Main-Device	Turn on device	10/03/2020 16:50	Yes	was
Main-Device	Open Wireshark	16:52	Yes	
Main-Device	Start capturing data using Wireshark	16:53	Yes	
Main-Device	Open Steam application	16:54	Yes	
Main-Device	Enter login details and login	16:55	Yes	
Secondary-Device	Top up account, using “Redeem a Steam Wallet Code” option and entering top-up code		No	Stem code returned invalid multiple times and a 30 minute time limit was required to re-enter the code.
Main-Device	Stop Wireshark from capturing data		Yes	Attempt ended early due to top up issues.

Steam Application (Attempt Three)

Device	Activity	Date/Time	Successful	Other notes

Main-Device	Turn on device	10/03/2020 17:46	Yes	
Main-Device	Open Wireshark	17:47	Yes	
Main-Device	Start capturing data using Wireshark	17:48	Yes	
Main-Device	Open Steam application	17:49	Yes	
Main-Device	Enter login details and login	17:50	Yes	
Main-Device	Top up account, using “Redeem a Steam Wallet Code” option and entering top-up code	17:57	No	Stem code returned invalid on Main-Device. Attempt to redeem on Secondary-Device was successful.
Secondary-Device	Send icp.secondarydevice2020 a friend request	18:01	Yes	
Main-Device	Accept friend request	18:02	Yes	
Main-Device	Using Steam chat send message “Steam 1 Ad astra per aspera” to icp.seconddevice2020	18:03	Yes	
Secondary-Device	Reply to message with “Steam 2 Acta deos numquam mortalia fallunt”	18:03	Yes	
Main-Device	Reply to message with http://www.google.co.uk	18:04	Yes	
Main-Device	Send voice chat request to icp.seconddevice2020	18:04	Yes	
Secondary-	Accept voice chat request	18:04	Yes	

Device				
Main-Device and Secondary-Device	Keep voice chat active for 1 minute	18:05	Yes	
Secondary-Device	Send icp.maindevice2020 ImageSteam.png	18:06	Yes	
Secondary-Device	Send icp.maindevice2020 VideoSteam.mov	18:07	No	File type now not supported, Attempt to change file type also not supported.
Main-Device	Open "Rubi The Wayward Mira" from Steams game library	18:08	Yes	
Main-Device	Send icp.seconddevice2020 an invite to watch	18:08	No	Steam will not allowing streaming without money on the account. Because money code would not redeem on this account. Only Secondary-Device has the capability to stream.
Secondary-Device	Open "Rubi The Wayward Mira" from Steams game library and send icp.maindevice2020 an invite to watch	18:13	Yes	Device Swapped
Main-Device	Accept invite to watch	18:13	Yes	Device Swapped
Main-Device and Secondary-Device	Keep Steam Broadcast active for 10 minutes	18:13	Yes	Device Swapped

While streaming				
Secondary-Device	Go into Steam broadcast settings and enable “Record video from all applications on this machine”, “Record audio from all applications on this machine” and “Record my microphone”	18:15	Yes	Device Swapped
Main-Device	Using Steam broadcast chat send message “Steam 3 Carpe vinum”		No	Account cannot comment without money in account
Secondary-Device	Using Steam broadcast chat send message “Steam 4 Alea iacta est”	18:15	Yes	
Main-Device	Open Internet explorer and search for “cute cat videos”	-	n/a	
Main-Device	Play a random video with the sound on	-	n/a	
After streaming				
Main-Device	Close “Rubi The Wayward Mira”	-	n/a	
Main-Device	Insert external storage device into device	18:23	Yes	
Main-Device	Stop Wireshark from capturing data, save data captured onto external storage device	18:23	Yes	
Main-Device	Close Wireshark	18:24	Yes	
Main-Device	Open Magnet RAM capture	18:24	Yes	
Main-Device	Save data collected by Magnet RAM capture onto	18:24-	Yes	

	external storage device	18:29		
Main-Device	Switch off device	18:28	Yes	

Figure 50 - Project Plan Amended

Title	Week of 16/03/20	Week of 23/03/20	Week of 30/03/20	Week of 06/04/20	Week of 13/04/20	Week of 20/04/20	Week of 27/04/20	Week of 04/05/20	Week of 11/05/20	Week of 18/05/20	Week of 25/05/20
Deadlines							Original Deadline				Project Deadline
Proof reading and final changes									🟦	🟦	🟦
Abstract and Introduction											
Title Page											
Abstract								🟦	🟦		
Introduction								🟦	🟦		
Analysis											
Objective 1: Research											
Chapter 2											
Objective 2: Research											
Chapter 3											
Objective 3: Research											
Chapter 4											
Synthesis											
Chapter 5/Objective 4											
Objective 5: Implement Plan	🟦	🟦									
Chapter 6/ Objectives 5,6		🟦	🟦	🟦	🟦						
Evaluation and conclusion											
Objective 7: Evaluation					🟦	🟦					
Objective 8: Conclusion						🟦	🟦				

Figure 51– Project Logbook

KV6003: Individual Computing Project
Student eLogbook

Student name and ID: Shona Start w17019752
Academic year: Year 4
Programme: Computer and Digital forensics
Project title: Investigation and comparison of the recoverable forensic artefacts from a selection of gaming and chat applications running on a Windows 10 platform
Supervisor: Philip Anderson
Supervisor email and room number: Philip.anderson@northumbria.ac.uk
Second marker: Petia Sice
Second marker email and room number: petia.sice@northumbria.ac.uk

Semester 1 Week 1:

Date and time of meeting: 03/10/2019 13:00	As scheduled: Yes
Brief description of work done since last meeting: n/a	
Number of hours spent on project since last meeting: 0	
Questions/items to discuss at meeting (agenda): Initial Project Discussion	
Agreed tasks for next meeting: Go over PID, Discuss TOR	
Documents discussed /any other issues: n/a	
Date and time of next meeting: 10/10/2019 14:30	

Semester 1 Week 2:

Date and time of meeting: 10/10/2019 14:30	As scheduled: Yes
Brief description of work done since last meeting: Draft of PID completed, studying of relevant academic texts	
Number of hours spent on project since last meeting: 6	
Questions/items to discuss at meeting (agenda): completion of PID and Starting of TOR	
Agreed tasks for next meeting: Discuss current work on TOR	
Documents discussed /any other issues: PID and TOR	
Date and time of next meeting: 17/10/2019 14:30	

Semester 1 Week 3:

Date and time of session: 17/10/2019 14:30	As scheduled: Yes
Brief description of work done since last meeting: Started working on TOR (Background to project, Aims, Objectives, Sources of information, Resources)	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Discuss current work on TOR	
Agreed tasks for next meeting: Discuss TOR	
Documents discussed /any other issues: TOR	
Date and time of next session: 24/10/2019 14:30	

Semester 1 Week 4:

Date and time of session: 24/10/2019 14:00	As scheduled: No
Brief description of work done since last meeting: Continued working on TOR (Proposed work, Skills, Structure, Marking Scheme)	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Last steps required to complete TOR	
Agreed tasks for next meeting: Completion of TOR	
Documents discussed /any other issues: TOR	
Date and time of next session: 31/10/2019 14:30	

Semester 1 Week 5:

Date and time of session: 31/10/2019 14:30	As scheduled: Yes
Brief description of work done since last meeting: Continued working on tor (Quality of practical work, Project plan), researched subjects to be covered in analysis chapters.	
Number of hours spent on project since last meeting: 7	
Questions/items to discuss at meeting (agenda): Completion of TOR, ethics form.	
Agreed tasks for next meeting: Ethics form approval, Meeting with second marker	
Documents discussed /any other issues: TOR, ethics form	
Date and time of next session: 07/11/2019 14:30	

Semester 1 Week 6:

Date and time of session: 07/11/2019 15:00	As scheduled: No
Brief description of work done since last meeting: Final touch ups to TOR, ethics form	
Number of hours spent on project since last meeting: 5	
Questions/items to discuss at meeting (agenda): Ethics form, Meeting with second marker	
Agreed tasks for next meeting: Discuss starting analysis chapters, meeting with second marker	
Documents discussed /any other issues: TOR, ethics form	
Date and time of next session: 14/11/2019 14:30	

Semester 1 Week 7:

Date and time of session: 14/11/2019 18:00	As scheduled: No
Brief description of work done since last meeting: Submitted ethics form, emailed second marker, research for analysis chapters	
Number of hours spent on project since last meeting: 5	
Questions/items to discuss at meeting (agenda): TOR Review, Analysis chapters	
Agreed tasks for next meeting: TOR Review	
Documents discussed /any other issues: TOR Review	
Date and time of next session: 21/11/2019 13:30	

Semester 1 Week 8: TOR Review

Date and time of session: 21/11/2019 13:30	As scheduled: Yes
Brief description of work done since last meeting: Minor changes to TOR in preparation for review, Notes and research for analysis chapters.	
Number of hours spent on project since last meeting: 7	
Questions/items to discuss at meeting (agenda): TOR Review	
Agreed tasks for next meeting: Discuss analysis chapters	
Documents discussed /any other issues: TOR	
Date and time of next session: 28/11/2019 14:00	

Semester 1 Week 9:

Date and time of session: 28/11/2019 14:00	As scheduled: Yes
Brief description of work done since last meeting: Research for analysis chapters	
Number of hours spent on project since last meeting: 7	
Questions/items to discuss at meeting (agenda): Analysis chapters	
Agreed tasks for next meeting: Discuss work on chapter 2	
Documents discussed /any other issues: Analysis chapters	
Date and time of next session: 05/12/2019 14:00	

Semester 1 Week 10:

Date and time of session: 05/12/2019 14:00	As scheduled: Yes
Brief description of work done since last meeting: Started chapter 2	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Chapter 2	
Agreed tasks for next meeting: Discuss chapter 2 and chapter 3	
Documents discussed /any other issues: Analysis chapters	
Date and time of next session: 12/12/2019 14:00	

Semester 1 Week 11:

Date and time of session: 12/12/2019 14:00	As scheduled: Yes
Brief description of work done since last meeting: Continued chapter 2, started chapter 3	
Number of hours spent on project since last meeting: 10+S	
Questions/items to discuss at meeting (agenda): Chapter 2 and Chapter 3	
Agreed tasks for next meeting: Discuss work for Christmas Break	
Documents discussed /any other issues: Chapter 2 and Chapter 3	
Date and time of next session: 19/12/2019 13:30	

Semester 1 Week 12:

Date and time of session: 19/12/2019 13:30	As scheduled: Yes
Brief description of work done since last meeting: Worked on analysis chapters	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Analysis chapters	
Agreed tasks for next meeting: Discuss work completed over Christmas break and next steps	
Documents discussed /any other issues: analysis chapters	
Date and time of next session: To be determined	

Semester 2 Week 1:

Date and time of session: 23/01/2020 14:00	As scheduled: N/A
Brief description of work done since last meeting: Completed Draft of analysis chapters, started chapter 5	
Number of hours spent on project since last meeting: 20+	
Questions/items to discuss at meeting (agenda): Analysis chapters, synthesis chapters, practical work	
Agreed tasks for next meeting: Discus chapter 5	
Documents discussed /any other issues: Chapters 2 to 5 and when to start practical work	
Date and time of next session: 31/01/2020 12:30	

Semester 2 Week 2:

Date and time of session: 31/01/2020 12:30	As scheduled: Yes
Brief description of work done since last meeting: Continued working on chapter 5	
Number of hours spent on project since last meeting: 8	
Questions/items to discuss at meeting (agenda): Reschedule next week's meeting, Chapter 5	
Agreed tasks for next meeting: Discus all work completed so far	
Documents discussed /any other issues: Chapter 5	
Date and time of next session: 10/02/2020 14:30	

Semester 2 Week 3:

Date and time of session: 10/02/2020 14:30	As scheduled: Yes
Brief description of work done since last meeting: Made changes to chapter 4, completed draft of chapter 5	
Number of hours spent on project since last meeting: 7	
Questions/items to discuss at meeting (agenda): Discus all work completed so far, and what to approach next	
Agreed tasks for next meeting: Discuss practical work, hand over all draft chapters for full reading	
Documents discussed /any other issues: All work so far	
Date and time of next session: 14/01/2020 12:30	

Semester 2 Week 4:

Date and time of session: 14/01/2020 12:30	As scheduled: Yes
Brief description of work done since last meeting: Changes and additions discussed at last meeting	
Number of hours spent on project since last meeting: 6	
Questions/items to discuss at meeting (agenda): Practical work	
Agreed tasks for next meeting: Discuss Practical work	
Documents discussed /any other issues: All work so far	
Date and time of next session: 21/02/2020 12:30	

Semester 2 Week 5:

Date and time of session: 28/02/2020 12:30	As scheduled: Yes
Brief description of work done since last meeting: Practical work (Discord)	
Number of hours spent on project since last meeting: 7	
Questions/items to discuss at meeting (agenda): Practical work	
Agreed tasks for next meeting: Discuss Practical work	
Documents discussed /any other issues: N/A	
Date and time of next session: 06/02/2020 12:30	

Semester 2 Week 6:

Date and time of session: 04/03/2020 12:30	As scheduled: No
Brief description of work done since last meeting: Practical work (Twitch, Steam)	
Number of hours spent on project since last meeting: 5	
Questions/items to discuss at meeting (agenda): Practical work	
Agreed tasks for next meeting: Discuss Practical work and imaging hard-drive	
Documents discussed /any other issues: Issue with Steam App	
Date and time of next session: 13/03/2020 12:30	

Semester 2 Week 7:

Date and time of session: 13/03/2020 12:30	As scheduled: Yes
Brief description of work done since last meeting: Practical work (Steam)	
Number of hours spent on project since last meeting: 5	
Questions/items to discuss at meeting (agenda): Impact of Covid-19 on project, Imaging hard-drive	
Agreed tasks for next meeting: Image hard drive	
Documents discussed /any other issues:	
Date and time of next session: 17/03/2020 No time set	

Semester 2 Week 8:

Date and time of session: 17/03/2020 13:30	As scheduled: N/A
Brief description of work done since last meeting: None	
Number of hours spent on project since last meeting: N/A	
Questions/items to discuss at meeting (agenda): contingency plan for closer of university buildings, hard-drive image.	
Agreed tasks for next meeting: None	
Documents discussed /any other issues: hard-drive imaged	
Date and time of next session: 20/03/2020 12:20 (Online)	

Semester 2 Week 8 (Meeting 2):

Date and time of session: 20/03/2020 12:20 (Online)	As scheduled: N/A
Brief description of work done since last meeting: Magnet Axiom and Autopsy contingency plan's	
Number of hours spent on project since last meeting: Unknown	
Questions/items to discuss at meeting (agenda): Problems with Magnet Axiom and Autopsy. Meetings moved to Microsoft teams.	
Agreed tasks for next meeting: Start Going through data collected	
Documents discussed /any other issues: Building closures, 2-week extension	
Date and time of next session: 27/03/2020 12:30 (Online)	

Semester 2 Week 9:

Date and time of session: 27/03/2020 12:30 (Online)	As scheduled: Yes
Brief description of work done since last meeting: Collected data from hard drive, started looking at volatile memory	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Progress on analysis,	
Agreed tasks for next meeting: Send first draft of chapter 6	
Documents discussed /any other issues: Difficulties of working from home	
Date and time of next session: 03/04/2020 12:30 (Online)	

Semester 2 Week 10:

Date and time of session: 03/04/2020 12:30 (Online)	As scheduled: Yes
Brief description of work done since last meeting: Started chapter 6	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Chapter 6, No detriment policy	
Agreed tasks for next meeting:	
Documents discussed /any other issues:	
Date and time of next session: 10/04/2020 12:30 (Online)	

Semester 2 Week 11:

Date and time of session: 09/04/2020 13:30 (Online)	As scheduled: No
Brief description of work done since last meeting: Started volatile memory capture, continued chapter 6	
Number of hours spent on project since last meeting: 6	
Questions/items to discuss at meeting (agenda):	
Agreed tasks for next meeting:	
Documents discussed /any other issues: Philip Annual leave	
Date and time of next session: 24/04/2020 13:30 (Online)	

Semester 2 Week 12:

Date and time of session: N/A - No meeting	As scheduled: N/A
Brief description of work done since last meeting: N/A	
Number of hours spent on project since last meeting: N/A	
Questions/items to discuss at meeting (agenda): N/A	
Agreed tasks for next meeting: N/A	
Documents discussed /any other issues: N/A	
Date and time of next session: N/A	

Semester 2 Week 13:

Date and time of session: 24/04/2020 13:30 (Online)	As scheduled: Yes
Brief description of work done since last meeting: Chapter 6, notes for introduction, evaluation and conclusion	
Number of hours spent on project since last meeting: 20+	
Questions/items to discuss at meeting (agenda): Network capture, Literature Review	
Agreed tasks for next meeting: Discuss evaluation/conclusion	
Documents discussed /any other issues:	
Date and time of next session: 01/05/2020 13:30 (Online)	

Semester 2 Week 14:

Date and time of session: 01/05/2020 13:30 (Online)	As scheduled: Yes
Brief description of work done since last meeting: Chapter 6, started evaluation.	
Number of hours spent on project since last meeting: 10+	
Questions/items to discuss at meeting (agenda): Network traffic analysis, evaluation, Viva	
Agreed tasks for next meeting: Go through evaluation and conclusion	
Documents discussed /any other issues:	
Date and time of next session: 08/05/2020 13:30 (Online)	

Semester 2 Week 15:

Date and time of session: 07/05/2020 13:30 (Online)	As scheduled: No
Brief description of work done since last meeting: Continued working on evaluation and conclusion	
Number of hours spent on project since last meeting: 8	
Questions/items to discuss at meeting (agenda): Evaluation, conclusion, extension, viva	
Agreed tasks for next meeting: No more meetings	
Documents discussed /any other issues: Extension till 28/05/2020	
Date and time of next session: N/A	