FAO Dr. Ian Kennedy

Department of Computing

BSc (Hons.) Computer Forensics and Security

2017–2018

IS 40

Retrieval of Digital Artefacts from TeamSpeak and Discord: A Forensic Investigation and Analysis of the Malicious Use of Gaming Communication Clients.

Author: Oliver George Bryant

Supervisor: Dr. Ian Kennedy

E-mail: `recruitme@kittymagician.com`
Former Student E-mail: `ob75@canterbury.ac.uk`

This report is submitted in partial fulfilment of the requirement for the BSc in Computer Forensics and Security at Canterbury Christ Church University.

I declare that this report is my own original work containing no personal data as defined in the Data Protection Act (1998) and that I have read, understood and accept the University's regulations on plagiarism/intellectual property rights/research ethics and the IS 40 Module Handbook.
Further, I accept that digital and/or hard copies of my Individual Study 40, or parts thereof, may be made available to other students, individuals and organisations after it has been marked.
Finally I accept that no (digital or hard) copy of my Individual Study 40 (including any optical/magnetic media and any other material that may have been submitted as part of my Individual Study 40) will ever be returned regardless of the circumstances.

Date of Submission: **2018–06–1**

Abstract

Gaming communication clients such as Discord and TeamSpeak have started to become an active choice for committing acts of crime, from being used to groom children to being used to organise crimes. The forensic examination of modern gaming communication clients has gone largely unexplored. This paper aims to understand the effectiveness of current moderation tools used to filter online abuse and to look at the possibility of extracting terrestrial artefacts that are left after use from these clients. In addition, a review into current legal cases highlights the need for further research into this specialist area of communication clients. Potential artefacts that may be detected during research includes data such as timestamps, conversations and transferred files. This research aims to contribute towards helping fill gaps by forensically analysing TeamSpeak and Discord.

Keywords: DiscordApp, TeamSpeak3, Digital Forensics, Gaming Communication Clients

Acknowledgements

Many Thanks to my supervisor Dr. Ian Kennedy for providing me support during my Dissertation. Thank you to Giri, Chris, Dan, Peter and Nicki for their amazing support and insight into the industry. Thanks to Teamspeak GmbH and DiscordApp for giving me permission to conduct a forensic analysis of their clients. I wish to thank Danny Werb for his support with LaTeX. I wish to thank my supportive family. My Auntie Wendy for providing me my first personal computer and introducing me to a laptop at the age of 3. My Mother and Nan for providing me support and helping me fight though Illness to get to this point. Finally thank you to my mentor Sophie and Malcolm who proof read this dissertation and Clare for being an excellent Student Facilitator over the past three years. Many Thanks to Cornwallis Academy for getting me interested in Computers. I dedicate this work to the Breck Foundation and Lorin and to my late Granddad Donald "Don" Thomas Edgar Davies who taught me that if you put your mind to things, anything is possible.

Contents

List of Figures

List of Tables

List of Listings

Chapter 1

Introduction

Communication Platforms for the online gaming culture provide a new frontier for forensic analysis. Game Consoles such as Xbox One, Xbox 360, Playstation 3 and 4 all rely on digital delivery and communications services. For Xbox the Xbox Live provides communication services and for PlayStation 3 and 4, which is carried out by the PSN (PlayStation Network). PC Gamers however have a larger choice of communication services which can rely on external third party gaming communication clients such as Discord and TeamSpeak. These clients combine both the use of instant messaging (IM) with Voice over IP (VoIP). These clients are being used to communicate between gamers while playing games online. There is currently very little research into Discord and TeamSpeak forensic artefacts for the PC Platform. In a Google Scholar search and another conducted through the Canterbury Christ Church University Library system no results were returned for "TeamSpeak" nor for "Forensics". While DiscordApp did not return any results on the University Library system, there was a single unpublished article found via Google thus suggesting little to no specific or standardised research on locating forensic artefacts for gaming communication clients on the PC Platform.

DiscordApp has at the time of writing got 9,000,000 peak players per day and over 200,000,000 messages are sent per day. (Discord, 2017c). TeamSpeak statistics are not provided by the company as the service is self-hosted by customers, however the TeamSpeak forums at the time of writing have 189,036 registered users (Teamspeak GmbH, 2017b). While TeamSpeak is a self-hosted solution managed by customers, Discord has greater control; providing the communication platform as a managed service provides users with the ability to create private servers hosted and managed by DiscordApp (kayygee, 2017).

While gaming clients are mainly being used legitimately by millions of gamers around the world legitimately, they are also being used for criminal activity. Discord was used as a communication tool in the Charlottesville protest by alt-right groups (Riot, 2017, Wong, 2017, Lee, 2017). Lee, 2017 argues that members of a discord channel called Pony Power had collected personal details of 50 members of ANIFA, a far left organisation, though a method known as

doxxing. Doxxing is a method in open source intelligence (OSINT) typically open information such as telephone directories, social media and personal websites are used to extract information for malicious intent. Using the information provided by Riot, 2017. Lee, 2017 claims the source of the information who was an anonymous user that had gained the trust of the different alt-right networks. According to Lee, 2017 members allegedly targeted organizations such as The Southern Poverty Law Center that researches hate groups however no further information was specified about other organisations that have been affected. Screenshots from the Discord chat show a discussion about doxxing a student with a t-shirt that included the statement "Punch more Nazis". The user "Albricht" said that he had developed a tool that could be used to extract data from the student. He had created his own url shortner service that had a link that would redirect the traffic to the desired destination. However, when doing so, the traffic would pass through a server that "Albricht" had control of which would allow them to obtain IP address; After allegedly interviewing the targeted individual they claimed they had not clicked the link as it was suspicious. This did not stop "Albricht" from obtaining information which included her "full name, age, current address, college major and the university she attends and her username on several social media sites". The implications of this was the target felt paranoid and had to warn friends that she had been pro-actively targeted by alt-right groups this had a psychological affect on the target (Lee, 2017).

(Muldowney, 2017) reported on how ANIFA, one of the far left groups that took part in the Charlotesville counter-protest also performs doxx attacks on alt-right protesters using doxxing techniques to reveal personal information. A person claiming to be a member of ANIFA using a pseudonym "Fallon" was interviewed. (Muldowney, 2017) claims that "Fallon" is in their mid-30s; has children and works a nine to five job. During the evenings "Fallon" doxxes individuals. Her targets attend far-right rallies, have sent rape or death threats online or are members of white supremacist groups such as the KKK and the National Socialist Movement. "Fallon" typically only has a name or photo to go by and then uses information such as tax documents, voter registration databases, social media, real estate websites, property records and real-life surveillance to verify information. Muldowney, 2017 states that alt-right members co-ordernate attacks from sites such as 4chan, 8chan and Discord. "Fallon" passes on the information to work places, churches and colleges with screenshots showing any questionable activities committed.

According to Keegan Hankes, an analyst at the Southern Poverty Law Center, the doxxing of platforms such as Twitter and Discord makes Hanke's job harder by removing the users being tracked in the active doxxing campaigns. The groups responsible are likely to move there operations to other sites and services which makes it difficult for them to be tracked again (Muldowney, 2017). Menegus, 2017a claims there have also been reports of Child Pornography being distributed via Discord using bots to 'blast' illegal content to users which they had no control over viewing. Since this initial report Discord has taken steps to try and add in protective layers to the application to protect users from image blasting. Implementing "safe direct messaging" which scans in-coming messages to detect content that has already been

previously flagged. Global messaging settings provide a way to switch off chat functionality from strangers. These are optional measures which were implemented to the clients as a response to the reported attacks (Nelly, 2017b).

Even though counter measures have been implemented it has not deterred criminals from using the service. Currently an active case has been discovered as reported by wicz-tv binghamton. This case is an FBI Investigation on an alleged paedophile gang in Michigan, USA which has led to an arrest of an alleged leader of an alleged online gang, Christian Maire. According to wicz-tv binghamton the gang used Discord as method of communication while attempting to locate and exploit children online on popular social media platforms. A member of the gang referred to as S2 in the filed complaint provided evidence and intelligence which led to the full complaint against Maire. The group used code words to describe actions being performed by victims and by the alleged perpetrators "hunt" for when the group was hunting minors. "win" used when a minor was captured sexually explicit on camera, "cap" or "capture" for recordings of victims and "bate" as an abbreviation to masturbate. They also used a minus numbering system to indicate how much younger their victims were than the age 18 (Neubauer, 2017b, Neubauer, 2017a). As described in the filed complaint (2:17-mj-30562-OUTY) the organisation and structure of the group was determined by the the way the server channel was organised (*USA vs Christian Maire* 2017).

In another current criminal investigation Andrew Lynch, 2017 reported on foxnews4k that William Lee Dela Cruz was charged with a two-count indictment and an additional charge on Wednesday, April 19, 2017 after attempting to travel across state lines to engage in illicit sexual conduct with a minor and enticing a minor to engage in illegal sexual activity. It is alleged that Dela Cruz used Facebook, Skype, Phone and Discord to communicate with the minor after meeting her on a Massively Multiplayer Online Game (MMO) called Onigiri (Justice, 2017a).

Looking at case *USA v. DeLa Cruz* 2017 an affidavit supporting the criminal complaint was raised by Amy L. Ramsey (FBI). She claims on April 7th 2017 at 1am the victim aged 12 (pseudonymed as Jane Doe) went missing from the family residence. The Blue Springs Police Department learned that the victim had been communicating on Discord. Forensic Investigators identified the profile "King William" which they linked to 22 year old, William Lee DeLa Cruz after the FBI subpoenaed Time Warner Cable and Discord which provided the FBI with an IP address that was linked to the house of DeLa Cruz. Jane Doe's profile was "William's Queen". The Family co-operated with the FBI and permitted the capture of messages between DeLa Cruz and Jane Doe. Between November 2016 and April 2017 messages were exchanged with some of a sexual nature between DeLa Cruz and Jane Doe. Images were exchanged and Jane Doe's age was discussed. Jane Doe said on her profile she was 15 and in 7th grade, On Jane Doe's Birthday, DeLa Cruz asked how old Jane Doe was. She responded with "15". DeLa Cruz said "we have 3 more years" followed by "iloveyousomuch" (*USA v. DeLa Cruz* 2017, no page) Jane Doe then disappeared on Apirl 9th 2017. An amber alert was issued to locals in the area to be on the lookout for the missing person. Jane Doe confirmed she met DeLa Cruz on the online MMO

Onigiri in early 2016. In November 2016 Jane Doe began to use Skype, Facebook and Discord to talk to DeLa Cruz. DeLa Cruz stated that the relationship between him and Jane doe was Boyfriend and Girlfriend. This was re-enforced by the forensic artefacts recovered by analysing Discord profile data. Jane Doe had stated that she was not allowed to use Facebook anymore as a result of a family fallout. She then used Discord to communicate with DeLa Cruz whom came to pick her up with his brother. Subsequently it is believed that illegal activity took place between DeLa Cruz and Jane Doe.

Shainee Chalk of Woodstock came forward in April 2018 claiming over 40 women's intimate images had been exchanged online via Discord and via Tumblr and other social networks. Woodstock Police are investigating, Chalk claimed that her images had been online for nearly two years but she had been tipped off by another victim about the distribution of her images online (Dubinski, 2018). In another example TeamSpeak was reported as being a tool that was used in the murder and rape of Breck Bednar by Lewis Dayne. TeamSpeak was used as a primary tool to communicate between Lewis Dayne and Breck Bednar which led to Lewis luring Breck to his death. Lewis Dayne was described as the group's ringmaster, had claimed he worked for the US Government and told the teenager that he would receive great wealth through a fictional computing business while playing games online with Dayne. Breck Bednar's mother was suspicious of the relationship that her son was developing with Dayne and at one point she contacted him online to confront him about his behaviour. She also contacted Surrey Police to express her concerns 2 months prior to Breck's death but felt no action was taken. (Halliday, 2015, Smith, 2015, News, 2015).

With closed cases such as Lewis Daynes Beck Bednar (TeamSpeak) and active cases such as USA vs Maire (Discord) and USA vs DeLa Cruz (Discord) digital artefacts from gaming communication clients are being used to help provide insight into illegal activity.

Furthermore gaming communication clients are allegedly being used on the dark web. Intsights, 2017 a digital intelligence company conducted research between July 2016 and July 2017 scraping the dark web. This included pastebins, hacking forums, black markets, IRC Channels, Social Media and Messaging applications for links to popular chat applications. InSights theorise that the closure of popular DarkWeb sites such as AlphaBay, Hansa and the suspected compromise of DreamMarket has damaged user trust in the DeepWeb as a secure environment for communication thus shaking user confidence. IntSights noted a 30x increase in mobile web deep activity over the past 12 months. It was concluded that several hundred thousand users are using mobile messaging apps including Telegram, Whatsapp and Discord to trade account credentials, drugs, hacking tools, and stolen credit cards. Discord is suggested as being the go-to application for mobile dark web discussions with 9x more dark web invitations than competing messaging applications (Intsights, 2017). DiscordApp has been used as a method of command and control server for malware. The report by Trend Micro (Hilt, 2017) details how the popular online game robolox had been exploited by a cookie stealer that uses Discord as a method to communicate the details required for an attacker to take over an account.

Attackers made use of the Discord API and programmatically developed an automated method of transfering the cookie string details using webhooks as a method of exphiltration.

Another challange facing digital forensic is encryption TeamSpeak3 currently implements AES Encryption which the developers state encrypts text messages, passwords and "commands" however the use of encryption for voice, telnet and file transfers are not encrypted (Peter, 2012), While Discord impliments SSL encryption between the Discord Server and Client and server side data is encrypted at rest (leigonof7, 2017) and researchers have already claimed to have found that cached data from the client contains messages in clear text (Williams, 2017) as a result community requests to provide end to end encryption has been declined by Discord. Instead a third party developer has created "better discord" which includes a plugin that provides end to end encryption (Bluscream, 2017).

The Literature Review will attempt to explore if there have been any attempts to forensically analyse gaming voip clients (TeamSpeak and Discord) and understand if there is a gap in research for a comparison of digital artefacts between clients. A digital investigation of Discord and TeamSpeak will be undertaken and artefacts generated by using the client and installing and uninstalling the gaming communication clients will be correlated and analysed.

1.1 Aims and Objectives

This paper aims to understand *"What malicious use of gaming communication clients is occurring in TeamSpeak and Discord?"* involving a comparison of the data from TeamSpeak and Discord. Digital artefacts will be studied. For example if the client has messages that can be retrieved forensically this would be an ideal evidence artefact. In order to understand this the following sub-questions need to be addressed.

- *Are the current mechanics for reporting, muting and blocking content effective?*

  In order to establish if mechanism to report, mute and block content is effective a survey will be conducted of a population of individuals that use Discord and TeamSpeak to identify if and how effective the use of moderation tools are.

- *What types of digital artefacts can be extracted from TeamSpeak and Discord?*

  Digital artefacts will be examined to determine connections between different individuals in order to establish if and what data has been transmitted.

- *What is the difference in digital artefacts extracted from TeamSpeak and Discord?*

Chapter 2

Literature Review

2.1 Introduction

A literature review of VoIP and Instant Messaging clients is required to understand techniques, research methodologies, forensic practice and tooling currently being used by other researchers to gain an insight into real world issues and malicious use surrounding the use of VoIP communication clients, focusing on research related to gaming communication clients. As part of this literature review a search was conducted using Google Scholar and Canterbury Christ Church University (CCCU) Library resources to identify research that has already been conducted in this area. Keywords such as "Discord", "TeamSpeak" with the combined keywords of "Law" and "Crime" helped provide context into active use cases of malicious usage of Gaming Communication Clients. The literature review will investigate how other types of similar applications have been forensically analysed.

2.2 Real World Issues And Malicious Use Of VOIP Clients

In a recent study by (Gregorio et al., 2017), a forensic analysis was conducted on telegram messenger for Windows phone to analyse how information is structured and to extract data such as chat and conversational data. Researchers applied three stages of analysis: open knowledge; analysis of artefacts; source code in order to attempt to obtain artefacts. The three step analysis allowed a range of information to be extracted, potentially helpful to forensic investigation. Gregorio et al., 2017 states that the communication services can transmit images, content and documents which could potentially be used for malicious purposes such as "threats, phishing, cyberbullying, grooming and terrorist propaganda" (Gregorio et al., 2017, p. 88) however citations provided only illustrate terrorist propaganda use cases of telegram. According to Jesse Cox Discord has had an increased presence in revenge pornographic material being distributed to the services according to media outlets. It is believed by the media outlets that after the closure of an

anonymous image board (AnonIB) users migrated to Discord and Slack (Cox, 2018a,c). Facebook has piloted the creation of a hash database that users can upload their explicit materials to in order to have them removed from the platform (Solon, 2017). This is conducted by comparing the unique MD5 hash of the file against images being uploaded to the service. Companies are already scanning photos being uploaded to the internet via Microsoft PhotoDNA however the Hashes are currently used for Child Exploitation only (Cox, 2018d). cox highlights the fact that the services are freely available and could easily be adapted for use in combating revenge porn.

2.3 Methods of Research

A forensic analysis of Skype and Facebook for the Microsoft Windows 8.1 platform was conducted by Yang et al., 2016a to capture terrestrial artefacts from both Skype and Facebook. The investigation included generating artefacts from general use and during installation and uninstallation of the client. Yang et al., 2016a states the methodology used in the research is based on the technique developed by McKemmish, 1999 which includes the identification and discovery of digital evidence ensuring that there is an understanding of what types of data that could be useful for examination, preserving the digital evidence. The data must be preserved in a method that could be used for legal scrutiny. Data must not be altered however if the data is altered an explanation of how this is done should be discussed. This ruleset follows the same guidelines developed for ACPO Principles 1, 2 and 3. (7Safe and Chief Police Officers, 2017). The processing of evidence which includes explaining the processes that are undertaken to obtain the information and finally the presentation of evidence which includes the qualifications of the individual undertaking the study and the credibility of processes being used to obtain the evidence (McKemmish, 1999). Applying the Mckemmish methodology, (Yang et al., 2016a) created an experiment of 8 fictional user accounts that would emulate victims and suspects. Unique names and profile icons were assigned to each user account. Two Virtual Machines for the victim and for the suspect were assigned.

2.4 Forensic Practice And Tooling

Yang et al., 2016a provides a style of forensic investigation that emulates a forensic lab report. Details such as the type of software being used and the log of each discovery are recorded for future use. Each piece of evidence of significance is labelled in a table for each phase of the study. This style of investigation has been emulated by (Williams, 2017) whom has conducted a non-peer reviewed study into Slack, Dropbox, Discord and Twitter. (Williams, 2017) who conducted the analysis on Windows and Macintosh. Williams, 2017 used an excel spreadsheet and collected data parsed from images, user activity and files uploaded by the user. SQLLite Browser (sqlitebrowser, 2017) and 010 (software, 2017) was used to view the SQLite Databases generated for Dropbox. However due to the accessibility of SQLite database files and GUI tools

evidence such as discovered by (Williams, 2017) in the DropBox application could be manipulated according to Teng and Lin, 2012). (Williams, 2017) also emulated the use of virtualisation for the project citing multiple examples of research that implemented the technique. The research group was able to find message logs in the Discord Cache folder, profile data and user login data. Each feature was tested which included file uploads, role changes, banning users messages (Williams, 2017) concluded that the research group undertaking the study had hypothesised that Discord would produce less data than Twitter and Dropbox however Discord had the most digital artefacts recorded. Furthermore the research team was unable to analyse Twitter as no official Twitter app was available to Windows 7 which reduced the amount of applications being researched. Analysing the reference list (Williams, 2017) only had two citations. This confirms that there is little literature available related to the gaming communication client Discord however using techniques developed by (Yang et al., 2016a), (Williams, 2017) was able to successfully obtain terrestrial artefacts from the client using methodologies developed for Facebook Messenger and Skype. Both (Williams, 2017) and (Yang et al., 2016a) have used virtual machines within the environment, Yang et al., 2016a used a technique developed by Quick and Choo (Quick and Choo, 2013b, Quick and Choo, 2014, Quick and Choo, 2013a) as this methodology provides a method of recovery after each experiment. An alteration to the method was made omitting the use of CCleaner from both the research conducted by Williams, 2017 and Yang et al., 2016a for snapshots for each phase of investigation. Quick and Choo noted that the use of the tool Process Monitor v3.03 by Sysinternals (Russinovich, 2017) generated large amounts of data that altered the forensic image as such; In order to remedy the additional data being created separate examinations took place to forensically image the machine after each use (Quick and Choo, 2013b).

2.5 Effective Countermeasures for Reporting, Blocking and Muting Communication Clients

On the 28th March 2017 Nelly from the Discord announced multiple improvements to the security of the client which included notifying users the destination of redirected links to prevent the malicious use of URL Forwarding services. The implementation of Explicit Content Filtering was also introduced to filter out explicit photos and messages. Direct Messaging was also locked down to prevent random external contacts from being able to contact users by direct message (Nelly, 2017b). Although these safety measures had been rolled out to the general public there where reports from the Discord community of the use of spam bots to send explicit materials to users on servers (Hilt, 2017). TeamSpeak3 includes it's own set of moderation tools however, these are configured by the server administrator. As TeamSpeak3 is self-hosted the responsibility of moderation falls on the administrator of the server. As such there is a gap that requires Quantitative research into if the current countermeasure (muting) works within the client.

2.6 Conclusion

In conclusion the literature review found small amounts of literature regarding forensic analysis of gaming communication clients. Methodology has been adapted from work conducted by Gregorio et al., 2017 who developed a framework for analysis of digital artefacts which can be applied to forensic analysis in phases of research. Furthermore Yang et al., 2016a forensic analysis of Skype and Facebook offers a method of recording data as it is being processed which complies with ACPO Guidelines Section 3. Moreover Yang et al., 2016a adopted the methodology used by McKemmish, 1999 that promotes the preservation of data, attempts to provide relevancy to digital artefacts and explains that evidence altered in the process of extracting it must be noted. This study is similar to the steps provided by ACPO Guidelines 1, 2 and 3. Research conducted by Teng highlights the possibility that a SQLite file could be tampered with using freely available software Teng and Lin, 2012 confirming the need to follow appropriate guidelines for processing digital evidence in future research. Quick and Choo, 2013b, Quick and Choo, 2014 implemented the use of Virtual Machines in the study of digital artefacts of DropBox and Google Drive illustrating that the use of Virtual Machines provided speed and the ability to restore a virtual machine to a safe state during the investigation providing repeatability of an experiment. However there were no papers or journal articles found which contained a forensic analysis of TeamSpeak. A previous digital forensic study on Twitter, DropBox and Discord had been conducted which found some positive results for locating digital artefacts from Discord, but these results have not been published in a academic/peer reviewed journal Williams, 2017. Therefore it is seems that there is a gap in the research literature at present particularly in regards to TeamSpeak and Discord which looks at protection against malicious activity. Furthermore, there is little research into extracting data from gaming communication clients which can assist forensic investigation particularly as these communities are very private in nature.

Chapter 3

Ethical and Legal Considerations

3.1 Legal Considerations

3.1.1 Computer Misuse Act 1990

As permission from both companies has been provided as well as the use of my own hardware and virtual machines to create the environments and the creation of the servers used for the experiment only in a controlled environment there are no issues that could occur in relation to the Computer Misuse Act 1990. Companies authorized consent of a forensic analysis of their gaming communication clients for this study. This was confirmed by the supervisor who reviewed the materials provided as proof.

3.1.2 Data Protection Act 1998

The Data Protection Act 1998 was heavily considered when writing the Survey. During the creation of the Survey participants are not asked for any personal identifiable information with the exception of gender which they can opt out of including. The Survey also includes a disclosure ensuring that participants could opt out upon request. No participants requested to opt out of the study. In the experiments the communication is occurring between the researcher's own controlled environment and no external communication channels that face the public. For TeamSpeak firewall rules were created so that only IP addresses that the researcher had access to could connect to the environment reducing additional risk of breach. The TeamSpeak3 server was password protected to ensure that no external clients from the general public could connect.

3.1.3 Discord Inc.

DiscordApp authorised a forensic investigation of the client as long as it followed the terms of service by following the rules.

- Only use and test on accounts and servers you directly own. Testing should never affect other users.
- Don't perform any actions that could harm the reliability or integrity of our services and data. Some examples of harmful activities that are not permitted under this bounty include: brute forcing, denial of service (DoS), spamming, timing attacks, etc. These types of attacks will result in an IP ban.
- No information about issues found should be publicly disclosed or shared until we've completed our investigation and resolution. After confirmation, you are free to document and publish any information about the issues you've found.
- Testing should be limited to sites and services that Discord directly operates. We will not accept reports for third-party services or providers that integrate with Discord through our APIs.
- Don't use scanners or automated tools to find vulnerabilities.
- Social engineering, phishing, or physical attacks are not permitted under the program.

During the explanation email details of the tools used during the investigation was outlined. During the creation of the data conversion tool for the SQLite database there was no indication that DiscordApp Inc wanted the information hosted locally on the Electron Client to be withheld. There was no Passwords protecting the SQLite Databases and as a result the tool was used to simply convert what could already be found in using an off the shelf database viewer into a tool that could be used to convert the open and available data and is able to do so without exploiting or finding vulnerabilities.

3.1.4 TeamSpeak GmbH

TeamSpeak GmBH provided full permission for a forensic analysis to be undertaken stating they would like a copy of the research after the analysis has been conducted. This was authorised by the Business Development Team on the 29th September 2017 via email, This was confirmed by the supervisor (Dr Ian Kennedy).

3.2 Ethical Considerations

The survey element of the study requires human participation however participants are introduced with the following message:

You are invited to take part in a Survey that is looking at how people use moderation tools on Discord and TeamSpeak. The study aims to forensically analyse both Discord and TeamSpeak and look at ways that people currently deal with moderation of malcious content. The Survey will ask if you have had to use tools to block, moderate or stop content from being consumed using moderation tools. However the study will not go into detail as to any incidents that may have required you to do so, The Survey does not include personally identifiable information such as your name, address or email address this is to ensure your Privacy. If you wish to withdraw from the study you are able to opt out at anytime without peanlty. Should you wish to be removed from the Survey please contact Oliver Bryant (o.g.bryant75@canterbury.ac.uk) noting your withdrawl from the service. Data is being processed on the Google Cloud. See https://bit.ly/2uXGI55 for steps taken to secure the data by Google. Once the survey has finished a downloaded copy of the results will be stored by Canterbury Christ Church University, Department of Computing with an encrypted password. During the study Survey data will be monitored by Oliver Bryant and Dr Ian Kennedy via Google Sheets. At the end of the study the data will be handed over to Canterbury Christ Church University in the form of statistics. As such the Google Sheets data will be downloaded onto a University Computer system for data analysis. For information about the University Research Policy please see https://www.canterbury.ac.uk/research-and-consultancy/documents/ethical-procedures.pdf

This Survey is part of a BSc Study and is being run by Oliver Bryant (o.g.bryant75@canterbury.ac.uk) and supervised by Dr Ian Kennedy (ian.kennedy@canterbury.ac.uk). If you have any issues or problems with the Survey please contact me in the first instance. If however you do not feel comfortable or wish to raise a complaint please contact Dr Ian Kennedy. The University also offers a formal complaints procedure. Please see https://www.canterbury.ac.uk/students/academic-services/policy-zone/complaints.aspx for details.

By clicking NEXT you agree to the participation in this Survey.

This message of disclosure includes the fact of Google Forms part of Google GSuite (Google Apps) is being used to store Survey participants data. participants are provided information on how Google protects the data and ensures security and compliance. Participants age was set to 18+ for the gathering of data. Participants have been made aware of how the Data is being retained and that the data will be downloaded onto University Computer Systems for analysis. The Survey does not include any personally identifiable information. Furthermore the participant is given the right to withdraw at any time as included in the disclosure. Participants are provided a method of escalating issues and of the University's complaints procedure. Before the Survey was sent out Dr Ian Kennedy looked over the messages. A discussion on if the questions required ethics clearance was discussed. Some questions where removed to ensure that no harm could come to the individuals participating and ultimately the decision was that the questions do not require an ethical board's clearance as they do not harm a participant psychologically, physically and/or emotionally. In the research proposal psychological stress and anxiety and sensitive topics had been ticked however after a discussion with Dr Kennedy messages had been removed that could have caused psychological stress and anxiety. The focus of the study shifted to the mechanics of the abuse reporting systems rather than the reason the person acted upon using the system. In the Digital Forensics experiments the company's game clients that where being digitally analysed was asked permission for the analysis to be conducted. Permission was granted from the companies to conduct the experiments. Careful consideration was made for ensuring that the experiments where conducted in a controlled environment that took into consideration the use of public based cloud systems. Server Channels for Discord and TeamSpeak where on created for the experiments. When the TeamSpeak server was setup a firewall policy was put in place to ensure that only ip addresses used by the research equipment was able to access the service. For Discord the channels where password protected to ensure that the server was only accessible to user accounts controlled by the researcher.

Chapter 4

Methodology

4.1 Introduction

The research was conducted in multiple phases in order to answer the research question. Firstly a survey was developed in order to understand how effective reporting, blocking and muting tools are on gaming communication clients. The second phase of this research is the forensic analysis of Discord and TeamSpeak using a base virtual machine that was cloned for each experiment. The experiments apply the methodology of investigation used by Quick and Choo, 2013b and Williams, 2017 which combines the use of freeware tools with commercial forensics tooling. In addition the methodologies developed by Williams, 2017 using a spreadsheet to track and audit the ongoing tests will used to provide a method of tracking the experiment. The digital artefacts being focused on will include any types of identifiable data (Images, conversations, Logs) this will be curated into a spreadsheet and finally into the dissertation. In order to deal with contamination issues and to adhere to ACPO Guidelines the methodology of Quick and Choo, 2013b combined with McKemmish, 1999's approach to handling evidence will be applied. The use of Virtual Machines will be conducted as part of the methodology to provide a roll back to a "clean" state after each experiment. This is modelled on the methodology conducted by (Yang et al., 2016a). A selection of tools where used in the experiments as well as the statistics associated with the survey.

4.2 Survey

4.2.1 Population

The population was calculated using Slovin's formula the population is modelled on the predicted UK Gaming Population provided by the GameTrack Quarter 3 digest statistics which state that 11.4 million people in the United Kingdom play games on Personal Computers (ISFE,

2017b). As Discord and TeamSpeak are the target market for these clients the statistical model has been developed to target a large group of people who play online games between a wide age range of 18-66+ The Survey was launched on the 03/03/2018 and was closed on 18/04/2018.

$$n = \frac{N}{1 + Ne^2}$$

E = margin of error
N = Population Size
n = Sample Size
95% confidence = 0.95
The margin of error was calculated to 95%

$$e = 1 - 0.95 = 0.05$$

Population = 11.4
Sample Size = 399.985 = 400
Calculation of the error margin is set to 0.5%

$$n = \frac{11.4 * 10^6}{1 + 11.4 * 10^6 * 0.05^2}$$

Total number of respondents required = 400

4.2.2 Analysis

As the Survey data is categorical, standardised tests such as the Student-T test is not applicable therefore the use of a Pearson Chi-Squared test of cross tabulation is used. Data is grouped into two categories and then the P-Values are evaluated. Anything below *0.05%* **is** significantly different. Anything above *0.05%* is **not** significantly different. If the value of any of the cells of data is less than 5 the Fishers exact test will be applied.

4.2.3 Survey Content

The Survey is set out to determine the effectiveness of current countermeasures employed by Discord and TeamSpeak to understand if and how effective abuse reporting tools are for Discord and TeamSpeak. Participants are asked if they have had to mute, block and report other users on Discord and TeamSpeak.

4.3 Experiments

Each experiment was logically isolated in order to prevent contamination and followed 5 stages.

- Installation Phase

  The analysis of artefacts dropped from the setup executable during the installation of the gaming communication clients. (if time allows)

- Execution Stage

  The analysis of artefacts dropped from the main application executable during general use with a simulated external user generating metadata.

- Uninstallation Phase

  The analysis of artefacts that remain on the file system after an application is uninstalled. (if time allows)

- Simulated Conversation

  A simulated conversation to establish what digital evidence that may have been exchanged between clients.

- Analysis

  After each experiment the file was exported as a RAW image file which will be later parsed by EnCase 7 for forensic analysis. (this was later changed to X-Ways and Autopsy)

4.3.1 Experimental Forensics

As there was very little literature related to a methodology of discovering digital artefacts for Gaming Communication clients inspiration was taken from (Yang et al., 2016a) whom used a mixture of forensics tools to locate metadata from windows based messaging applications. Yang et al. was able to obtain artefacts from SQLite files in the AppData section of the windows operating system and using memory forensics to obtain hidden artefacts. During each experiment careful consideration was taken into trying to improve the forensic integrity of the data being handled. During the research phase the original hypervisor (Parallels Desktop) used to run the virtual machines was unable to export out to a file format that EnCase and X-Ways would be able to mount. As such the decision was made to switch to Oracle VirtualBox. During the analysis stage for the TeamSpeak Execution Lab the acquisition time was 12 hours. As such a new method of rapid analysis was required, a decision was made to use X-Ways Forensics to preform the analysis on the raw image files using the EnCase FastSE Writeblocker to prevent contamination of changes to the raw disk. During the experimental forensics phase of the Dissertation Discord Forensic analysis a memory forensic analysis was conducted to identify the use of Node.JS and ElectronJS to determine if cache artefacts could be connected to the chromium elements that

cache data from Electron Applications. Due to time constraints 2 phases of the experiment were not conducted, the Installation Phase and the Uninstallation Phase.

4.4 Tooling

The tooling that was used in the forensics experiments is detailed in table 4.1 and the tooling used for in the survey statistics are shown in table 4.2.

Software Name	Version	Use Case
Fiddler	4.6	Decryption of HTTPS traffic from the DiscordApp Client
Sysinterals Process Monitor	v3.50	De-construct the processes executed in the client
DB Browser for SQLite	v3.10.1	Browse .sqlite database files
Nirsoft ChromeCacheView	v1.77	View cache files taken from the Discord-App Client.
Falcon Sandbox/Hybrid Analysis	v7.21	Provides an automated analysis of the executable that can be compared with the manual analysis.
Volatility Foundation Volatility Framework	2.6	Memory DMP Forensic Analysis suite.
comae-toolkit-light	3.0.20180307.1	Using the comae toolkit for DumpIT. DumpIT.exe is used for the capture of RAM/Memory.
Discord Extractor	1.0	Extractor that converts the http_discordapp.com_0.localstorage SQLite into a .CSV file for analysis developed by Oliver Bryant).
TeamSpeak3 Extractor	1.0	TeamSpeak 3 Data Extractor which extracts bookmarks,
FastBlocSE	n/a	USB Writeblocker bundled with EnCase 7, Used to forensically writeblock the external hard drive that contains the virtual machines on.

Parallels Desktop	13.3.0	a virtual machine hypervisor. Originally during the experimental forensics phase but terminared due to the inabiality to export raw images.
Oracle VirtualBox	5.2.10	a virtual machine hypervisor. Used as the hypervisor for the published experiments. The ability to export out disks to raw images from command line made VirtualBox the best choice for the experiment.
EnCase Forensics Training	7.10.00.103	Forensic Examination Tool used to view, report and acquire digital artefacts.
X-Ways Forensics	18.1 SR-8	Forensic Examination Tool used to view, report and acquire digital artefacts.
SQLite2009 Pro	N/A	The default SQLite Viewer used by X-Ways. Used to view the TeamSpeak3 SQLite Cache and Settings files.
Autopsy	4.7.0	Autopsy is an open source forensic analysis tool. It was used as a method of verifying the data discovered in X-Ways.
AccessData Registry Viewer	1.8.0.5	Registry Viewer for viewing Windows Registry Hives.
Forensic Registry EDitor (FRED)	0.1.1	Registry Viewer for viewing Windows Registry Hives on a Linux operating system.
AWS Cloud9	N/A	Portable Python IDE. Used for the analysis of the localstorage discord files with the Discord Extractor tool.

Table 4.1: Tools used in forensic investigation.

Software Name	Version	Use Case
Google Sheets	N/A	Data Storage for Google Sheets
Google Forms	N/A	Survey Platform for the Survey
Minitab 18	18.1	Statistical Software for analysing data using Pearson Chi-Sqaured and Fisher's Exact Testing
Tableau Desktop	2018.1	Data Visualization and Processing

Table 4.2: Tools used in Statistical Analysis.

Chapter 5

Findings

5.1 Forensic Analysis

The aim of preforming a forensics analysis of Discord and TeamSpeak is to locate and find new types of artefacts that can be successfully used to trace communications, artefacts that could be of significant use (images) and identify if users connect to the same communication systems. As applications store data often in the %AppData% folder this was a area of interest within the investigation in both clients. The Registry HIVE was also an area of investigation.

5.2 Experimental Forensics

In April 2018 a small mock experiment was conducted on Discord as a mock victim and attacker simulated conversation. During this experimental phase a new methodgy was developed called the "Media Traversal Theory" for Discord. The artefacts generated by using the Discord client provided ways of monitoring not just the user's activities from inside the client but also any embedded external services though the localstorage and cache, This has become the Media Traversal Theory. The theory is that communication between two clients can be found though using multiple local artefacts generated from the localstorage files and caches. See (figure F.4). During this phase it became clear that current forensic tools struggled with exporting Discord's localstorage SQLite content. As such a new tool was developed called DiscordExactor (see listing F.1) was created to provide a simple way of exporting and viewing the discord localstorage file which then exported out a demonstration file (see listing F.4).

5.2.1 Artefacts Retrieved from Discord

25th May 2018 - Execution Lab Introduction

On the 26th May, at 19:00 the execution experiment for Discord was conducted. It attempted to identify the types of metadata that is generated from Discord. The experiment was conducted on a virtual machine, a user was created for the experiment and a private discord server. The user uploaded the `Kermit.jpg` image to the server and also linked a channel called "royal rumble" from Twitch.TV. The livestream was played inside the Discord client to see if it left any traces.

Execution Lab Capturing Evidence

a raw immage was taken of the virtualbox by using the following command.

```
VBoxManage clonehd Discord\ Execution\ Lab-disk1.vdi
\Volumes\LaCIE\Discord\Discord\ Execution\
Lab\DiscordExecutionLab.raw --format RAW
```

which generated a raw image of the local virtual machine onto an external hard drive that could be write blocked on the forensics machine using FastBlock SE.

25th May 2018 - Execution Lab Forensic Analysis

On the 25th of May the execution forensics was conducted. Using the methodologies developed during the experimental phase with the media traversal theory an investigation into the `AppData\Roaming\discord\Local Storage` section of the client commenced. Within the folder a file called `https_discordapp.com_0.localstorage` was found. An attempt to open the Database in SQLite2009 Pro Enterprise Manager resulted in the request to enter a password protected key (see figure F.49) and Autospy's in built SQL Browser was unable to view localstorage files as well (see figure F.45 and while DB Browser for SQLite was able to open the file it could only show the output in a hexadecimal format. As such the Discord Extractor tool was used to export out a CSV version of the settings. (see listing F.3) Inside the `https_discordapp.com_0.localstorage` SQLite3 file the experiment user's email address, the locale of the keybaord, channel ID and the last connected times to channels, the security token to upload content and draft (empty). This information could be paired with another client's information to determine if the client's have communicated with each other. The Cookies folder was exported out of the client via X-Ways and the Chrome Cache Viewer by NirSoft was used to view the client's cache activities (See figure F.46). Within the Cache there was links to the `kermit.jpg` image: `https://media.discordapp.net/attachments/449692697431769102/449693897225142288/kermit.jpg?width=400&height=269` and `https://media.discordapp.net/attachments/449692697431769102/449693897225142288/`

kermit.jpg?width=610&height=410 these images are stored on DiscordApp's own content delivery network, the images are accessible to anyone who has access to the link and there are no protective measures for ensuring that the image is private. In addition to the image links there was also a link to https://player.twitch.tv/?channel=rumbleroyale&player=facebook&autoplay=1&auto_play=1 and https://images-ext-2.discordapp.net/external/C2YgmRLpnTvGtUzrKVk7rwPJq0LzZxw_l6mbOTcKhi8/https/static-cdn.jtvnw.net/jtv_user_pictures/rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg these links related to the twitch.tv link that was shared in the group as the user had clicked on the video a copy of the player and a profile image from twitch.tv was stored on the client (see figure F.47). In the same localstorage folder a secondary localstorage file was found called https_player.twitch.tv the SQLite3 file included information such as if mute was enabled and times when the player was resumed (see figure F.50 and figure F.51).

29th May 2018 - Execution Lab Network Forensics

A network analysis was conducted on the uploading and downloading method used by Discord. Using Wireshark a network capture was conducted while uploading an image to the Discord service. The capture showed that Discord encrypts the network traffic during transit with TLS1.2 (see figure F.63). The web proxy capture tool Fiddler was then used to decrypt the TLS1.2 encryption. Fiddler acts as a MITM (Man In The Middle) by installing a root certificate on the client machine as seen in figure F.62 the decryption of the file being uploaded was successful.

28th May 2018 - Simulated Conversation from Discord

The simulated conversation experiment took place on two virtual machines, the victim and the attacker. The attacker created a local server and the invite link was used by the victim client. A small conversation between the attacker (John Doe) and the victim (Jane Doe) was conducted by the research switching between the two virtual machines. Image artefacts where transmitted to the victim over the discord server (ducky.jpg) and via direct messages (Kermit.jpg) (see figure F.52), a link to a twitch.tv channel was also included in the chat. The user Jane clicked on the live stream video and then closed the video. The attacker did not click on the video. Looking at the Cache for the Attacker the files ducky.jpg and kermit.jpg are viable from inside the cache. (See appendix I. The attacker left a message in the drafts while talking to Jane Doe over Private Message saying *"I love you"* (see figure F.53). The Cache on the Attacker's machine contained links to the ducky.jpg and kermit.jpg images that had been uploaded to the server created by the Attacker client and the direct message to Jane Doe, During the use of the Discord Extractor tool there was a informative string in the scientist row in the https_discordapp.com_0.localstorage file which included the string user|2018-03_friend-invite-guild-create indicating that the Attacker client had invited another user to the server see figure F.61. On the Victim's client the localstorage

folder contained the `https_discordapp.com_0.localstorage` which contained the same channel IDs as the Attacker Virtual Machine (see listing F.5, listing F.6 and figure F.61). In same folder as `https_discordapp.com_0.localstorage` an additonal local storage file called `https_player.twitch.tv_0.localstorage`. The file is used to record data from the embedded twitch.tv player that was played during the simulation (see figure F.56, appendix I). In the file there was multiple tables for volume, quality of the stream and if the Stream was marked mature (see figure F.57). In the `Cache` multiple artefacts was discovered. The image sent from the attacker `Kermit.jpg` was found in the Victim Cache folder as artefact `f_000025` (see figure F.58). An image that was sent from the attacker to the victim via a private chat (ducky.jpg) was also found in the Cache as artefact `f_000027`. The embedded player address (`https://player.twitch.tv/?channel=elegy&player=facebook&autoplay=1&auto_play=1`) was found inside the Cache (see appendix I). The Cache was also observed from Autopsy to ensure integrity of the findings (see figure F.59).

5.2.2 Artefacts Retreieved from TeamSpeak

21st May 2018 - Execution Lab Introduction

On 21 May, at 19.22, an execution experiment was conducted. This attempted to identify and understand how TeamSpeak3 generated metadata. In order to carry out this experiment, the use of a virtual machine and the administrator user on the host operating system was used to send and receive files. a user uploaded a file called `kermit.png` the experiment aimed to figure if metadata could be located during the execution of TeamSpeak3 from sources such as Databases and the registry.

21st May 2018 - Execution Lab Capturing Evidence

a raw image was taken of the virtualbox after generating user interaction by uploading the image kermit.png. The experiment continued into the next day.

21st May 2018 - Execution Lab Memory Analysis

A memory analysis was conducted on the virtual machine using DumpIT (See figure F.10). The forensic analysis of the memory dump was conducted using the volatility framework. In order to analyse the teamspeak3 executable the PID had to be obtained which was done by using the `pslist` command with volatility (see figure F.11). Once the pslist was obtained the dllist flag was used to get a list of dll files from the executable `ts3_client6` (see figure F.12. During the setup of TeamSpeak3 there was issues running the application during execution. After enabling DirectX support from Oracle VirtualBox the application was able to run without issues. During the forensic analysis the discovery of the .dll `d3dcompiler.dll` indicated the use of DirectX by TeamSpeak3 and qsqlite.dll indicated the use of SQLite as a database for TeamSpeak3 (See

figure F.13). A registry dump was conducted to ascertain if any traces from memory could point to the TeamSpeak3 client. This was conducted by running the dumpregistry flag (see figure F.14), The file `registry.0xfffff8a000ca9010.ntuserdat.reg` contained the registry entries for QTProject which included a key called `LastVisited` which was found in the `filedialog` folder. The entry included a value `file:///C:/Users/Public/Pictures/SamplePictures` (see figure F.15) which is the location that was used to upload a sample picture from. To verify the data twice the use of two registry viewer was used. FRED (see figure F.15) and AccessData Registry Viewer (see figure F.16).

22nd May 2018/23rd May 2018 - Execution Lab Forensic Analysis

EnCase 7 was loaded up and FastBlocSE commenced writeblocking the hard drive. a new case was created for the Execution Lab. After establishing that the disk had been writeblocked the ts3execute.raw file was selected for acquisition. During the initial review it could take 12 hours to process a logical image of the device and upon returning back to the lab in the morning the forensic machine had crashed. As such a new method had to be created to rapidly analyse the data. FastBlocSE was used to writeblock the hard drive (see figure F.18). X-Ways Forensic Investigator was used to examine the ts3client.raw file which contained the contents of the virtual machine. X-Ways contains an option to "Interpret Image as Disk" (See figure F.19). Files were found within the folders and sub-folders of %AppData&\AppData\TS3Client. The `Settings.db` file contained a table called `FileTransfer` which includes three useful keys. the key `UploadDir` which contains the last known upload directory path for files uploaded to the TeamSpeak3 server which was `C:/Users/John Doe/Pictures`. The `SimutaniousUploads` key which specifies how many uploads have occured from the client (2) and The `SimutaniousDownloads` key which specifies how many downloads have occurred from the client (2). (See figure F.22). This was verified with Autopsy (see figure F.28). The `cookies` file contained strings such as `__cfduid` cookie which is connected to CloudFlare a web access firewall proxy and cookies for MyTeamSpeak (see figure F.24 The TeamSpeak Cookies file is used by the MyTeamSpeak Cloud. The cookies file was reverified using Autopsy (see figure F.26).

During the simulation of the execution phase a simple connection, file upload and download commenced. No simulated text chat occured. As such the main focus of the analysis was the residual data in the SQLite Databases. Both the Cookies and Settings SQLite databases where exported out of X-Ways as new files (See figure F.20) for analysis with SQLPro 2009. Autopsy has it's own built-in SQLite Viewer as such there was no additional requirement for a secondary SQLite Viewer.

22nd May 2018 - Execution Lab Network Forensics

On the 22nd May 2018 a network analysis was conducted on the Execution Lab virtual machine. During the analysis the TeamSpeak client was connected to the server and files was uploaded by

the user who downloaded `Kermit.jpg` while downloading the file the wire capture software Wireshark was used to capture network packets. The connection was transmitted over TCP, (See figure F.29). The connection was unencrypted as such the image was viewable from within the network capture and no method of encryption is used to upload and download files within TeamSpeak3. Although there are options to encrypt the voice transmissions within the client there are no options to enforce encryption of file uploads and downloads from the client.

25th May 2018 - Simulated Conversation from TeamSpeak

A simulation of a conversation between two users was conducted on a TeamSpeak server on May the 24th 2018. The conversation included a discussion in a private channel between the user "Jane" and "John". The client "John" uploads an image called `Kermit.jpg` to the server and asks the user "Jane" to open it. Upon opening the image Jane then communicates via a public channel to inform other users that she has come across an offensive image.

Attacker

The `Settings.db` file provides useful nagivation of the last known upload location for a file. Upon looking in the directory (C:/Users/John Doe/Pictures) which was found in the Settings.db FileTransfer an image called `Kermit.jpg` was found with the hash `79dfc0fcb6526e93fd2ec89f792219e2` (see figure F.39 and appendix I). In the `urls.db` database a single result for a link to google.co.uk was found sent from John however no channel is specified (see figure F.30. In reviewing the `channel.html` and `server.html` logs it is determined that the url was sent to another user on the server however no logs of the link being broadcast in the channels was found within the artefacts as such the clients communicated over a private channel (See figures F.33 and F.34).

Victim

The File Transfer table in the `Settings.db` file on the victim virtual machine contained the statistics that a file had been uploaded and downloaded from the client but no destination was provided for the download. In the downloads directory the file `kermit.jpg` was found with the MD5 hash of `79dfc0fcb6526e93fd2ec89f792219e2`. In the `urls.db` file the link to google.co.uk from John was also found with the same timestamp. In the chat logs (channel.html and server.html). The client connected twice to the TeamSpeak server. The first time the image was downloaded onto the machine and communications between John on the channel "Lobby" concluded that the communication was unsolicited this was discovered by comparing the timestamps from `server.html` and `urls.db` (see figures F.33, F.36 and F.37). The timestamps indicate that the url was sent during the second connection to the client and no information reguarding the url in the public channels indicates that the communication of the link was sent

directly to the client from John. Therefore it is established that John sent the image and the link to the Victim (Jane).

5.3 Statistical Analysis

5.3.1 Question One: Gender

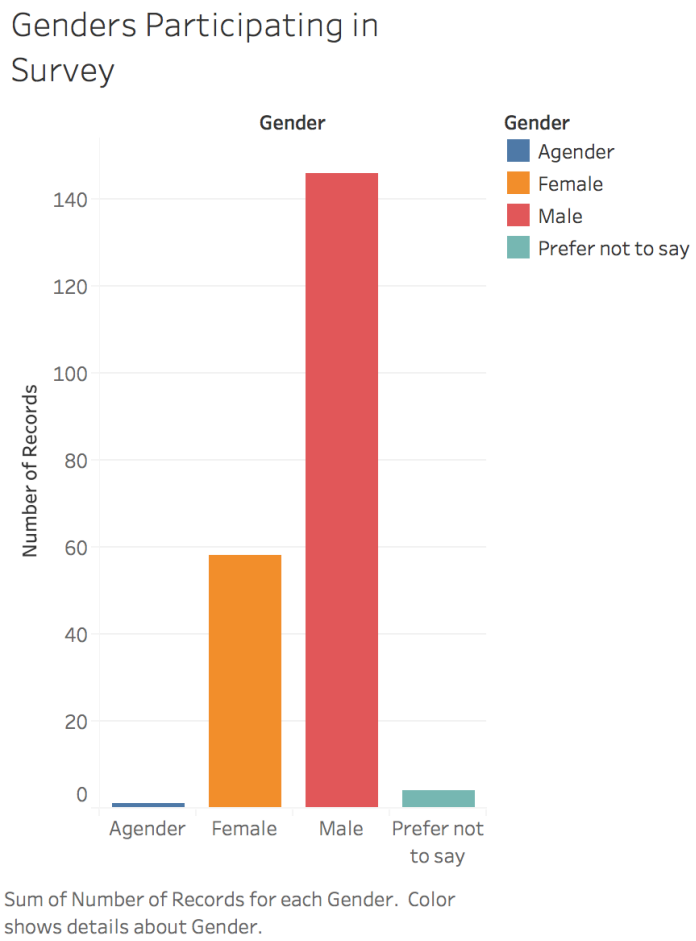


Figure 5.1: Gender of participants in Survey

Gender	Number
Agender	1
Female	58
Male	146
Prefer not to say	4

Table 5.1: Age of participants sorted by number.

There was a larger population of Male (146) to Female (58) participants with a 155.17% increase. 4 participants preferred not to say there gender and 1 was recorded as Agender.

5.3.2 Question Two: Age

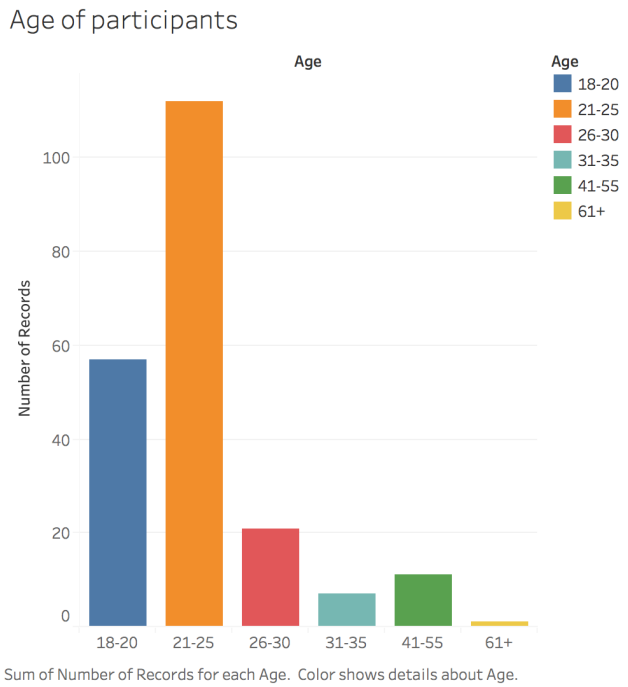


Figure 5.2: Age of participants in Survey

Age	Number
18-20	57
21-25	112
26-30	21
31-35	7
41-55	11
61+	1

Table 5.2: Age of participants sorted by number.

5.3.3 Question Three: Have you ever used Discord?

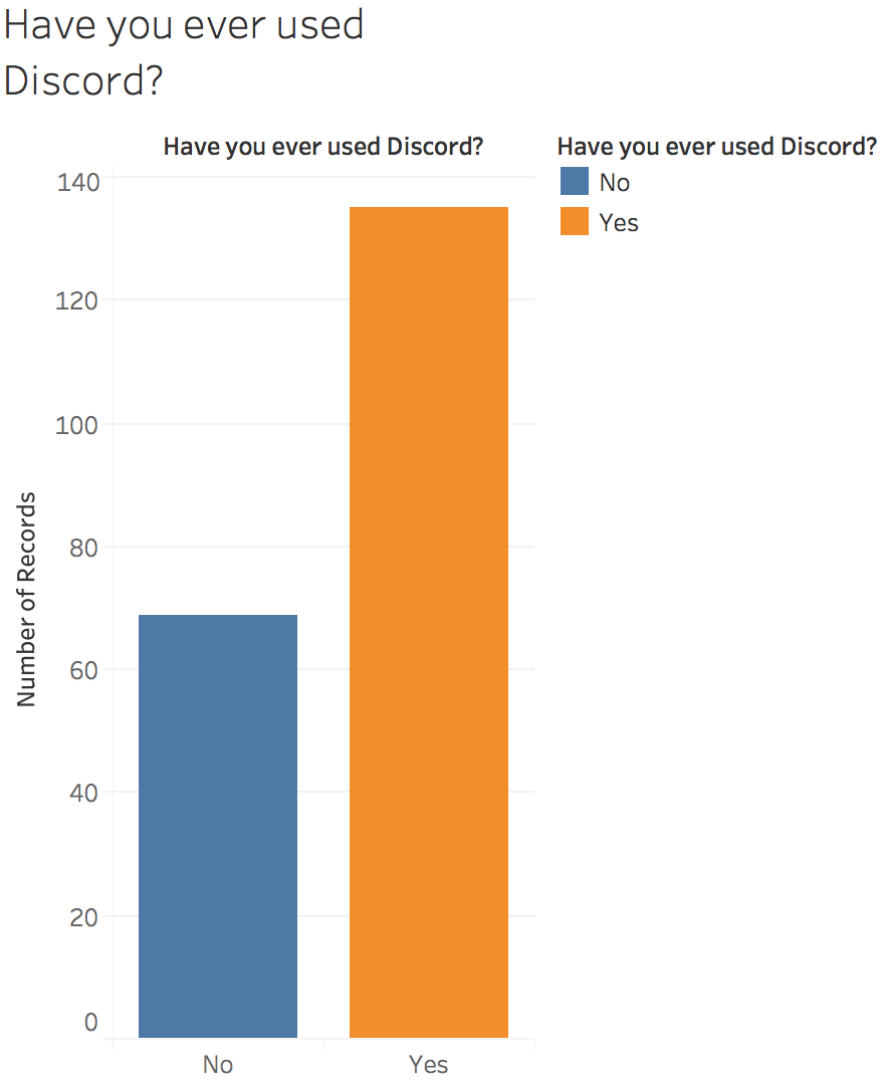


Figure 5.3: Normalized: *"Have you ever used Discord"* sorted by Gender Male and Female

The largest group of participants in the survey where around the 21-25 age group (112) with 18-20 in second place.

Yes	No
135	69

Table 5.3: Normalized: "Have you ever used Discord" sorted by Gender Male and Female"

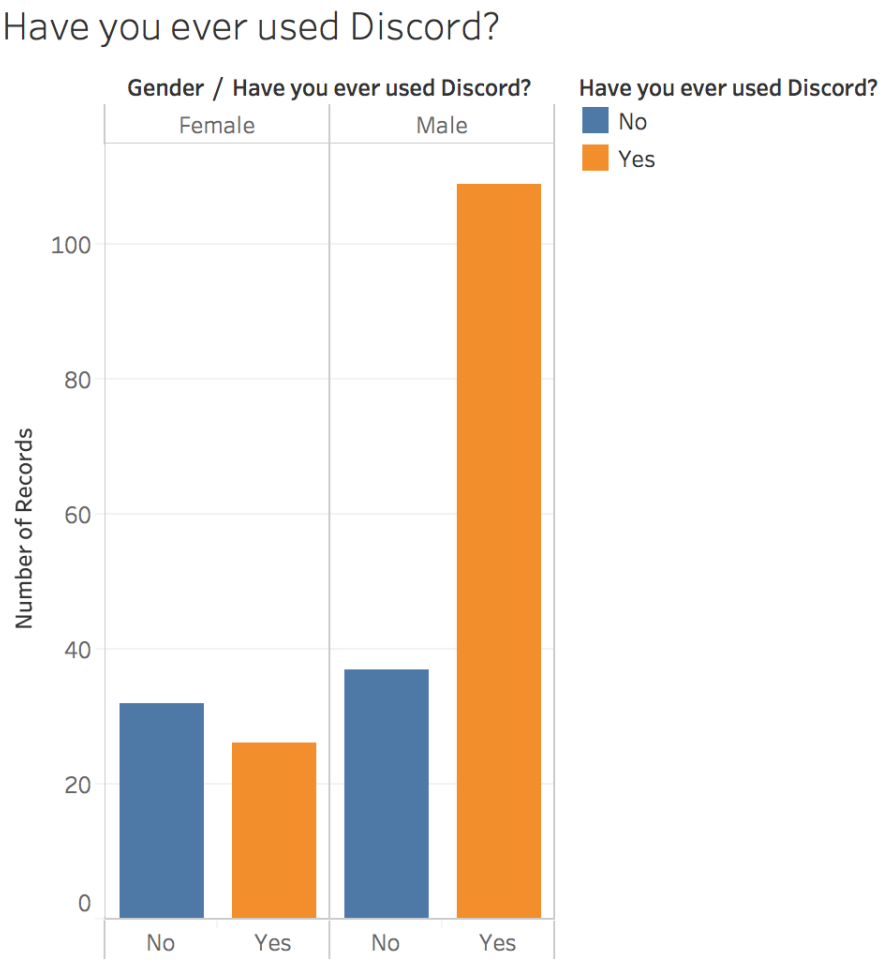


Figure 5.4: *"Have you ever used Discord?"* sorted by Gender.

Gender	Value	Number
Male	Yes	109
Male	No	37
Female	Yes	26
Female	No	32

Table 5.4: Normalized: "Have you ever used Discord" sorted by Gender Male and Female"

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	16.502	1	0.000
Likelihood Ratio	15.987	1	0.000

Figure 5.5: Pearson Chi-Squared test for the question *"Have you ever used Discord"*

A statistical analysis was conducted on the male and female groups of the population on the question *"Have you ever used Discord?"*. 204 people participated with 135 (66%) people voting yes and 69 (33%) voting no and 109 men (53%) and 26 (12%) women said Yes to using Discord while 37 men (18%) and 32 women (15%) said no to using Discord (see table 5.4 and figure 5.4). In order to understand if there was significant difference in the categorical data a person chi-squared test was conducted. As the P Values where lower than 0.5% there is a significance in the categorical data between men and women's responses (see figure 5.5). In conclusion ore men than women have used Discord.

5.3.4 Question Four: Have you ever had to mute a bot or users?

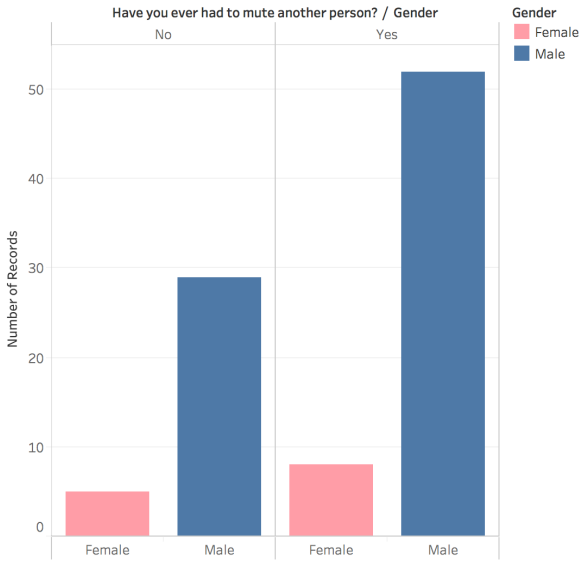


Figure 5.6: Have you ever had to mute a bot/users? Sorted by Genders Male and Female.

Gender	Value	Number

Male	Yes	52
Male	No	29
Female	Yes	8
Female	No	5

Table 5.5: Number of Male and Female participants that said yes and no to *"Have you ever had to mute a bot/users?"*

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	0.034	1	0.853
Likelihood Ratio	0.034	1	0.854

Figure 5.7: Pearson Chi-Sqaured Test for the question *"Have you ever had to mute a bot/users?"*

94 people participated in this question. 81 men participated and 13 women. 52 men (55%) voted yes while 8 women said yes, 29 Men voted no and 5 women voted no. 65% of men muted bots while only 8% of women did the same (see table 5.5). The Pearson Chi-Sqaured showed there was not difference to the population size as the p values where greater than 0.05 (see figure 5.7) this indicated was no significant difference with men and women likely to have both muted users and bots (see figure 5.7).

5.3.5 Question Five: Did muting the bot/user resolve the issue?

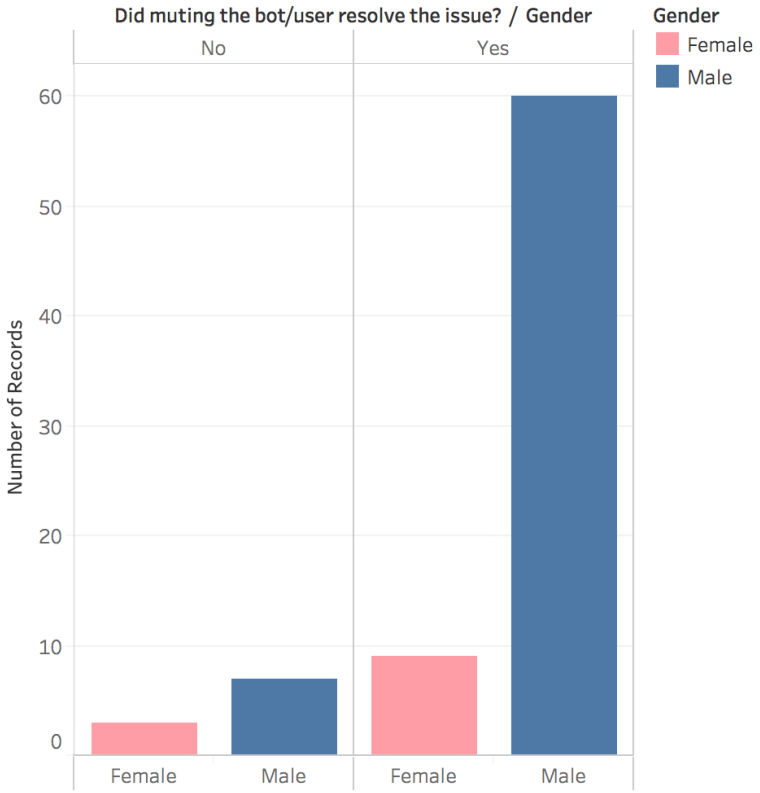


Figure 5.8: *"Did muting the bot/user resolve the issue?"* sorted by Gender.

Gender	Value	Number
Male	Yes	60
Male	No	7
Female	Yes	9
Female	No	3

Table 5.6: Number of Male and Female Participants that said yes and no to *"Did muting the bot/user resolve the issue?"*

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	1.949	1	0.163
Likelihood Ratio	1.654	1	0.198

1 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.172917

Figure 5.9: Pearson Chi-Sqaured and Fisher's Test for the question *"Did muting the bot/user resolve the issue?"*

79 people participated in the question *"Did muting the bot/user resolve the issue?"*. 60 Males (75%) and 9 Female (11%) participants voted Yes. 7 Males (8%) and 3 women (3%) voted no. (See figure 5.8 and table 5.6). a Pearson Chi-Sqaured test of categorical associations was conducted on the two largest gender groups (Male and Female). There was a significantly larger amount of male participants than female participants (see table 5.6). For men the muting mechanic had a much greater affect of resolution. As one of the values equalled less than 5 a Fisher's Exact Test as well as a Pearson Chi-Sqaured test of categorical associations was conducted. As the P-Values equalled more than 0.05 (see figure 5.9) there are no categorical significances related to this question. Overall muting users had a (Males 60 + Females 9 / total 79 * 100) = 87% success rate for participants.

5.3.6 Question Six: Did the user/bot attempt to make contact again via a new account?

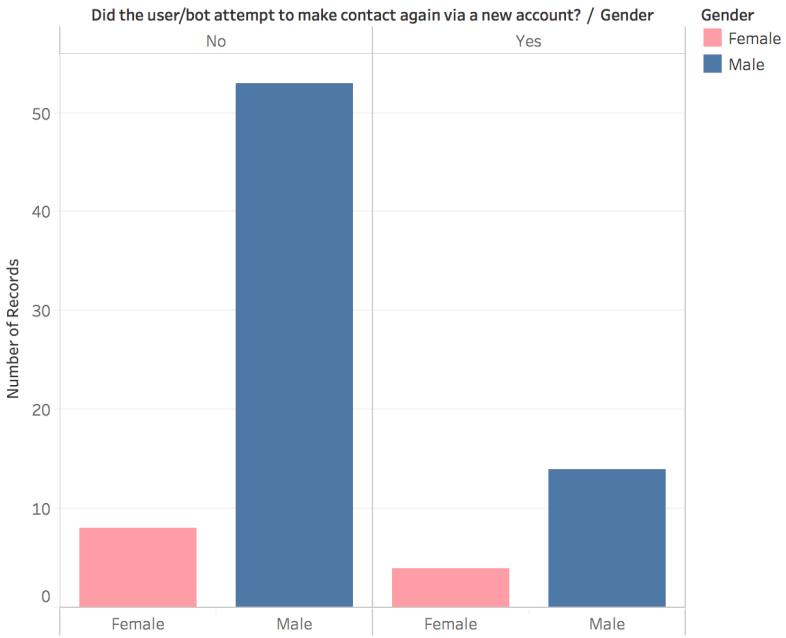


Figure 5.10: *"Did the user/bot attempt to make contact again via a new account?"* sorted by Gender.

Gender	Value	Number
Male	Yes	14
Male	No	53
Female	Yes	4
Female	No	8

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	0.895	1	0.344
Likelihood Ratio	0.832	1	0.362

1 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.454244

Figure 5.11: Pearson Chi-Sqaured and Fisher's Test for the question *"Did the user/bot attempt to make contact again via a new account?"*

a population of 81 participants answered the question *"Did the user/bot attempt to make contact again via a new account?"*. Data was sorted into the largest two gender populations (Male and Female). 14 Men (17%) and 4 (4%) Women said they had be reconnected by the same user and bot via a new account while 53 (65%) men and 8 (9%) women said they had not been re-contacted again after muting a user/bot. A fisher's and Pearson Chi-Sqaured test was conducted to see if there was any categorical significances. As the values where above 0.05% there where no categorical significance related to the question. 22% of people who participated in the Survey had been re-contacted by a user/bot after they had muted the old offending accounts while 75% of participants had not had the same person contact them again after muting them via new accounts.

5.3.7 Question Eight: On a scale of 1-5 (1 being the least and 5 being the most) how satisfied was you with the final outcome.

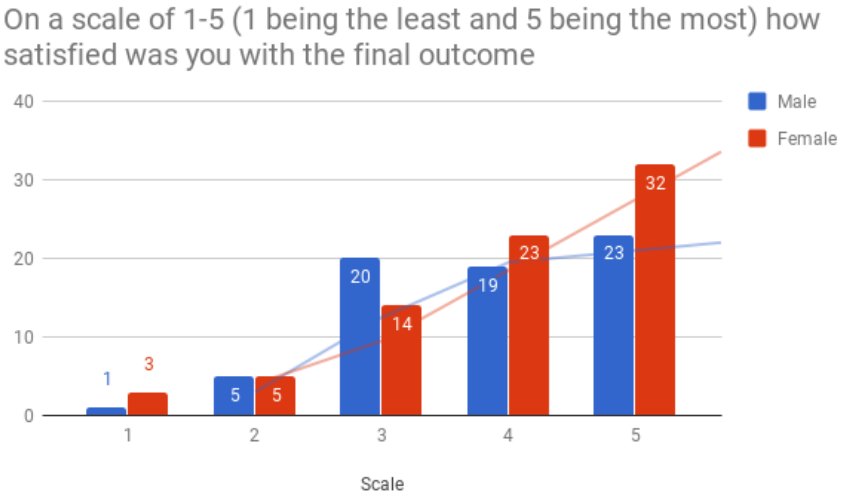


Figure 5.12: *"On a scale of 1-5 how satisfied was you with the final outcome."* sorted by Gender.

Gender	Scale	Value
Male	1	1
Male	2	5
Male	3	20
Male	4	19
Male	5	23
Female	1	3
Female	2	5
Female	3	14
Female	4	23
Female	5	32

Table 5.8: Number of Male and Female Participants that said yes and no to *"On a scale of 1-5 how satisfied was you with the final outcome."* sorted by Gender

Most of the participants who answered this question indicated that they where satisfied to very satisfied with the final outcome of muting individuals.

5.3.8 Question Nine: Have you ever had to block a bot or users?

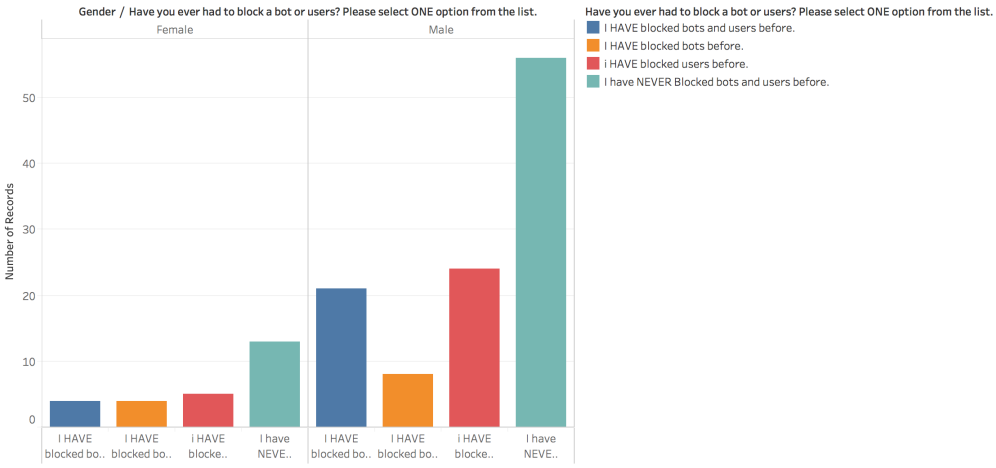


Figure 5.13: *"Have you ever had to block a bot or users"* Sorted by Gender.

Gender	Response	Value
Male	I have blocked users and bots before.	21
Male	I have blocked bots before.	8
Male	I have blocked users before	24
Male	I have never blocked users and bots before	56
Female	I have blocked users and bots before.	4
Female	I have blocked bots before.	4
Female	I have blocked users before	5
Female	I have never blocked users and bots before	13

Table 5.9: Number of male and female participants that responded to "Have you ever had to block a bot or users"

Response	Total
I have blocked users and bots before	25
I have blocked bots before	12
I have blocked users before	29
I have never blocked users and bots before	69

Table 5.10: Total of people responding to the question *"Have you ever had to block a bot or users"*

The majority of male and female participants had never blocked a bot or a user before. However more males (39%) had blocked both users and bots than females (9%).

5.3.9 Question Ten: Did blocking the bot/user resolve the issue?

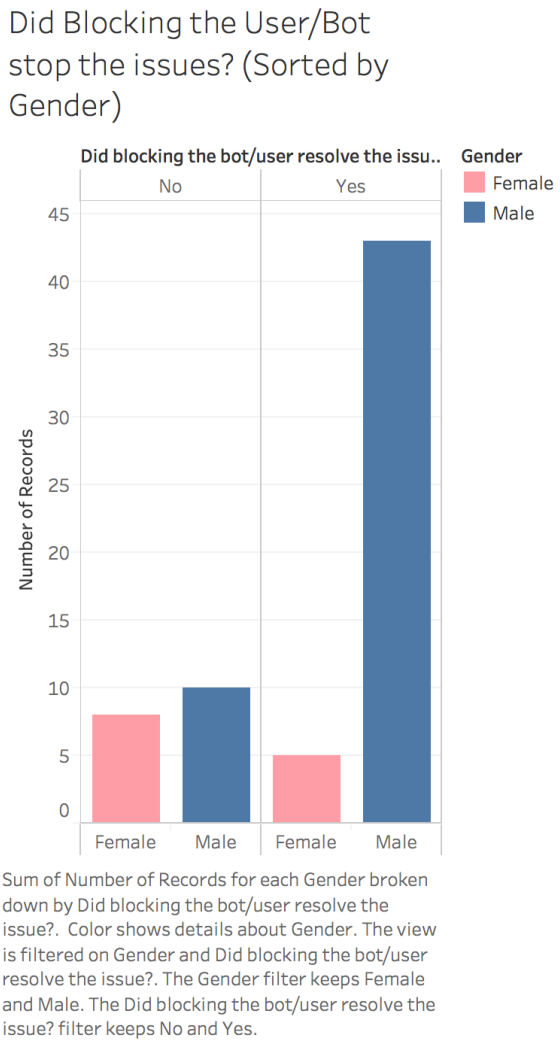


Figure 5.14: Did blocking the bot/user resolve the issue? Sorted by Genders Male and Female.

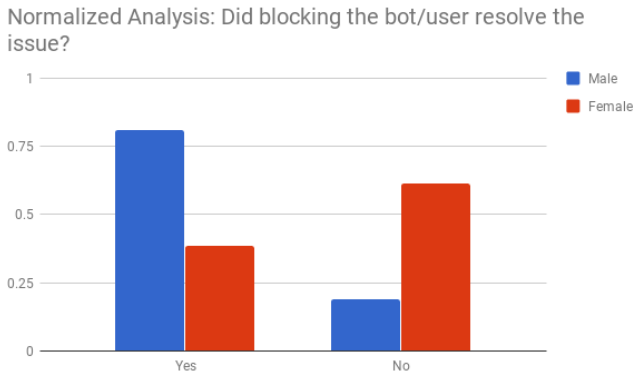


Figure 5.15: Normalised: Did blocking the bot/user resolve the issue? Sorted by Genders Male and Female.

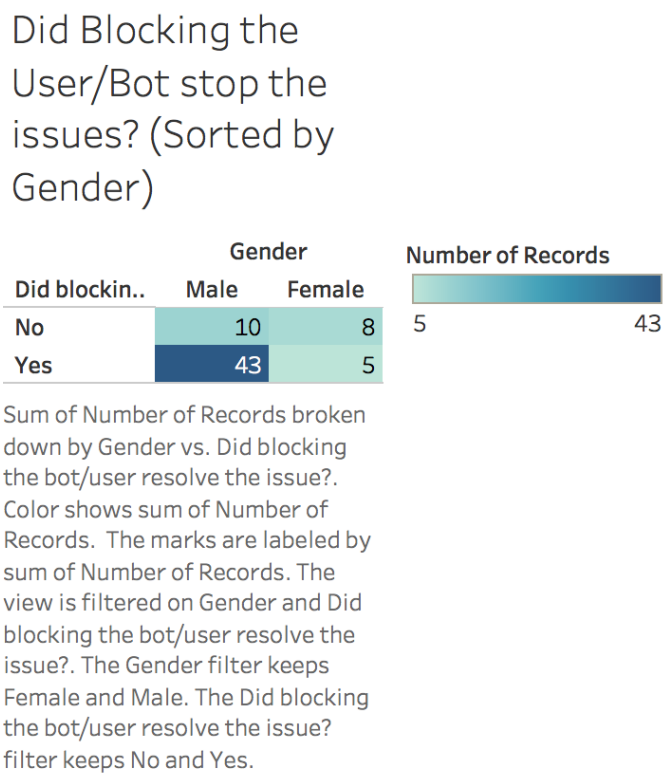


Figure 5.16: Did blocking the bot/user resolve the issue? Sorted by Genders Male and Female.

The Pearson Chi-Sqaured and Fisher's Exact Test was conducted to test the null hypothesis that there is no significant difference in the effectiveness of the blocking tool on discord.

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	9.583	1	0.002
Likelihood Ratio	8.686	1	0.003

1 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.0041656

Figure 5.17: Chi-squared table of association test plus Fishers exact test.

A statistical analysis was conducted on the groups of the population on the question *"Did Blocking the User/Bot stop the issues?"*. In order to do this the use Chi Squared test of categorical association analysis was conducted on the two largest gender groups (Male and Female). The Question was a Yes/No response. 66 participations took part including 13 Female, 53 Men (See figure 5.16). There was a significantly larger amount of Men within the population. Men had a much greater effectiveness to the blocking mechanisms than women did (See figure 5.14, The data was normalized to give a more accurate sense of scale in difference to the population size (See figure 5.15). The Pearson Chi-Squared and Fisher's Exact Test showed that there is a significant difference between men and women's responses as the P-Values where less than 0.05. The Fisher's Exact Test was conducted as one of the results was less than 5 to ensure certainty of association See (figure 5.17).

5.3.10 Question Eleven: Did the user/bot attempt to make contact again via a new account?

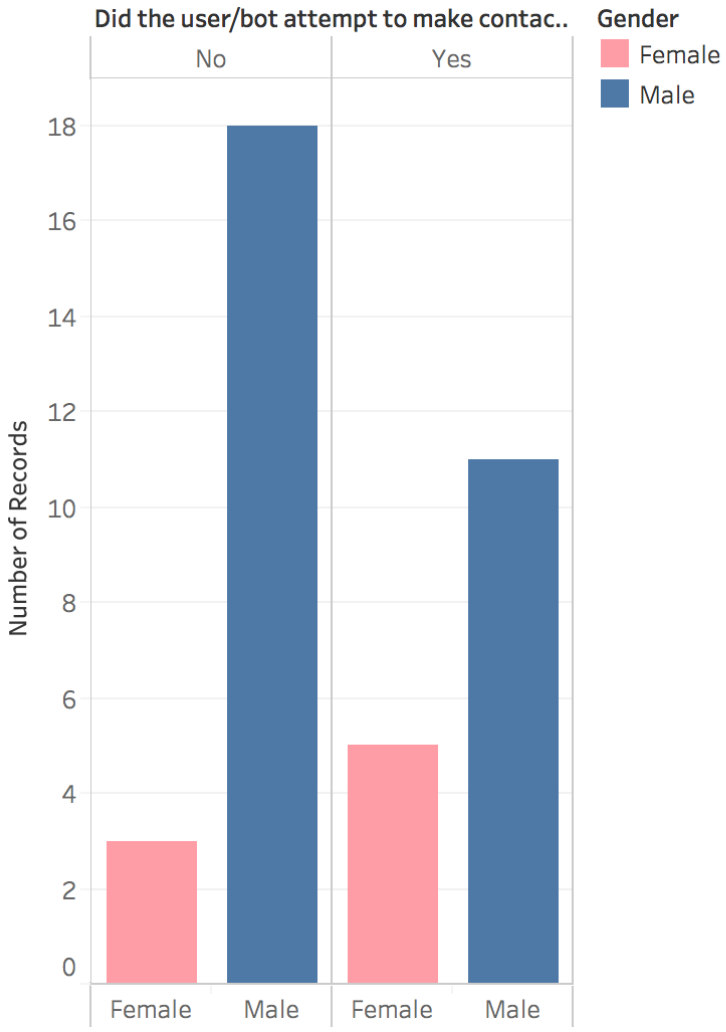
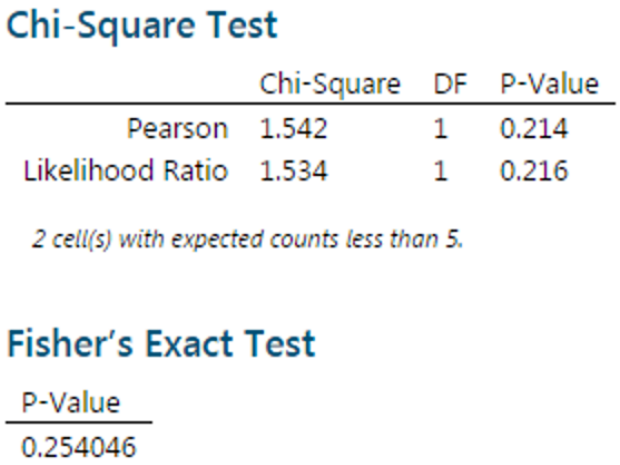


Figure 5.18: Did the user/bot attempt to make contact again via a new account? Sorted by Gender.

Gender	Response	Result
Male	Yes	11
Male	No	18
Female	Yes	5
Female	No	3

Table 5.11: Number of male and female participants that responded to *"Did the user/bot attempt to make contact again via a new account?"*



Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	1.542	1	0.214
Likelihood Ratio	1.534	1	0.216

2 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.254046

Figure 5.19: Chi-Sqaure and Fisher's Exact Test for the question *"Did the user/bot attempt to make contact again via a new account?"*

37 participants answered this question with 11 Males (29%), 5 Females (13%) saying they had been contacted again via a new bot/account after blocking a user and 18 Males (48%) and 3 Females (8%) saying that there was no re-contact. The Chi-Squared test was conducted on the Normalized data from the two largest gender groups (Male and Female). The Fisher's exact test was conducted as one of the values was less than 5. The P-Values for the Fisher's Exact test and the Chi-Squared test returned results greater than 0.05 therefore the data is not statistically significant. (see figure 5.19)

5.3.11 Question Twelve: On a scale of 1-5 (1 being the least and 5 being the most) how satisfied was you with the final outcome.

Gender	Scale	Result
Male	1	0
Male	2	3
Male	3	5
Male	4	3
Male	5	4

Female	1	2
Female	2	1
Female	3	3
Female	4	1
Female	5	5

Table 5.12: Total number of male and female participants that responded to "How satisfied was you with the final outcome" (of using the block mechanic)

There was a mixed response to the question with no clear overall majority.

5.3.12 Question Thirteen: Have you ever had to report a bot or users?

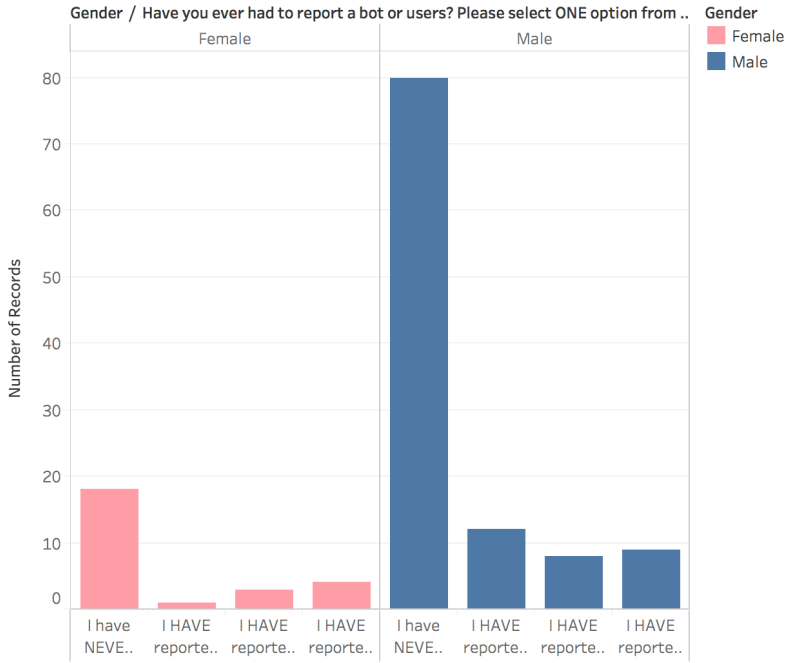


Figure 5.20: *Have you ever had to report a bot or users?* Sorted by Gender.

Gender	Response	Value
Male	I have reported users and bots before.	12
Male	I have reported bots before.	8

Male	I have reported users before.	9
Male	I have never reported bots and users before	80
Female	I have reported users and bots before	1
Female	I have reported bots before	3
Female	I have reported users before	4
Female	I have never reported bots or users before	18

Table 5.13: Number of male and female participants that responded to *"Have you ever had to report a bot or users?"*

135 participants took part in this question. 21% of males reported accounts that are bots or users. 6% of females also reported users and bots while 59% of males and 13% of females have never reported bots or users.

5.3.13 Question Fourteen: Did reporting the bot/user resolve the issue?

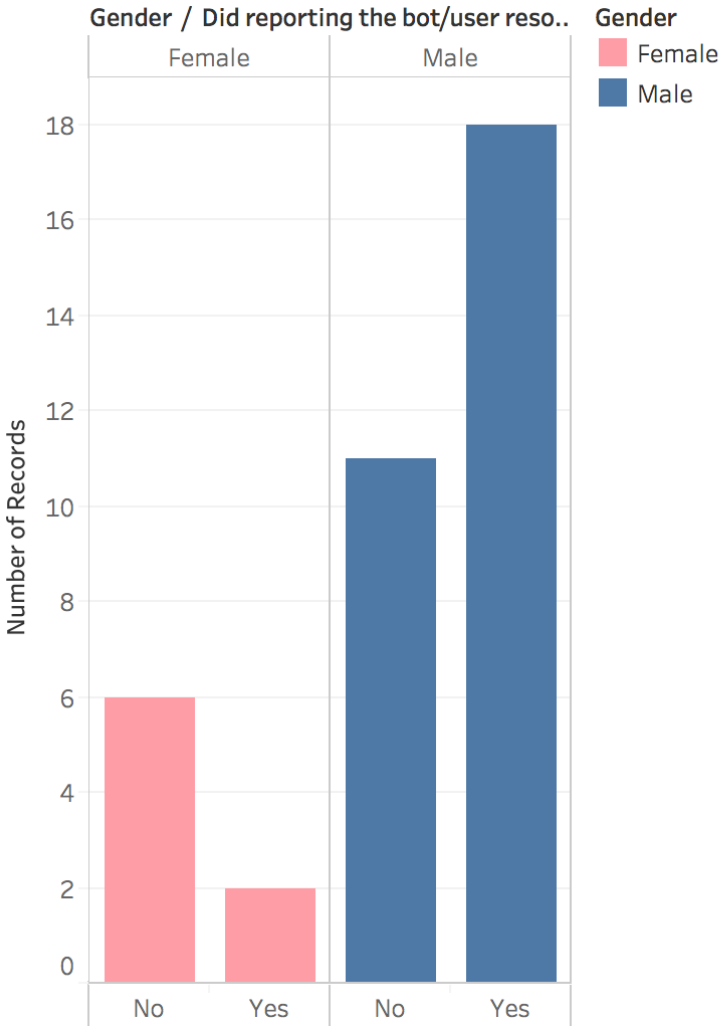


Figure 5.21: *"Did reporting the bot/user resolve the issue?" sorted by Gender.*

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	3.469	1	0.063
Likelihood Ratio	3.556	1	0.059

2 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.109006

Figure 5.22: Chi-Square Test and Fisher's Exact Test for the question *"Did reporting the bot/user resolve the issue?"*

Answer	Result
Yes	20
No	17

Table 5.14: Grand Total of Responses to the question *"Did reporting the bot/user resolve the issue?"*

Gender	Answer	Result
Male	Yes	18
Male	No	11
Female	Yes	2
Female	No	6

Table 5.15: Total number of participants that took part in the question *"Did reporting the bot/user resolve the issue"* sorted by gender.

A population of 37 participants took part in the Survey. 20 participants said that reporting a user/bot resolved issues. 20 participants said that reporting users resolved issues with 18 Males (54%) and 2 Females (5%). 11 Males (29%) and 6 Females (16%). In the female population only 25% of women said that the reporting tool was not affective verse the male population (62%) see figure 5.21. A Chi-Squared test of association was conducted as well as Fisher's Test as one of the

results was less than 5. The P-Values are less than 0.05 therefore there is no statistical significance to the the data however women felt reporting was not as effective.

5.3.14 Question Fifteen: Did the user/bot attempt to make contact again via a new account?

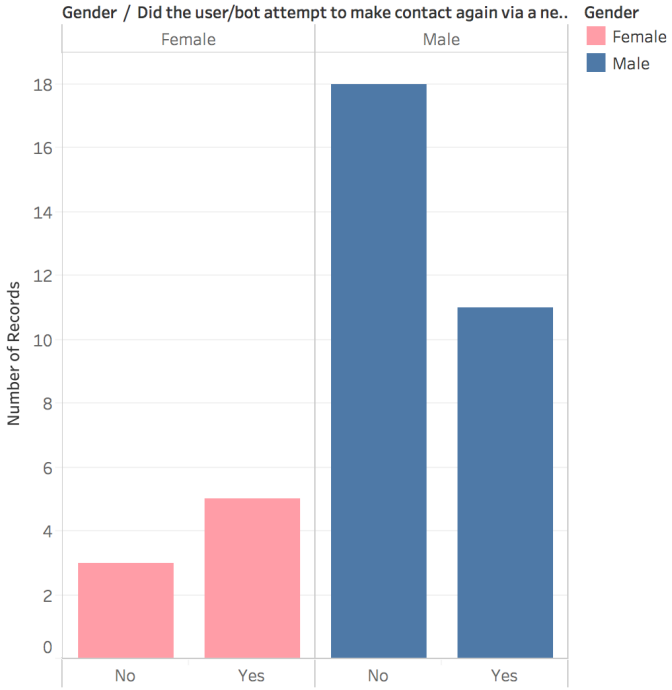


Figure 5.23: *"Did the user/bot attempt to make contact again?* sorted by gender.

Answer	Result
Yes	16
No	20

Table 5.16: Grand Total of Responses to the question "Did the user/bot attempt to make contact again?"

Gender	Response	Result
Male	Yes	11
Male	No	18

Female	Yes	5
Female	No	3

Table 5.17: Grand Total of Responses to the question *"Did the user/bot attempt to make contact again?"* sorted by Gender.

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	2.563	1	0.109
Likelihood Ratio	2.589	1	0.108

2 cell(s) with expected counts less than 5.

Fisher's Exact Test

P-Value
0.203554

Figure 5.24: Chi-Square Test and Fisher's Exact Test for the question "Did reporting the bot/user resolve the issue?"

A population of 37 participants took part in this question. 16 (44%) people said the user/bot made contact with them after being reported (See table 5.16) while 55% said that the user/bot did not make contact again. 11 Males (30%) and 5 females (13%) said they had been contacted again after reporting a user while 18 males (50%) and 3 females (8%) said they had not been. A Chi-Sqaured test and Fisher's Test was conducted. Fisher's Test used as there where two results less than 5. The P-Values where greater than 0.05 therefore there was no statistical significance in this question.

Chapter 6

Evaluation and Discussion

6.1 Forensics

6.1.1 Discord

Execution Lab

The Execution Lab for Discord was much faster to work upon due to the previous experimental forensics work conducted during the pilot forensic analysis phase (see appendix G). The methodlogy previously developed for obtaining artefacts from files related to media via the media traversal method provided multiple pieces of useful artefacts that could determine the origin of the user, the location, the email address, files viewed by the user from the and videos watched by the user via the client. This was a highly successful forensic extraction of data in a non-evasive manner. The development of the Discord Extractor python script provides a faster and more rapid method of viewing the discord localstorage file. The Chrome Cache Viewer displayed data generated by the user's interaction (playing the royal rumble video from twitch.tv) and provided a method of viewing files that had been uploaded to the channel. Discord displays the images online from it's own content delivery system (CDN). During this experiment issues with using the SQLite Manager 2009 Pro and Autopsy applications to view the SQLite localstorage files highlighted the need for updated SQLite database management systems and for the development of tools that could extract the localstorage data. During the experiment the Discord Extractor tool was developed as a way to review the content of the https_discord.com_0.localstorage file without having to switch in between Hex viewer on the DB Browser for SQLite tool which only supported Hex view for the Binary Blobs. The script was designed to decode the data as UTF-16 strings into a CSV portable format.

Simulated Conversation

In the simulated conversation artefacts sent by the Attacker machine to the Victim machine was traceable thanks to applying the media traversal theory. By looking for the Cache, the image that had been sent to the victim could be found a locally cached copy in the Discord Cache at `AppData/Roaming/discord/Cache`. Furthermore artefacts generated by the Twitch.tv player became viewable within the cache providing a new way of tracking user activity from the embedded player. In the `https_player.twitch.tv_0.localstorage` file useful information such as if the content was registered as mature, if the video had been muted and the resume and play times for videos could be found within the database file.

6.1.2 TeamSpeak3

Execution Lab

The Execution Lab Experiment took place between 21nd of May 2018 and the 23rd of May 2018, The first analysis was conducted for memory forensics. In the memory dump taken using DumpIT the machine's local registry was dumped into the Kali Linux virtual machine. The editor FRED was then used to view registry artefacts. The artefacts discovered in FRED was the use of the QT user interface library. A dialogue key from the registry included the same location for the upload as the FileUpload table in the Settings.db file found within the roaming ts3client folder. This indicates that the QT Library also stores the upload location of images and files and can be accessed via the registry on a memory dump. As such if the settings.db file has been deleted there is still an opportunity to access the files though other methods. In the second phase of forensic investigation the disk was analysed originally using EnCase 7 as the main forensic examination tool. On the night of the 22nd a digital acquisition was conducted on the ts3exectlab.raw image that contained the simulated lab of a client being executed and uploading a photo to the server. During the acquisition phase the forensic machine conducting the experiment crashed. As such it was decided that a different forensic tool would have to be used to examine the evidence. a discussion with Dr. Ian Kennedy via email resulted in a request for the forensic investigation to be conducted on multiple forensic tools. As such Autopsy and X-Ways Forensics was selected due to there availability on the forensic machines. During the analysis multiple SQLite databases where found that contained useful information such as the number of times a individual client uploaded images to the internet and a database for storing urls if clients exchanged them via chat. This stage helped develop the new methodology for obtaining useful artefacts from TeamSpeak3 by changing the process of examining the artefacts from EnCase 7 to X-Ways 18.1 SR and Autopsy 4.7.

Simulated Conversation

A simulated conversation between two users on seperate virtual machines was conducted as one of the experiments. The two users exchanged metadata by communicating between channels. By default TeamSpeak3 logs the channel and server history in the `AppData/Roaming/TS3Client` folder. The timestamps from the `server.html` and `channel.html` folders on both the victim and attacker clients provided useful information about user activity. The `urls.db` database proved to be very useful as it was found on both Jane and John's machines. there was no evidence of the link being shared in the public channels therefore it is deduced that John sent a link to Jane which was registered between both clients and timestamped at the same time. The `Kermit.jpg` was found on both systems. In the Pictures folder on the Attackers machine and in the Downloads folder of the Victim's machine. An MD5 hash of the file (`79dfc0fcb6526e93fd2ec89f792219e2`) was reported on both machine in the Autopsy report (see appendix I) Therefore it is possible to connect users of these clients based upon the metadata generated by multiple artefacts from the client.

6.2 Statistics

The Survey was created to understand how effective different types of moderation mechanics are being used and understand if they are affective. The Survey was published online on Reddit and shared with students at Canterbury Christ Church University. During the Survey a larger population of male participants made the Survey a challenge to balance. The Female population was able to obtain much more affective support than the Male population for using the moderation tools. Females had more problems with reoccurring contact from clients after muting them. The Chi-Squared and Fishers test showed only question had statistically significant data which was the responses to if people had used the Discord client.

Chapter 7

Conclusions

7.1 Limitations of Investigation

The experiments where heavily impacted by the amount of time available for each study, Due to setbacks with EnCase and having to use new tooling a reduction in the experiments was conducted to ensure delivery on time. As the survey did not meet the population requirements originally set out a new survey with a longer date and time for capturing data should be considered in the future. Technological issues (crashing) with the digital forensics machines and with EnCase 7 meant that alternative tools had to be used to preform the forensic investigation.

7.2 Evaluation of Investigation

The investigation was able to successfully identify new ways of connecting clients to each other. The development of new tools to export open data provided by both TeamSpeak and Discord has been created providing a new avenue of forensic analysis for gaming communication clients. The use of a web cache by the DiscordApp application provides a method of retrieving images uploaded and downloaded onto the client as well as external website activities from inside the client. The settings.db file provides a new method of tracking the file location where files have been uploaded and the amount of files being uploaded to TeamSpeak. The url.db file provides a method for tracking links sent from clients to other clients which can also be used to connect clients together during an incident. Memory forensics provided a new method of extracting the location of uploaded files by exploiting the QTProject registry hive which contains the dialogue registry information for the last use of the upload file location that is also used by TeamSpeak3 as it is part of the same framework. The TS3Client folder in the `/AppData/Roaming/chats` included timestamps, chat logs and the name of channels/servers which in conjunction with the artefacts previously stated provides a new method of extracting intelligence from user clients during an incident. Finally a network analysis conducted on TeamSpeak3 concluded

that the Upload and Download service is unencrypted and could be intercepted. Discord however provides an encrypted upload and download service using TLS 1.2. The file is hosted on Discord's own content delivery network and is viewable to the general public without the requirement of an authorisation key to the client. This means the image could be distributed to individuals outside of the discordapp ecosystem. Discord's Cache provided localized copies of images downloaded from the Discord media service. This made tracing the evidence very easy to do, Discord's LocalStorage files provided a new avenue of investigation. The discord localstorage file contained personal identifable information such as the user's email address and channels they had been connected to as well as the timestamp of when the connection occured. This could be paired with the Victim and Attacker machine to determine the presence of each individual. A similar technique was used on TeamSpeak with the server channel and server logs. Overall it was possible to fingerprint communications between to clients side by side during the forensic analysis due to the open nature of the SQLite files being viewed. TeamSpeak logged urls being shared between clients via urls.db and Discord cached external media player information and the cache also create an additional entry for new sites. For example Twitch.TV included information about if the user had muted the channel, looked at mature content and the last time the stream had been viewed. One of the biggest issues with conducting the research with the incompatibility with some of the digital forensic tools. Autopsy had problems opening SQLite3 files and so did SQLite 2009 Pro as such the creation of Discord Extractor and TeamSpeak Extractor was conducted to provide new methods of exporting the content for view. DB Browser for SQLite was also able to open up the Database files but only in hexadecimal format. Discord Extractor was able to export the data out into a standard .CSV file format with UTF-16 encoding (text format). The experiments highlighted that during a digital forensic examination the requirement for multiple tools to verify data being extract is essential as forensic tools may be unable to display certain types of data. In the case of the Discord localstorage files Autospy and SQLite 2009 Pro use outdated implementation of the SQLite3 database driver as such viewing newer SQLite3 database files requires applications that support newer versions of SQLite3. In the development of the Discord Python Extractor and TeamSpeak extractor an external library had to be used as the compiled version of Python's embedded SQLite driver is out of date in comparison to third party libraries.

At the start of the dissertation the main aim was to *What malicious use of gaming communication clients is occurring in TeamSpeak and Discord?* and as part of the main objective the focus on the sub-questions *What types of digital artefacts can be extracted from TeamSpeak and Discord?, Digital artefacts will be examined to determine connections between different individuals in order to establish if and what data has been transmitted and What is the difference in digital artefacts extracted from TeamSpeak and Discord?* have all been answered within this Dissertation from the forensics perspective. In the quantitative analysis the survey different mechanics where tested. Overall the muting of users was 87% effective, Blocking was 75% effective and Reporting was 69% effective. Muting proved to be the most effective method of moderating users. Currently the moderation tools are

providing a high rate of success in preventing online abuse. The population size of 200 users was not as high as the original population estimate of 400 participants, Therefore the Survey is incomplete. In the Survey the data heavily reflected that Males struggled more than Females to have affective moderation using block, muting and reporting methods. Male Participants where more likely to be re-contacted after blocking and muting the offending users. A larger study into the effectiveness of moderation tools for gaming communication clients and a broader demographic of individuals should partake in the study.

7.3 Future Work

Further investigation into the encryption methods, network traffic and server/API forensics should be conducted in the future as there are many new avenues of extracting the information without having to directly go though the clients. A more in-depth survey should be conducted to understand why people are blocking each other online with a larger demographic, Information such as geographic location could help to determine if people in certain countries are affected more than others. Further studies should include an analysis of TeamSpeak and Discord from other forensic tools such as EnCase and FTK Imager. Furthermore with the development of third party encryption add-ons further work is required to understand how third party encryption tools could disrupt the forensic analysis of gaming communication clients. The further development of specialist forensic tools should also be considered to extract data from gaming communication client for forensic analysis. Finally Research should also be conducted into the impact of Revenge Porn in communication clients.

References

3dsexploits (2017). *DiscordRaidBots: Discord chat spam bots to raid Discord Servers. Made by ejected-matrix/ethical (idk the reel name :U) I just forked it*. original-date: 2017-02-27T15:55:36Z. Available at: https://github.com/3dsexploits/DiscordRaidBots (Accessed: 27th November 2017).

7Safe and Chief Police Officers, A. of (2017). *ACPO Guidelines | Publications | 7Safe*. Available at: https://www.7safe.com/about-7Safe/downloads/acpo-guidelines (Accessed: 25th May 2017).

AccessData (2017). *Forensic Toolkit (FTK)*. Available at: https://accessdata.com/products-services/forensic-toolkit-ftk (Accessed: 24th May 2017).

Adam Christenson, FBI. *United States of America v. CHRISTIAN MAIRE*. Available at: https://docs.google.com/viewerng/viewer?url=http://WICZ.images.worldnow.com/library/f558e2b4-971c-4ef7-bf1e-4a3cd91ac807.pdf.

Adrian Crenshaw (2017). *Steam Browser Forensics*. Available at: http://aoighost.github.io/penguinpoweredinfosec/#!dfir/browserforensics/steam/steam_browserforensics.md (Accessed: 17th February 2017).

Adrian Crenshaw (2013). *BSidesDE 2013 2 3 playing the forensics game forensic analysis of gaming applications for fun and pr*. Available at: https://www.youtube.com/watch?v=XTUEAQAPjOc (Accessed: 17th February 2017).

Alexander, J. (2017). *Discord has a major raiding issue, but the developers are trying to fix it*. Available at: https://www.polygon.com/2017/7/27/16046030/discord-raiding (Accessed: 27th November 2017).

Andrew Lynch (2017). *US Attorney files federal charge against Maryland man accused of enticing Blue Springs girl for sex*. Available at: http://fox4kc.com/2017/04/10/us-attorney-files-federal-charge-against-maryland-man-accused-of-enticing-blue-springs-girl-for-sex/ (Accessed: 23rd November 2017).

Anthony Borrelli (2018). *Hunters. Talkers. Loopers. How the FBI cracked an online child exploitation ring*. Available at: https://www.pressconnects.com/story/news/public-safety/2018/03/02/hunters-talkers-loopers-how-fbi-cracked-online-child-exploitation-ring/384608002/ (Accessed: 30th March 2018).

Arts, E. (2017). *Terms of Service*. Available at: http://tos.ea.com/legalapp/eula/US/en/ORIGIN (Accessed: 5th October 2017).

Backes, M., Doychev, G., Dürmuth, M. and Köpf, B. (2010). 'Speaker recognition in encrypted voice streams'. *Computer Security–ESORICS 2010*, pp. 508–523.

Banerjee, J. (2014). 'Jihad and Counter-jihad in Germany'. *Jadavpur Journal of International Relations* 18.2, pp. 103–136. DOI: 10.1177/0973598415569933. Available at: http://dx.doi.org/10.1177/0973598415569933 (Accessed: 18th May 2017).

Beaver cops' arrest of 3 is vindication for anti-revenge porn group (2018). Available at: http://www.vindy.com/news/2018/mar/29/arrests-vindication-for-anti-revenge-por/ (Accessed: 30th March 2018).

Binns, R. (2018). *apsw: Another Python SQLite wrapper*. original-date: 2013-12-29T02:36:05Z. Available at: https://github.com/rogerbinns/apsw (Accessed: 6th April 2018).

Bluscream (2017). *BetterDiscord Encrypted Text*. Available at: https://r4p3.net/threads/betterdiscord-encrypted-text.2008/ (Accessed: 7th December 2017).

Brown, I. and Korff, D. (2009). 'Terrorism and the proportionality of internet surveillance'. *European Journal of Criminology* 6.2, pp. 119–134.

Canavan, J. *The Evolution of Malicious IRC Bots*. Available at: https://www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf.

CARBON - VIRTUAL FORENSIC SUITE (2017). Available at: https://sumuri.com/software/carbon/ (Accessed: 5th October 2017).

Carrier, B. (2017). *Digital (Computer) Forensics Tool Testing Images*. Available at: http://dftt.sourceforge.net/ (Accessed: 14th June 2017).

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Google-Books-ID: lUnMz_WDJ8AC. Academic Press.

Chapman, A. (2017). *Child Sexual Exploitation Detective Inspector Angie Chapman. - ppt download*. Available at: http://slideplayer.com/slide/10343049/ (Accessed: 2nd October 2017).

Cheshire, T. (2017). *WhatsApp rejected Government request to access encrypted messages*. Available at: http://news.sky.com/story/whatsapp-denies-government-access-to-encrypted-messages-11043069 (Accessed: 24th October 2017).

CNBC (2015a). *'Let's go' text found on Paris attacker's cell phone*. Available at: https://www.cnbc.com/2015/11/17/lets-go-text-found-on-paris-attackers-cell-phone.html (Accessed: 17th October 2017).

CNBC (2015b). *'Let's go' text found on Paris attacker's cell phone*. Available at: https://www.cnbc.com/2015/11/17/lets-go-text-found-on-paris-attackers-cell-phone.html (Accessed: 17th October 2017).

Cohen, N. (2006). 'Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication'. *New Eng. J. on Crim. & Civ. Confinement* 32, p. 313.

Computer messaging before the Web – A visual timeline (1960-1990) (2009). Available at: http://royal.pingdom.com/2009/09/04/computer-messaging-before-the-web-a-visual-timeline-1960-1990/ (Accessed: 28th November 2017).

Computer Misuse Act (1990). *Computer Misuse Act 1990*. Available at: http://www.legislation.gov.uk/ukpga/1990/18/section/3.

Conlan, K., Baggili, I. and Breitinger, F. (2016). 'Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy'. *Digital Investigation* 18, Supplement, S66–S75. DOI: 10.1016/j.diin.2016.04.006. Available at: http://www.sciencedirect.com/science/article/pii/S1742287616300378 (Accessed: 25th May 2017).

Conservatives (2017). *The Conservative Party Manifesto 2017*. Available at: https://www.conservatives.com/manifesto (Accessed: 19th May 2017).

Cowley, R. and Editor, D. (2017). *Gamer messaging app Discord hits 45 million users in two years*. Available at: http://www.pocketgamer.biz/news/65773/discord-45-million-users/ (Accessed: 26th November 2017).

Cox, J. (2018a). *Revenge Porn Moves to Slack*. Available at: https://motherboard.vice.com/en_us/article/vbpaj8/revenge-porn-moves-to-slack (Accessed: 31st May 2018).

Cox, J. (2018b). *The FBI Used Classified Hacking Tools in Ordinary Criminal Investigations*. Available at: https://motherboard.vice.com/en_us/article/7xdxg9/fbi-hacking-investigations-classified-remote-operations-unit (Accessed: 30th March 2018).

Cox, J. (2018c). 'This Gaming Site Is Revenge Porn's New Front'. *The Daily Beast*. Available at: https://www.thedailybeast.com/the-gaming-site-discord-is-the-new-front-of-revenge-porn (Accessed: 1st June 2018).

Cox, J. (2018d). *Which Tech Giant Will Build a Revenge Porn Database?* Available at: https://motherboard.vice.com/en_us/article/bjp7jm/revenge-porn-database (Accessed: 31st May 2018).

d (2017). *What's awesome and not awesome to do on Discord*. Available at: https://discordapp.com (Accessed: 28th November 2017).

Daniel, L. E. (2012). *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. Elsevier.

Day, J. (2001). 'Microsoft game taken off shelves'. *The Guardian*. Available at: https://www.theguardian.com/technology/2001/sep/13/games.terrorismandthemedia (Accessed: 9th February 2017).

Discord (2017a). *Discord - Free voice and text chat for gamers*. Available at: https://discordapp.com (Accessed: 24th May 2017).

Discord (2017b). *Discord Jobs and Company Information*. Available at: https://discordapp.com (Accessed: 29th October 2017).

Discord (2017c). *Discord Jobs and Company Information*. Available at: https://discordapp.com (Accessed: 4th December 2017).

Discord (2017d). *Discord - Tools For Streamers, YouTubers, Communities*. Available at: https://discordapp.com (Accessed: 24th November 2017).

Discord (2017e). *What Features Does Discord Have?* Available at: https://discordapp.com (Accessed: 26th October 2017).

Discord (2016). *The limit cap is 5,000 online concurrent users atm*. Tweet. Available at: https://twitter.com/discordapp/status/734275551037423616?lang=en (Accessed: 26th October 2017).

Discord (2017f). *We use electron for the desktop app, so it's all javascript and react!* Tweet. Available at: https://twitter.com/discordapp/status/822874230631100416?lang=en (Accessed: 16th March 2018).

Discord | Apps | Electron (2018). Available at: /apps/discord (Accessed: 16th March 2018).

Discord's Slack-meets-Skype service is growing quickly among gamers (2017). Available at: https://webcache.googleusercontent.com/search?q=cache:HwabbNCk2KgJ:mashable.

com/2017/05/16/discord-two-year-anniversary-growth-stats/+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b (Accessed: 24th October 2017).

Dubinski, K. (2018). *Sexting victim calls out men trading photos as Woodstock police investigate | CBC News*. Available at: http://www.cbc.ca/news/canada/london/london-woodstock-ontario-intimate-images-discord-app-1.4605936 (Accessed: 8th April 2018).

Elementary Statistics (2003). *Elementary Statistics : a Modern Approach' 2003 Ed.* Google-Books-ID: 52_CgfJwWZQC. Rex Bookstore, Inc.

Elliott, J. (2013). *World of Spycraft: NSA and CIA Spied in Online Games - ProPublica*. Available at: https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games?utm_source=et&utm_medium=email&utm_campaign=dailynewsletter (Accessed: 9th February 2017).

Eric Lawrence (2015). *The CertEnroll Certificate Generator*. Available at: https://www.telerik.com/blogs/the-certenroll-certificate-generator (Accessed: 27th March 2018).

Farivar, C. (2015). *Paris police find phone with unencrypted SMS saying "Let's go, we're starting"*. Available at: https://arstechnica.co.uk/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ (Accessed: 12th May 2017).

Foundation, T. V. (2017). *The Volatility Foundation - Open Source Memory Forensics*. Available at: http://www.volatilityfoundation.org (Accessed: 24th May 2017).

Foundation, V. (2018). *The Volatility Foundation - Open Source Memory Forensics*. Available at: http://www.volatilityfoundation.org (Accessed: 14th April 2018).

Gallagher, S. (2014). *Newly published NSA documents show agency could grab all Skype traffic*. Available at: https://arstechnica.com/tech-policy/2014/12/newly-published-nsa-documents-show-agency-could-grab-all-skype-traffic/ (Accessed: 4th December 2017).

GameTrack Digest: Quarter 2 2017.

Gaming chat app Discord starts shutting down racist accounts (2017). Available at: https://www.engadget.com/2017/08/14/discord-shuts-down-racist-accounts/ (Accessed: 28th November 2017).

Gault, M. (2017). *Porn and Swastikas Have Infiltrated 'Roblox'*. Available at: https://motherboard.vice.com/en_us/article/3kaxb5/roblox-porn-nazis (Accessed: 27th November 2017).

Golub, A. (2018). *DiscordChatExporter: Exports Discord chat logs to a file*. original-date: 2017-07-12T17:18:19Z. Available at: https://github.com/Tyrrrz/DiscordChatExporter (Accessed: 10th April 2018).

Google (2016). *Google Cloud Security and Compliance Whitepaper*. Available at: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf (Accessed: 6th April 2018).

GoogleTechTalks (2017). *A Brief Prehistory of Voice over IP parts 1 & 2*. Available at: https://www.youtube.com/watch?v=av4KF1j-wp4 (Accessed: 29th October 2017).

Gray, R. M. (2005). 'The 1974 origins of VoIP'. *IEEE Signal Processing Magazine* 22.4, pp. 87–90. DOI: 10.1109/MSP.2005.1458295.

Great Britan, E. (2017). *Data Protection Act 1998*. Text. Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/54A (Accessed: 12th June 2017).

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S. and Rushe, D. (2013). 'Microsoft handed the NSA access to encrypted messages'. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (Accessed: 4th December 2017).

Gregorio, J., Gardel, A. and Alarcos, B. (2017). 'Forensic analysis of Telegram Messenger for Windows Phone'. *Digital Investigation*. DOI: 10.1016/j.diin.2017.07.004.

Guan, S.-S. A. a. and Subrahmanyam, K. b. (2009). 'Youth Internet use: risks and opportunities'. *Current Opinion in Psychiatry* 22.4, pp. 351–356. DOI: 10.1097/YCO.0b013e32832bd7e0.

Hall, Z. (2018). *Apple abruptly pulled Telegram last week when it learned app was serving child pornography*. Available at: https://9to5mac.com/2018/02/05/apple-telegram-illegal-content/ (Accessed: 6th February 2018).

Halliday, J. (2015). 'Teenager who killed Breck Bednar in 'sadistic' attack jailed for life'. *The Guardian*. Available at: http://www.theguardian.com/uk-news/2015/jan/12/lewis-daynes-stabbed-breck-bednar-essex-sentenced-chelmsford-crown-court (Accessed: 21st November 2017).

Hancke, P. " (2015). 'Messenger Exposed Investigative Report'. *&yet*, p. 16. Available at: https://webrtchacks.com/wp-content/uploads/2015/05/messenger-report.pdf.

Haskins, C. (2017). *Offensive Messages Found in Freshman Tandon Group Chat*. Available at: https://www.nyunews.com/2017/08/28/offensive-messages-found-in-freshman-tandon-group-chat/ (Accessed: 19th October 2017).

Haworth, J. and Rogers, D. (2016). *Missing 12-year-old boy 'kidnapped' by man he met while playing Minecraft*. Available at: http://www.mirror.co.uk/news/world-news/missing-12-year-old-boy-8299401 (Accessed: 17th March 2017).

Hester, B. (2017). *Discord Shuts Down Its Alt-Right Server After Charlottesville Protests*. Available at: http://www.rollingstone.com/glixel/news/discord-shuts-down-alt-right-server-after-charlottesville-w497856 (Accessed: 25th November 2017).

Hill, K. (2017). *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. Available at: https://splinternews.com/these-two-diablo-iii-players-stole-virtual-armor-and-go-1793847840 (Accessed: 27th November 2017).

Hilt, S. (2017). *How Chat App Discord Is Abused by Cybercriminals to Attack ROBLOX Players*. Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/chat-app-discord-abused-cybercriminals-attack-roblox-players/ (Accessed: 19th October 2017).

Hof, S. v. d., Berg, B. v. d. and Schermer, B. (2014). *Minding Minors Wandering the Web: Regulating Online Child Safety*. Springer Science & Business Media.

Intsights (2017). *IntSights Threat Report Messaging Applications: The New Dark Web*. Available at: https://www.intsights.com/messaging-applications-the-new-dark-web.

ISFE (2017a). *GameTrack Digest: Quarter 3 2017*. Available at: https://www.isfe.eu/sites/isfe.eu/files/gametrack_european_summary_data_2017_q3.pdf (Accessed: 14th April 2018).

ISFE (2017b). *Industry Facts | Interactive Software Federation of Europe*. Available at: https://www.isfe.eu/industry-facts (Accessed: 18th February 2018).

ISFE (2017c). *Industry Facts | Interactive Software Federation of Europe*. Available at: https://www.isfe.eu/industry-facts (Accessed: 14th April 2018).

ISO/IEC 27037:2012 - Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (2017). Available at: https://www.iso.org/standard/44381.html (Accessed: 5th December 2017).

Justice, D. of (2017a). *Additional Charge Against Maryland Man for Enticing a Minor for Sex*. Available at: https://www.justice.gov/usao-wdmo/pr/additional-charge-against-maryland-man-enticing-minor-sex (Accessed: 23rd November 2017).

Justice, D. of (2017b). *Maryland Man Charged with Enticing a Minor for Sex*. Available at: https://www.justice.gov/usao-wdmo/pr/maryland-man-charged-enticing-minor-sex (Accessed: 23rd November 2017).

kayygee (2017). *How do I create a server?* Available at: http://support.discordapp.com/hc/en-us/articles/204849977-How-do-I-create-a-server- (Accessed: 4th December 2017).

Keragala, D. and Walker, C. (2016). 'Detecting Malware and Sandbox Evasion Techniques'. *SANS Institute InfoSec Reading Room*. Available at: Detecting%20Malware%20and%20Sandbox%20Evasion%20Techniques.

Kiley, M., Dankner, S. and Rogers, M. (2008a). 'Forensic Analysis of Volatile Instant Messaging'. *Advances in Digital Forensics IV*. IFIP — The International Federation for Information Processing. Springer, Boston, MA, pp. 129–138. DOI: 10.1007/978-0-387-84927-0_11. Available at: https://link.springer.com/chapter/10.1007/978-0-387-84927-0_11 (Accessed: 10th November 2017).

Kiley, M., Dankner, S. and Rogers, M. (2008b). 'Forensic Analysis of Volatile Instant Messaging'. *Advances in Digital Forensics IV*. IFIP — The International Federation for Information Processing. Springer, Boston, MA, pp. 129–138. DOI: 10.1007/978-0-387-84927-0_11. Available at: https://link.springer.com/chapter/10.1007/978-0-387-84927-0_11 (Accessed: 6th December 2017).

Kopecký, K. (2017). 'Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors)'. *Telematics and Informatics* 34.1, pp. 11–19. DOI: 10.1016/j.tele.2016.04.004. Available at: http://www.sciencedirect.com/science/article/pii/S0736585316300090 (Accessed: 18th May 2017).

LCDI (2017). *Application Analysis*. Available at: https://www.champlain.edu/Documents/ApplicationAnalysis_S17.pdf (Accessed: 10th November 2017).

Lee, M. (2017). *How Right-Wing Extremists Stalk, Dox, and Harass Their Enemies*. Available at: https://theintercept.com/2017/09/06/how-right-wing-extremists-stalk-dox-and-harass-their-enemies/ (Accessed: 26th November 2017).

legionof7 (2016). *Implement WhisperSystems Encryption for Voice and Text*. Available at: https://discordapp.uservoice.com/forums/326712-discord-dream-land/suggestions/17094256-implement-whispersystems-encryption-for-voice-and (Accessed: 7th December 2017).

Legislation.gov.uk (2003). *Communications Act 2003*. Text. Available at: http://www.legislation.gov.uk/ukpga/2003/21/section/127 (Accessed: 31st May 2017).

leigonof7 (2017). *Implement WhisperSystems Encryption for Voice and Text*. Available at: https://discordapp.uservoice.com/forums/326712-discord-dream-land/suggestions/17094256-implement-whispersystems-encryption-for-voice-and (Accessed: 19th October 2017).

Liptak, A. (2018). *Dutch police have shut down Anon-IB in the course of a revenge porn investigation*. Available at: https://www.theverge.com/2018/4/29/17299020/anon-ib-the-netherlands-dutch-police-revenge-porn-shut-down (Accessed: 31st May 2018).

Ludlow, P. and Wallace, M. (2007). *The Second Life Herald: The Virtual Tabloid that Witnessed the Dawn of the Metaverse*. MIT Press.

Mabuto, E. K. and Venter, H. S. (2017). 'State of the Art of Digital Forensic Techniques.' Available at: http://icsa.cs.up.ac.za/issa/2011/Proceedings/Research/Mabuto_Venter.pdf (Accessed: 19th May 2017).

Margaret Rouse (2018). *What is ISO 27001? - Definition from WhatIs.com*. Available at: https://whatis.techtarget.com/definition/ISO-27001 (Accessed: 6th April 2018).

markruss (2018). *Process Monitor - Windows Sysinternals*. Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon (Accessed: 14th April 2018).

Matters, I. (2017). *Apps guide for parents*. Available at: https://www.internetmatters.org/advice/apps-guide/ (Accessed: 23rd March 2017).

McKemmish, R. (1999). *What is forensic computing?* Australian Institute of Criminology Canberra. Available at: http://aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf.

Mee, V., Tryfonas, T. and Sutherland, I. (2006). 'The Windows Registry as a forensic artefact: Illustrating evidence collection for Internet usage'. *Digital Investigation* 3.3, pp. 166–173. DOI: 10.1016/j.diin.2006.07.001. Available at: http://www.sciencedirect.com/science/article/pii/S1742287606000946 (Accessed: 6th December 2017).

Menegus, B. (2017a). *How A Video Game Chat Client Became The Web's New Cesspool Of Abuse*. Available at: https://www.gizmodo.com.au/2017/02/how-a-video-game-chat-client-became-the-webs-new-cesspool-of-abuse/ (Accessed: 31st May 2017).

Menegus, B. (2017b). *Discord Has a Child Porn Problem [Updated]*. Available at: https://gizmodo.com/discord-has-a-child-porn-problem-1793682247 (Accessed: 19th October 2017).

MIT Lincoln Laboratory: News: Real-time speech communication on packet networks named an IEEE Milestone (2017). Available at: https://www.ll.mit.edu/news/ieee-milestone-packetspeech.html (Accessed: 28th November 2017).

Moore, A. (2016). 'I couldn't save my child from being killed by an online predator'. *The Guardian*. Available at: https://www.theguardian.com/lifeandstyle/2016/jan/23/breck-bednar-murder-online-grooming-gaming-lorin-lafave (Accessed: 9th February 2017).

Muldowney, D. (2017). *Doxx Racists: How Antifa Uses Cyber Shaming to Combat the Alt-Right*. Available at: https://psmag.com/news/doxxing-the-alt-right-racists (Accessed: 26th November 2017).

Mumble (2017a). *FAQ/English - Mumble Wiki*. Available at: https://wiki.mumble.info/wiki/FAQ#Is_Mumble_encrypted.3F (Accessed: 19th October 2017).

Mumble (2017b). *Overlay - Mumble Wiki*. Available at: https://wiki.mumble.info/wiki/Overlay (Accessed: 26th October 2017).

Nelly (2017a). *7.21.17 — Change Log*. Available at: https://blog.discordapp.com/7-21-17-change-log-c9acad667d67 (Accessed: 27th November 2017).

Nelly (2017b). *Discord Safety Boost*. Available at: https://blog.discordapp.com/discord-safety-boost-2d592ea3b14a (Accessed: 21st November 2017).

Nelly (2017c). *Discord Safety Boost*. Available at: https://blog.discordapp.com/discord-safety-boost-2d592ea3b14a (Accessed: 22nd May 2018).

Neubauer, S. (2017a). *Binghamton Man Charged As Leader in Online Child Porn Network*. Available at: http://www.wicz.com/story/36673574/binghamton-man-charged-as-leader-in-online-child-porn-network (Accessed: 21st November 2017).

Neubauer, S. (2017b). *Wife and Kids of Accused Child Porn Leader Christian Maire Were Home During FBI Search*. Available at: http://www.wicz.com/story/36683893/wife-and-kids-of-accused-child-porn-leader-christian-maire-were-home-during-fbi-search (Accessed: 21st November 2017).

News, B. (2015). 'Breck Bednar murder: Lewis Daynes sentenced to life in prison'. *BBC News*. Available at: http://www.bbc.co.uk/news/uk-england-30786021 (Accessed: 23rd March 2017).

Newton, D. (2010). *SANS Digital Forensics and Incident Response Blog | Digital Forensics: How to configure Windows Investigative Workstations | SANS Institute*. Available at: https://digital-

forensics.sans.org/blog/2010/12/17/digital-forensics-configure-windows-investigative-workstations (Accessed: 4th December 2017).

Nirsoft (2017). *ChromeCacheView - Cache viewer for Google Chrome Web browser*. Available at: http://www.nirsoft.net/utils/chrome_cache_view.html (Accessed: 14th June 2017).

Nugent, A. (2017). *The Obscure 4chan Religion That Promises a Cyberpunk Afterlife*. Available at: https://motherboard.vice.com/en_us/article/ne3p9z/the-obscure-4chan-religion-that-promises-a-cyberpunk-afterlife (Accessed: 27th November 2017).

O'Brien, L. (2017). 'The Making of an American Nazi'. *The Atlantic*. Available at: https://www.theatlantic.com/magazine/archive/2017/12/the-making-of-an-american-nazi/544119/ (Accessed: 23rd November 2017).

Oikarinen, J. and Reed, D. (1993). *Internet Relay Chat Protocol*. Available at: https://tools.ietf.org/html/rfc1459 (Accessed: 24th November 2017).

Ong, T. (2017). *WhatsApp reportedly refused to build a backdoor for the UK government*. Available at: https://www.theverge.com/2017/9/20/16338128/whatsapp-reportedly-refused-request-uk-government-access-encrypted-messages (Accessed: 16th October 2017).

Order a Mumble Voice Comms Server (2017). Available at: https://www.multiplaygameservers.com/order/voice-comms/murmur-mumble/ (Accessed: 26th October 2017).

Order a Teamspeak 3 Voice Comms Server (2017). Available at: https://www.multiplaygameservers.com/order/voice-comms/ts3-teamspeak-3/ (Accessed: 26th October 2017).

Overwolf (2017). *Take your TeamSpeak experience in-game!* Available at: http://www.overwolf.com/teamspeak/ (Accessed: 26th October 2017).

Peter (2012). *Encryption Question - What exactly is encrypted in TS3? - TeamSpeak*. Available at: http://forum.teamspeak.com/threads/65261-Encryption-Question-What-exactly-is-encrypted-in-TS3 (Accessed: 7th December 2017).

Petronzio, M. (2012). *A Brief History of Instant Messaging*. Available at: http://mashable.com/2012/10/25/instant-messaging-history/ (Accessed: 24th November 2017).

Poster - Overleaf (2017). Available at: https://www.overleaf.com/9823323ppyrgcdttbhd (Accessed: 14th June 2017).

Prayudi, Y. and Ashari, A. (2015). 'A Study on Secure Communication for Digital Forensics Environment'. *Int. J. Sci. Eng. Res* 6.1, pp. 1036–1043. Available at: http://www.ijser.org/researchpaper%5CA-Study-on-Secure-Communication-for-Digital-Forensics-Environment.pdf (Accessed: 19th May 2017).

Quick, D. and Choo, K.-K. R. (2013a). 'Digital droplets: Microsoft SkyDrive forensic data remnants'. *Future Generation Computer Systems*. Including Special sections: High Performance Computing in the Cloud & Resource Discovery Mechanisms for P2P Systems 29.6, pp. 1378–1394. DOI: 10.1016/j.future.2013.02.001. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X13000265 (Accessed: 8th December 2017).

Quick, D. and Choo, K.-K. R. (2013b). 'Dropbox analysis: Data remnants on user machines'. *Digital Investigation* 10.1, pp. 3–18. DOI: 10.1016/j.diin.2013.02.003. Available at: http://www.sciencedirect.com/science/article/pii/S174228761300011X (Accessed: 8th December 2017).

Quick, D. and Choo, K.-K. R. (2014). 'Google Drive: Forensic analysis of data remnants'. *Journal of Network and Computer Applications* 40.Supplement C, pp. 179–193. DOI: 10.1016/j.jnca.2013.09.016. Available at: http://www.sciencedirect.com/science/article/pii/S1084804513002051 (Accessed: 8th December 2017).

Riot, U. (2017). *LEAKED: The Planning Meetings that Led Up to Neo-Nazi Terrorism in Charlottesville*. Available at: https://www.unicornriot.ninja/2017/leaked-planning-meetings-led-neo-nazi-terrorism-charlottesville/ (Accessed: 19th October 2017).

Rosenberg, A. (2017). *Discord approaches 50 million users as it celebrates its second birthday*. Available at: http://mashable.com/2017/05/16/discord-two-year-anniversary-growth-stats/#CTzKMbcEjiqR (Accessed: 24th October 2017).

Russinovich, M. (2017). *Process Monitor - Windows Sysinternals*. Available at: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon (Accessed: 8th December 2017).

SANS (2013). *Acquiring Memory Images with Dumpit*. Available at: https://isc.sans.edu/forums/diary/17216/ (Accessed: 14th April 2018).

Scherer, A. (2017). *discord-anti-raid-bot: Discord AntiRaidBot*. original-date: 2017-04-23T04:03:06Z. Available at: https://github.com/aequasi/discord-anti-raid-bot (Accessed: 27th November 2017).

Schneier, B. (2017). *Paris Terrorists Used Double ROT-13 Encryption - Schneier on Security*. Available at: https://www.schneier.com/blog/archives/2015/11/paris_terrorist.html (Accessed: 12th May 2017).

ScP (2017). *TeamSpeak Mentioned in South Park Episode - TeamSpeak*. Available at: http://forum.teamspeak.com/threads/42453-TeamSpeak-Mentioned-in-South-Park-Episode (Accessed: 29th October 2017).

Senior Software Engineer - Anti-Abuse | Discord | LinkedIn (2018). Available at: https://www.linkedin.com/jobs/view/senior-software-engineer-anti-abuse-at-discord-602262656/ (Accessed: 5th March 2018).

Sgaras, C., Kechadi, M.-T. and Le-Khac, N.-A. (2015). 'Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications'. *Computational Forensics*. Lecture Notes in Computer Science. Springer, Cham, pp. 188–199. DOI: 10.1007/978-3-319-20125-2_16. Available at: https://link.springer.com/chapter/10.1007/978-3-319-20125-2_16 (Accessed: 8th December 2017).

Sgaras, C., Kechadi, M.-T. and Le-Khac, N.-A. (2016). 'Forensics Acquisition and Analysis of instant messaging and VoIP applications'. *arXiv:1612.00204 [cs]*. arXiv: 1612.00204. Available at: http://arxiv.org/abs/1612.00204 (Accessed: 31st October 2017).

Shortall, A. and Azhar, M. H. B. (2015). *Forensic acquisitions of WhatsApp data on popular mobile platforms*. IEEE Press.

Skype (2017). *Skype on Xbox One | Skype*. Available at: https://www.skype.com/en/download-skype/skype-for-xbox-one/ (Accessed: 29th October 2017).

Smith, J. (2015). 'Breck Bednar murder: How Lewis Daynes manipulated his victim'. *BBC News*. Available at: http://www.bbc.co.uk/news/uk-england-essex-30730807 (Accessed: 17th March 2017).

Software, G. (2017). *EnCase Forensic Software - Top Digital Investigations Solution*. Available at: https://www.guidancesoftware.com/encase-forensic (Accessed: 14th June 2017).

software, sweetscape (2017). *010 Editor - Professional Text/Hex Editor with Binary Templates*. Available at: https://www.sweetscape.com/010editor/ (Accessed: 6th December 2017).

Solon, O. (2017). 'Facebook asks users for nude photos in project to combat 'revenge porn''. *The Guardian*. Available at: http://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos (Accessed: 1st June 2018).

Sorokanich, B. (2014). *The NSA Was Going to Fine Yahoo $250K a Day If It Didn't Join PRISM*. Available at: https://gizmodo.com/the-nsa-was-going-to-fine-yahoo-250k-a-day-if-it-didnt-1633677548 (Accessed: 4th December 2017).

sqlitebrowser (2017). *DB Browser for SQLite*. Available at: http://sqlitebrowser.org/ (Accessed: 6th December 2017).

Squirrel (2018). *Squirrel.Windows: An installation and update framework for Windows desktop apps*. original-date: 2014-07-28T10:10:39Z. Available at: https://github.com/Squirrel/Squirrel.Windows (Accessed: 13th March 2018).

Tassi, P. (2017). 'How ISIS Terrorists May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]'. *Forbes*. Available at: https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/ (Accessed: 16th October 2017).

Teamspeak GmbH (2017a). *Choose A License*. Available at: http://sales.teamspeakusa.com/licensing.php?page=choose (Accessed: 25th May 2017).

Teamspeak GmbH (2017b). *Community Forum - TeamSpeak*. Available at: http://forum.teamspeak.com/ (Accessed: 25th November 2017).

Teamspeak GmbH (2017c). *Does TeamSpeak 3 encrypt my voice packets?* Available at: https://support.teamspeakusa.com/index.php?/Knowledgebase/Article/View/328/12/does-teamspeak-3-encrypt-my-voice-packets (Accessed: 19th October 2017).

Teamspeak GmbH (2017d). *myTeamSpeak*. Available at: https://www.myteamspeak.com/?search=&type= (Accessed: 24th November 2017).

Teamspeak GmbH (2009). *Teamspeak 3 Client Quickstart Guide - Mac OS X*. Available at: http://dl.4players.de/ts/releases/ts3_client_qs_mac_20091218.pdf.

Telerik (2018a). *Configure Fiddler to decrypt HTTPS traffic*. Available at: http://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/DecryptHTTPS (Accessed: 14th April 2018).

Telerik (2018b). *Fiddler - Free Web Debugging Proxy - Telerik*. Available at: https://www.telerik.com/fiddler (Accessed: 14th April 2018).

Teng, S.-Y. and Lin, Y.-L. (2012). 'Skype Chat Data Forgery Detection'. *Computer Applications for Communication, Networking, and Digital Contents*. Communications in Computer and Information Science. Springer, Berlin, Heidelberg, pp. 108–114. DOI: 10.1007/978-3-642-35594-

3_15. Available at: https://link.springer.com/chapter/10.1007/978-3-642-35594-3_15 (Accessed: 8th December 2017).

The games industry in numbers | Ukie (2017). Available at: https://ukie.org.uk/research#demographics (Accessed: 4th December 2017).

The U.K. Gamer | 2017 (2017). Available at: https://newzoo.com/insights/infographics/the-u-k-gamer-2017/ (Accessed: 4th December 2017).

Thomsen, M. (2017). *When Videogame Companies Help Prosecute Their Players*. Available at: https://www.forbes.com/sites/michaelthomsen/2015/05/30/when-videogame-companies-help-prosecute-their-players/ (Accessed: 27th November 2017).

Tobin, K. (2017). *National White Collar Crime Center Discord*. Available at: https://www.nw3c.org/docs/research/discord.pdf.

Tsotsis, A. (2013). *Why Was Apple Late To The PRISM Party?* Available at: http://social.techcrunch.com/2013/06/17/apple-nsa/ (Accessed: 4th December 2017).

Turner, B. and Woodward, A. (2008). 'Network security isn't all fun and games: An analysis of information transmitted while playing Team Fortress 2'. *Australian Information Security Management Conference*, p. 57. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1056&context=ism (Accessed: 17th February 2017).

UKIE (2018). *The games industry in numbers | Ukie*. Available at: https://ukie.org.uk/research#demographics (Accessed: 14th April 2018).

USA v. DeLa Cruz (2017). Available at: https://ecf.mowd.uscourts.gov/cgi-bin/DktRpt.pl?267829296057311-L_1_0-1.

USA vs Christian Maire (2017).

Van Vleck, T. (2012). 'Electronic Mail and Text Messaging in CTSS, 1965-1973'. *IEEE Annals of the History of Computing* 34.1, pp. 4–6. DOI: 10.1109/MAHC.2012.6. Available at: http://ieeexplore.ieee.org/document/6161671/ (Accessed: 24th November 2017).

vectors, I. (2017). *Discord Android App Review - DFIR*. Available at: https://abrignoni.blogspot.com/2017/07/discord-app-forensic-artifacts-in.html (Accessed: 10th November 2017).

Vishnevskiy, S. (2017). *How Discord Scaled Elixir to 5,000,000 Concurrent Users*. Available at: https://blog.discordapp.com/scaling-elixir-f9b8e1e7c29b (Accessed: 15th March 2018).

Weinberger, M. (2017). *A popular chat app just shut down a major online hangout for the alt-right after Charlottesville*. Available at: http://uk.businessinsider.com/discord-nazi-white-supremacist-alt-right-ban-2017-8 (Accessed: 17th October 2017).

WhatsApp (2017). *WhatsApp Legal Info*. Available at: https://www.whatsapp.com/legal/#terms-of-service (Accessed: 24th May 2017).

Whitaker, G. 'for the UK Police Project Lantern', p. 21.

Williams, J. (2017). *Application Analysis*. Available at: https://www.champlain.edu/Documents/ApplicationAnalysis_S17.pdf.

Wireshark (2018). *Wireshark · Go Deep.* Available at: https://www.wireshark.org/ (Accessed: 14th April 2018).

Wong, J. C. (2017). 'Tech companies turn on Daily Stormer and the 'alt-right' after Charlottesville'. *The Guardian*. Available at: http://www.theguardian.com/technology/2017/aug/14/daily-stormer-alt-right-google-go-daddy-charlottesville (Accessed: 21st November 2017).

Wu, S., Zhang, Y., Wang, X., Xiong, X. and Du, L. (2017). 'Forensic analysis of WeChat on Android smartphones'. *Digital Investigation* 21.Supplement C, pp. 3–10. DOI: 10.1016/j.diin.2016.11.002. Available at: http://www.sciencedirect.com/science/article/pii/S1742287616301220 (Accessed: 7th December 2017).

Yang, T. Y., Dehghantanha, A., Choo, K.-K. R. and Muda, Z. (2016a). 'Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies'. *PLOS ONE* 11.3, e0150300. DOI: 10.1371/journal.pone.0150300. Available at: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0150300 (Accessed: 21st November 2017).

Yang, T. Y., Dehghantanha, A., Choo, K.-K. R. and Muda, Z. (2016b). 'Windows Instant Messaging App Forensics: Facebook and Skype as Case Studies'. *PLOS ONE* 11.3, e0150300. DOI: 10.1371/journal.pone.0150300. Available at: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0150300 (Accessed: 7th December 2017).

Yasin, M., Cheema, A. R. and Kausar, F. (2010). 'Analysis of Internet Download Manager for collection of digital forensic artefacts'. *Digital Investigation* 7.1–2, pp. 90–94. DOI: 10.1016/j.diin.2010.08.005. Available at: https://www.sciencedirect.com/science/article/pii/S1742287610000575 (Accessed: 9th February 2017).

Yin-Poole, W. (2015). *Sony responds to claim PS4 used for terrorist communications*. Available at: `http://www.eurogamer.net/articles/2015-11-16-sony-responds-to-claim-ps4-used-for-terrorist-communications` (Accessed: 12th May 2017).

zoltanszabodfw (2012). *Parallels hard drive image converting for analysis*. Available at: `https://articles.forensicfocus.com/2012/07/05/parallels-hard-drive-image-converting-for-analysis/` (Accessed: 24th May 2017).

Bibliography

Altheide, C. and Carvey, H. (2011). *Digital Forensics with Open Source Tools*. Google-Books-ID: J8h8VWUmDuYC. Elsevier.

Bjelland, P. C., Franke, K. and Årnes, A. (2014). 'Practical use of Approximate Hash Based Matching in digital investigations'. *Digital Investigation*. Proceedings of the First Annual DFRWS Europe 11, S18–S26. DOI: 10.1016/j.diin.2014.03.003. Available at: http://www.sciencedirect.com/science/article/pii/S1742287614000085 (Accessed: 1st June 2018).

Bragadóttir 1974, A. (2011). 'Men who love women : behaviour of men towards women in virtual reality : case of Eve Online'. Thesis. Available at: https://skemman.is/handle/1946/7607 (Accessed: 1st June 2018).

Farokhmanesh, M. (2018). *Discord has a new problem: revenge porn*. Available at: https://www.theverge.com/2018/1/17/16901218/discord-revenge-porn-social-media (Accessed: 31st May 2018).

Horsman, G. (2018). '"I couldn't find it your honour, it mustn't be there!" – Tool errors, tool limitations and user error in digital forensics'. *Science & Justice*. DOI: 10.1016/j.scijus.2018.04.001. Available at: http://www.sciencedirect.com/science/article/pii/S1355030617301508 (Accessed: 1st June 2018).

Hutchings, A. and Clayton, R. (2016). 'Exploring the Provision of Online Booter Services'. *Deviant Behavior* 37.10, pp. 1163–1178. DOI: 10.1080/01639625.2016.1169829. Available at: https://www.tandfonline.com/doi/abs/10.1080/01639625.2016.1169829 (Accessed: 1st June 2018).

Michael Hale Ligh, Andrew Case, Jamie Levy and AAron Walters (2018). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Available at: https://www.wiley.com/en-us/The+Art+of+Memory+Forensics%3A+Detecting+Malware+and+Threats+in+Windows%2C+Linux%2C+and+Mac+Memory-p-9781118825099 (Accessed: 31st May 2018).

Sarah Perez (2014). *Why The Gmail Scan That Led To A Man's Arrest For Child Porn Was Not A Privacy Violation*. Available at: `http://social.techcrunch.com/2014/08/06/why-the-gmail-scan-that-led-to-a-mans-arrest-for-child-porn-was-not-a-privacy-violation/` (Accessed: 1st June 2018).

Scheller, S. H. (2014). 'A Picture Is Worth a Thousand Words: The Legal Implications of Revenge Porn Comment'. *North Carolina Law Review* 93, pp. 551–595.

Spreitzenbarth, D. M. and Uhrmann, D. J. (2015). *Mastering Python Forensics*. Google-Books-ID: ofl_CwAAQBAJ. Packt Publishing Ltd.

Appendix A

Glossary

TS3 - TeamSpeak3

TLS - Transport Layer Security

DOXX - Searching for public and private information about a individual for malicious intent.

Discord - a gaming communication client

TeamSpeak3 - a gaming communication client

SQLite3 - a compact database

X-Ways - a digital forensic examination tool.

DumpIT - a memory acquisition tool

Volatility - a memory forensics framework for analysing memory dumps.

EnCase - a digital forensic examination tool.

Autopsy - a digital forensic examination tool.

Appendix B

Proposal

Canterbury Christ Church University

Computing, Digital Forensics and Cybersecurity

BSc (Hons) Computer Forensics and Security

Individual 40 Research Proposal

Forensic Analysis of Gaming VoIP Clients

Oliver Bryant

o.g.bryant75@canterbury.ac.uk

OB75

October 5, 2017

Contents

Glossary of unfamiliar terms

- VoIP - Voice over Internet Protocol
- NSA - National Security Agency
- PSN - PlayStation Network
- PS4 - PlayStation 4
- Freeware - Software that is distributed for free.
- Teamspeak3 - VoIP Client
- Discord - VoIP Client
- Skype - VoIP Client
- Mumble - VoIP Client
- Origin - Game Downloader Client

Chapter 1

Introduction and background

The forensic world has turned a blind eye to the study and understanding of gaming clients and gaming VoIP applications. These systems are used on a daily basis by a large populace, who consume and talk across a range of networks; With consumers discussing their daily lives and using the tools for conferencing and even business. As such, a forensic analysis into these systems is essential, especially within the realm of national security and child grooming cases. In the Snowden revelations, it was revealed that the National Security Agency (NSA) had spied on users of World of Warcraft and Second Life (Elliott, 2013). The press recently spread rumours that terrorists in the Belgium/Paris 2015 terrorist attack, had used the Playstation 4 PSN network, to communicate with each other, planning operations. The Belgium Minister of the Interior and Security, Jan Jambon, even stated " ...it's very hard for our services (and other services) to decrypt the communication" (Yin-Poole, 2015). However, it was later revealed that an unencrypted SMS message was used to communicate the strike of the attack and not, as people had originally speculated, the PS4 PSN network (Farivar, 2015). This does not, however, reduce the factor of the current threat. At the time of writing this proposal, the UK Conservative Party have been pledging, to improve capabilities, to pressure companies to hand over data, due to these ongoing threats (Conservatives, 2017). As PlayStation Network and other gaming clients are freely available communication platforms, the idea has been planted into the general public's minds that this is a possible communication system that could be potentially used by terrorists. Video games have after all been used by terrorists in the past to train toward committing acts of terror (see Day, 2001). In the case of child grooming, one the first reported deaths was of Breck Bednar, who was groomed using the gaming voice over IP client TeamSpeak3. Breck played games with his murderer, which involved the popular game Minecraft (BBC, 2015). In turn, this expands the scope of the investigation into the usage of Digital Game Distribution Clients, as these systems can also be freely used for instant messaging and VoIP. At the time of writing this proposal, there have been no other research studies into these specialised gaming clients and VoIP Clients. However, a popular VoIP Client Skype has had papers published, such as: "Online blackmail of Czech children focused on so-referred to as "sextortion" (analysis of culprit and victim behaviours)" (Kopecký, 2017) and (Banerjee, 2014)

This highlights the current possible threat of threat-actors who are using online communication tools for causing harm to other individuals. This investigation aims to help forensic investigators understand the ability and availability of chat logs; browsing data; file transfer mechanism; registry edits; hidden files/folders and artefacts that are left behind in caches. The investigation will also explore if a forensic practitioner should extract data from volatile internal systems, such as caches, by using freely available tools.

Chapter 2

Proposed Investigation

The aim of the investigation into the game and Voice over IP (VoIP) clients, is to extract as much data from the clients, locally, as could be used in a live criminal investigation. Data such as browsing history; system logs; chat logs; caches and image stores will be collected and investigated. A guide for extracting the data will be provided. By investigating not only the gaming VoIP clients but also the gaming downloader clients, the aim is to attempt to provide an historical log and trail of evidence, in which two users interact between both the VoIP game client, and the game downloader client. The intention would be to investigate two popular VoIP Gaming Clients (Discord, Mumble) and one of the most popular gaming downloader clients (Origin). The investigation aims to provide information to the local police services about these clients and how they can extract the new types of data from the clients for deeper analysis. The investigation will simulate a child grooming case and in this hypothetical scenario, a computer has been seized from the child's family and an investigation of the game downloader client and VoIP game client is required, to attempt to connect the child to a possible grooming incident. Once the investigation has been completed and a report produced, the investigation would be sent to the Breck Foundation for circulation, to their contacts within police forces and for educational purposes. The investigation will comprise of a live forensic investigation, using freeware tools and memory forensics. The static investigation will use commercial and freeware tools, to extract artefacts that could be used in a criminal investigation. Below, is a diagram of the three stages of gathering data, the installation, the execution and the uninstallation of the software and the artefacts extracted from them during each process. Furthermore a survey will be conducted to ask a group of undergraduate students about their experiences with gaming clients and gaming VoIP clients. The survey will explore the use cases of privacy settings, report functionality and the ability to block and remove content.

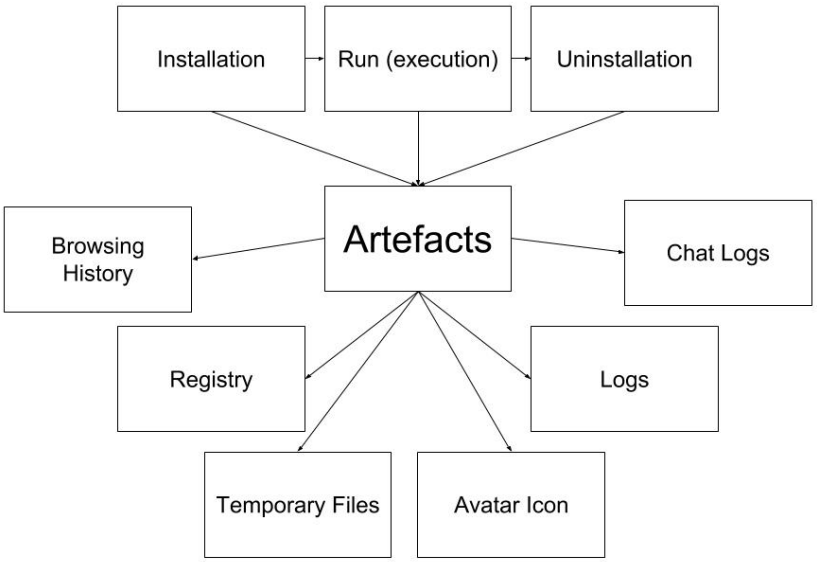


Figure 2.1: Artefacts to be collected from VoIP and Game clients.

Chapter 3

Proposed Methodology of Investigation

Static forensic investigation, with consideration given to the volatile data, which if the system has not been powered down, may be visible to the forensic client. Volatile Data could be used to find a trail of small artefacts of data that could identify user activity on a system. Live Forensics will extract data that may not be visible to Static clients, such as FTK Imager and back up claims made with static analysis. For example, in live forensics, it may be possible to retrieve wire capture data, that can be cross referenced with Wireshark.

Live forensic investigation, in compliance with ACPO guidelines (7Safe and Chief Police Officers, 2017), will ensure the integrity of data. Freeware tools will extract data from applications including registry edits, cache, browsing history, logs and chat logs; volatile data may be lost if the machine is powered off. Live investigation is required, to extract how the application will be installed, executed and uninstalled, together with how and where files are stored (if in a database or within registry).

3.1 Static Forensic and Dynamic Analysis

In both dynamic and static forensic analysis, there are multiple stages of processing and evaluating incoming data (Menegus, 2017). During a memory forensic analysis, typical use of the program will be conducted (chatting to friends, sending files and browsing the chat window). As per ACPO Guidelines, (7Safe and Chief Police Officers, 2017) the acquisition device will be a USB stick (a new memory stick per experiment). The memory dump will use multiple tools for reliability. In a static forensic analysis, a write blocker protects the computer from writing data to the incoming medium. Static file analysis will be conducted, using a write blocker, to prevent accidental data being transferred from the system image written from the forensic practitioner's machine. If a Virtual hard drive file, a write blocker will not be required. In the simulation, Parallels Desktop will be used. Test data will be processed and examined, to determine accuracy, each forensic tool being paired with an identically functioning secondary tool for reproducing the evidence.

Commercially available static forensics tools will be used to view areas and files that might contain data within the program file system and the volatile temporary files to locate the following artefacts:

Artefact Type	Purpose	Summary
Registry	System Operations	could be used to locate settings, file locations and preconfigured elements of the client.
Temporary Files	Personal Data	may include logs and caches that could be used to identify user activity.
Cache Files	Volatile Storage for web requests	may provide a fingerprint of user activity on the client from the embedded browser.
Client logs	User Activity	may provide stamps of when a user connected and what server they connected to.

Two virtual machines will be created from the same windows 7 iso with a snapshot of a clean image; client software will be installed on both systems.

Analysis 1: static investigation. An image of the parallels virtual disk will be transferred to the forensic machine, with writeblocker connected to prevent data being written to after transfer from the host machine. The disk will be converted over to a format readable by FTK Imager and other forensic tools, using QEMU to convert the Parallels disk to a .dd file format (see zoltanszabodfw, 2012) for analysis. The analysis will be set across 3 scenarios: Installation, Execution and Uninstallation. Figure 2.1 shows the type of artefacts to be extracted.

Analysis 2: live forensic analysis and inspection of the registry, to ascertain types of files being created and dropped during installation and if changes are temporary during the installation phase. This will be performed with live forensic tools and a forensic image of the memory using FTK Imager (AccessData, 2017) and the Volatility Framework (Foundation, 2017). Using both static and dynamic forensic analysis will capture data not active during a static state and reconfirm evidence found between investigations. Having two virtual machines will ensure that artefacts can be generated and duplicated between static and live analysis.

The study will require scientific analysis of evidence provided both logically with the file system and physically with the virtual machine. The digital "crime scene" will be a single snapshot of the Windows environment, including the same tools, drivers and software on both machines. After each test the snapshot for all virtual machines will be rolled back to the initial state, providing a clean environment to ensure results are from the experiment being created.

3.2 Student Survey

100 Canterbury Christ Church University students will be surveyed on how they control, secure and maintain privacy by using functionalities built into the Game Download Clients and Voice over IP Game Clients. On consent participants will be given a code which they may use to withdraw from the study. The survey will be conducted to the standards required under the University's research guidelines which include referral to ethics committee.

Chapter 4

Legal and Ethical Considerations

4.1 Legal Considerations

A literature review on how academia have performed analysis on systems reveals an apparent grey area within performing analysis on some systems. Shortall and Azhar, 2015 claim forensic analysis of WhatsApp has been performed however, under their terms and conditions (WhatsApp, 2017) state under "Harm to WhatsApp or Our Users" that the person using the software must not "access, use, copy, adapt, modify" and "(a) reverse engineer, alter, modify, create derivative works from, decompile, or extract code from our Services". However, academics have continued to write about the client and produce materials around providing forensic data from the client ignoring the legal terms of service provided by the company. Each company will be emailed to inform them of the research and to say they may be excluded from the study if required. Discord has rules for performing security analysis on their client (Discord, 2017) after emailing discord security I was told I could perform the analysis as long as there was no malicious intent. After contacting Discord, Oliver Bryant was given permission to perform forensic analysis of Discord by the security operations team. As of writing this dissertation EA Games and Discord have agreed to analysis of their client. Mumble, an open source client, is open and self-hosted so no risks are involved. Electronic Arts has stated that they require a legal review of my proposal from their legal team as the research violates their EULA (Section 3) (ea.com, 2017)

The communications act 2003 (Legislation.gov.uk, 2003) will not apply to the investigation however section 127 may be used to charge an individual during a forensic examination due to the fact that internet trolls have used services such as Discord to send unwanted, illicit materials (Menegus, 2017).

The Computer Misuse Act 1990 Section 1 (legislation.gov.uk, 2017) states that a person is not permitted to gain access to unauthorised data. As the data is being lifted directly from a local client on a personal computing system section 1 is invalidated. Communication will be sent between two clients owned by the researcher.

During the student survey data will be anonymised in compliance with the Data Protection Act 1998; the survey will be conducted Digitally using Google Forms) or qualtrics (pending permission from the University).

4.2 Ethical Considerations

4.2.1 Forensic Investigation

As part of the disclosure process, there is a non-disclosure agreement with Oliver Bryant, who has been interning with Electronic Arts (EA Games), Guildford, for 3 months. His role within the organisation was "Cyber Investigations" focusing on developer operations and tooling, as well as threat research. Oliver has agreed with Electronic Arts to provide a copy of the Dissertation before submission. EA will, just like the other partners, be allowed to withdraw from the study at any time. Electronic Arts has requested more time for legal negotiations to occur before agreeing to the study. As such, a different client may be used, such as Mumble and the title of the study would change from "Forensic Analysis of Game Downloader Clients and VoIP Clients" to "Forensic Analysis of Game VoIP Clients".

Criminals might analyse these publicly accessible files, as a technically apt criminal would be able to detect the file types, with a simple search on the internet. The information will not present a risk to the public but will assist the police in investigating future cases. Information will be gathered, using freely available and commercial tools, with minimal risk. Any discoveries will be reported to the participating companies. If they request the information to be withheld, this will be respected. Companies involved in the study have provided permission to do so after being briefed on the investigation.

User accounts for the online services will be created and controlled by Oliver Bryant. They will not interact with external users and will only be used for the purposes of this research reducing the factor of human participation within this section to 0. This companies will company policies which require no external interaction with users during this experiment and further it negates the potential for distress among external users.

Company	Communication	Status
Teamspeak GmbH	Email	Permission Granted by Business Development Team.
Electronic Arts	Email	Awaiting Legal Consultation (May Pivot to Mumble)
Mumble	Open Source	Information about reverse engineering the client for data can be already found on the Mumble Wiki. Open Source free to reverse engineer.
DiscordApp	Email	Permission Granted by Security Team. (If following EULA and without malicious intent.)

4.2.2 Survey

The Survey will be sent out to students at Canterbury Christ Church University. The Gaming and Tabletop Society will be posting a link to the survey. The Survey will include questions such as "When was the last time you had to block a contact?" and "When you blocked a contact/reported a contact was your problem resolved?". A disclosure at the start of the survey will state that the survey focuses on how people react and block contacts and the perception of the public on how companies react to these situations. The survey sample will be taken from individuals interested in gaming. As such the gaming society has given permission for the survey to be included on the facebook group for Canterbury Christ Church University. As the topic includes blocking contacts there could be an element of psychological distress for some participants. Information will be given to potential participants prior to beginning the survey to ensure they fully understand the implications of participating within the research, in order to avoid any potential distress. Participants will be aware that they are able withdraw from the research at any time without the need to give an explanation. Information will be made available at the end of the survey regarding the helplines and support available should participants experience any distress.

4.2.3 Checklist

		Yes	No
1.	Does the study involve participants who are particularly vulnerable or unable to give informed consent (e.g. children, people with learning disabilities, your own students)?	☐	☒
2.	Will the study require the co-operation of a gatekeeper for initial access to vulnerable groups or individuals to be recruited (e.g. students at school, members of self-help group, residents of nursing home)?	☐	☒
3.	Will it be necessary for participants to take part in the study without their knowledge and consent at the time (e.g. covert observation of people in non-public places)?	☐	☒
4.	Will the study involve discussion of sensitive topics (e.g. sexual activity, drug use, crime, etc.)?	☒	☐
5.	Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants?	☐	☒
6.	Does the study involve invasive or intrusive procedures such as blood taking or muscle biopsy from participants?	☐	☒
7.	Is physiological stress, pain, or more than mild discomfort likely to result from the study?	☐	☒
8.	Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?	☒	☐
9.	Will the study involve prolonged or repetitive testing?	☐	☒
10.	Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?	☐	☒
11.	Will the study involve recruitment of participants (including staff) from other Faculties at Canterbury Christ Church University?	☐	☒
12.	Will the study involve recruitment of participants (including staff) through a Local Authority (e.g. Kent County Council) Department of Social Services?	☐	☒
13.	Will the study involve recruitment of patients or staff through the NHS?	☐	☒

If you have answered 'NO' to all the questions above then no further action is required.

If you have answered 'YES' to any of the questions above then you will need to describe more fully how you plan to deal with the ethical issues raised. This does not necessarily mean that you cannot proceed with your proposals but it does mean that your proposals will need to be approved by your supervisor/second marker.

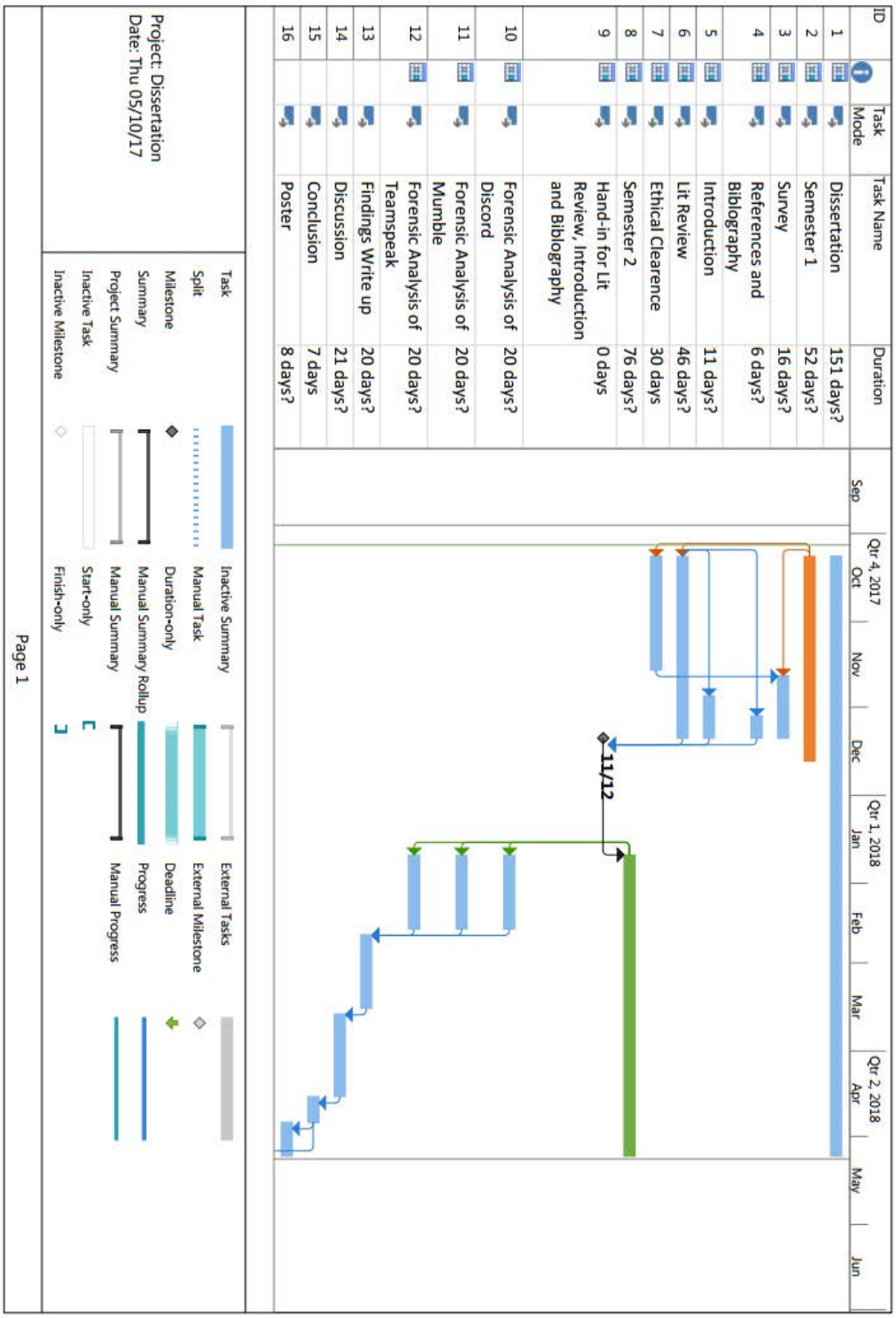
Chapter 5

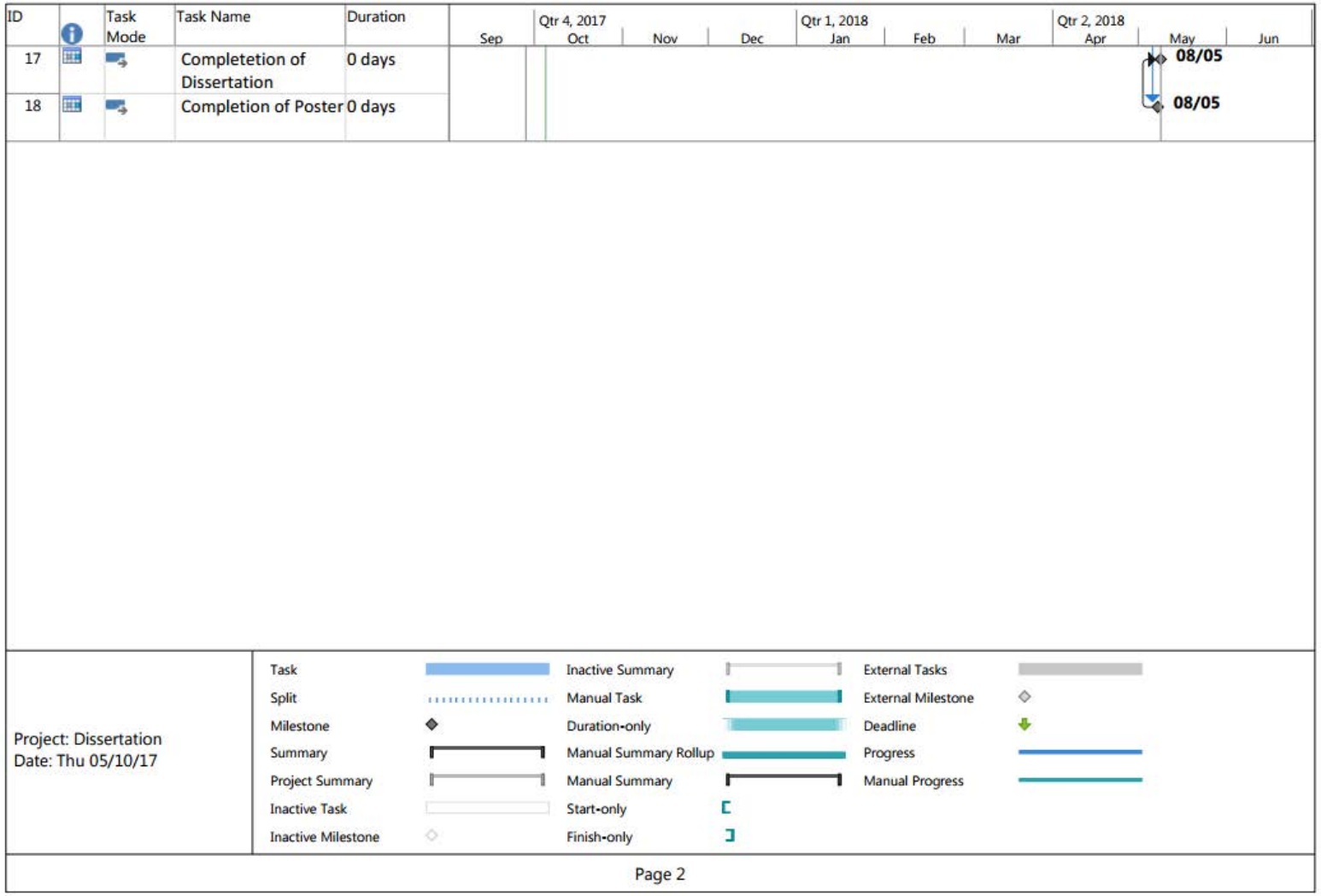
Risks and Their Management

Name	Risk	Mitigation
Detection as Virtual Machine	Medium	Do not install System Drivers. (Keragala and Walker, 2016)
Legal Challenges to forensic analysis of clients	High	Withdrawal of clients from study
Data processed with errors	Low	Testing and Analysis conducted over two systems to reduce rate of error.
User interaction with external services	Low	External users could attempt to connect or communicate with user. Steps will be taken to isolate the test accounts from the public environment (password protected servers).
Questionnaire Data may be compromised	Low	If using Google Forms (a personal account not a University account) there is a personal risk to Data Protection laws.
Virtual Machines may be compromised during research	Low	After each installation of the clients a re-installation of a base snapshot of the windows operating system and tools used for analysis will be applied, thus reducing the threat of possible infections.

Chapter 6

Research Plan




ID
Task Mode
Task Name
Duration
Sep
Qtr 4, 2017
Oct
Nov
Dec
Qtr 1, 2018
Jan
Feb
Mar
Qtr 2, 2018
Apr
May
Jun
17
Completetion of Dissertation
0 days
18
Completion of Poster
0 days
08/05
08/05
Project: Dissertation
Date: Thu 05/10/17
Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress
Page 2

Chapter 7

References and Appendix

7.1 Appendix A: Costs and Resources

3 x Windows 7 - Acquired before dissertation. 1 x Linux 1GB Instance (Digital Ocean) $10 per month x 6 months = $60 (£46)
AccessData FTK Imager - Freeware
EnCase Forensic Investigator 7 - Use forensic lab for analysis
Autopsy - Freeware
TeamSpeak3 Server Licence - (Free/Unlicensed for upto 32 slots for non-commercial use) (Teamspeak, 2017)
PALADIN Forensic Suite - Freeware ($25 donation will be made from Maintenance Allowance)
Cerbero Profiler Advanced - (Purchased with Maintenance Allowance)
WinHex - Freeware
PAExplorer - (Purchased with Maintenance Allowance) DumpIt - Freeware

7.2 Appendix B: Software Artefact

Not applicable

7.3 Apexdix C: Choice of Supervisor

Supervisor's Name: Choice 1: Georgina Humphries
Choice : Danny Webb
Choice 3: Ian Kennady

Please use default marking scheme.

7.4 Appendix D: Supervisor's Sign off

Please add a tick or 'N/A' to the appropriate boxes:

The student has read the relevant sections of the University's Research Governance Handbook, available on University Research web pages at: http://www.canterbury.ac.uk/Research/GovernanceandEthics/	☐
The topic merits further research.	☐
The student has the skills to carry out the Individual Study.	☐
The participant information sheet or leaflet is appropriate.	☐
The procedures for recruitment and obtaining informed consent are appropriate	☐
If a CRB check is required, this has been carried out.	☐

The Individual Study cannot proceed until all the above boxes have been completed.

Supervisors Signature: …… Date: ……..[1]

7.5 References

7Safe and Chief Police Officers, A. of (2017). *ACPO Guidelines — Publications — 7Safe*. Available at: https://www.7safe.com/about-7Safe/downloads/acpo-guidelines (Accessed: May 25, 2017).

AccessData (2017). *Forensic Toolkit (FTK)*. Available at: https://accessdata.com/products-services/forensic-toolkit-ftk (Accessed: May 24, 2017).

Banerjee, J. (2014). 'Jihad and Counter-jihad in Germany'. *Jadavpur Journal of International Relations* 18.2, pp. 103–136. DOI: 10.1177/0973598415569933. Available at: http://dx.doi.org/10.1177/0973598415569933 (Accessed: May 18, 2017).

BBC (2015). 'Breck Bednar murder: Lewis Daynes sentenced to life in prison'. *BBC News*. Available at: http://www.bbc.co.uk/news/uk-england-30786021 (Accessed: March 23, 2017).

Conservatives (2017). *The Conservative Party Manifesto 2017*. Available at: https://www.conservatives.com/manifesto (Accessed: May 19, 2017).

Day, J. (2001). 'Microsoft game taken off shelves'. *The Guardian*. Available at: https://www.theguardian.com/technology/2001/sep/13/games.terrorismandthemedia (Accessed: February 9, 2017).

Discord (2017). *Discord - Free voice and text chat for gamers*. Available at: https://discordapp.com (Accessed: May 24, 2017).

ea.com (2017). *Terms of Service*. Available at: http://tos.ea.com/legalapp/eula/US/en/ORIGIN (Accessed: October 5, 2017).

Elliott, J. (2013). *World of Spycraft: NSA and CIA Spied in Online Games - ProPublica*. Available at: https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games?utm_source=et&utm_medium=email&utm_campaign=dailynewsletter (Accessed: February 9, 2017).

Farivar, C. (2015). *Paris police find phone with unencrypted SMS saying "Let's go, we're starting"*. Available at: https://arstechnica.co.uk/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ (Accessed: May 12, 2017).

Foundation, T. V. (2017). *The Volatility Foundation - Open Source Memory Forensics*. Available at: http://www.volatilityfoundation.org (Accessed: May 24, 2017).

Keragala, D. and Walker, C. (2016). 'Detecting Malware and Sandbox Evasion Techniques'. *SANS Institute InfoSec Reading Room*. Available at: Detecting%20Malware%20and%20Sandbox%20Evasion%20Techniques.

Kopecký, K. (2017). 'Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors)'. *Telematics and Informatics* 34.1, pp. 11–19. DOI: 10.1016/j.tele.2016.04.004. Available at: http://www.sciencedirect.com/science/article/pii/S0736585316300090 (Accessed: May 18, 2017).

Legislation.gov.uk (2003). *Communications Act 2003*. Text. Available at: http://www.legislation.gov.uk/ukpga/2003/21/section/127 (Accessed: May 31, 2017).

legislation.gov.uk (2017). *Computer Misuse Act 1990*. Text. Available at: http://www.legislation.gov.uk/ukpga/1990/18/section/1 (Accessed: May 24, 2017).

Menegus, B. (2017). *How A Video Game Chat Client Became The Web's New Cesspool Of Abuse*. Available at: https://www.gizmodo.com.au/2017/02/how-a-video-game-chat-client-became-the-webs-new-cesspool-of-abuse/ (Accessed: May 31, 2017).

Shortall, A. and Azhar, M. H. B. (2015). *Forensic acquisitions of WhatsApp data on popular mobile platforms*. IEEE Press.

Teamspeak (2017). *Choose A License*. Available at: http://sales.teamspeakusa.com/licensing.php?page=choose (Accessed: May 25, 2017).

WhatsApp (2017). *WhatsApp Legal Info*. Available at: https://www.whatsapp.com/legal/#terms-of-service (Accessed: May 24, 2017).

Yin-Poole, W. (2015). *Sony responds to claim PS4 used for terrorist communications*. Available at: http://www.eurogamer.net/articles/2015-11-16-sony-responds-to-claim-ps4-used-for-terrorist-communications (Accessed: May 12, 2017).

zoltanszabodfw (2012). *Parallels hard drive image converting for analysis*. Available at: https://articles.forensicfocus.com/2012/07/05/parallels-hard-drive-image-converting-for-analysis/ (Accessed: May 24, 2017).

Appendix C

Changes to the Proposal

Prior to launching the survey in consultation with Dr. Ian Kennedy an amended Survey was compiled to remove intrusive questions that may have caused psychological harm and discussion of sensitive topics. Therefore a new ethical checklist was completed see appendix H.

On December 30th 2017 Dr. Ian Kennedy suggested the downsizing of the dissertation from 4 clients; TeamSpeak, Discord, Origin and Steam to Discord and TeamSpeak Furthermore the only two companies that approved the use of there clients for forensic analysis was Discord and TeamSpeak which was confirmed by Dr. Ian Kennedy whom checked the emails from both companies. Mumble was not forensically analysed due to timing constraints.

During the survey creation a decision was made not to send a link to the Tabletop Top and Gaming Society at CCCU due to time constraints.

On the 2nd May 2018 a decision was made to switch virtualization platforms from Parallels to VirtualBox as VirtualBox provides a method to export data out to a raw image file which can be ingested by EnCase and could be writeblocked as Fastblock SE provides a built in method of writeblocking a USB hard drive. With Parallels a forensic image could be conducted using the EnCase Imager tool however it would leave traces behind of use on the hard drive as there was issues writeblocking the device using the Imager product.

On the 22nd of May 2018 a forensic acquisition of the TeamSpeak3 Executable raw image was attempted using EnCase 7. EnCase repeatedly crashed when attempting to ingest the RAW 35gb image. The image was left to process overnight however EnCase crashed. As such it was decided that alternative forensic tools would need to be used to preform the forensic analysis. The FastBloc SE write-blocker was still used from inside EnCase to shield the hard drive from possible threats. X-Ways Forensics was picked during the analysis to preform the initial forensics. Autopsy was also used to verify the integrity of the original findings.

During the experimental research phase tools originally suggested for the proposal was reduced down from the original proposal to focus on tools that where readily available such as EnCase (provided by the University) and freeware tools such as NirSoft ChromeCacheView. The

major cost was the DigitalOcean droplet which cost £3.69.

Appendix D

Project Management

Date	Time	Event
22/06/2017	16:48:06	Creation of the Literature Review
23/07/2017	14:56:12	Finished editing Literature Review and uploaded to University.
24/07/2017	00:00:00	Mile Stone 1 Research Paper Completed
04/12/2017	18:00:00	Commenced work written on dissertation.
18/01/2018	20:00:00	The configuration of the experiments starts
02/04/2018	19:00:00	Initial experiments for Discord conducted and the development of Discord Extractor had been created to fill the gap of the SQLite Clients.
14/06/2018	18:00:00	Recommenced work after Ill Health.
21/06/2018	20:00:00	Commenced work on Discord Execution Lab.
22/06/2018	09:00:00	EnCase large scale test conducted with the execution lab, estimated time for completion - 19 hours.
23/06/2018	11:00:00	EnCase has frozen, New method developed using X-Ways to review content
24/06/2018	18:00:00	Autopsy and write up of analysis.
25/06/2018	13:00:00	Discord Analysis Execution
26/06/2018	18:00:00	Write up in LaTeX.
29/06/2018	23:54:00	[MILESTONE] Discord and TeamSpeak analysis completed.

30/06/2018	00:22:00	Statistical Analysis begins
06/06/2018	13:00:00	Hand in Dissertation

Appendix E

Meetings with the Supervisor

Date	Time	Event
10/10/2017	14:01:00	Email sent to Dr Kennedy to request feedback on Survey questions.
24/10/2017	09:42:00	Dr Ian Kennedy sends feedback on Survey questions.
25/10/2017	00:37:00	Oliver Bryant asks for clarification on population size and on the use of research materials containing the same author.
27/10/2017	08:55:00	Dr Ian Kennedy states requirement for population size and informs Oliver to remain sceptical about non-government information.
27/10/2017	10:37:00	Oliver Bryant requests meeting during the week.
27/10/2017	10:41:00	Meeting date not provided by Dr Kennedy, asks if question is outide of previous scope discussed in meeting
27/10/2017	12:07:00	Oliver Bryant explains that he is struggling to find a number that will quantify the use of gaming based voip clients
27/10/2017	12:11:00	Dr Ian Kennedy suggests the use of the Office of National Statistics population and migration data.
30/10/2017	16:15	(email) Dr Ian Kennedy asks for amendment to the research question reducing
04/12/2017	18:00:00	Commenced work written on dissertation.
18/01/2018	20:00:00	The configuration of the experiments starts
28/01/2018	22:00:00	Experiment on individual client forensics starts

28/01/2018	22:30:00	User "Plato005" created for individual client study, creates single server and publishes messages to channel. Wireshark detects TLS 1.2 encryption.
15/03/2018	12:12:00	Discovery of circumvention of HTTPS encryption by using the tool Fiddler is discovered.
15/03/2018	23:00:00	Memory forensics on virtual machine concludes that Discord is using node.js and electron as the development platform.
15/03/2018	01:15	Arrange Meeting with IK on Monday at 11:30am to discuss statistics and the revised experiment (3 forensic images per experiment excluding the individual analysis.)
16/03/2018	11:30	Meeting with IK at Ag29 to discuss Statistics and the new revised forensic experiment.
20/03/2018	10:30	Meeting with IK at Ag29 to discuss Chi-Square test of Independence statistics.

Appendix F

Materials Related to Forensic Analysis

Date	Time	Procedure
06/02/2018	19:31:00	Installed EnCase Imager 7.10, NirSoft Process Monitor v3.40, NirSoft BrowsingHistoryView v2.15 and Fiddler 4.6 onto Seagate Hard Drive, Files extracted onto the folder
06/02/2018	19:44:00	Create Snapshot: Baseline
06/02/2018	19:44:00	Victim Virtual Machine Turned on.
06/02/2018	19:51:00	Navigate to `https://discordapp.com` via Internet Explorer
06/02/2018	19:53:00	Click "Download Discord for Windows"
06/02/2018	19:55:00	DiscordSetup.exe saved to Downloads.
06/02/2018	19:55:00	Opened up cmd.exe ran "cd Downloads", "CertUtil -hashfile DiscordSetup.exe MD5"
06/02/2018	19:58:00	MD5 Hash: 77 bd 31 10 9d f9 7c 5d 3c 1e 86 3f 14 b3 a9
06/02/2018	20:03:00	Shutdown of Virtual Machine for break. (watching falcon heavy launch)
06/02/2018	21:22:00	Resuming Virtual Machine
06/02/2018	21:23:00	Executing Process Explorer v3.40 from Hard Drive. Set to capture running processes
06/02/2018	21:25:00	Appication DiscordSetup.exe is executed
06/02/2018	21:27:00	Filtering Results into Result Table 1
06/02/2018	22:00:00	Initial analysis from ProcMon suggests the use of DiscordSetup.exe spawns the process Update.exe from a newly created Squirrel folder. the application Squrriel.exe is then executed before the DiscordApp.exe is created. Further analysis is required to understand what these processes do.
06/02/2018	22:28:00	Experiment suspended for the evening. Further investigation into each of the processes is required. the Windows Process log has been saved onto a external hard drive for safe keeping.
06/02/2018	13:52:00	Hibernated

07/02/2018	21:00:00	Resuming Virtual Machine
07/02/2018	21:35:00	Filtering ReadFIle operations as there's quite a few! (Filter >Filter >PID: 1492, Operation ReadFile, Path: C:\Users\Jane Doe\Downloads\DiscordSetup.exe)
07/02/2018	17:41:00	Uploaded Hybrid Analysis of DiscordSetup.exe. The PE drops the process Update.exe which was created by GitHub, Squirel.exe has also been spawned from Github. Sample: `https://bit.ly/2JkMzqp`
11/02/2018	17:44:00	Searched Term: Squirrel.exe Github which returned with the repository `https://github.com/Squirrel/Squirrel.Windows` a automatic updating and installation system.
11/02/2018	19:30	EnCase Image taken of the Hard Drive stored on an external drive.
11/20/2018	20:50	Installation Experiment Complete.

Table F.1: Discord Client installation phase log

Time	Discovery	Observation	Reference Code
21:25:00	Permissions Check	Explorer.exe requests permission to read DiscordSetup.exe (Triggers UAC).	R1
21:25:20	Attempted Creation of file	DiscordSetup.exe spawns process Update.exe (Attempt Create File: C:\Users\Jane Doe\AppData\Local\SquirrelTemp\Update.exe) in the Squirrel Temp folder with NAME NOT FOUND: Read Attributes, Delete	R2
21:25:20	Successful Creation of file	Creation of Update.exe inside the SquirrelTemp folder. (SUCCESS: Generic Read Attributes, Read Attributes created)	R3
N/A	Internet Artefact	a remote procedure call back to discordapp.com to confirm installation of the discord client. `http://discordapp.com/handoff?rpc=5463&key=395c5994-e53f-4c8f-84cb-e481819d540e`	R4
N/A	Internet Artefact	Location of Node.js being identified as Shellcode in a automated analysis has demonstrated that Discord is running on a form of Electron. proof found online at `https://electronjs.org/apps/discord`	R5
N/A	Nuget Package Discovered	The nuget package file created by DiscordSetup.exe was discovered while the Proccess Monitor capture was running. File was not found however a SquirrelSetup.txt was found at C:\Users\Jane Doe\AppData\Local\SquirrelSetup which contains the movement of .dll files from C:Users\Jane Doe\AppData\Local\Discord\app-0.0.300\lib\net45\ to C:\Users\Jane Doe\AppData\Local\Discord\app-0.0.300, The .DLLs moved over were part of the .NET 4.5 framework.	R6

Table F.2: Artefact Recovered During Installation Phase

Artefact	Time	Description
Dumpit.exe	18:54	Executed Dumpit.exe from external hard drive mounted onto the Windows 7 Victim Virtual Machine
Kali start	19:02	Boot up Kali Linux and mount the .dmp image in read-only mode. Using Volatility Framework 2.6 to inspect the running DiscordApp .dll files being executed during operation.
node.dll (3796)	20:02	found node.dll being executed by discord.exe process.
discord_overlay2.node (4896)	20:03	Found first use of a ṅode module being used by the Discord.exe process, This extension refers to the Discord overlay.
discord_utils.node (4896)	20:05	Utility library for Discord, content unknown.
discord_erlpack.node (4896)	20:07	ErLang Library for Discord client.
discord_contact_import.node (4896)	20:07	contact import data from Discord client.
Experiment Finished	23:54	

Table F.3: Observations taken from Memory Capture during live execution.

Time/Date	Database	Observation	Reference Code
19:40:21 02/04/2018	https_discordapp.com_0.localstorage	email_cache (blob): Email Address *".d.i.s.c.o.r.d.t.e.s.t.e.r.5.@g.m.a.i.l...c.o.m.".*	D1
19:51:20 02/04/2018	https_discordapp.com_0.localstorage	SelectedChannelStore (blob) *{"selectedVoiceChannelId":null, "lastConnectedTime":1519855890455, "selectedChannelIds": {"418523018696982530": "418523019158224897","41771983423143937" :"144156862021894144"}}* The selectedChannelIds lists all the channels connected to the client, The lastConnected-Time provides an Epoch time stamp that could be used to determine when the client was last connected to Discord.	D2
20:02:00 02/04/2018	https_discordapp.com_0.localstorage	DraftStore (blob) *{"418523019158224897": {"timestamp":1522695445085, "draft":"test"}}* Stores Draft copies of text left behind in chats. The first part contains the channel ID, the second part contains the timestamp, the third part includes the draft message.	D3

20:20:01 02/04/2018	https_discordapp.com_0.localstorage	Token (blob) *"NDE4NTIwMTk0NzIyMjk5OTA0* *.DXizFQ.b3h7ebc__x4SSnQrTl5DwQLIu_I"* The authentication token used to send and receive data by the client, it is unique. See figure F.3 for usecase.	D4
21:55:01 02/04/2018	Cookies	host_key (text) *.twitch.tv* indicates that a user has clicked on/played a twitch.tv video inside the Discord client. This could be coupled up with the ChromeViewHistory.exe to determine the specific site visited.	D5

Table F.4: Data extracted from https_discordapp.com_0.localstorage

Date	Time	Procedure
05/04/2018	14:53:58	Commenced Uninstallation of Discord. Start Menu > Control Panel > Uninstall a program > Uninstall
05/04/2018	14:53:58	Update.exe is invoked with commands from Registry (See figure F.2)
05/04/2018	14:53:59	Discord.exe (PID: 5772) Commences –squirrel-uninstall 0.0.300 flag.
05/04/2018	14:53:59	Spawned by Discord 5572 Update.exe (PID: 2644) Invokes –removeShortcut Discord.exe
05/04/2018	14:54:01	PID 5772 spawns the default discord.exe process before closing instantly.
05/04/2018	14:54:01	Reg.exe (PID: 3752) is spawned to delete the current version of Discord that was runable from inside the Registry. `delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Discord /f`
05/04/2018	14:54:01	Reg.exe (PID: 3008) deleting the classes record for Discord. `delete HKCU\Software\Classes\Discord /f`
05/04/2018	15:00:00	Files have been left behind in `C:\Users\Jane Doe\AppData\Roaming\discord` including folders `Local Storage`, `Cache`, `GPUCache`, `0.0.300` (however Discord.exe is missing, only the modules folder remains).
05/04/2018	15:30:00	Development of Discord Extractor commences focusing on the localstorage file located at `C:\Users\Jane Doe\AppData\Roaming\discord\Local Storage\https_figscordapp.com.0.localstorage`

05/04/2018	17:00:00	An error message kept reoccurring `sqlite3.DatabaseError: malformed database schema (MmapStatus) - near "(": syntax error` After inspecting the version of SQLite being used by default by Python 3.5 (3.8.2) the decision was made to switch to using the Library apsw (Another Python SQLite Wrapper). (Binns, 2018)
05/04/2018	18:00:00	Machine Image was taken using EnCase Imager onto secondary hard drive for later review.
05/04/2018	19:00:00	Decoding issues meant not all data was being decoded correctly. The decicison was made to Decode ALL data in UTF-16 which resulted in the data being parsed out in a readable format.
05/04/2018	18:30:00	Modifications made to turn the script into a CLI application. Flags introduced to provide a method to point to a custom file.
05/04/2018	19:00:00	Error checking developed into the application.
05/04/2018	21:33:00	Program demo sent to Dr Ian Kennedy for review.

Table F.5: Discord client uninstallation Proccess Monitor log

Artefact	Figure Reference	Description
Settings.db	See figure F.22	The Settings.DB contains general settings saved by the TeamSpeak client locally. It also includes useful information such as the number of File Upload, Download and the last Upload Folder Location.
urls.db	See figure F.30	The database that stores links shared between clients. During this analysis no URLs where found in the Database as there had been no chat/text conversations.
cookies	See figure F.24	Cookies contained information related to the MyTeamSpeak cloud. Data indicated the use of CloudFlare as a method of protection to the external application.
channel.html	figure F.32	Channel log shows channelid://1 lobby is being connected to via the client.
server.html	See figure F.31	server logs showed that the client connected to the server "CCCU" Lab 4 times between 19:49:35

Table F.6: TeamSpeak3 execution artefact analysis

Artefact	Figure Reference	Description
Cache	figures F.46, F.59 and F.60	Cache that stores cookies generated from the sites and players used in the client.
Cookies	appendix I and figure F.6	Storage of cookies used in the embedded media player. e.g.: Twitch.tv
https_discordapp.com_0.localstorage	listing F.4 and figure F.61	Locale, Email, Channel IDs, Time Stamps, Emoji Statistics, user invites, Unique Authorisation Token
https_player.twitch.tv_0.localstorage	figure F.57	The time the player was resumed and played, If mature content was displayed, volume setting and if mute had been used.

Table F.7: Discord Execution Artefact Analysis

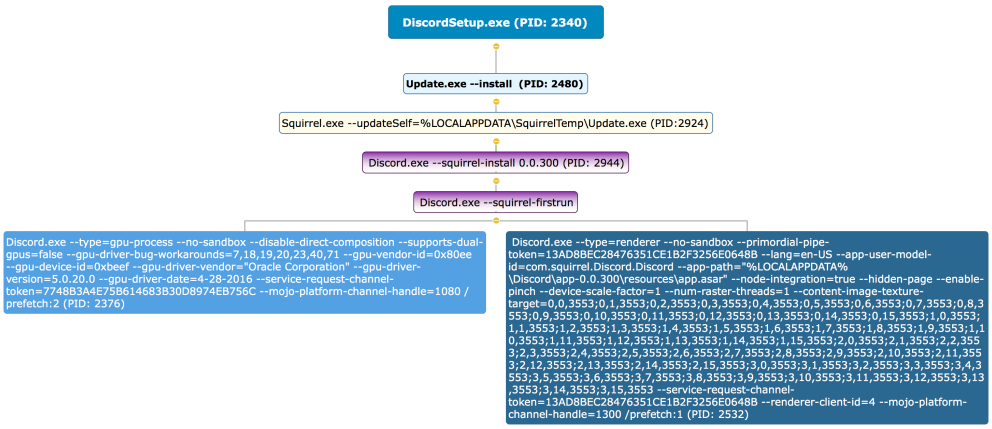


Figure F.1: A graphical view of the spawning processes recorded in Hybrid Analysis - `https://bit.ly/2JkMzqp`.

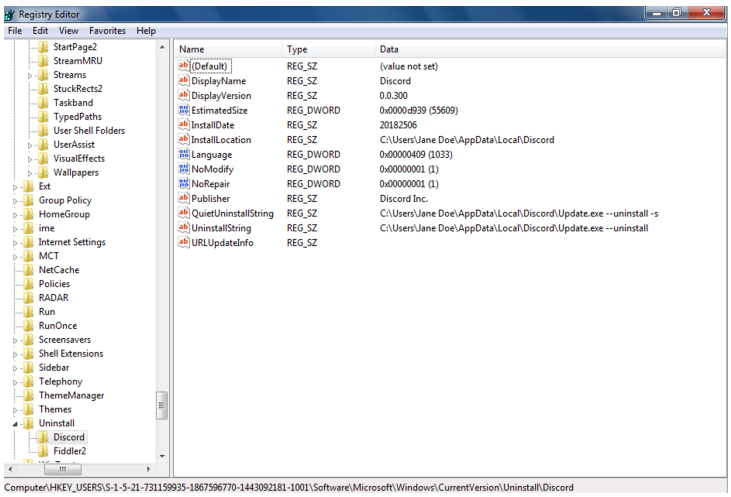


Figure F.2: Registry view of Discord.exe artefact. Update.exe is used to uninstall the Discord.exe application.

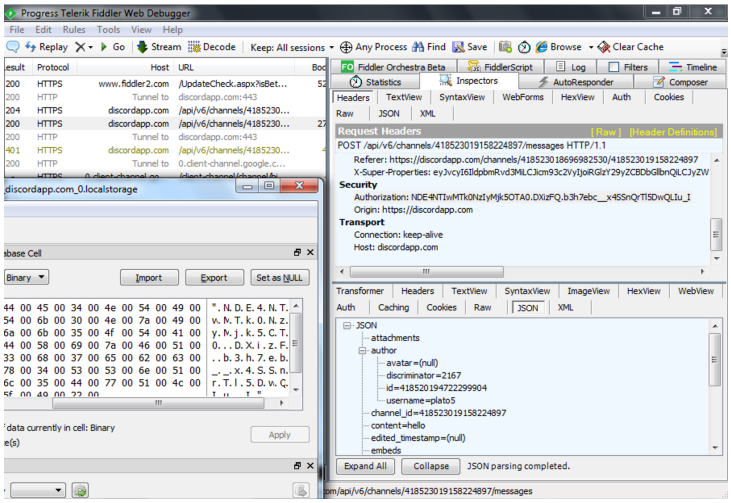


Figure F.3: Security Token used to authorise and post messages. SQLBrowser shows the "token" row from the localstorage database. Fiddler HTTPS intercept shows the security authentication layer when sending a message to a server on discord.

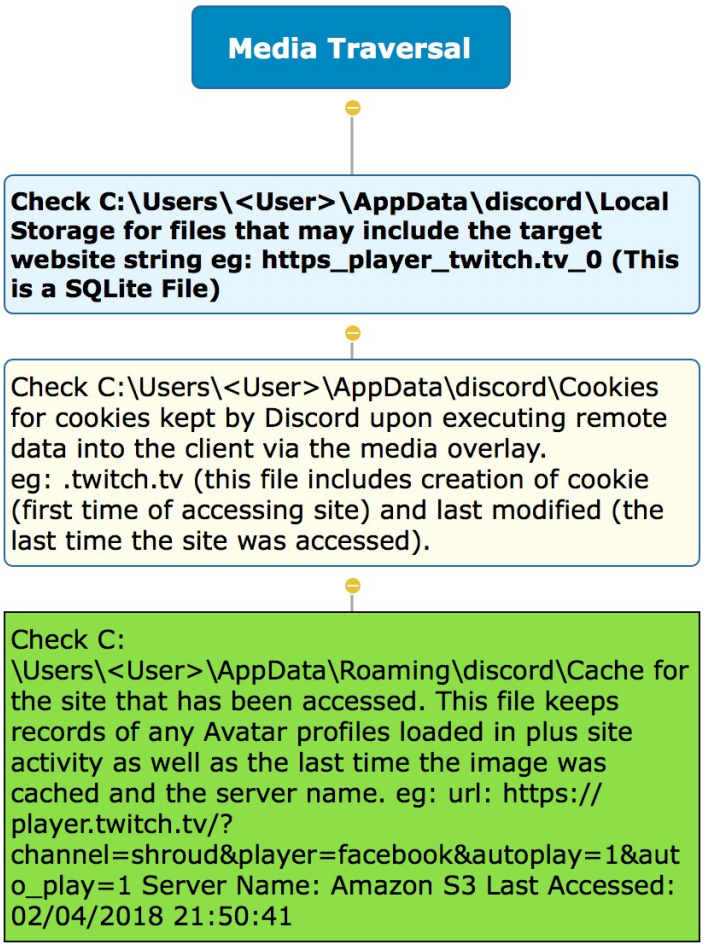


Figure F.4: Methodlogy of locating playable media from Discord.

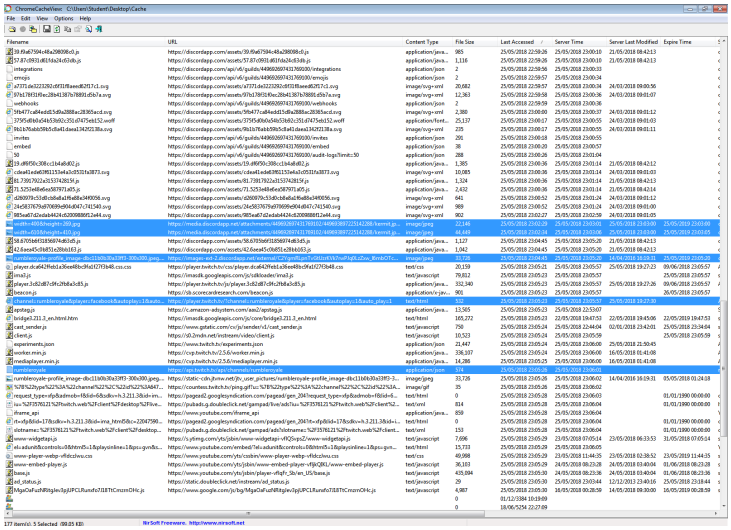


Figure F.5: Discord Cache displayed in ChromeCacheViewer.

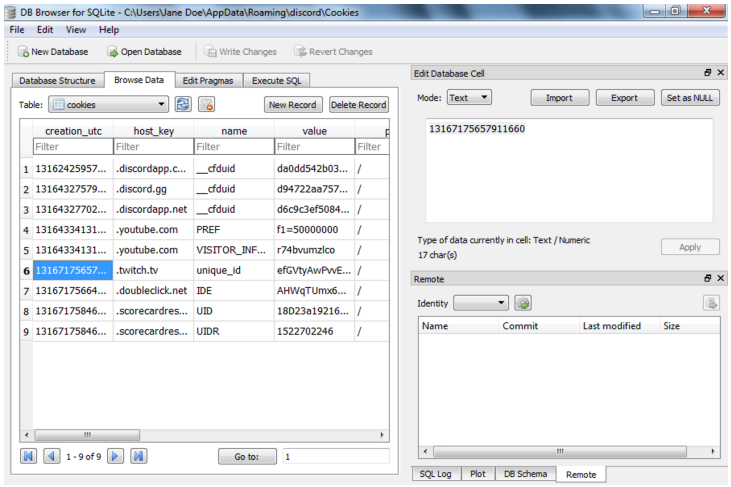


Figure F.6: Cookies retained by the Discord Client including any used to play media inside of the client (Twitch.tv)

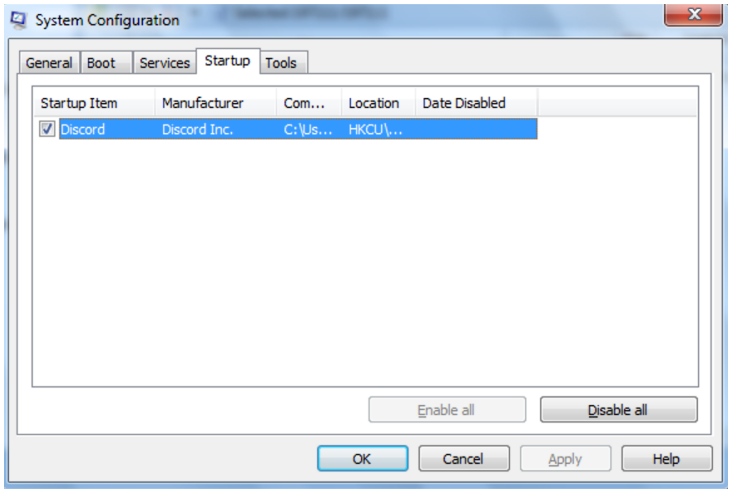


Figure F.7: msconfig shows that Discord.exe is set to run on start-up

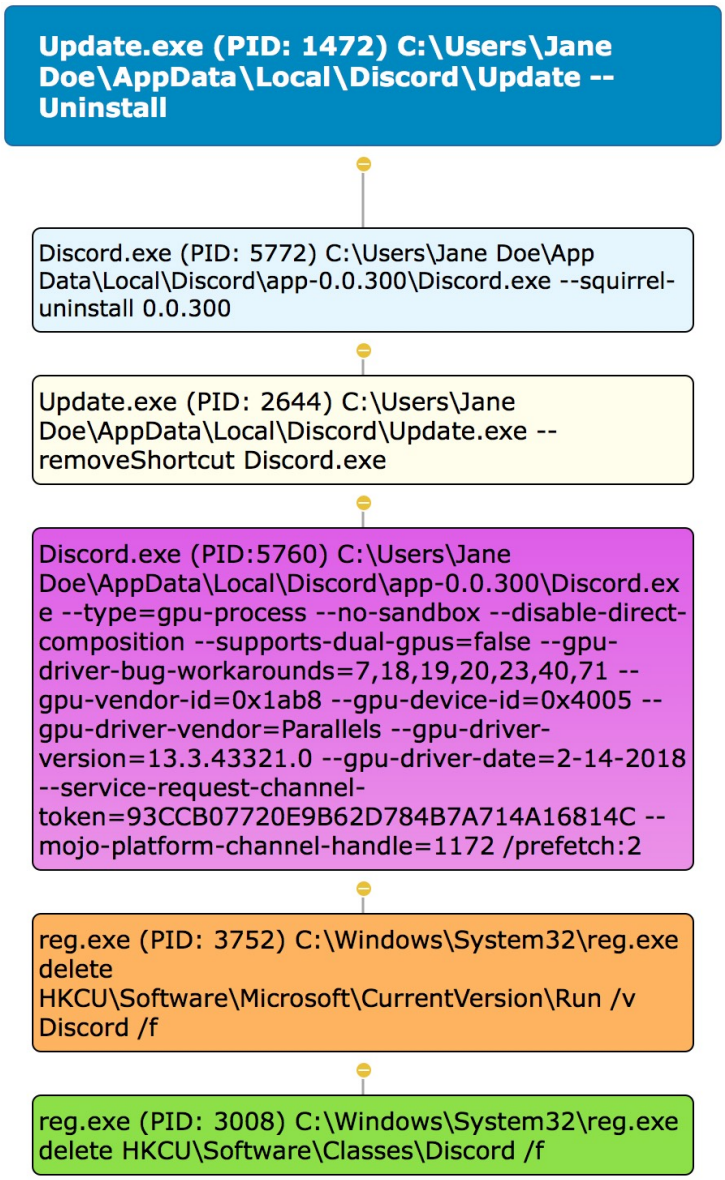


Figure F.8: Uninstallation Process Tree for the discord.exe client.

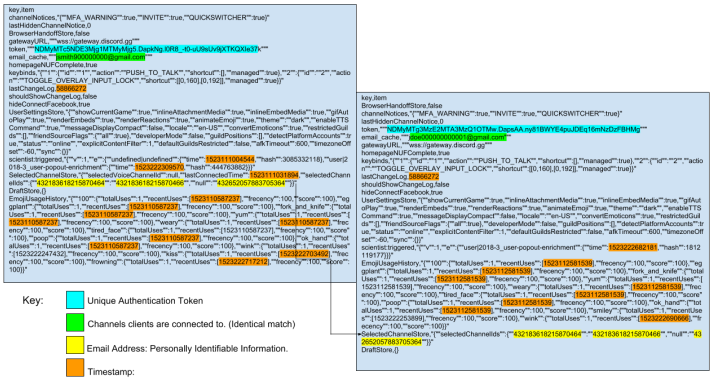


Figure F.9: local storage comparison from the http_discordapp.com_0.localstorage files extracted with the Discord Extractor

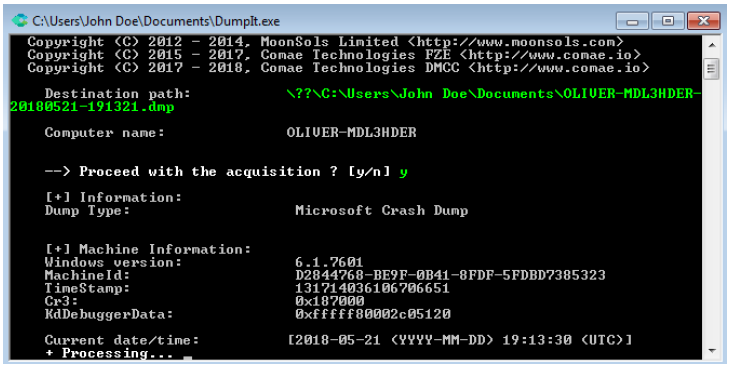


Figure F.10: Memory Dump for TeamSpeak3 Execution Lab via DumpIT.

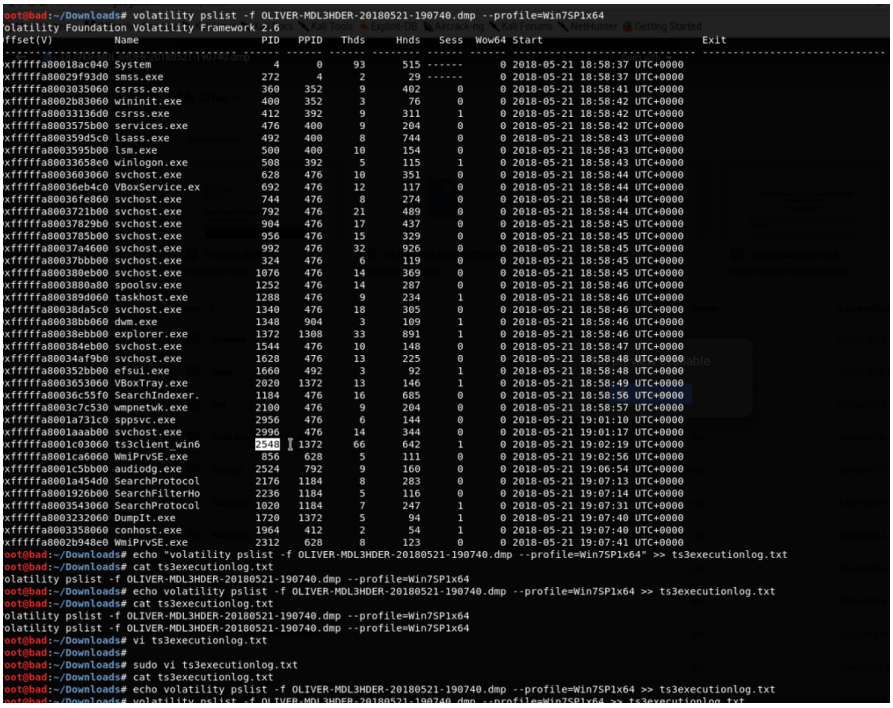


Figure F.11: pslist shows active processes which includes the PID for TeamSpeak 3 executable.

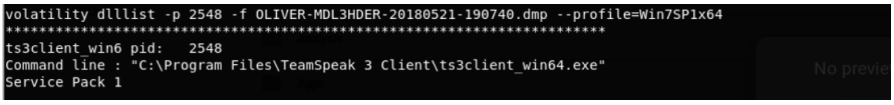


Figure F.12: dlllist command to display active dll files.

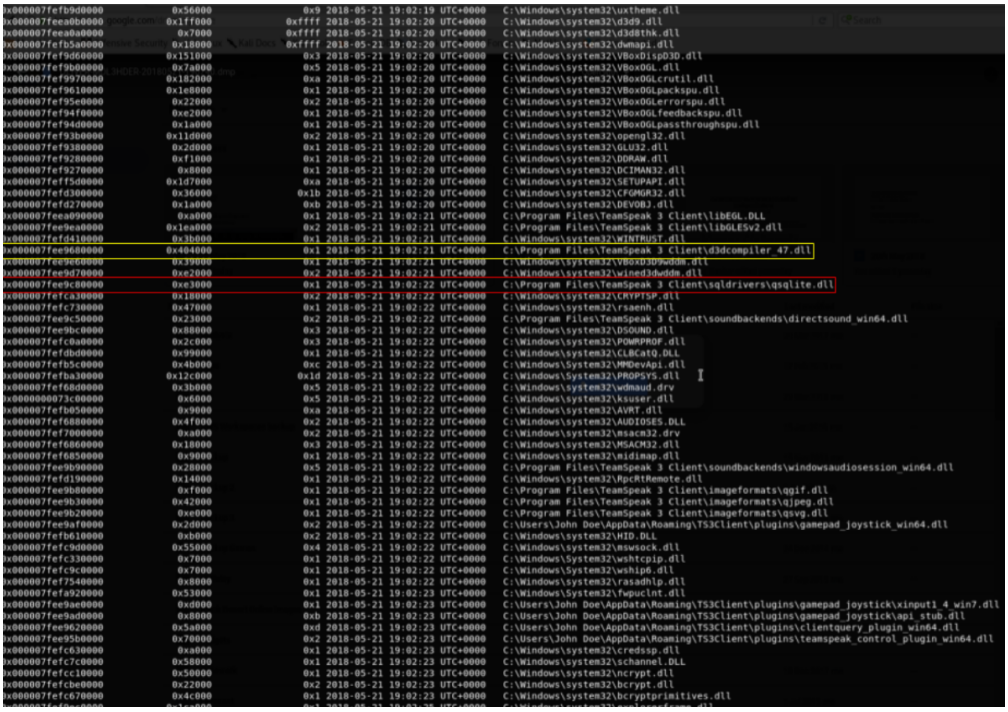


Figure F.13: the qsqlite.dll (red) indicates that TeamSpeak3 is using a SQLite Database. The d3dcompiler_47.dll shows that TeamSpeak utilizes DirectX (Yellow)

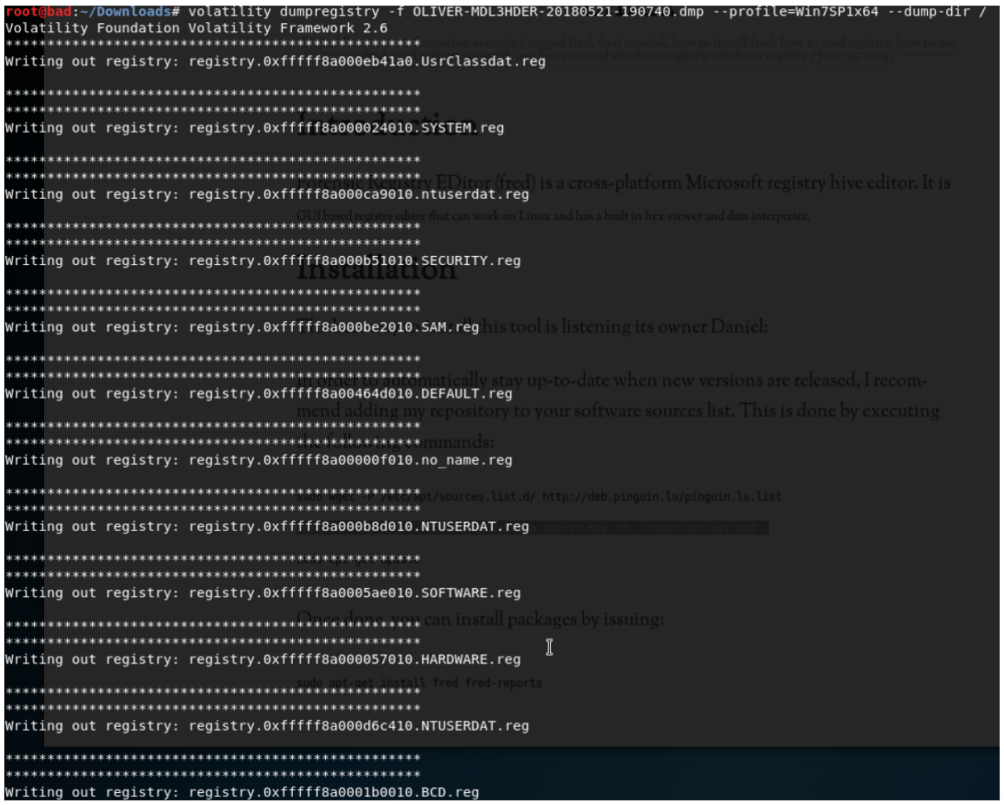


Figure F.14: a registry dump taken using the dumpregistry command.

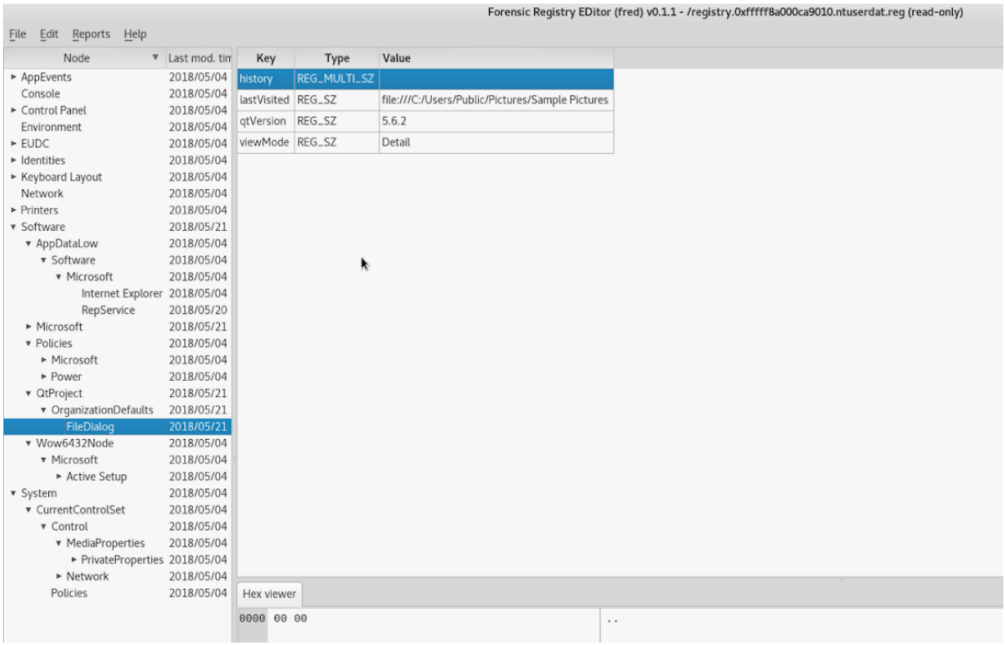


Figure F.15: FRED used to view the registry hive. Discovery of the QtProject registry keys in memory includes the lastVisited file location which is the same file location that files have been uploaded from.

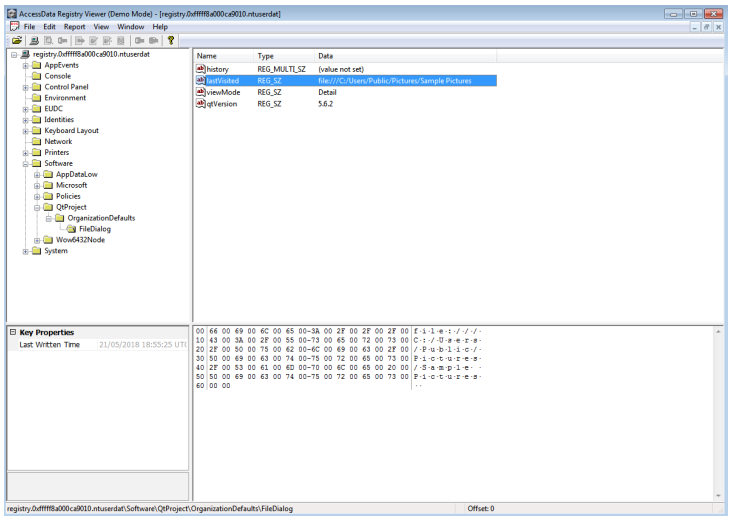


Figure F.16: Access Data Registry Viewer was used to view the same registry hive as figure F.15 to verify the data.

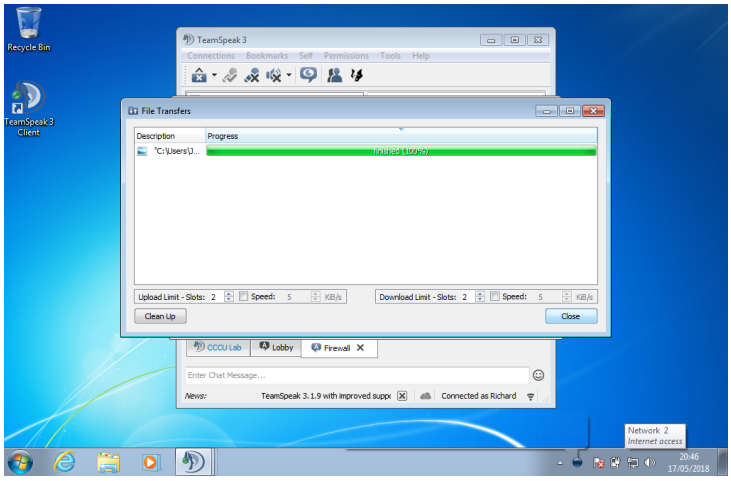


Figure F.17: Demonstration of a file being uploaded to the TeamSpeak3 server.

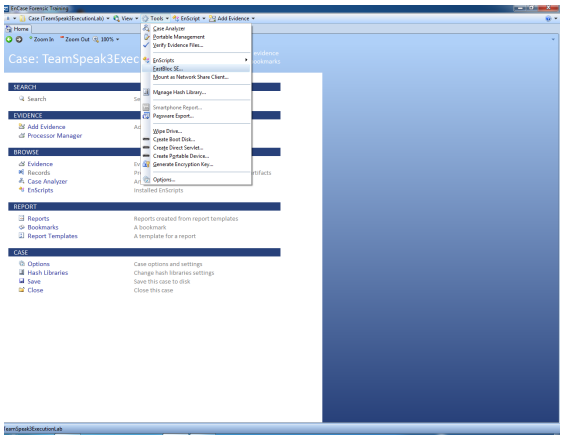


Figure F.18: FastBloc SE used to writeblock the evidence hard drive.

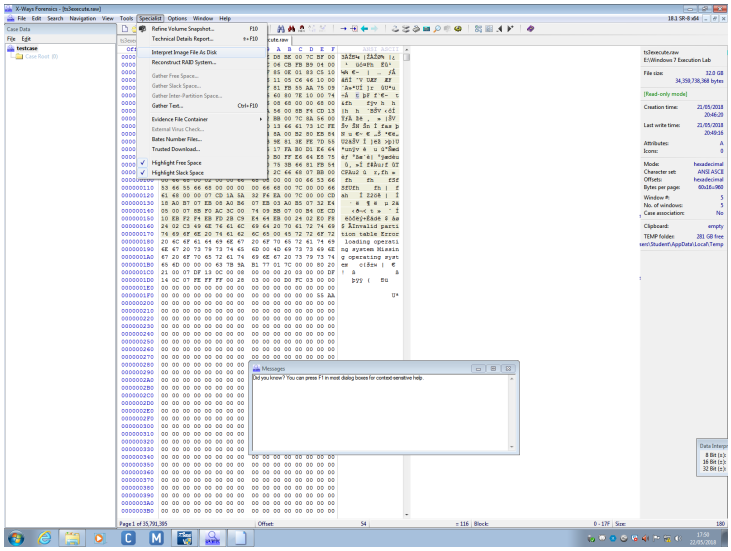


Figure F.19: X-Ways Forensics provides an option to view raw image data as a disk.

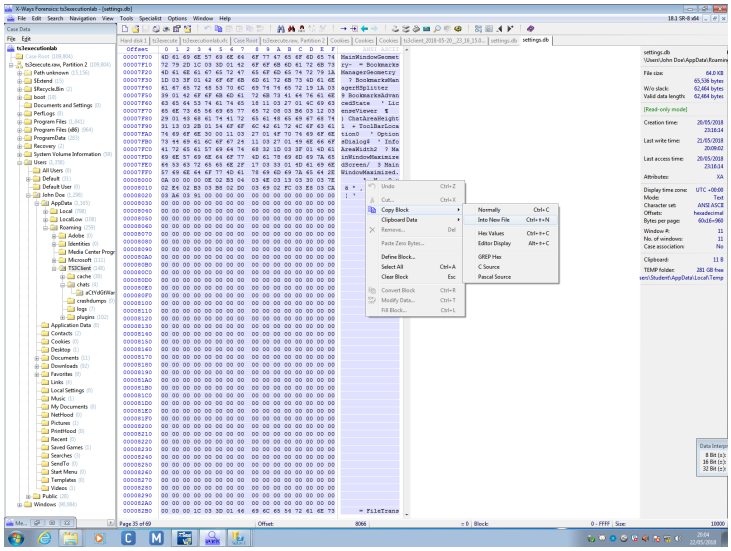


Figure F.20: Exporting settings.db from X-Ways

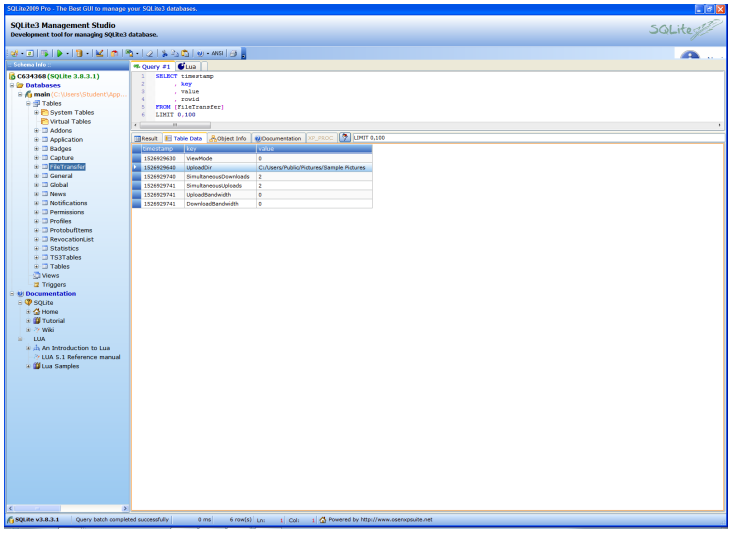


Figure F.21: Viewing the FileTransfer table from Settings.db in SQLite2009 Pro for the TeamSpeak Execution Lab.

timestamp	key	value
1526929630	ViewMode	0
1526929640	UploadDir	C:/Users/Public/Pictures/Sample Pictures
1526929740	SimultaneousDownloads	2
1526929741	SimultaneousUploads	2
1526929741	UploadBandwidth	0
1526929741	DownloadBandwidth	0

Figure F.22: The FileTransfer Table from settings.db which includes the last known upload folder.

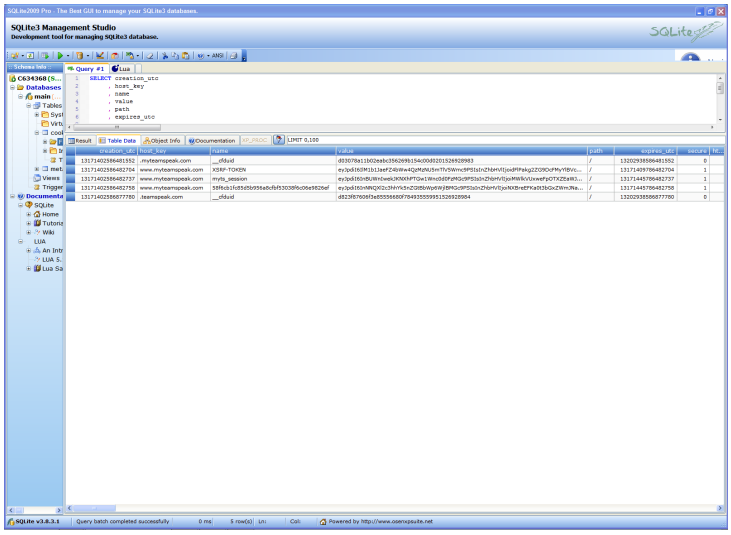


Figure F.23: The Cookies database with artefacts that indicate that the cache is developed for the MyTeamSpeak service. Cookies contain data that indicates CloudFlare cookies.

creation_utc	host_key	name	value	path	expires_utc	secure
13171402586481552	.myteamspeak.com	__cfduid	d03078a11b02eabc356269b154c00d0201526928983	/	13202938586481552	0
13171402586482704	www.myteamspeak.com	XSRF-TOKEN	eyJpdiI6IlM1b1JaeFZ4bWw4QzMzNUSmTlV5Wmc9PSIsInZhbHVlIjoidFlPakg2ZG9DcFMyYlBVc...	/	13171409786482704	1
13171402586482737	www.myteamspeak.com	myts_session	eyJpdiI6InBUWnIwekJKNXhPTGw1Wnc0d0FzMGc9PSIsInZhbHVlIjoiMWlkVUxweFpOTXZEaWJ...	/	13171445786482737	1
13171402586482758	www.myteamspeak.com	58f6cb1fc85d5b956a8cfbf53038f6c06e9826ef	eyJpdiI6InNNQXI2c3hhYk5nZGtBbWp6WjlBMGc9PSIsInZhbHVlIjoiNXBreEFKa0t3bGxZWmJNa...	/	13171445786482758	1
13171402586877780	.teamspeak.com	__cfduid	d823f87606f3e85556680f7849355599515269289 84	/	13202938586877780	0

Figure F.24: The cookies found from the Cookies file.

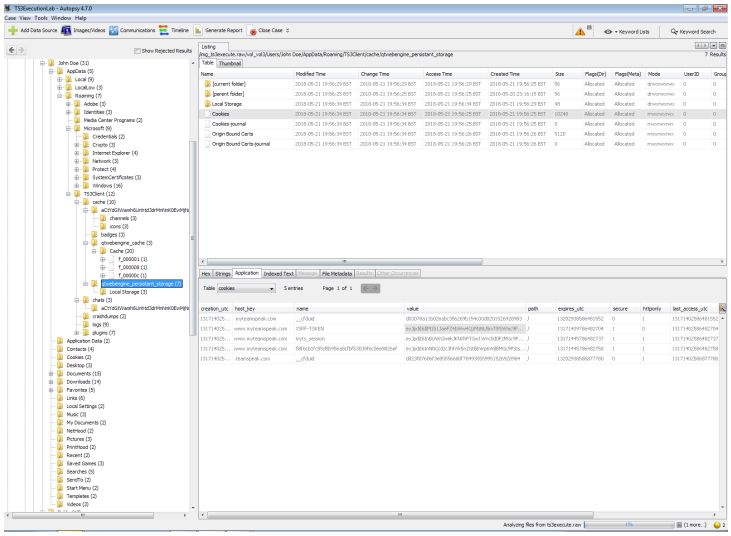


Figure F.25: The cookies found from the Cookies file in Autopsy.

creation_utc	host_key	name	value	path	expires_utc	secure	httponly	last_access_utc
131714025…	.myteamspeak.com	__cfduid	d03078a11b02eabc356269b154c00d0201526928983	/	13202938586481552	0	1	13171402586481552
131714025…	www.myteamspeak.com	XSRF-TOKEN	eyJpdiI6IlM1b1JaeFZ4bWw4QzMzNU5mTlVSWmc9P…	/	13171409786482704	1	0	13171402586482704
131714025…	www.myteamspeak.com	myts_session	eyJpdiI6InBUWn1wekJKNXhPTGw1Wnc0d0FzMGc9P…	/	13171445786482737	1	1	13171402586482737
131714025…	www.myteamspeak.com	58f6cb1fc85d5b956a8cfbf53038f6c06e9826ef	eyJpdiI6InNNQXl2c3hhYk5nZGtBbWp6WjBMGc9P5Is…	/	13171445786482758	1	1	13171402586482758
131714025…	.teamspeak.com	__cfduid	d823f87606f3e855556680f78493555995152692898 4	/	13202938586877780	0	1	13171402586877780

Figure F.26: Cookies file in Autopsy

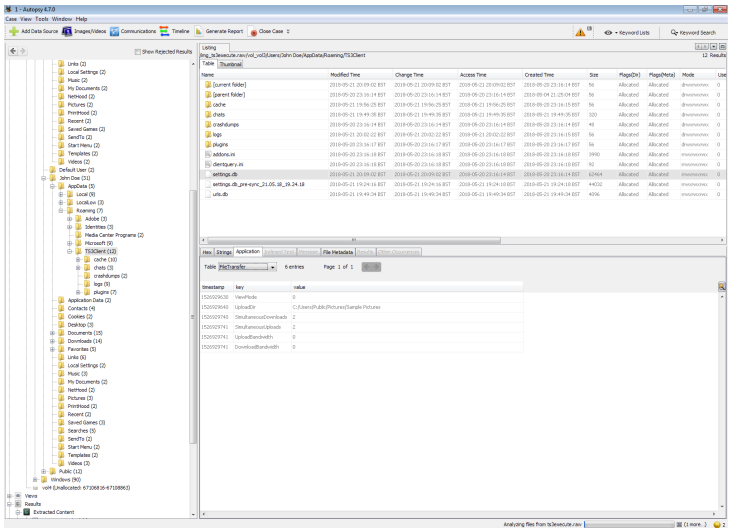


Figure F.27: Settings.db file in Autopsy displaying the FileTransfer Table.

Table FileTransfer 6 entries Page 1 of 1

timestamp	key	value
1526929630	ViewMode	0
1526929640	UploadDir	C:/Users/Public/Pictures/Sample Pictures
1526929740	SimultaneousDownloads	2
1526929741	SimultaneousUploads	2
1526929741	UploadBandwidth	0
1526929741	DownloadBandwidth	0

Figure F.28: FileTransfer Table in Autopsy

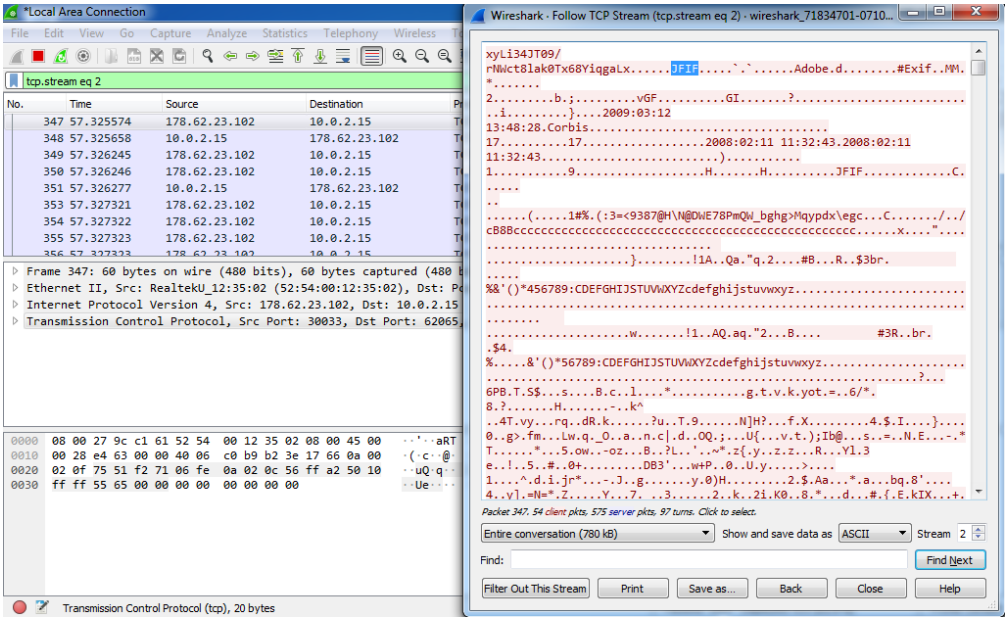


Figure F.29: File Uploads are not encrypted to TeamSpeak3 Server.

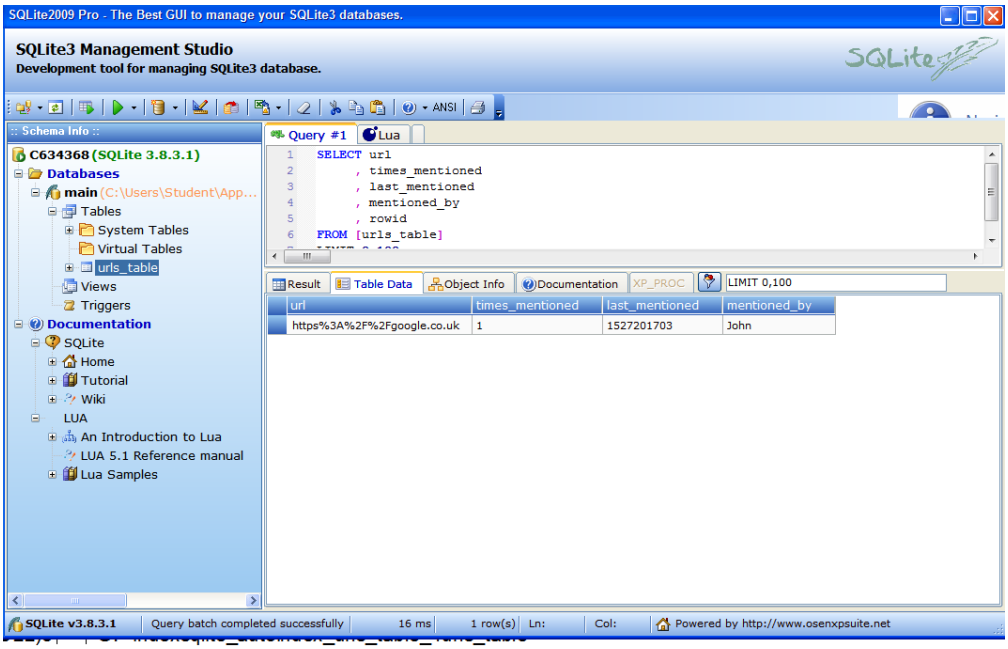


Figure F.30: the urls.db file contains links said by different users in public and private channels.

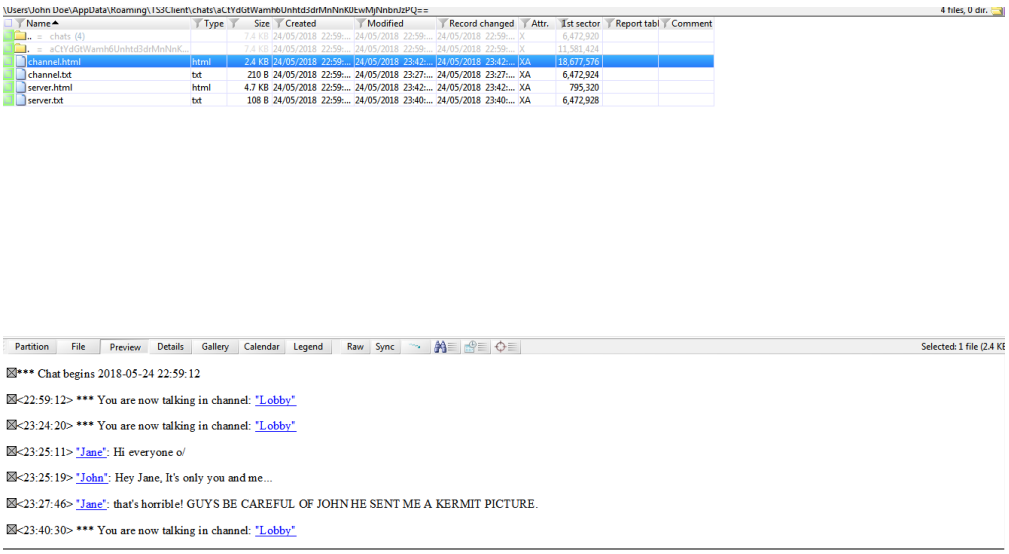


Figure F.31: Communication logs from the channel generated by the attacker's TeamSpeak3 client by default.

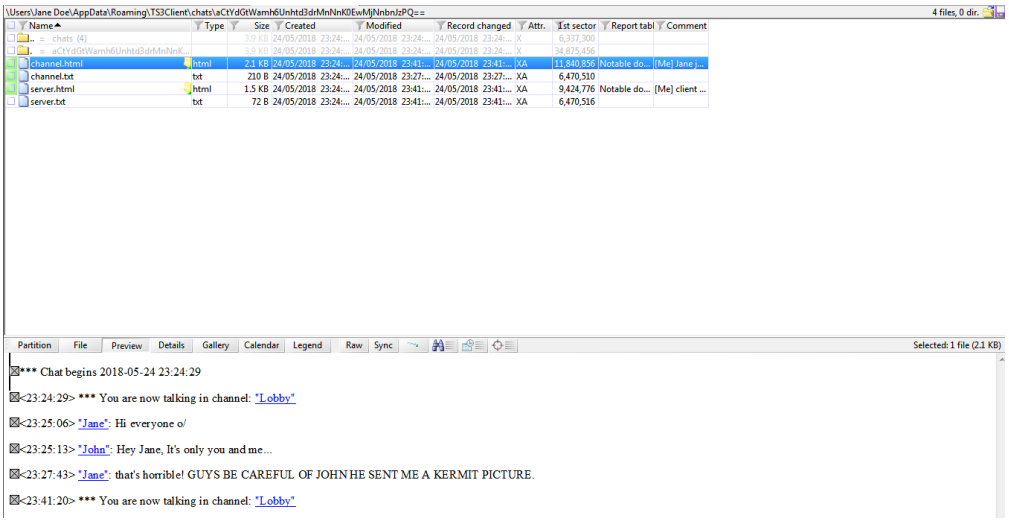


Figure F.32: Channel.html taken from the TeamSpeak3 Victim image.

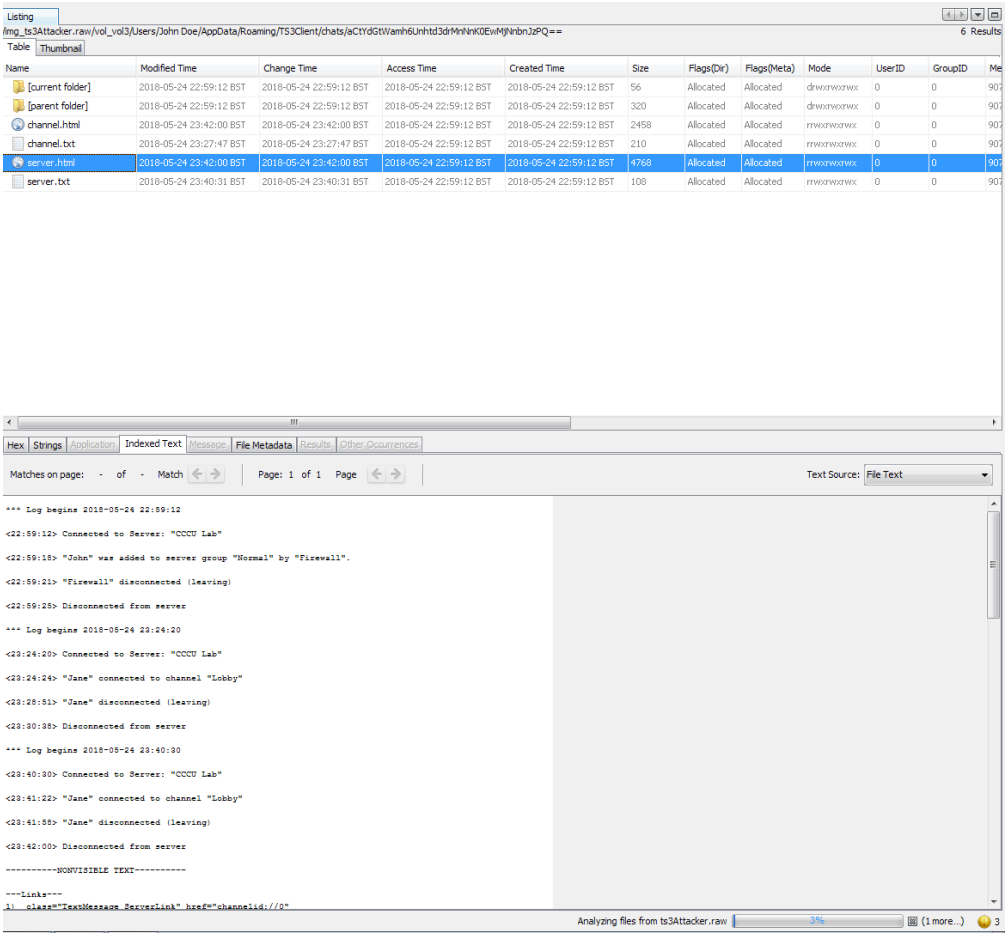


Figure F.33: Attacker Virtual Machine server.html file viewed in X-Ways Forensic Investigator.

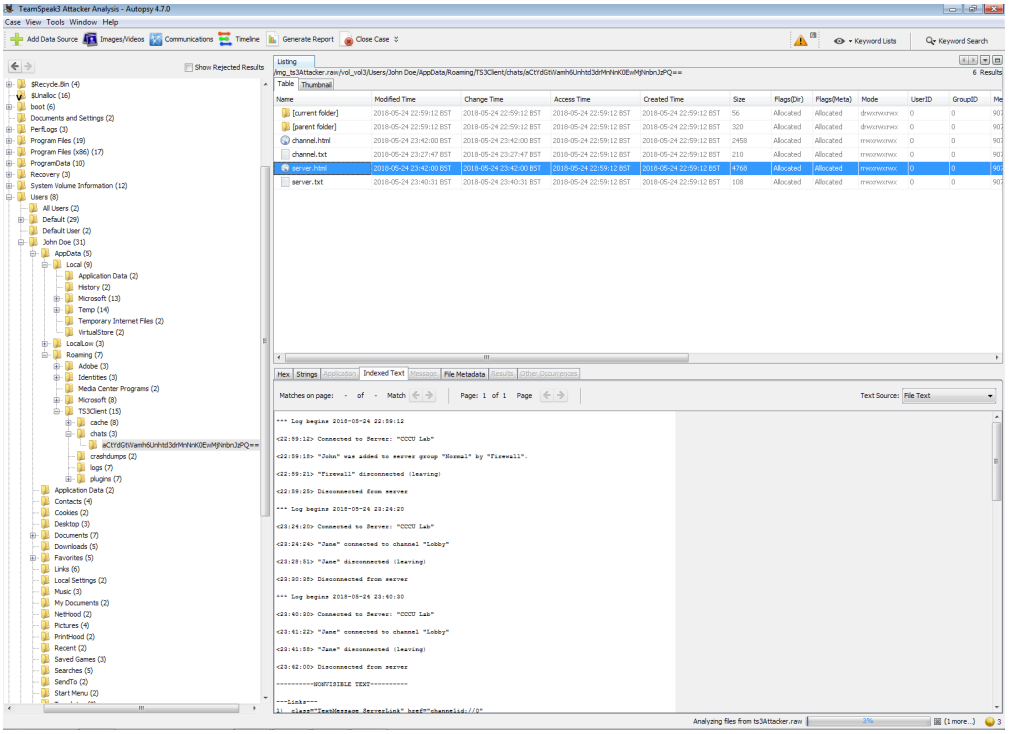


Figure F.34: Attacker Virtual Machine server.html file viewed in Autopsy.

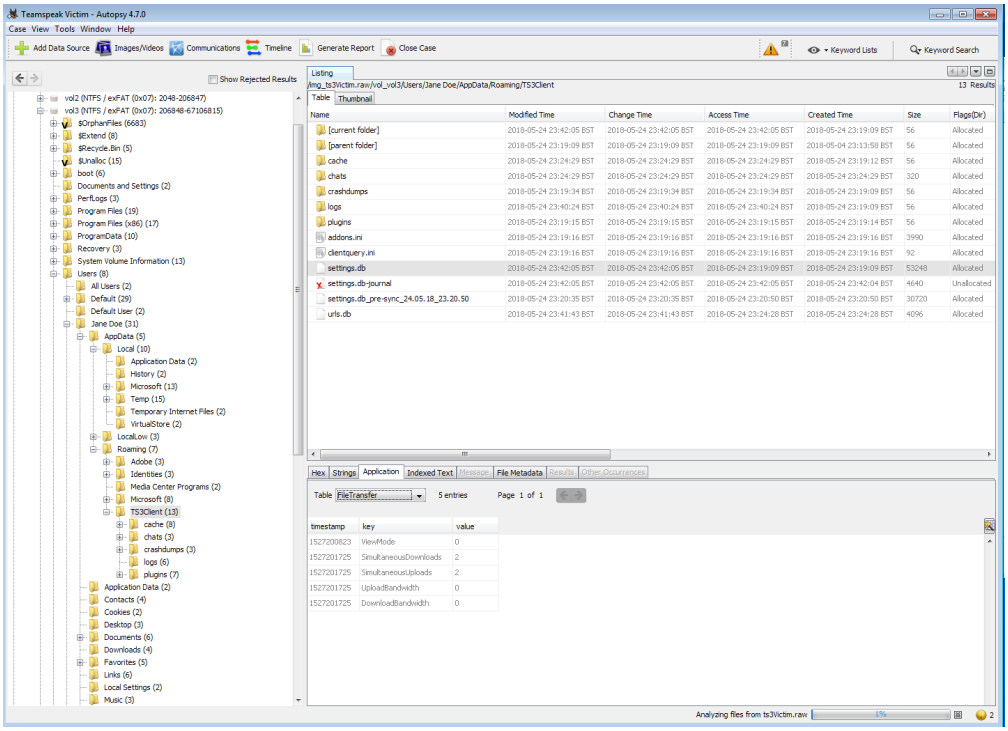


Figure F.35: Victim Virtual Machine settings.db shows 2 uploads and 2 downloads have occured on the client.

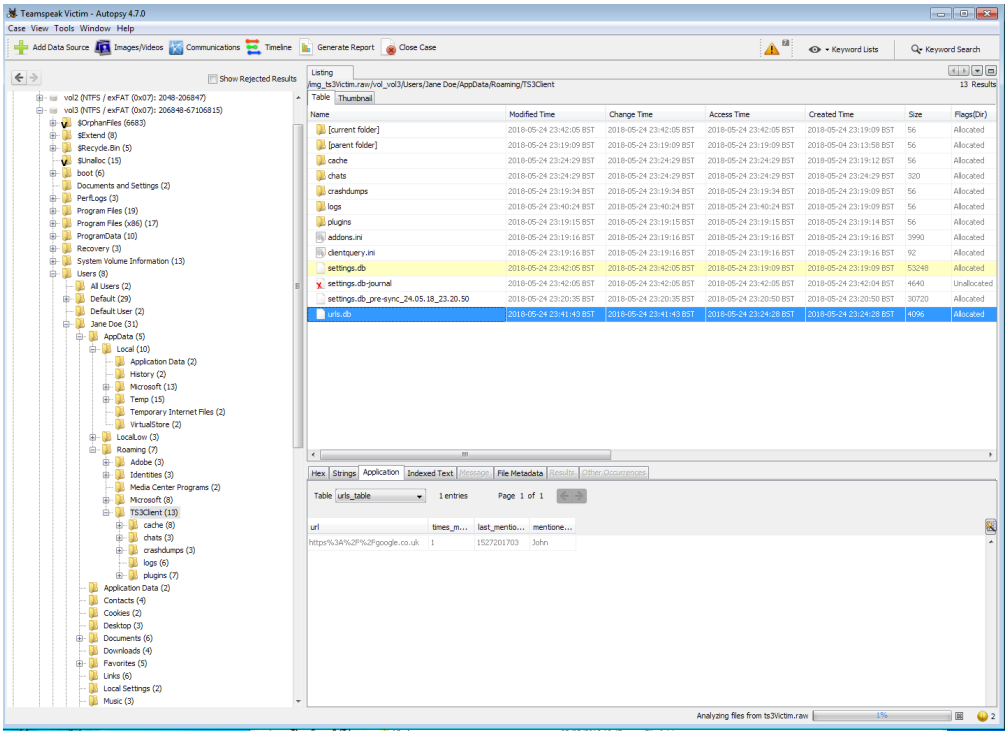


Figure F.36: Victim Virtual Machine urls.db shows a link shared with the Victim client from the Attacker client.

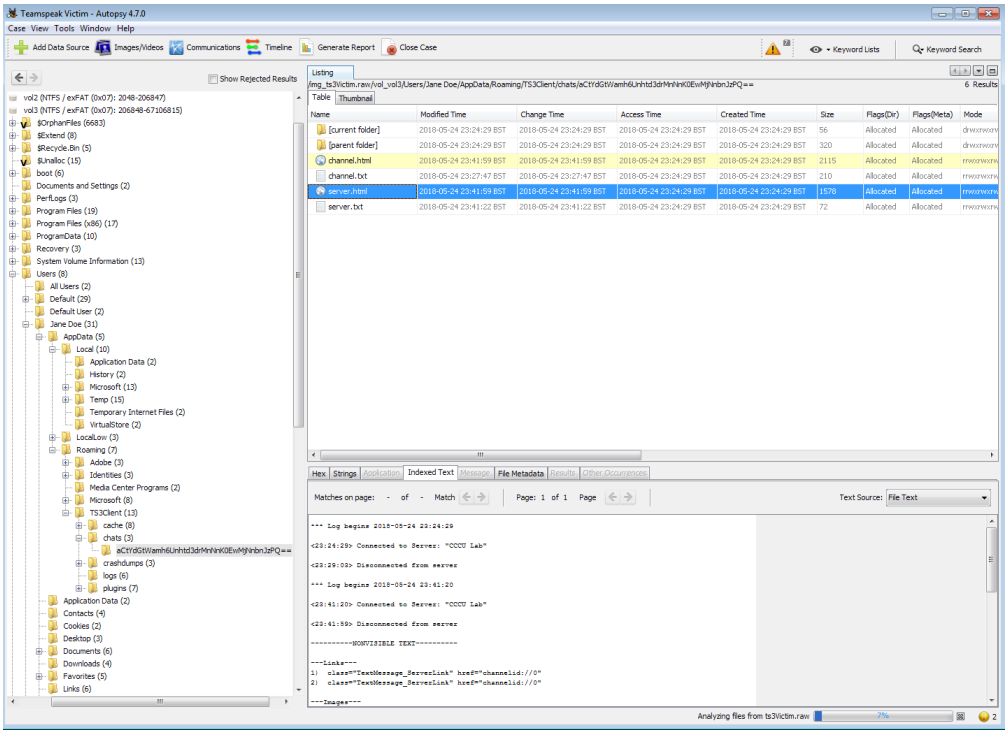


Figure F.37: Server.html on the victim client shows the client connected after the Attacker client and left after the image was sent.

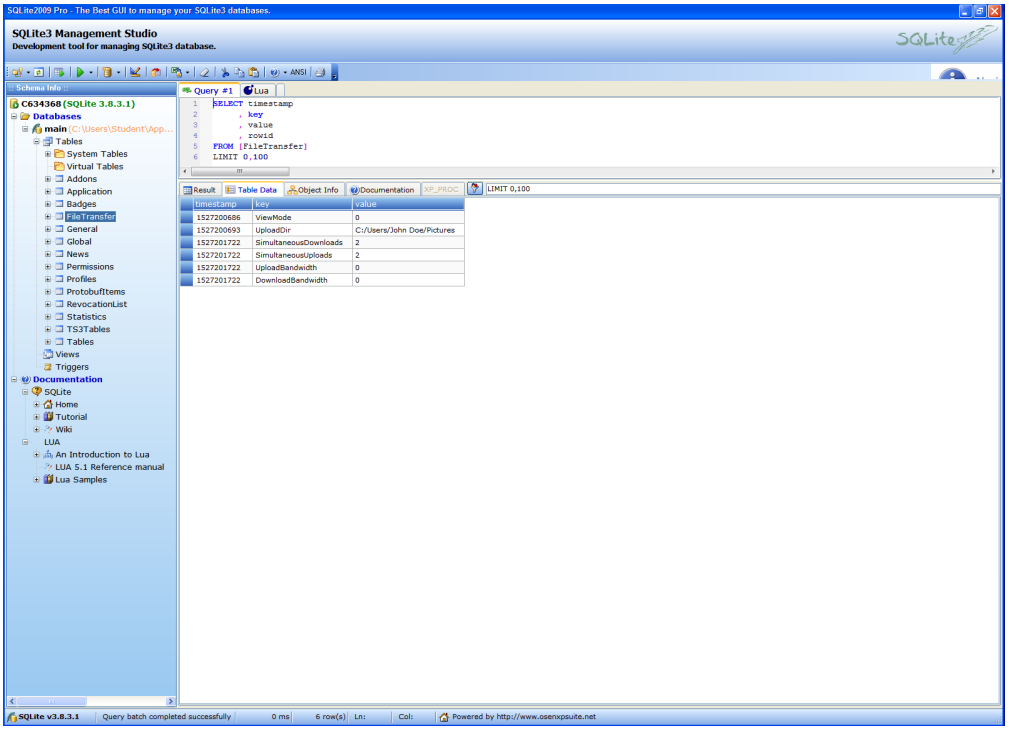


Figure F.38: SQLite2009 Pro overview of the Settings.db file.

	timestamp	key	value
	1527200686	ViewMode	0
	1527200693	UploadDir	C:/Users/John Doe/Pictures
	1527201722	SimultaneousDownloads	2
	1527201722	SimultaneousUploads	2
	1527201722	UploadBandwidth	0
	1527201722	DownloadBandwidth	0

Figure F.39: Closeup view of the FileTable view of Settings.db file which includes the Upload directory used by the attacker to transmit the Kermit.jpg file.

	timestamp	key	value
	1527200823	ViewMode	0
	1527201725	SimultaneousDownloads	2
	1527201725	SimultaneousUploads	2
	1527201725	UploadBandwidth	0
	1527201725	DownloadBandwidth	0

Figure F.40: Closeup view of the FileTable view of Settings.db file taken from the Victim machine.

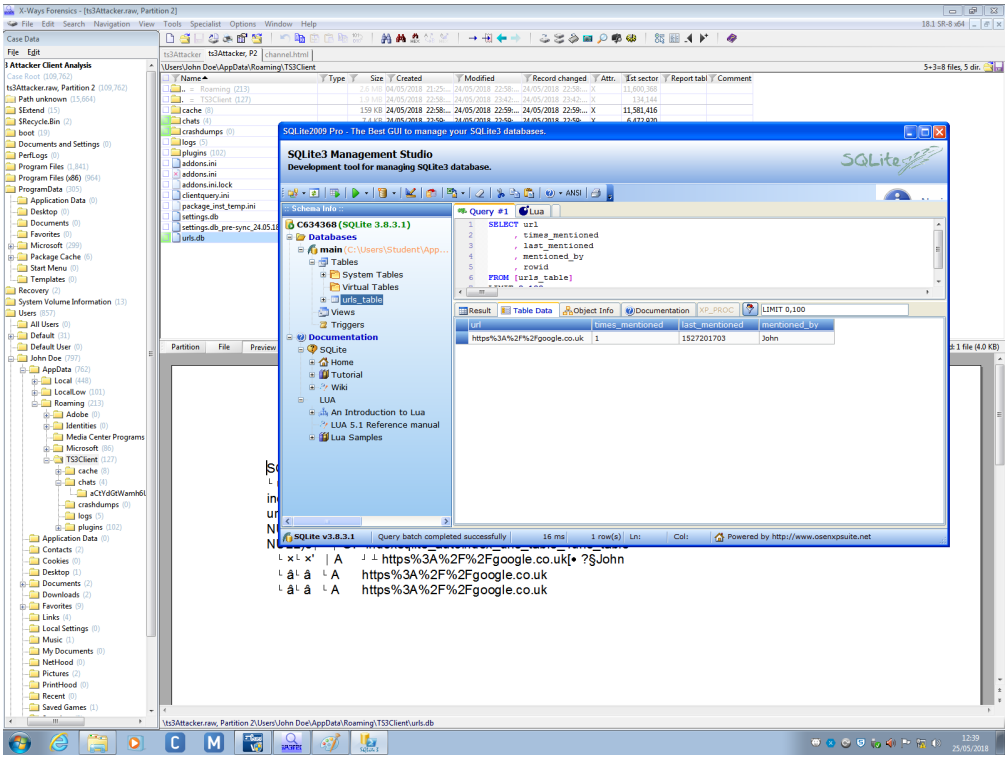


Figure F.41: URLs.db file found on attacker machine included url: google.co.uk from John to another user.

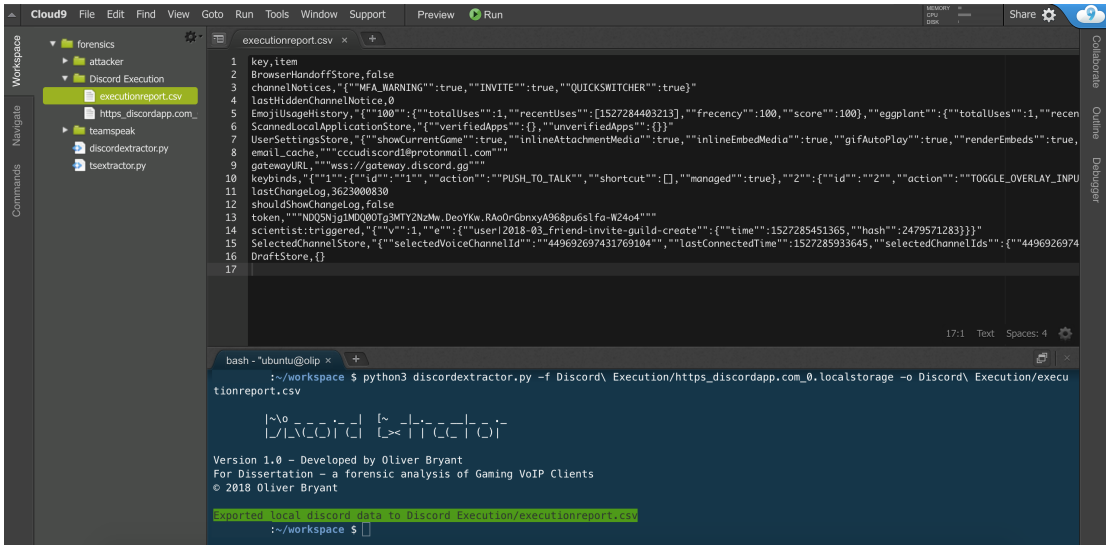


Figure F.42: Discord Extractor exporting data from Execution Client

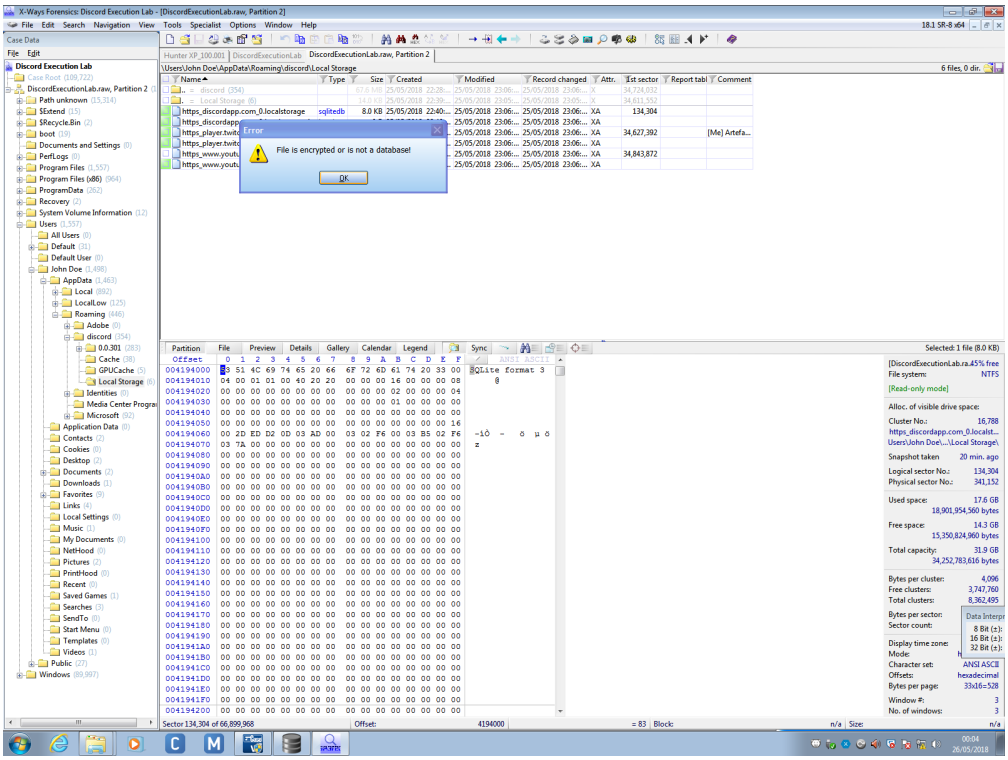


Figure F.43: SQLite2009 Pro Enterprise Manager is unable to open https_discordapp.com_0.localstorage and other .localstorage files.

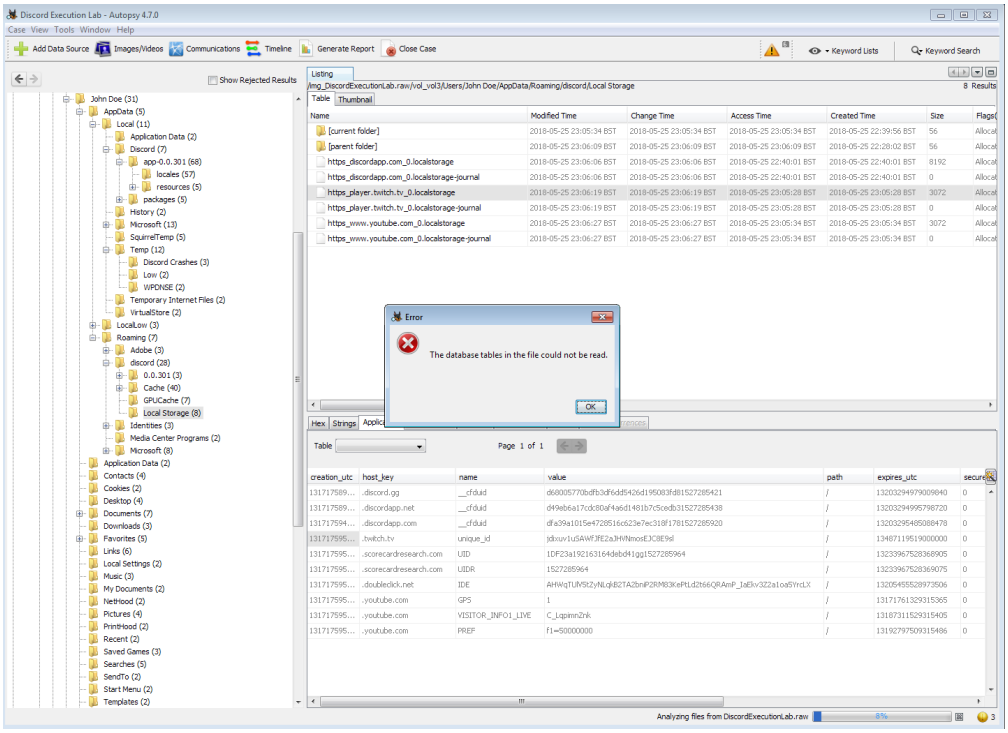


Figure F.44: Autopsy is unable to open the .localstorage files.

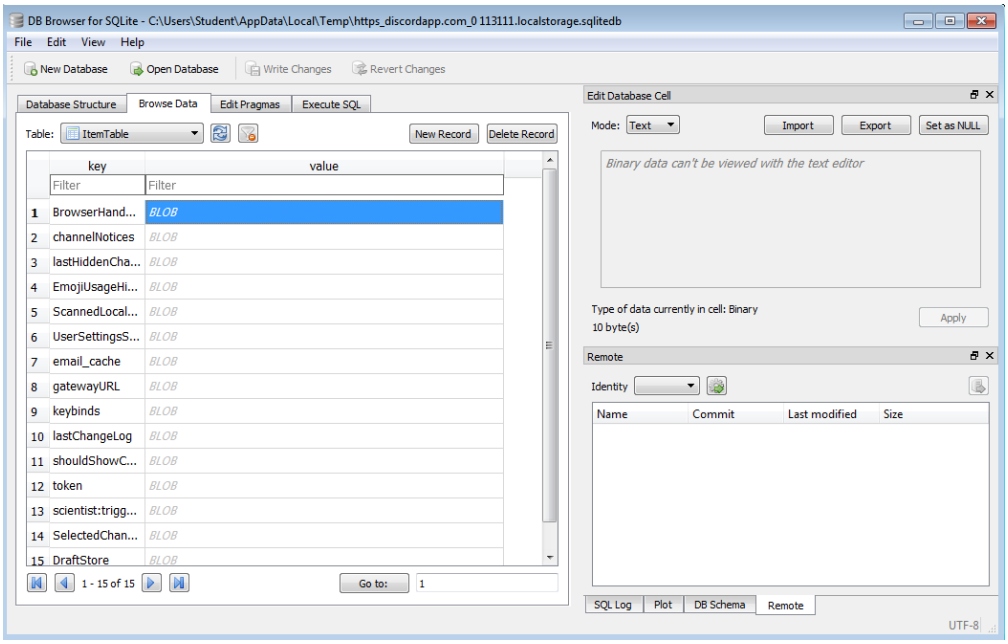


Figure F.45: DB Browser for SQLite provides no text display of content for LocalStorage and instead provides the data in the Hex view only

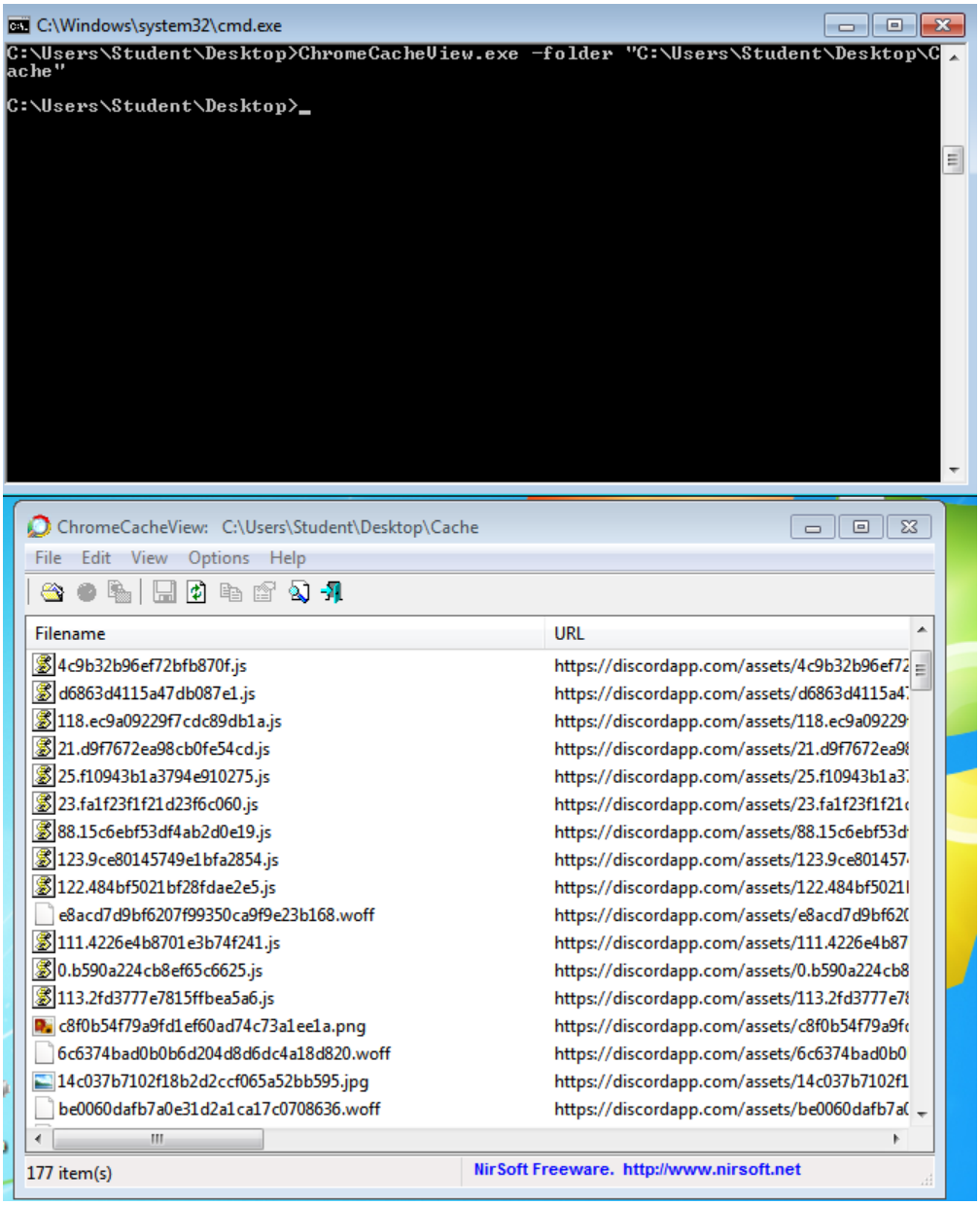


Figure F.46: Chrome Cache Viewer launched from the command line pointing at the cache exported from Discord.

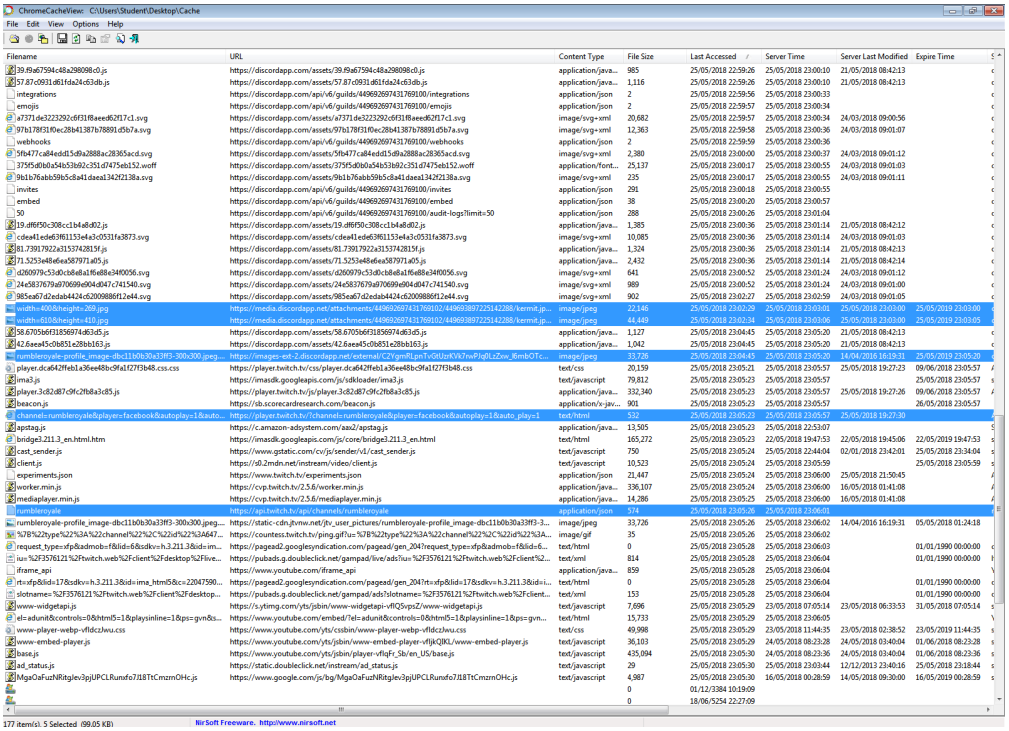


Figure F.47: Location of Kermit.jpg image that was uploaded to the server channel is stored locally on the cache as well as API calls to Twitch.tv to the channel royal rumble which was viewed at the time of analysis in the client.

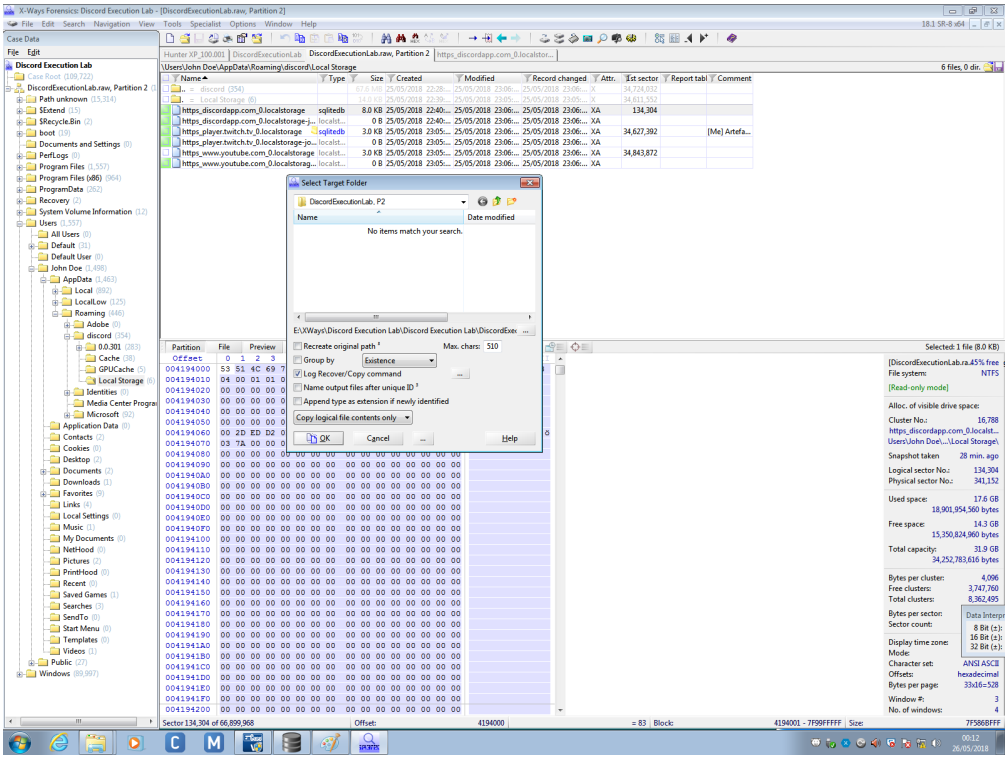


Figure F.48: Exporting the https_discordapp.com_0.localstorage locally for analysis

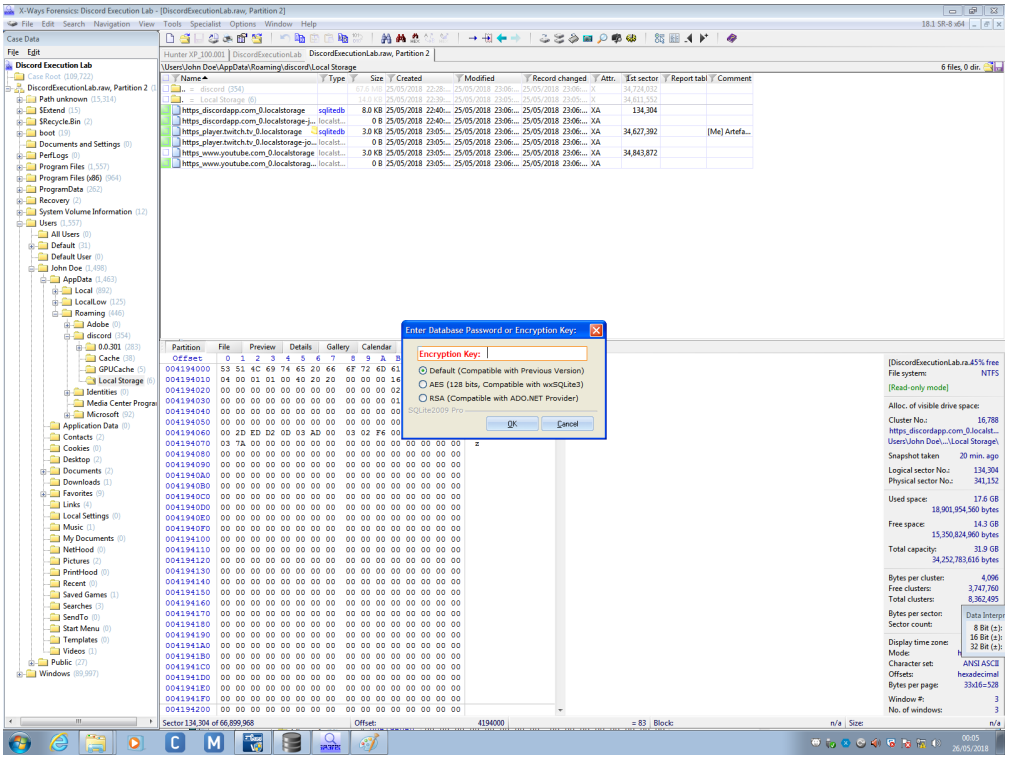


Figure F.49: SQLite2009 Pro Enterprise Manager asks for password on https_discordapp.com_0.localstorage file.

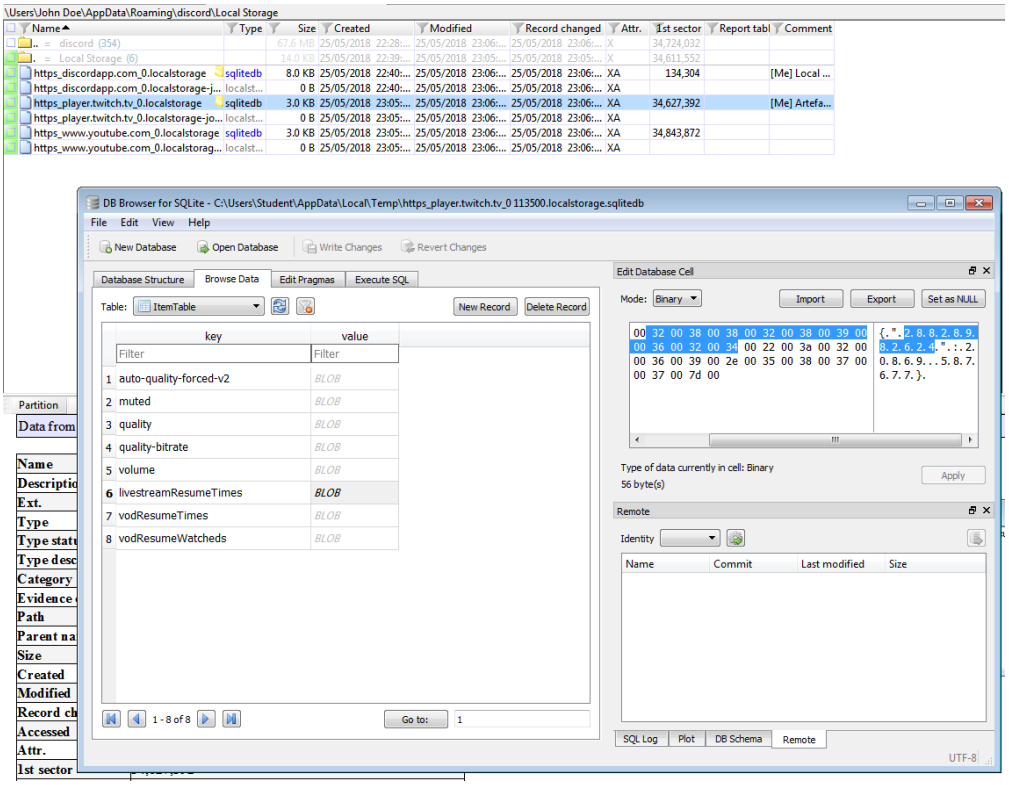


Figure F.50: The resume times for plays on a livestream stored in the twitch.tv localstorage file.

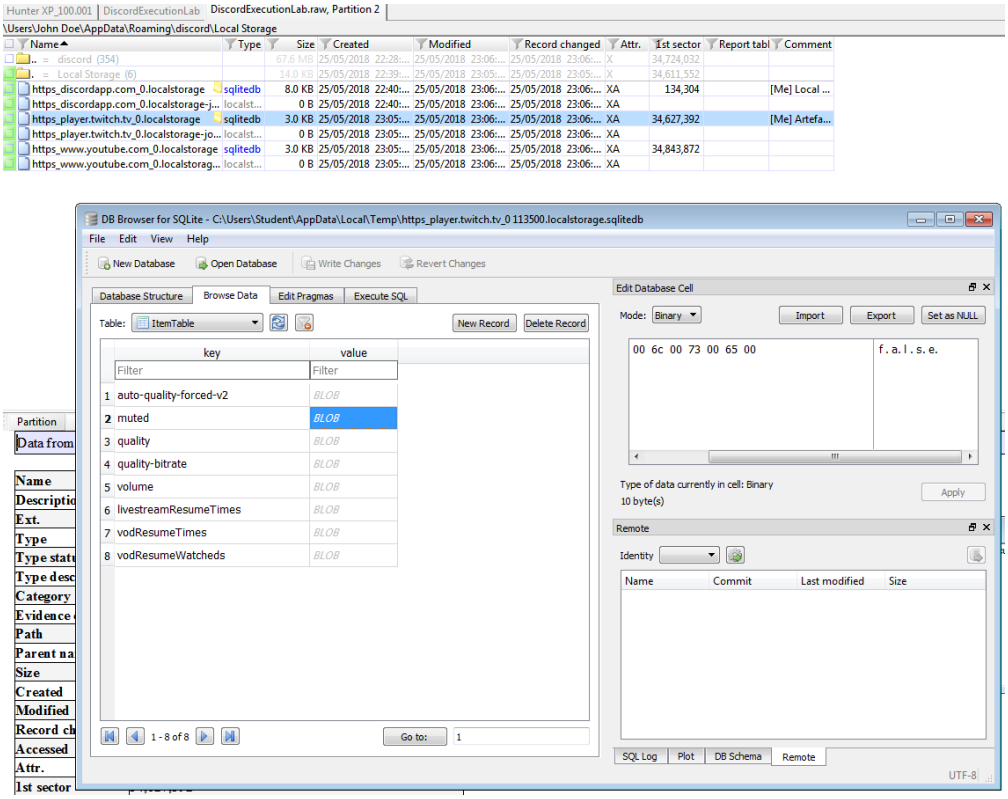


Figure F.51: Mute activation from within the twitch.tv localstorage file.

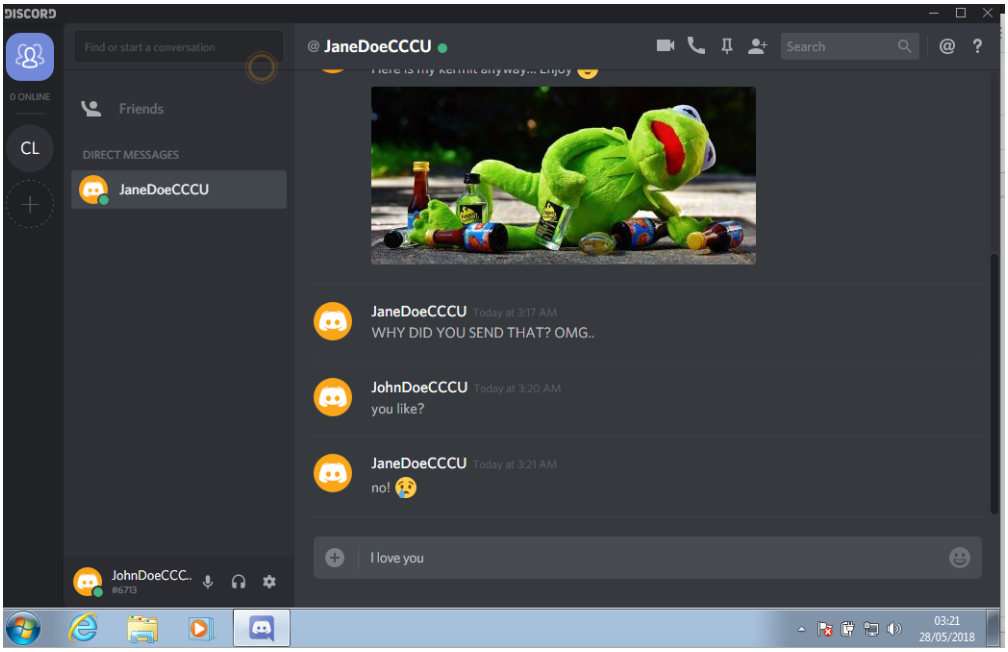


Figure F.52: The simulated conversation taking place on Discord between John and Jane.

```
0000 7b 00 22 00 34 00 35 00 30 00 34 00 38 00 32 00  {.".4.5.0.4.8.2.
0010 32 00 38 00 33 00 30 00 39 00 39 00 34 00 35 00  2.8.3.0.9.9.4.5.
0020 35 00 34 00 39 00 30 00 22 00 3a 00 7b 00 22 00  5.4.9.0.".:.{.".
0030 74 00 69 00 6d 00 65 00 73 00 74 00 61 00 6d 00  t.i.m.e.s.t.a.m.
0040 70 00 22 00 3a 00 31 00 35 00 32 00 37 00 34 00  p.".:.1.5.2.7.4.
0050 37 00 34 00 30 00 36 00 35 00 31 00 30 00 36 00  7.4.0.6.5.1.0.6.
0060 2c 00 22 00 64 00 72 00 61 00 66 00 74 00 22 00  ,.".d.r.a.f.t.".
0070 3a 00 22 00 49 00 20 00 6c 00 6f 00 76 00 65 00  :.".I. .l.o.v.e.
0080 20 00 79 00 6f 00 75 00 22 00 7d 00 7d 00         .y.o.u.".}.}.
```

Figure F.53: draft message found in the https_discordapp.com_0.localstorage database.

```
import os, sys, time, apsw, csv
import argparse
#print(apsw.sqlitelibversion())
motd = '''
         |~\o _ _ _ ._ _|   [~  _|_._ _ __|_ _ ._
         |_/|_\(_(_)| (_|   [_>< | | (_(_ | (_)|
        '''
print(motd)
print("Version 1.0 - Developed by Oliver Bryant")
```

```
print("For Dissertation - a forensic analysis of Gaming VoIP Clients")
print("© 2018 Oliver Bryant")
print(" ")
parser = argparse.ArgumentParser()
parser.add_argument("--file", "-f", type=str, required=True, help="Specify your .localstorage file. typically located at AppData\Roaming\discord\Local Storage")
parser.add_argument("--output", "-o", type=str, required=False, help="Specify output file eg: -o /directory/file.csv")
args = parser.parse_args()
key = []
item = []
argdis = False
try:
    connection=apsw.Connection(args.file)
except:
    print('\x1b[1;31m'+'ERROR! Unable to open SQL file '+ args.file +'are you specifying the correct http_discordapp.com_0.localstorage file?' + '\x1b[0m')
    print('Press ENTER to terminate the application.')
    input()
    exit()

cursor=connection.cursor()

try:
    for row in cursor.execute("SELECT * FROM ItemTable"):
        cItem = row[0]
        key.append(cItem)
        tItem = row[1].decode('utf-16')
        item.append(tItem)
except:
    print('\x1b[1;31m'+'ERROR! The input file specified is invaild '+ args.file +'are you specifying the correct http_discordapp.com_0.localstorage file?' + '\x1b[0m')
    print('Press ENTER to terminate the application.')
    input()
    exit()
```

```
41
42  try:
43      if args.output is None:
44          f = open("report.csv", 'w')
45      else:
46          f = open(args.output, 'w')
47          argdis = True
48  except:
49      print('\x1b[1;31m'+'ERROR! Unable to open' + args.output + 'are
        ↪ you specifying the correct path?' + '\x1b[0m')
50      print('\x1b[1;31m'+'Be sure to specify the ABSOLUTE path. You
        ↪ can use PWD on linux to find the Absolute Path' + '\x1b[0m')
51      print('\x1b[1;31m'+'Here\'s an example of a pathway searchcli.py
        ↪ -f file.localstorage -o
        ↪ /home/ubuntu/workspace/test/file.csv'+ '\x1b[0m')
52      print('Press ENTER to terminate the application.')
53      input()
54      exit()
55
56
57
58  with f:
59      fnames = ['key', 'item']
60      writer = csv.writer(f)
61      writer = csv.DictWriter(f, fieldnames=fnames)
62      writer.writeheader()
63      maxNum = len(key) # Get the MAX number of Keys.
64      counter = 0
65      while counter < maxNum:
66          writer.writerow({'key':key[counter],'item':item[counter]})
67          counter = counter + 1
68
69  f.close()
70  if argdis == True:
71      print('\x1b[6;30;42m' + 'Exported local discord data to ' +
        ↪ args.output + '\x1b[0m')
72  else:
73      print('\x1b[6;30;42m' + 'Exported local discord data to ' +
        ↪ 'report.csv' + '\x1b[0m')
```

Source Code F.1: https_discordapp.com_0.localstorage Discord Extractor written in Python.

```
import os, sys, time, apsw, csv
import urllib.parse
import argparse
#print(apsw.sqlitelibversion())
motd = '''
       |_   _|__ __ _ _ __ / __|_ __  ___ __ _| |_|__ / | __|_ _| |_ _ _ __ _ __| |_ ___ _ _
         | |/ -_) _` | '  \\__ \ '_ \/ -_) _` | / /|_ \ | _|\ \ /  _| '_/ _` / _|  _/ _ \ '_|
         |_|\___\__,_|_|_|_|___/ .__/\___\__,_|_\_\___/ |___/_\_\\__|_|  \__,_\__|\__\___/_|
                               |_|
       '''
print(motd)
print("Version 1.0 - Developed by Oliver Bryant")
print("For Dissertation - a forensic analysis of Gaming VoIP Clients")
print(" ")
parser = argparse.ArgumentParser()
parser.add_argument("--urls", "-u", type=str, required=False, help="Specify your urls.db file.
  ↪  found in /TS3Client/urls.db")
parser.add_argument("--settings", "-s", type=str, required=False, help="Specify your settings.db
  ↪  found in /TS3Client/settings.db")
parser.add_argument("--output", "-o", type=str, required=False, help="Specify output file eg: -o
  ↪  /directory/file.csv")
args = parser.parse_args()
url = [] # urls.db
timeMentioned = []
lastMentioned = []
mentionedBy = []
timeStamp = [] # settings.db
key = []
value = []
argdis = False

def executesqlsettings():
    argdis = False
    try:
        connection=apsw.Connection(args.settings)
    except:
        exit()
    cursor=connection.cursor()
    try:
        for row in cursor.execute("SELECT * FROM FileTransfer"):
            timeStamp.append(row[0])
            key.append(row[1])
            value.append(row[2])
        try:
            if args.output is None:
                f = open("settingsreport.csv", 'w')
            else:
                f = open(args.output, 'w')
                argdis = True
            with f:
                fnames = ['timestamp', 'key', 'value']
                writer = csv.writer(f)
                writer = csv.DictWriter(f, fieldnames=fnames)
                writer.writeheader()
                maxNum = len(timeStamp)
```

```
                counter = 0
                while counter < maxNum:
                    writer.writerow({'timestamp':timeStamp[counter],'key':key[counter],
                    'value':value[counter]})
                    counter = counter + 1
            f.close()
            if argdis == True:
                print('\x1b[6;30;42m' + 'Exported local TS3 Settings data to ' + args.output +
                  ↪  '\x1b[0m')
            else:
                print('\x1b[6;30;42m' + 'Exported local TS3 Settings data to ' +
                  ↪  'settingsreport.csv' + '\x1b[0m')
        except:
            print('\x1b[1;31m'+'ERROR! Unable to open' + args.output + 'are you specifying the
              ↪  correct path?' + '\x1b[0m')
            print('\x1b[1;31m'+'Be sure to specify the ABSOLUTE path. You can use PWD on linux to
              ↪  find the Absolute Path' + '\x1b[0m')
            print('\x1b[1;31m'+'Here\'s an example of a pathway searchcli.py -f file.localstorage
              ↪  -o /home/ubuntu/workspace/test/file.csv'+ '\x1b[0m')
            print('Press ENTER to terminate the application.')
            input()
            exit()
    except:
        print('\x1b[1;31m'+'ERROR! Unable to open SQL file '+ args.urls +'are you specifying the
          ↪  correct urls.db/settings.db file?' + '\x1b[0m')
        print('Press ENTER to terminate the application.')
        input()
        exit()


def executesqlurls():
    argdis = False
    try:
        connection=apsw.Connection(args.urls)
    except:
        exit()
    cursor=connection.cursor()
    try:
        for row in cursor.execute("SELECT * FROM urls_table"):
            tUrl = row[0]
            nUrl = urllib.parse.unquote(tUrl)
            url.append(nUrl)
            timeMentioned.append(row[1])
            lastMentioned.append(row[2])
            mentionedBy.append(row[3])
        try:
            if args.output is None:
                f = open("urlsreport.csv", 'w')
            else:
                f = open(args.output, 'w')
                argdis = True
            with f:
                fnames = ['url', 'time_mentioned', 'last_mentioned', 'mentioned_by']
                writer = csv.writer(f)
                writer = csv.DictWriter(f, fieldnames=fnames)
                writer.writeheader()
                maxNum = len(url)
                counter = 0
                while counter < maxNum:
```

```
                    writer.writerow({'url':url[counter],'time_mentioned':timeMentioned[counter],
                    'last_mentioned':lastMentioned[counter],
                      ↪  'mentioned_by':mentionedBy[counter]})
                    counter = counter + 1
            f.close()
            if argdis == True:
                print('\x1b[6;30;42m' + 'Exported TS3 Urls data to ' + args.output + '\x1b[0m')
            else:
                print('\x1b[6;30;42m' + 'Exported TS3 Urls data to ' + 'urlsreport.csv' +
                  ↪  '\x1b[0m')
        except:
            print('\x1b[1;31m'+'ERROR! Unable to open' + args.output + 'are you specifying the
              ↪  correct path?' + '\x1b[0m')
            print('\x1b[1;31m'+'Be sure to specify the ABSOLUTE path. You can use PWD on linux to
              ↪  find the Absolute Path' + '\x1b[0m')
            print('\x1b[1;31m'+'Here\'s an example of a pathway searchcli.py -f file.localstorage
              ↪  -o /home/ubuntu/workspace/test/file.csv'+ '\x1b[0m')
            print('Press ENTER to terminate the application.')
            input()
            exit()
    except:
        print('\x1b[1;31m'+'ERROR! Unable to open SQL file '+ args.urls +'are you specifying the
          ↪  correct http_discordapp.com_0.localstorage file?' + '\x1b[0m')
        print('Press ENTER to terminate the application.')
        input()
        exit()


if args.urls != None:
    executesqlurls()
if args.settings != None:
    executesqlsettings()
```

Source Code F.2: urls.db and settings.db (FileTransfer Data) TeamSpeak3 Extractor written in Python.

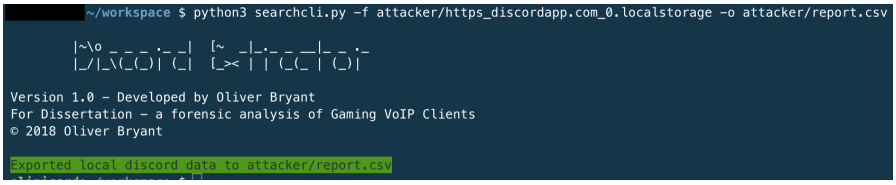


Figure F.54: Discord Extractor used on forensics machine to extract data from John Smith's machine (Attacker) to .csv.

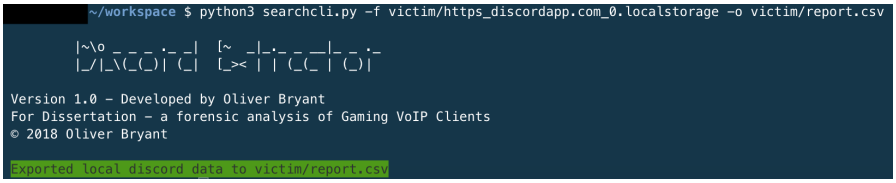


Figure F.55: Discord Extractor used on forensics machine to extract data from Jane Doe's machine (Victim) to .csv.

```
key,item
BrowserHandoffStore,false
channelNotices,"{""MFA_WARNING"":true,""INVITE"":true,""QUICKSWITCHE
↪ R"":true}"
lastHiddenChannelNotice,0
EmojiUsageHistory,"{""100"":{""totalUses"":1,""recentUses"":[1527284
↪ 403213],""frecency"":100,""score"":100},""eggplant"":{""totalUse
↪ s"":1,""recentUses"":[1527284403213],""frecency"":100,""score"":
↪ 100},""fork_and_knife"":{""totalUses"":1,""recentUses"":[1527284
↪ 403213],""frecency"":100,""score"":100},""yum"":{""totalUses"":1
↪ ,""recentUses"":[1527284403213],""frecency"":100,""score"":100},
↪ ""weary"":{""totalUses"":1,""recentUses"":[1527284403213],""frec
↪ ency"":100,""score"":100},""tired_face"":{""totalUses"":1,""rece
↪ ntUses"":[1527284403213],""frecency"":100,""score"":100},""poop"
↪ ":{""totalUses"":1,""recentUses"":[1527284403213],""frecency"":1
↪ 00,""score"":100},""ok_hand"":{""totalUses"":1,""recentUses"":[1
↪ 527284403213],""frecency"":100,""score"":100}}"
ScannedLocalApplicationStore,"{""verifiedApps"":{},""unverifiedApps"
↪ ":{}}"
UserSettingsStore,"{""showCurrentGame"":true,""inlineAttachmentMedia
↪ "":true,""inlineEmbedMedia"":true,""gifAutoPlay"":true,""renderE
↪ mbeds"":true,""renderReactions"":true,""animateEmoji"":true,""th
↪ eme"":""dark"",""enableTTSCommand"":true,""messageDisplayCompact
↪ "":false,""locale"":""en-US"",""convertEmoticons"":true,""restri
↪ ctedGuilds"":[],""friendSourceFlags"":{""all"":true},""developer
↪ Mode"":false,""guildPositions"":[],""detectPlatformAccounts"":tr
↪ ue,""status"":""online"",""explicitContentFilter"":1,""defaultGu
↪ ildsRestricted"":false,""afkTimeout"":600,""timezoneOffset"":-60
↪ }"
email_cache,"""cccudiscord1@protonmail.com"""
gatewayURL,"""wss://gateway.discord.gg"""
keybinds,"{""1"":{""id"":""1"",""action"":""PUSH_TO_TALK"",""shortcu
↪ t"":[],""managed"":true},""2"":{""id"":""2"",""action"":""TOGGLE
↪ _OVERLAY_INPUT_LOCK"",""shortcut"":[[0,160],[0,192]],""managed""
↪ :true}}"
lastChangeLog,3623000830
shouldShowChangeLog,false
```

```
13 token,"""NDQ5Njg1MDQ0OTg3MTY2NzMw.DeoYKw.RAoOrGbnxyA968pu6slfa-W24o4
    ↪ """
14 scientist:triggered,"{""v"":1,""e"":{""user|2018-03_friend-invite-gu
    ↪ ild-create"":{""time"":1527285451365,""hash"":2479571283}}}"
15 SelectedChannelStore,"{""selectedVoiceChannelId"":""4496926974317691
    ↪ 04"",""lastConnectedTime"":1527285933645,""selectedChannelIds"":
    ↪ {""449692697431769100"":""449692697431769102""}}"
16 DraftStore,{}
```

Source Code F.3: Data extracted during the Discord Execution Lab from https_discordapp.com_0.localstorage.

```
key,item
BrowserHandoffStore,false
lastHiddenChannelNotice,0
email_cache,"""discordtester5@gmail.com"""
keybinds,"{""1"":{""id"":""1"",
""action"":
""PUSH_TO_TALK"",
""shortcut"":[],
""managed"":true},""2"":{""id"":""2"",
""action"":""TOGGLE_OVERLAY_INPUT_LOCK"",
""shortcut"":[[0,160],[0,192]],
""managed"":true}}"
token,"""NDR4NTIwMTk0NzIyMjk5OTA0.DXizFQ.b3h7ebc__x4SSnQrTl5DwQLIu_I
 ↪ """
hideConnectFacebook,true
audio,"{""permission"":true,
""mode"":""VOICE_ACTIVITY"",
""modeOptions"":
{""threshold"":-40,
""autoThreshold"":false,
""vadLeading"":5,
""vadTrailing"":25,
""delay"":20,
""shortcut"":[]},
""mute"":false,
""deaf"":true,
""echoCancellation"":true,
""noiseSuppression"":true,
""automaticGainControl"":true,
""silenceWarning"":true,
""attenuation"":0,
""attenuateWhileSpeakingSelf"":false,
""attenuateWhileSpeakingOthers"":true,
""localMutes"":{},""localVolumes"":{},""localPans"":{},
""inputVolume"":100,
""outputVolume"":100,
""inputDeviceId"":""default""
,""outputDeviceId"":""default"",
```

```
38 ""videoDeviceId"":""default"",
39 ""qos"":true,
40 ""soundshareVolume"":20,
41 ""soundshareDucking"":80}"
42 SelectedChannelStore,"{""selectedVoiceChannelId"":null,
43 ""lastConnectedTime"":1519855890455,""selectedChannelIds"":{""418523
    ↪ 018696982530"":""418523019158224897"",""417719834231439 37"":""31
    ↪ 7332199374585856""}}"
44 DraftStore,{}
45 UserSettingsStore,
46 "{""showCurrentGame"":true,
47 ""inlineAttachmentMedia"":true,
48 ""inlineEmbedMedia"":true,
49 ""gifAutoPlay"":true,
50 ""renderEmbeds"":true,
51 ""renderReactions"":true,
52 ""animateEmoji"":true,
53 ""theme"":""dark"",
54 ""enableTTSCommand"":true,
55 ""messageDisplayCompact"":false,
56 ""locale"":""enGB"",
57 ""convertEmoticons"":true,
58 ""restrictedGuilds"":[],
59 ""friendSourceFlags"":{""all"":true},
60 ""developerMode"":false,""guildPositions"":[],
61 ""detectPlatformAccounts"":true,
62 ""status"":""online"",
63 ""explicitContentFilter"":1,
64 ""defaultGuildsRestricted"":false,
65 ""afkTimeout"":600,
66 ""timezoneOffset"":-60,""sync"":{}}"
67 channelNotices,"{""MFA_WARNING"":true,""INVITE"":true,""QUICKSWITCHE
    ↪ R"":true}"
68 scientist:triggered,"{""v"":1,""e"":{""undefined|undefined"":{""time
    ↪ "":1522702583403,""hash"":3085332118}}}"
69 gatewayURL,"""wss://gateway.discord.gg"""
70 EmojiUsageHistory,"{""100"":{""totalUses"":1,""recentUses"":[1519853
    ↪ 977004],""frecency"":30,
71 ""score"":30},""eggplant"":{""totalUses"":1,
```

```
72 ""recentUses"":[1519853977004],
73 ""frecency"":30,
74 ""score"":30},
75 ""fork_and_knife"":{""totalUses"":1,
76 ""recentUses"":[1519853977004],
77 ""frecency"":30,
78 ""score"":30},
79 ""yum"":{""totalUses"":1,
80 ""recentUses"":[1519853977004],
81 ""frecency"":30,
82 ""score"":30},
83 ""weary"":{""totalUses"":1,
84 ""recentUses"":[1519853977004],
85 ""frecency"":30,
86 ""score"":30},
87 ""tired_face"":{""totalUses"":1,
88 ""recentUses"":[1519853977004],
89 ""frecency"":30,
90 ""score"":30},
91 ""poop"":{""totalUses"":1,
92 ""recentUses"":[1519853977004],
93 ""frecency"":30,
94 ""score"":30},
95 ""ok_hand"":{""totalUses"":1,
96 ""recentUses"":[1519853977004],
97 ""frecency"":30,
98 ""score"":30},
99 ""gun"":{""totalUses"":3,
100 ""recentUses"":[1522699635602,1522699635603,1522699635603],""frecenc⌋
    ↪ y"":300,""score"":300}}"
101 lastChangeLog,58866272
102 shouldShowChangeLog,false
```

Source Code F.4: Example of the data extracted in CSV format using the Discord Extractor application in listing F.1

```
1 key,item
2 BrowserHandoffStore,false
3 channelNotices,"{""MFA_WARNING"":true,""INVITE"":true,""QUICKSWITCHE⌋
    ↪ R"":true}"
```

```
lastHiddenChannelNotice,0
email_cache,"""cccudiscordt2@protonmail.com"""
gatewayURL,"""wss://gateway.discord.gg"""
keybinds,"{""1"":{""id"":""1"",""action"":""PUSH_TO_TALK"",""shortcut"":[],""managed"":true},""2"":{""id"":""2"",""action"":""TOGGLE_OVERLAY_INPUT_LOCK"",""shortcut"":[[0,160],[0,192]],""managed"":true}}"
lastChangeLog,3623000830
shouldShowChangeLog,false
token,"""NDUwNDYxMDkyOTQ3MTY1MTg0.DezkFg.bU0_9Rpm6FsSXYcvpl050JWKGqs"""
ScannedLocalApplicationStore,"{""verifiedApps"":{},""unverifiedApps"":{}}"
scientist:triggered,"{""v"":1,""e"":{""user|2018-03_friend-invite-guild-create"":{""time"":1527468770662,""hash"":2479571283}}}"
UserSettingsStore,"{""showCurrentGame"":true,""inlineAttachmentMedia"":true,""inlineEmbedMedia"":true,""gifAutoPlay"":true,""renderEmbeds"":true,""renderReactions"":true,""animateEmoji"":true,""theme"":""dark"",""enableTTSCommand"":true,""messageDisplayCompact"":false,""locale"":""en-US"",""convertEmoticons"":true,""restrictedGuilds"":[],""friendSourceFlags"":{""all"":true},""developerMode"":false,""guildPositions"":[],""detectPlatformAccounts"":true,""status"":""online"",""explicitContentFilter"":1,""disableGamesTab"":false,""defaultGuildsRestricted"":false,""afkTimeout"":600,""timezoneOffset"":-60,""sync"":{}}"
hideConnectFacebook,true
```

```
15 EmojiUsageHistory,"{""100"":{""totalUses"":1,""recentUses"":[1527468
    ↪ 512298],""frecency"":100,""score"":100},""eggplant"":{""totalUse
    ↪ s"":1,""recentUses"":[1527468512298],""frecency"":100,""score"":
    ↪ 100},""fork_and_knife"":{""totalUses"":1,""recentUses"":[1527468
    ↪ 512298],""frecency"":100,""score"":100},""yum"":{""totalUses"":1
    ↪ ,""recentUses"":[1527468512298],""frecency"":100,""score"":100},
    ↪ ""weary"":{""totalUses"":1,""recentUses"":[1527468512298],""frec
    ↪ ency"":100,""score"":100},""tired_face"":{""totalUses"":1,""rece
    ↪ ntUses"":[1527468512298],""frecency"":100,""score"":100},""poop"
    ↪ ":{""totalUses"":1,""recentUses"":[1527468512298],""frecency"":1
    ↪ 00,""score"":100},""ok_hand"":{""totalUses"":1,""recentUses"":[1
    ↪ 527468512298],""frecency"":100,""score"":100},""wink"":{""totalU
    ↪ ses"":2,""recentUses"":[1527473507422,1527473710336],""frecency"
    ↪ ":200,""score"":200}}"
16 SelectedChannelStore,"{""selectedVoiceChannelId"":null,""lastConnect
    ↪ edTime"":1527470265960,""selectedChannelIds"":{""450461385437085
    ↪ 716"":""450461385437085719"",""null"":""450482283099455490""}}"
17 DraftStore,"{""450482283099455490"":{""timestamp"":1527474065106,""d
    ↪ raft"":""I love
    ↪ you""}}"
```

Source Code F.5: The https_discordapp.com_0.localstorage file extracted from Discord Attack Virtual Machine in the CSV format.

```
1 key,item
2 BrowserHandoffStore,false
3 channelNotices,"{""MFA_WARNING"":true,""INVITE"":true,""QUICKSWITCHE
    ↪ R"":true}"
4 lastHiddenChannelNotice,0
5 token,"""NDUwNDc2NTg5OTY5NDQwNzc4.DezyhQ.1gwWbPWO4VPGVGa9oWgl0K_XQag
    ↪ """
```

```
6  UserSettingsStore,"{""showCurrentGame"":true,""inlineAttachmentMedia
    ↪  "":true,""inlineEmbedMedia"":true,""gifAutoPlay"":true,""renderE
    ↪  mbeds"":true,""renderReactions"":true,""animateEmoji"":true,""th
    ↪  eme"":""dark"",""enableTTSCommand"":true,""messageDisplayCompact
    ↪  "":false,""locale"":""en-US"",""convertEmoticons"":true,""restri
    ↪  ctedGuilds"":[],""friendSourceFlags"":{""all"":true},""developer
    ↪  Mode"":false,""guildPositions"":[],""detectPlatformAccounts"":tr
    ↪  ue,""status"":""online"",""explicitContentFilter"":1,""disableGa
    ↪  mesTab"":false,""defaultGuildsRestricted"":false,""afkTimeout"":
    ↪  600,""timezoneOffset"":-60}"
7  email_cache,"""cccudiscordt3@protonmail.com"""
8  gatewayURL,"""wss://gateway.discord.gg"""
9  keybinds,"{""1"":{""id"":""1"",""action"":""PUSH_TO_TALK"",""shortcu
    ↪  t"":[],""managed"":true},""2"":{""id"":""2"",""action"":""TOGGLE
    ↪  _OVERLAY_INPUT_LOCK"",""shortcut"":[[0,160],[0,192]],""managed""
    ↪  :true}}"
10 lastChangeLog,3623000830
11 shouldShowChangeLog,false
12 ScannedLocalApplicationStore,"{""verifiedApps"":{},""unverifiedApps"
    ↪  ":{}}"
13 hideConnectFacebook,true
14 SelectedChannelStore,"{""selectedChannelIds"":{""450461385437085716"
    ↪  ":""450461385437085719"",""null"":""450482283099455490""}}"
15 DraftStore,{}
```

```
16 EmojiUsageHistory,"{""100"":{""totalUses"":1,""recentUses"":[1527472
   ↪ 022404],""frecency"":100,""score"":100},""eggplant"":{""totalUse
   ↪ s"":1,""recentUses"":[1527472022404],""frecency"":100,""score"":
   ↪ 100},""fork_and_knife"":{""totalUses"":1,""recentUses"":[1527472
   ↪ 022404],""frecency"":100,""score"":100},""yum"":{""totalUses"":1
   ↪ ,""recentUses"":[1527472022404],""frecency"":100,""score"":100},
   ↪ ""weary"":{""totalUses"":1,""recentUses"":[1527472022404],""frec
   ↪ ency"":100,""score"":100},""tired_face"":{""totalUses"":1,""rece
   ↪ ntUses"":[1527472022404],""frecency"":100,""score"":100},""poop"
   ↪ ":{""totalUses"":1,""recentUses"":[1527472022404],""frecency"":1
   ↪ 00,""score"":100},""ok_hand"":{""totalUses"":1,""recentUses"":[1
   ↪ 527472022404],""frecency"":100,""score"":100},""heart"":{""total
   ↪ Uses"":1,""recentUses"":[1527473525114],""frecency"":100,""score
   ↪ "":100},""frowning"":{""totalUses"":1,""recentUses"":[1527473700
   ↪ 837],""frecency"":100,""score"":100},""cry"":{""totalUses"":1,""
   ↪ recentUses"":[1527474026932],""frecency"":100,""score"":100}}"
```

Source Code F.6: The https_discordapp.com_0.localstorage file extracted from Discord Victim Virtual Machine in the CSV format.

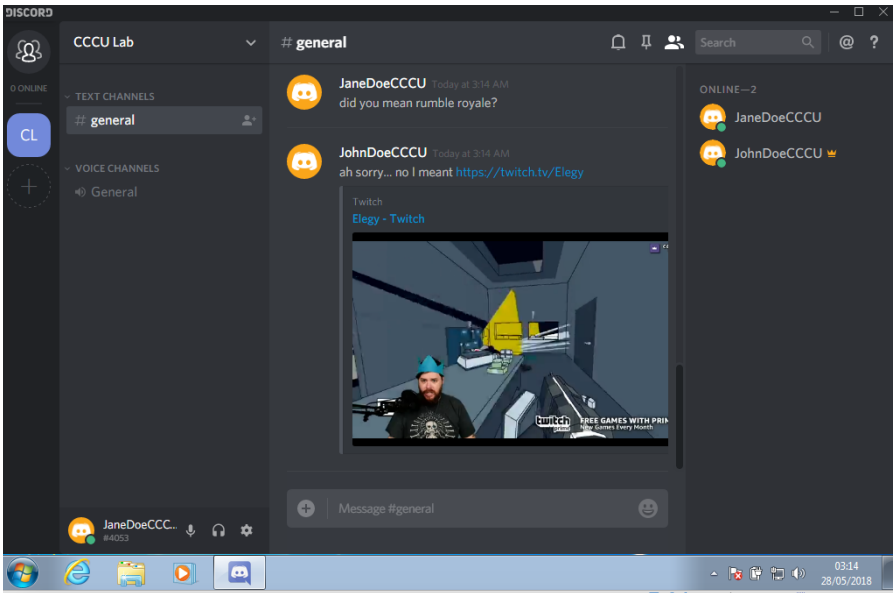


Figure F.56: Screenshot of Twitch.tv embedded player being used inside the Discord client.

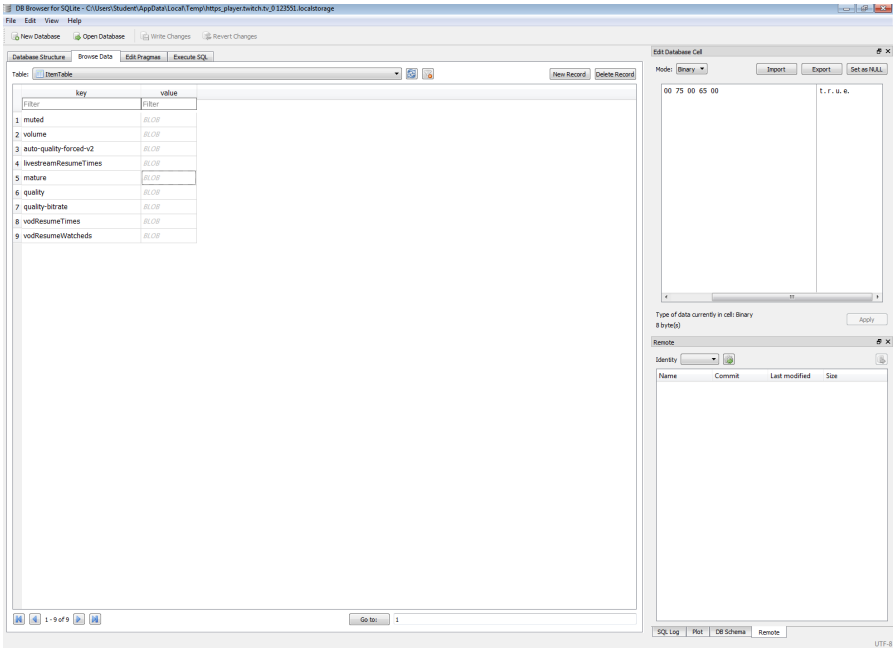


Figure F.57: Screenshot of the `Mature` table from https_player.twitch.tv_0.localstorage database.

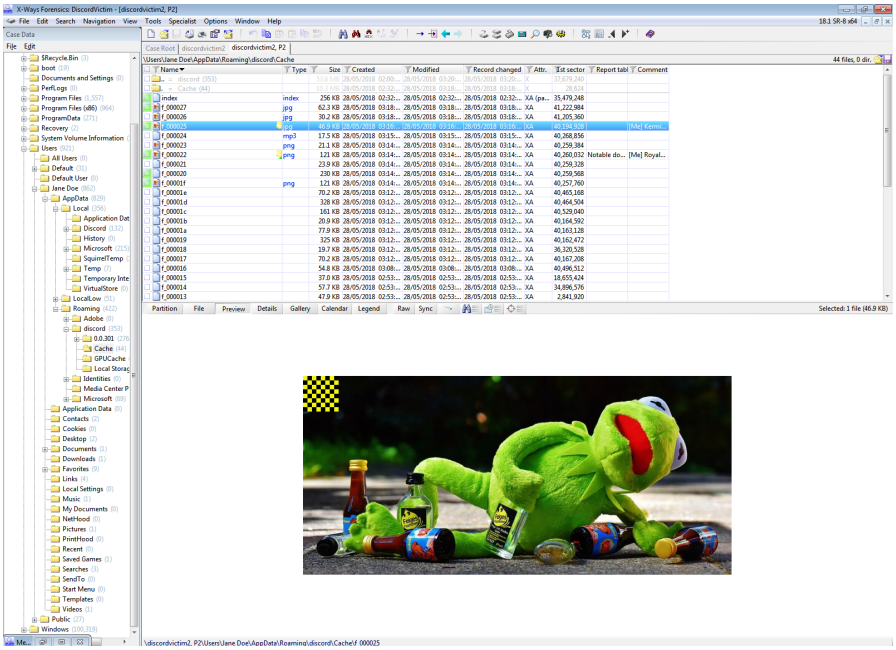


Figure F.58: Image sent from the attacker to the victim sorted in the Cache as artefact `f_000025`

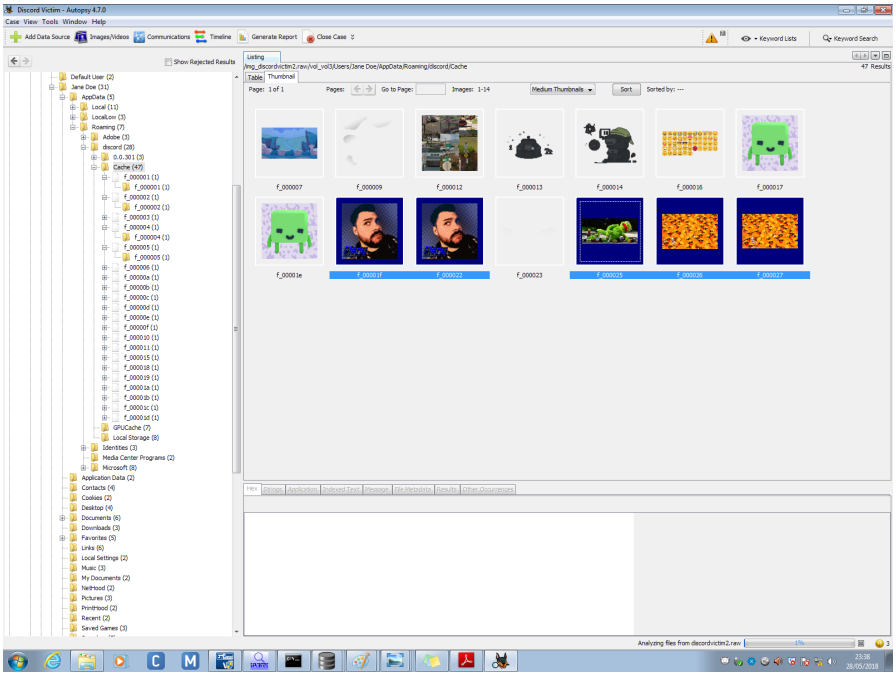


Figure F.59: Cache displayed in Autopsy

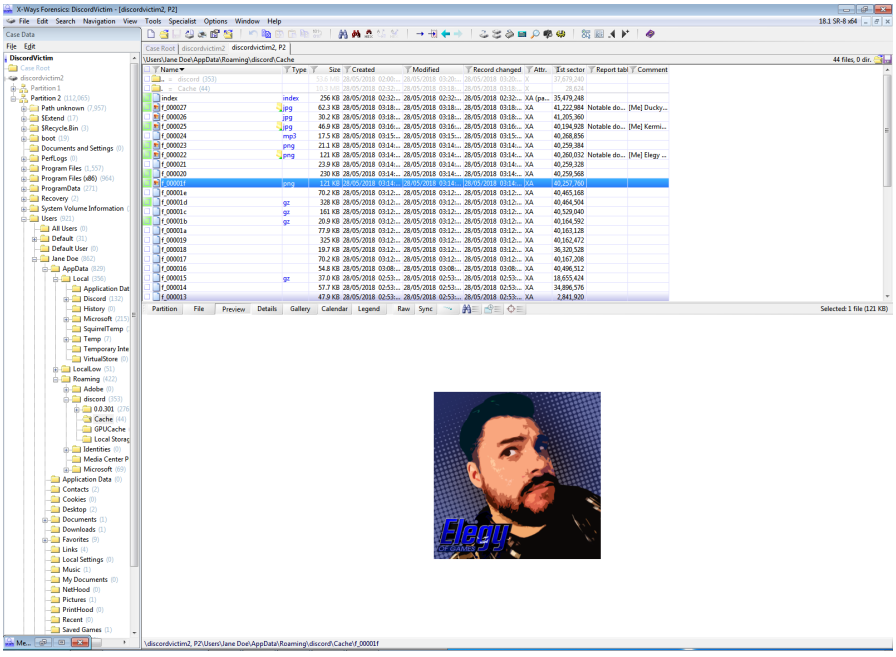


Figure F.60: Twitch.tv Artefact from the embedded player. The profile icon for Elegy found in the Cache as artefact `f_000022`

Figure F.61: a comparison and overview of https_discordapp.com_0.localstorage taken from the Attacker and Victim virtual machine.

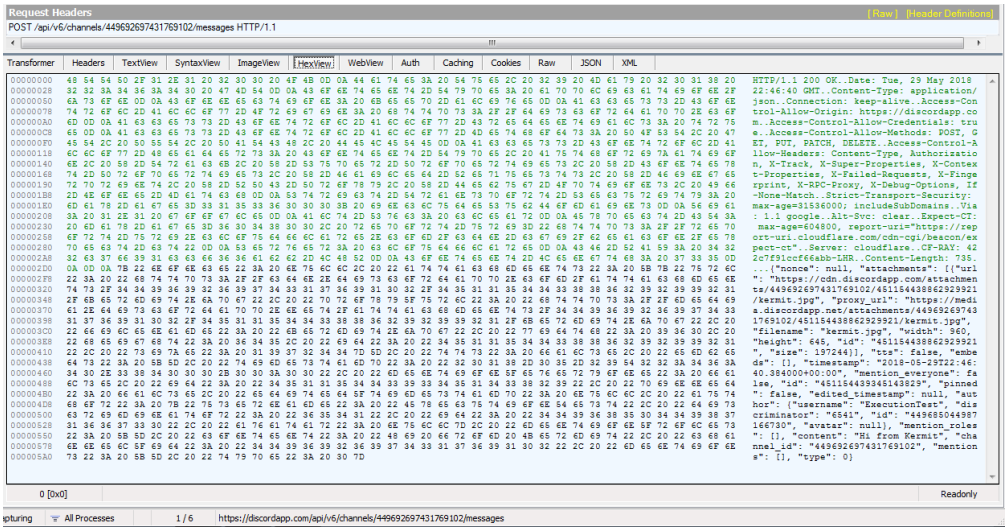


Figure F.62: The Upload process for Discord is encrypted with TLS 1.2. The encryption can be bypassed by Fiddler.

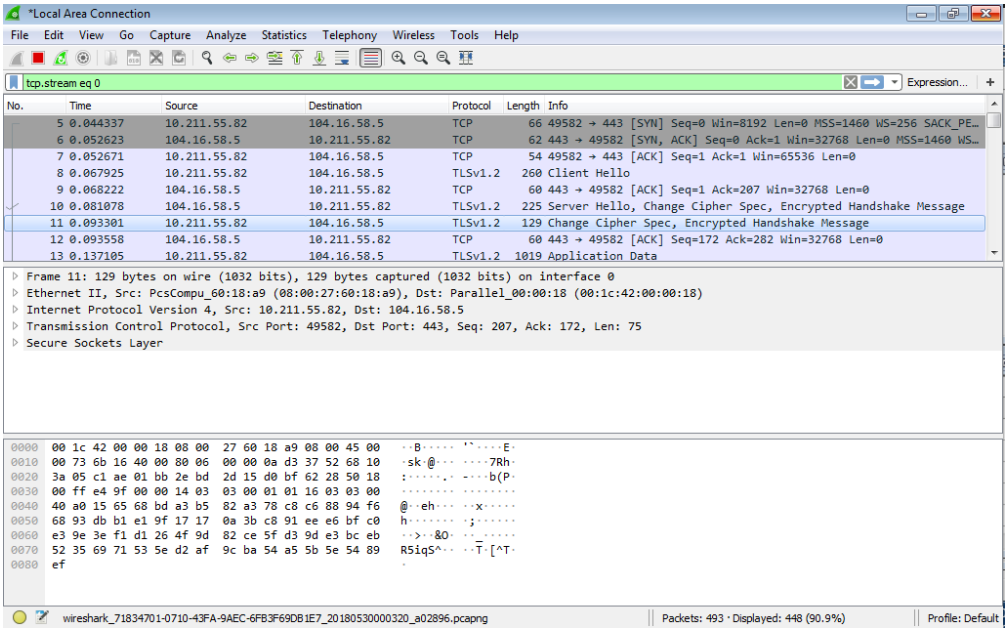


Figure F.63: The Upload process for Discord is encrypted with TLS 1.2. Captured in Wireshark.

Appendix G

Pilot Forensic Analysis

G.1 Introduction

As there have been no peer reviewed journals for analysis of Discord and TeamSpeak a pilot forensic analysis of both Discord and TeamSpeak was conducted.

G.2 TeamSpeak

The discovery of artefacts in teamspeak started with locating chat logs. By default TeamSpeak3 logs all communications in .text and .html formats which are found within the the `%AppData%` folder. During the forensic analysis of TeamSpeak the decision was made to switch from Parallels Desktop to VirtualBox as a raw image could be carved directly from the host machine to an external hard drive from the command line. During the analysis in the Lab the sample file `Windows 7 Execution Lab.raw` was loaded onto EnCase and an acquisition was created with an estimated time of 12 hours to process the 32gb image, when the evidence was looked at the in the morning EnCase had crashed and had stopped parsing the file as the forensics machine had run out of physical disk space to process the file. This then meant new ways of examining the images had to be conducted to get the work within the deadline set. As such FastBloc SE was used to writeblock the USB drive. X-Ways Forensics was then used to examine the files in read-only mode and a report was generated with the artefacts and screen shots was also taken during the analysis. The results was also emulated using Autopsy 4.70 to ensure that the data was forensically sound.

G.3 Discord

The discovery of artefacts in Discord started at looking at the AppData folder for possible folders that contain the string discord. In the roaming section of the file system located at

`AppData\local\discord` a folder called `Cache` looked like a Chrome cache folder which posed the question "Is this application using some form of the Chromium/Webkit Framework?" As such a forensic tool was found called "ChromeCacheViewer" by Nirsoft. Cache data including avatar (profile) images, external media (Twitch.tv/YouTube) and images sent to and from the client. After this analysis in order to determine the architecture of the application a RAM capture was preformed using DumpIt! this resulted in the discovery of .NODE files that show that node.js is being partly used. The characteristics of the client's execution at runtime which included the use of a Chrome Cache and Node.JS library provided within reason the plausibility that the electron framework was being used. The electronjs website includes a directory of applications that run on the framework which combines both Node.JS and the Chromium Framework therefore the use of an embedded software cache highly useful in tracing evidence. It was noted during this phase that multiple files could be used to determine NODE usage. Furthermore a search of the ElectronJS website concluded with finding Discord in the application directory of applications that use the ElectronJS Platform. During the initial tests, EnCase Imager was used to image the disk however, there was a drawback. Data could not be writeblocked and EnCase Imager would often include residual artefacts from the imager on the virtual machine.

G.4 Changes to the methodology

Multiple changes to the experiments occurred during the experimental phase. The first major change was the reduction in experiments due to running out of time and physical storage capacity (with 3 experiments totalling 600+ GBs.). During the experimental phase the analysis EnCase Imager was used to extract the data however, it left traces during the analysis and as a result the decision was made to change the visualization layer of the virtual machines being used from Parallels Desktop to Oracle VirtualBox as VirtualBox has the ability to export raw images from the command line to a desired destination such as a hard drive. EnCase FastBlockSE was then used as a software writeblocker and XWays and Autospy replaced EnCase as the forensics investigation tool. During the initial test DB Browser for SQLite was used to examine the data however the data was not available to preview in a text panel as such a new tool was developed called Discord Extractor to provide a method of exporting the Discord Extractor data to a CSV file.

G.5 DirectX Issues

As TeamSpeak3 and Discord rely on the DirectX modules for rendering parts of the user interface the experimental Direct3D drivers had to be installed. As such Oracle Guest tools had to be installed on the guest virtual machines. During the setup a web browser and 2 virtual machines ran at the same time which caused the Host to crash. As such during each experiment the web

browser is closed down and the allocated V-RAM for the Virtual Machines is set to around 256mb/s per machine.

Appendix H

Revised Ethical Checklist

		Yes	No
1.	Does the study involve participants who are particularly vulnerable or unable to give informed consent (e.g. children, people with learning disabilities, your own students)?	☐	☒
2.	Will the study require the co-operation of a gatekeeper for initial access to vulnerable groups or individuals to be recruited (e.g. students at school, members of self-help group, residents of nursing home)?	☐	☒
3.	Will it be necessary for participants to take part in the study without their knowledge and consent at the time (e.g. covert observation of people in non-public places)?	☐	☒
4.	Will the study involve discussion of sensitive topics (e.g. sexual activity, drug use, crime, etc.)?	☐	☒
5.	Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants?	☐	☒
6.	Does the study involve invasive or intrusive procedures such as blood taking or muscle biopsy from participants?	☐	☒
7.	Is physiological stress, pain, or more than mild discomfort likely to result from the study?	☐	☒
8.	Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?	☐	☒
9.	Will the study involve prolonged or repetitive testing?	☐	☒
10.	Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?	☐	☒
11.	Will the study involve recruitment of participants (including staff) from other Faculties at Canterbury Christ Church University?	☐	☒
12.	Will the study involve recruitment of participants (including staff) through a Local Authority (e.g. Kent County Council) Department of Social Services?	☐	☒
13.	Will the study involve recruitment of patients or staff through the NHS?	☐	☒

If you have answered 'NO' to all the questions above then no further action is required.

If you have answered 'YES' to any of the questions above then you will need to describe more fully how you plan to deal with the ethical issues raised. This does not necessarily mean that you cannot proceed with your proposals but it does mean that your proposals will need to be approved by your supervisor/second marker.

Appendix I

Forensic Case Reports

ts3executionlab

Description:
Forensic Analysis of TeamSpeak3 in Execution Lab Phase.
Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: F:\XWays\ts3executionlab.xfc
Creation time: 22/05/2018 18:04:26
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Notable documents (8 items)

Name: **urls.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 4.0 KB
Created: 21/05/2018 19:49:34 +1
Modified: 21/05/2018 19:49:34 +1
Record changed: 21/05/2018 19:49:34 +1
Accessed: 21/05/2018 19:49:34 +1
Attr.: XA
1st sector: 321,144
ID: 22713
Int. ID: 25063
Int. parent: 112101
Unique ID: 0-25063
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Report table: Notable documents
Comment: [Me] This is the URLs database. It would typically include the username and the URL however as the experiment focused more on the execution this was not included in this experiment.

Name: **channel.txt**
Description: existing file
Ext.: txt
Type: txt
Type status: confirmed
Type descr.: Text
Category: Plain Text
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 37 B
Created: 21/05/2018 19:49:35 +1
Modified: 21/05/2018 19:49:37 +1
Record changed: 21/05/2018 19:49:37 +1
Accessed: 21/05/2018 19:49:35 +1
Attr.: XA
1st sector: 6,470,934
ID: 89739
Int. ID: 112103
Int. parent: 112100
Unique ID: 0-112103
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Report table: Notable documents

Name: **channel.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed
Type descr.: HTML
Category: Internet
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 1.6 KB
Created: 21/05/2018 19:49:35 +1
Modified: 21/05/2018 20:08:58 +1
Record changed: 21/05/2018 20:08:58 +1
Accessed: 21/05/2018 19:49:35 +1
Attr.: XA
1st sector: 2,595,896
ID: 89749
Int. ID: 112113
Int. parent: 112100
Unique ID: 0-112113
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] Channel log shows channelid://1 lobby is being connected to via the client.

Name: **settings.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed

Name: **server.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed

Name: **rubberduck.jpg**
Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed

Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 61.0 KB
Created: 20/05/2018 23:16:14 +1
Modified: 21/05/2018 20:09:02 +1
Record changed: 21/05/2018 20:09:02 +1
Accessed: 20/05/2018 23:16:14 +1
Attr.: XA
1st sector: 9,376
ID: 89750
Int. ID: 112114
Int. parent: 112101
Unique ID: 0-112114
Owner: Builtin\Administrators
Link count: 1
Report table: Notable documents
Comment: [Me] Settings.db includes FileTransfer table. The table includes the count of downloads (SimulatniousDownloads) = 2, Number of uploads SimulatniousUploads= 2 and the last known file upload directory UploadDir: C:/Users/Public/Pictures/Sample Pictures

Type descr.: HTML
Category: Internet
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 3.0 KB
Created: 21/05/2018 19:49:35 +1
Modified: 21/05/2018 20:08:58 +1
Record changed: 21/05/2018 20:08:58 +1
Accessed: 21/05/2018 19:49:35 +1
Attr.: XA
1st sector: 3,092,992
ID: 89848
Int. ID: 112212
Int. parent: 112100
Unique ID: 0-112212
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] Attempt to upload image was unsuccessful. Log demonstrates user activity. User connected 4 times to the TeamSpeak3 server "CCCU Lab" between 19:49:35 - 20:06:56.

[Me] channelid://0 extracted from hyperlink.

Type descr.: JPEG
Category: Pictures
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\Downloads
Parent name: Downloads
Size: 134 KB
Created: 21/05/2018 19:55:31 +1
Modified: 21/05/2018 19:55:31 +1
Record changed: 21/05/2018 19:55:31 +1
Accessed: 21/05/2018 19:55:31 +1
Attr.: A
1st sector: 494,848
ID: 90082
Int. ID: 112446
Int. parent: 594
Unique ID: 0-112446
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Pixels: 0.5 MP
Report table: Notable documents
Comment: [Me] Image downloaded from TeamSpeak3 server.

Name: **kermit.jpg**
Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed
Type descr.: JPEG
Category: Pictures
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\Downloads
Parent name: Downloads
Size: 140 KB
Created: 21/05/2018 19:55:47 +1
Modified: 21/05/2018 19:55:47 +1
Record changed: 21/05/2018 19:55:47 +1
Accessed: 21/05/2018 19:55:47 +1
Attr.: A
1st sector: 512,000
ID: 90086
Int. ID: 112450
Int. parent: 594
Unique ID: 0-112450
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Pixels: 0.4 MP
Report table: Notable documents
Comment: [Me] Image downloaded fromTeamSpeak3 Server

Name: **Cookies**
Description: existing file
Type: sqlitedb
Type status: confirmed
Type descr.: Google Chrome cookies
Category: Internet
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\cache\qtwebengine_persistant_storage
Parent name: qtwebengine_persistant_storage
Size: 10.0 KB
Created: 21/05/2018 19:56:25 +1
Modified: 21/05/2018 19:56:34 +1
Record changed: 21/05/2018 19:56:34 +1
Accessed: 21/05/2018 19:56:25 +1
Attr.: XA
1st sector: 95,320
ID: 90090
Int. ID: 112454
Int. parent: 112452
Unique ID: 0-112454
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Report table: Notable documents
Comment: [Me] Cookies related to myteamspeak.com. (The hosted sync service)

ts3execute.raw, Partition 2

Internal designation: [E:\Windows 7 Execution Lab\ts3execute.raw], Partition 2
Date added: 22/05/2018 18:08:24

Hash: n/a
Description File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 2,380,374 = 28% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)
Serial No.: 2618238392 (dec, rev)

kermit.jpg

Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed
Type descr.: JPEG
Category: Pictures
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\Downloads
Parent name: Downloads
Child objects:
Size: 140 KB
Created: 21/05/2018 19:55:47 +1
Created²:
Modified: 21/05/2018 19:55:47 +1
Modified²:
Record changed: 21/05/2018 19:55:47 +1
Record changed²:
Accessed: 21/05/2018 19:55:47 +1
Deleted:
Content created:
Attr.: A
1st sector: 512,000
ID: 90086
Int. ID: 112450
Int. parent: 594
Unique ID: 0-112450
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Author:
Sender:
Recipients:
Link count: 1
File count:
Term count:
Search terms:
Page count:
Pixels: 0.4 MP
SC%:
Hash:
Hash set:
Hash category:


Feiges
Feiges

rubberduck.jpg

Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed
Type descr.: JPEG
Category: Pictures
Evidence object: ts3execute.raw, Partition 2
Path: \Users\John Doe\Downloads
Parent name: Downloads
Child objects:
Size: 134 KB
Created: 21/05/2018 19:55:31 +1
Created²:
Modified: 21/05/2018 19:55:31 +1
Modified²:
Record changed: 21/05/2018 19:55:31 +1
Record changed²:
Accessed: 21/05/2018 19:55:31 +1
Deleted:
Content created:
Attr.: A
1st sector: 494,848
ID: 90082
Int. ID: 112446
Int. parent: 594
Unique ID: 0-112446
Owner: S-1-5-21-1362272797-2432772758-3627158256-1000
Author:
Sender:
Recipients:
Link count: °1
File count:
Term count:
Search terms:
Page count:
Pixels: 0.5 MP
SC%:
Hash:
Hash set:
Hash category:

TeamSpeak3 Execution Analysis Lab

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_ts3execute.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/server.html	Connection to the server "CCCU Lab" made between 19:49 - 20:08:58 4 times.	2018-05-21 20:08:58 BST	2018-05-21 20:08:58 BST	2018-05-21 19:49:35 BST	2018-05-21 19:49:35 BST	3108	7338a3455d919054d549776b73bf268a
Notable Item (Notable)	/img_ts3execute.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/channel.html	Connection to lab made 4 times. This lines up with the server log that shows the client entering CCCU Lab.	2018-05-21 20:08:58 BST	2018-05-21 20:08:58 BST	2018-05-21 19:49:35 BST	2018-05-21 19:49:35 BST	1628	d17ac36fa1597af0f50cd246cd7f6ae5
Notable Item (Notable)	/img_ts3execute.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/settings.db	Contains last known upload directory for the TeamSpeak client.	2018-05-21 20:09:02 BST	2018-05-21 20:09:02 BST	2018-05-20 23:16:14 BST	2018-05-20 23:16:14 BST	62464	e94aa947f33c4bb92b042c7b8ba58e4f
Notable Item (Notable)	/img_ts3execute.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/urls.db	URL Database. Tyipcally stores URLs processed by the client however due to no transmission between clients the database is blank.	2018-05-21 19:49:34 BST	2018-05-21 19:49:34 BST	2018-05-21 19:49:34 BST	2018-05-21 19:49:34 BST	4096	96780f073f96d508ac0a84a5853b4887
Notable Item (Notable)	/img_ts3execute.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/cache/qtwebengine_persistant_storage/Cookies	Cookies related to the MyTeamSpeak Cloud service which is using CloudFlare as a Web Access Firewall. This can be determined by the __cfduid which is unqiue to Cloudflare.	2018-05-21 19:56:34 BST	2018-05-21 19:56:34 BST	2018-05-21 19:56:25 BST	2018-05-21 19:56:25 BST	10240	c77927a4f144e70a3ccfea4c3c7f3085

TS3 Attacker Client Analysis

Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: E:\XWays\TS3 Attacker Client Analysis.xfc
Creation time: 25/05/2018 12:27:02
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Notable documents (5 items)

Name: **kermit.jpg**
Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed
Type descr.: JPEG
Category: Pictures
Evidence object: ts3Attacker.raw, Partition 2
Path: \Users\John Doe\Pictures
Parent name: Pictures
Size: 140 KB
Created: 24/05/2018 22:51:34 +1
Modified: 24/05/2018 22:51:17 +1
Modified²: 24/05/2018 22:51:34 +1
Record changed: 24/05/2018 22:51:35 +1
Record changed²: 24/05/2018 22:51:34 +1
Accessed: 24/05/2018 22:51:34 +1
Attr.: IA
1st sector: 34,732,232
ID: 90147
Int. ID: 112511
Int. parent: 590
Unique ID: 0-112511
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Pixels: 0.4 MP
Report table: Notable documents
Comment: [Me] The kermit the frog image mentioned in the chat logs by Jane. This file was transmitted to the server.

Name: **settings.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3Attacker.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 52.0 KB
Created: 24/05/2018 22:58:21 +1
Modified: 24/05/2018 23:42:02 +1
Record changed: 24/05/2018 23:42:02 +1
Accessed: 24/05/2018 22:58:21 +1
Attr.: XA
1st sector: 795,312
ID: 90394
Int. ID: 112758
Int. parent: 38184
Unique ID: 0-112758
Owner: Builtin\Administrators
Link count: 1
Report table: Notable documents
Comment: [Me] The FileTransfer table shows 2 files have been uploaded and downloaded to the client. The upload folder destination C:\Users\John Doe\Pictures

Name: **urls.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3Attacker.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 4.0 KB
Created: 24/05/2018 22:59:10 +1
Modified: 24/05/2018 23:41:43 +1
Record changed: 24/05/2018 23:41:43 +1
Accessed: 24/05/2018 22:59:10 +1
Attr.: XA
1st sector: 35,850,848
ID: 90729
Int. ID: 113093
Int. parent: 38184
Unique ID: 0-113093
Owner: Builtin\Administrators
Link count: 1
Report table: Notable documents
Comment: [Me] John sends the link http://google.co.uk to a user. This is logged in the urls.db. Epoch value for sending the link is 23:41:43 on Thursday 24th May 2018

Name: **channel.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed

Name: **server.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed

Type descr.: HTML
Category: Internet
Evidence object: ts3Attacker.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 2.4 KB
Created: 24/05/2018 22:59:12 +1
Modified: 24/05/2018 23:42:00 +1
Record changed: 24/05/2018 23:42:00 +1
Accessed: 24/05/2018 22:59:12 +1
Attr.: XA
1st sector: 18,677,576
ID: 90735
Int. ID: 113099
Int. parent: 113097
Unique ID: 0-113099
Owner: Builtin\Administrators
Link count: °1
Report table: Notable documents
Comment: [Me] Conversation between Jane and John in public lobby. John connects at 22:59:12. Jane is already on the server. at 23:27:46 Jane says John has sent her an image of kermit.

Type descr.: HTML
Category: Internet
Evidence object: ts3Attacker.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 4.7 KB
Created: 24/05/2018 22:59:12 +1
Modified: 24/05/2018 23:42:00 +1
Record changed: 24/05/2018 23:42:00 +1
Accessed: 24/05/2018 22:59:12 +1
Attr.: XA
1st sector: 795,320
ID: 90738
Int. ID: 113102
Int. parent: 113097
Unique ID: 0-113102
Owner: Builtin\Administrators
Link count: °1
Report table: Notable documents
Comment: [Me] Jane connects to the server at 22:24:24 and leaves at 23:28:51 after being exposed to the kermit image. 23:41:22 Jane reconnects to the same server and leaves shortly after at 23:41:58.

ts3Attacker.raw, Partition 2

Internal designation: [F:\Windows 7 NG Attacker TeamSpeak3\ts3Attacker.raw], Partition 2
Date added: 25/05/2018 12:29:39
Hash: n/a
Description Windows Installation
Domain: WORKGROUP
Computer name: OLIVER-MDL3HDER
Owner: John Doe
Version: Windows 7 Professional
Time zone: 0 min
Installation date: 04/05/2018 20:24:57 +0
Number of accounts: 1

File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 3,762,404 = 45% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)

Serial No.: 2618238392 (dec, rev)

TeamSpeak Forensics Attacker Analysis Autopsy

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_ts3Attacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/settings.db	Upload Folder specified for John Doe's machine. (UploadDir). 2 uploads and downloads.	2018-05-24 23:42:02 BST	2018-05-24 23:42:02 BST	2018-05-24 22:58:21 BST	2018-05-24 22:58:21 BST	53248	08a4dd446fb70bce92e8a93c41efbd36
Notable Item (Notable)	/img_ts3Attacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/urls.db	google.co.uk shared by John in private chat	2018-05-24 23:41:43 BST	2018-05-24 23:41:43 BST	2018-05-24 22:59:10 BST	2018-05-24 22:59:10 BST	4096	48cd78467e31fa76462e8d7c591e4b2c
Notable Item (Notable)	/img_ts3Attacker.raw/vol_vol3/Users/John Doe/Pictures/kermit.jpg	The image uploaded by the attacker.	2018-05-24 22:51:17 BST	2018-05-24 22:51:35 BST	2018-05-24 22:51:34 BST	2018-05-24 22:51:34 BST	143304	79dfc0fcb6526e93fd2ec89f792219e2
Notable Item (Notable)	/img_ts3Attacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/channel.html	conversation between 22:25:11 - 22:27:46 John sends kermit picture to Jane.	2018-05-24 23:42:00 BST	2018-05-24 23:42:00 BST	2018-05-24 22:59:12 BST	2018-05-24 22:59:12 BST	2458	730c55a162c7d5a84b9ed5fcf3f60128
Notable Item (Notable)	/img_ts3Attacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/server.html	log shows Jane connected to lobby at 22:24:24 to the channel lobby. disconnected at 22:20:28, reconnected at 23:40:30 - 22:42:00 when a link was shared between John and Jane via a private conversation.	2018-05-24 23:42:00 BST	2018-05-24 23:42:00 BST	2018-05-24 22:59:12 BST	2018-05-24 22:59:12 BST	4768	a728a5713bd80e7c58f7f0af1d0f9e2d

TeamSpeak3 Victim Analysis

Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: E:\XWays\TeamSpeak3 Victim Analysis.xfc
Creation time: 25/05/2018 12:57:32
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Notable documents (5 items)

Name: **channel.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed
Type descr.: HTML
Category: Internet
Evidence object: ts3Victim.raw, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 2.1 KB
Created: 24/05/2018 23:24:29 +1
Modified: 24/05/2018 23:41:59 +1
Record changed: 24/05/2018 23:41:59 +1
Accessed: 24/05/2018 23:24:29 +1
Attr.: XA
1st sector: 11,840,856
ID: 89528
Int. ID: 111941
Int. parent: 111933
Unique ID: 0-111941
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] Jane joins chat at 23:24:29. At 23:27:43 Jane reports that John has sent her an image of kermit.

Name: **settings.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3Victim.raw, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 52.0 KB
Created: 24/05/2018 23:19:09 +1
Modified: 24/05/2018 23:42:05 +1
Record changed: 24/05/2018 23:42:05 +1
Accessed: 24/05/2018 23:19:09 +1
Attr.: XA
1st sector: 36,926,520
ID: 89703
Int. ID: 112116
Int. parent: 112115
Unique ID: 0-112116
Owner: Builtin\Administrators
Link count: 1
Report table: Notable documents
Comment: [Me] FileTransfer field includes two downloads and uploads but no indicators of the location of the file being downloaded.

Name: **server.html**
Description: existing file
Ext.: html
Type: html
Type status: confirmed
Type descr.: HTML
Category: Internet
Evidence object: ts3Victim.raw, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\TS3Client\chats\aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Parent name: aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==
Size: 1.5 KB
Created: 24/05/2018 23:24:29 +1
Modified: 24/05/2018 23:41:59 +1
Record changed: 24/05/2018 23:41:59 +1
Accessed: 24/05/2018 23:24:29 +1
Attr.: XA
1st sector: 9,424,776
ID: 89710
Int. ID: 112123
Int. parent: 111933
Unique ID: 0-112123
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] client connects at 23:24:29, disconnects at 23:29:03, reconnects at 23:41:20 and disconnects at 23:41:59.

Name: **urls.db**
Description: existing file
Ext.: db
Type: sqlitedb
Type status: confirmed
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: ts3Victim.raw, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\TS3Client
Parent name: TS3Client
Size: 4.0 KB

Name: **kermit.jpg**
Description: existing file
Ext.: jpg
Type: jpg
Type status: confirmed
Type descr.: JPEG
Category: Pictures
Evidence object: ts3Victim.raw, Partition 2
Path: \Users\Jane Doe\Downloads
Parent name: Downloads
Size: 140 KB

Created: 24/05/2018 23:24:28 +1
Modified: 24/05/2018 23:41:43 +1
Record changed: 24/05/2018 23:41:43 +1
Accessed: 24/05/2018 23:24:28 +1
Attr.: XA
1st sector: 11,839,704
ID: 90461
Int. ID: 112874
Int. parent: 112115
Unique ID: 0-112874
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Report table: Notable documents
Comment: [Me] John mentions link to Jane. This isn't reflected in the main chat logs for the channel therefore the urls being stored are from the private chat between John and Jane.

Created: 24/05/2018 23:27:06 +1
Modified: 24/05/2018 23:27:06 +1
Record changed: 24/05/2018 23:27:51 +1
Accessed: 24/05/2018 23:27:06 +1
Attr.: IA
1st sector: 6,202,328
ID: 92296
Int. ID: 114709
Int. parent: 112445
Unique ID: 0-114709
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 0.4 MP
Report table: Notable documents
Comment: [Me] Kermit image found in the downloads section of Jane's computer.

ts3Victim.raw, Partition 2

Internal designation: [F:\Windows 7 NG Victim TeamSpeak3\ts3Victim.raw], Partition 2
Date added: 25/05/2018 12:59:46
Hash: n/a
Description Windows Installation
Domain: WORKGROUP
Computer name: JANEDOE
Owner: John Doe
Version: Windows 7 Professional
Time zone: 0 min
Installation date: 04/05/2018 20:24:57 +0
Number of accounts: 2

File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 3,701,899 = 44% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)
Serial No.: 2618238392 (dec, rev)

TeamSpeak Forensics Victim Analysis Autopsy

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_ts3Victim.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/TS3Client/settings.db	2 Uploads and 2 Downloads from the client. found in FileTable.	2018-05-24 23:42:05 BST	2018-05-24 23:42:05 BST	2018-05-24 23:19:09 BST	2018-05-24 23:19:09 BST	53248	d933128 13d94b2c14523291 58cc16e28
Notable Item (Notable)	/img_ts3Victim.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/channel.html	Jane joins the channel "Lobby" at 23:24:29. Leaving at 23:41:20	2018-05-24 23:41:59 BST	2018-05-24 23:41:59 BST	2018-05-24 23:24:29 BST	2018-05-24 23:24:29 BST	2115	094ddbd83fc68e37b6b24f53f3323699
Notable Item (Notable)	/img_ts3Victim.raw/vol_vol3/Users/Jane Doe/Downloads/kermit.jpg	Offending Image of Kermit downloaded from the TeamSpeak3 server.	2018-05-24 23:27:06 BST	2018-05-24 23:27:51 BST	2018-05-24 23:27:06 BST	2018-05-24 23:27:06 BST	143304	79dfc0fcb6526e93fd2ec89f792219e2
Notable Item (Notable)	/img_ts3Victim.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/TS3Client/urls.db	url sent from john. epoch 1527201703, url: google.co.uk	2018-05-24 23:41:43 BST	2018-05-24 23:41:43 BST	2018-05-24 23:24:28 BST	2018-05-24 23:24:28 BST	4096	48cd78467e31fa76462e8d7c591e4b2c
Notable Item (Notable)	/img_ts3Victim.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/TS3Client/chats/aCtYdGtWamh6Unhtd3drMnNnK0EwMjNnbnJzPQ==/server.html	Jane connected to the server "CCCU Lab" twice. 23:24:29 - 23:29:03, 23:41:20 - 23:41:59 "CCCU Lab"	2018-05-24 23:41:59 BST	2018-05-24 23:41:59 BST	2018-05-24 23:24:29 BST	2018-05-24 23:24:29 BST	1578	52db82fa29374cc4eb55dcb8c685269b

Discord Execution Lab

Description:
Forensic Examination of Discord in execution.
Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: E:\XWays\Discord Execution Lab\Discord Execution Lab.xfc
Creation time: 25/05/2018 23:42:40
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Notable documents (7 items)

Name: **Cookies**
Description: existing file
Type: sqlitedb
Type status: confirmed
Type descr.: Google Chrome cookies
Category: Internet
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord
Parent name: discord
Size: 7.0 KB
Created: 25/05/2018 22:39:55 +1
Modified: 25/05/2018 23:06:31 +1
Record changed: 25/05/2018 23:06:31 +1
Accessed: 25/05/2018 22:39:55 +1
Attr.: XA
1st sector: 34,732,280
ID: 52962
Int. ID: 71066
Int. parent: 112745
Unique ID: 0-71066
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Report table: Notable documents
Comment: [Me] Cookies found related to Twitch.tv found in the database. Embedded players are cached by Discord.

Name: **discord_erlpack.node**
Description: existing file
Ext.: node
Type: dll
Type status: confirmed
Type descr.: Dynamic-Link Library
Category: Programs
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord\0.0.301 \modules\discord_erlpack
Parent name: discord_erlpack
Size: 501 KB
Created: 25/05/2018 22:28:45 +1
Modified: 25/05/2018 22:28:45 +1
Record changed: 25/05/2018 22:28:45 +1
Accessed: 25/05/2018 22:28:45 +1
Attr.: XA
1st sector: 36,589,696
ID: 89675
Int. ID: 112036
Int. parent: 112035
Unique ID: 0-112036
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] ErLang Node module

Name: **Cache**
Description: existing directory
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord
Parent name: discord
Size: 9.9 MB
Created: 25/05/2018 22:39:56 +1
Modified: 25/05/2018 23:05:29 +1
Record changed: 25/05/2018 23:05:29 +1
Accessed: 25/05/2018 23:05:29 +1
Attr.: X
1st sector: 34,789,936
ID: 89719
Int. ID: 112080
Int. parent: 112745
Unique ID: 0-112080
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
File count: 38
Report table: Notable documents
Comment: [Me] Cache for storage of images and the media player links.

[Me] Found url for an image that had been uploaded to Discord (kermit.jpg) - https://media.discordapp.net/attachments/449692697431769102/449693897225142288/kermit.jpg?width=400&height=269, a player link for twitch.tv/royalrumble as api.twitch.tv/royalrumble was also found in the cache including an image from the channel https://static-cdn.jtvnw.net/jtv_user_pictures/rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg

Name: **Discord.lnk**
Description: existing file
Ext.: lnk
Type: lnk
Type status: confirmed
Type descr.: Shortcut
Category: Windows Internals
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\Desktop
Parent name: Desktop
Size: 2.1 KB
Created: 25/05/2018 22:28:19 +1
Modified: 25/05/2018 22:28:21 +1
Record changed: 25/05/2018 22:28:21 +1
Accessed: 25/05/2018 22:28:19 +1
Attr.: A
1st sector: 34,812,368
ID: 90393
Int. ID: 112754
Int. parent: 596
Unique ID: 0-112754
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: 1
Report table: Notable documents
Comment: [Me] Icon for Discord on Desktop. Shows working directory of Discord is C:\Users\John Doe\AppData\Local\Discord\

Name: **discord_rpc.node**
Description: existing file
Ext.: node
Type: dll
Type status: confirmed
Type descr.: Dynamic-Link Library
Category: Programs
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord\0.0.301\modules\discord_rpc
Parent name: discord_rpc
Size: 2.6 MB
Created: 25/05/2018 22:32:30 +1
Modified: 25/05/2018 22:32:30 +1
Record changed: 25/05/2018 22:32:30 +1
Accessed: 25/05/2018 22:32:30 +1
Attr.: XA
1st sector: 34,710,728
ID: 90514
Int. ID: 112875
Int. parent: 112487
Unique ID: 0-112875
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] Node.JS is mainly used for the deployment of modules in Discord such as the RPC node.

Name: **https_discordapp.com_0.localstorage**
Description: existing file
Ext.: localstorage
Type: sqlitedb
Type status: newly identified
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 8.0 KB
Created: 25/05/2018 22:40:01 +1
Modified: 25/05/2018 23:06:06 +1
Record changed: 25/05/2018 23:06:06 +1
Accessed: 25/05/2018 22:40:01 +1
Attr.: XA
1st sector: 134,304
ID: 90750
Int. ID: 113111
Int. parent: 113106
Unique ID: 0-113111
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] Local storage SQL file for collecting statistics, email address, emoji statistics and channel information such as the channel ID. This file is very useful. The SQLite 2009 Pro browser was unable to open the file however DB Browser for SQLite was able to successfully open the file but not display the content in text format. As such the file is being exported out for investigation with the Discord Extractor tool.

[Me] Email Address: cccudiscord1@protonmail.com, Keyboard Locale: EN-US, Last Connected to Discord: 1527285933645, Channel ID: 449692697431769100 and 449692697431769102

Name: **https_player.twitch.tv_0.localstorage**
Description: existing file
Ext.: localstorage
Type: sqlitedb
Type status: newly identified
Type descr.: SQLite 3.x database
Category: Database, Finance
Evidence object: DiscordExecutionLab.raw, Partition 2
Path: \Users\John Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 3.0 KB
Created: 25/05/2018 23:05:28 +1
Modified: 25/05/2018 23:06:19 +1
Record changed: 25/05/2018 23:06:19 +1
Accessed: 25/05/2018 23:05:28 +1
Attr.: XA
1st sector: 34,627,392
ID: 91139

Int. ID: 113500
Int. parent: 113106
Unique ID: 0-113500
Owner: John Doe S-1-5-21-1362272797-2432772758-3627158256-1000
Link count: °1
Report table: Notable documents
Comment: [Me] Artefact indicates use of the site Twitch.TV.

DiscordExecutionLab.raw, Partition 2

Internal designation: [F:\Discord\Discord Execution Lab\DiscordExecutionLab.raw], Partition 2
Date added: 25/05/2018 23:46:25
Hash: n/a
Description Windows Installation
Domain: WORKGROUP
Computer name: OLIVER-MDL3HDER
Owner: John Doe
Version: Windows 7 Professional
Time zone: 0 min
Installation date: 04/05/2018 20:24:57 +0
Number of accounts: 1

File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 3,747,760 = 45% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)
Serial No.: 2618238392 (dec, rev)

Discord Execution Lab

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_DiscordExecutionLab.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Cache	Cache file that includes twitch.tv/royalrumble and Kermit.jpg cache data.	2018-05-25 23:05:29 BST	2018-05-25 23:05:29 BST	2018-05-25 23:05:29 BST	2018-05-25 22:39:56 BST	56	
Notable Item (Notable)	/img_DiscordExecutionLab.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Local Storage/https_discordapp.com_0.localstorage	local storage that contains email data. SQLite viewer in Autospy is faulty and unable to display results.	2018-05-25 23:06:06 BST	2018-05-25 23:06:06 BST	2018-05-25 22:40:01 BST	2018-05-25 22:40:01 BST	8192	b4c8b2623e892719e10bd3d9ca5eefcf
Notable Item (Notable)	/img_DiscordExecutionLab.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Local Storage/https_player.twitch.tv_0.localstorage	twitch.tv player storage. SQL file not viewable in Autospy.	2018-05-25 23:06:19 BST	2018-05-25 23:06:19 BST	2018-05-25 23:05:28 BST	2018-05-25 23:05:28 BST	3072	89776ce2c4b980d7e9907351a2266ca7
Notable Item (Notable)	/img_DiscordExecutionLab.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/0.0.301/modules/discord_erlpack/discord_erlpack.node	Discord uses node.js modules as part of the application framework.	2018-05-25 22:28:45 BST	2018-05-25 22:28:45 BST	2018-05-25 22:28:45 BST	2018-05-25 22:28:45 BST	512856	616cec14415639dcd67bacbc916e1e5b
Notable Item (Notable)	/img_DiscordExecutionLab.raw/vol_vol3/Users/John Doe/Pictures/kermit.jpg	Kermit image found in the pictures section on John's machine	2018-05-25 23:01:52 BST	2018-05-25 23:01:52 BST	2018-05-25 23:02:08 BST	2018-05-25 23:02:08 BST	197466	44826870492ba55eec193ddfd0230c71

Chrome Cache

Created by using ChromeCacheView

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Content Encoding	Cache Name	
width=400&height=269.jpg	https://media.discordapp.net/attachments/449692697431769102/449693897225142288/kermit.jpg?width=400&height=269	image/jpeg	22,146	25/05/2018 23:02:29	25/05/2018 23:03:01	25/05/2018 23:03:00	25/05/2019 23:03:00	cloudflare	HTTP/1.1 200		f_000015	public
width=610&height=410.jpg	https://media.discordapp.net/attachments/449692697431769102/449693897225142288/kermit.jpg?width=610&height=410	image/jpeg	44,449	25/05/2018 23:02:34	25/05/2018 23:03:06	25/05/2018 23:03:00	25/05/2019 23:03:05	cloudflare	HTTP/1.1 200		f_000016	public
rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg.jpg	https://images-ext-2.discordapp.net/external/C2YgmRLpnTvGtUzrKVk7rwPJq0LzZxw_l6mbOTcKhi8/https/static-cdn.jtvnw.net/jtv_user_pictures/rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg	image/jpeg	33,726	25/05/2018 23:04:45	25/05/2018 23:05:20	14/04/2016 16:19:31	25/05/2019 23:05:20	cloudflare	HTTP/1.1 200		f_000017	public
channel=rumbleroyale&player=facebook&autoplay=1&auto_play=1.htm	https://player.twitch.tv/?channel=rumbleroyale&player=facebook&autoplay=1&auto_play=1	text/html	532	25/05/2018 23:05:23	25/05/2018 23:05:57	25/05/2018 19:27:30		AmazonS3	HTTP/1.1 200	gzip	data_1 [79872]	public
rumbleroyale	https://api.twitch.tv/api/channels/rumbleroyale	application/json	574	25/05/2018 23:05:26	25/05/2018 23:06:01			nginx	HTTP/1.1 200		data_1 [89344]	max-a
rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg.jpg	https://static-cdn.jtvnw.net/jtv_user_pictures/rumbleroyale-profile_image-dbc11b0b30a33ff3-300x300.jpeg	image/jpeg	33,726	25/05/2018 23:05:26	25/05/2018 23:06:02	14/04/2016 16:19:31	05/05/2018 01:24:18		HTTP/1.1 200		f_00001e	max-a

DiscordVictim

Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: E:\XWays\DiscordVictim.xfc
Creation time: 28/05/2018 21:55:03
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Evidence objects:
discordvictim2
Partition 1
Partition 2

Notable documents (7 items)

Name: **Cache**
Description: existing directory
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord
Parent name: discord
Size: 10.3 MB
Created: 28/05/2018 02:32:57 +1
Modified: 28/05/2018 03:18:50 +1
Record changed: 28/05/2018 03:18:50 +1
Accessed: 28/05/2018 03:18:50 +1
Attr.: X
1st sector: 28,624
ID: 90577
Int. ID: 112963
Int. parent: 112079
Unique ID: 12-112963
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
File count: 44
Report table: Notable documents
Comment: [Me] Twitch.tv images saved in the cache from a twitch.tv profile, The image ducky.jpg sent via a private message was displayed in the cache and kermit.jpg was also sent in a public chat. All the links are publically accessible with no authentication methods required to view the content.

Name: **Cookies**
Description: existing file
Type: sqlitedb
Type status: confirmed
Type descr.: Google Chrome cookies
Category: Internet
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord
Parent name: discord
Size: 7.0 KB
Created: 28/05/2018 02:32:59 +1
Modified: 28/05/2018 03:20:55 +1
Record changed: 28/05/2018 03:20:55 +1
Accessed: 28/05/2018 02:32:59 +1
Attr.: XA
1st sector: 18,690,832
ID: 90585
Int. ID: 112971
Int. parent: 112079
Unique ID: 12-112971
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Report table: Notable documents
Comment: [Me] Twitch.tv cookie shows that user accessed Twitch.tv.

Name: **https_discordapp.com_0.localstorage**
Description: existing file
Ext.: localstorage
Type: localstorage
Type status: not verified
Type descr.: localstorage
Category: Other/unknown type
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 8.0 KB
Created: 28/05/2018 02:47:02 +1
Modified: 28/05/2018 03:20:28 +1
Record changed: 28/05/2018 03:20:28 +1
Accessed: 28/05/2018 02:47:02 +1
Attr.: XA
1st sector: 135,128
ID: 90620
Int. ID: 113006
Int. parent: 113002
Unique ID: 12-113006
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] email: cccudiscordt3@protonmail.com, locale: US-Eng, Channels: 450461385437085716, 450461385437085719, 450482283099455490

Name: **https_player.twitch.tv_0.localstorage**
Description: existing file
Ext.: localstorage
Type: localstorage
Type status: not verified
Type descr.: localstorage
Category: Other/unknown type
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 3.0 KB
Created: 28/05/2018 03:12:45 +1
Modified: 28/05/2018 03:14:58 +1
Record changed: 28/05/2018 03:14:58 +1
Accessed: 28/05/2018 03:12:45 +1
Attr.: XA
1st sector: 36,320,592
ID: 101173
Int. ID: 123551
Int. parent: 113002
Unique ID: 12-123551
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] Content marked as mature sent to Jane Doe. Resume Times/Epoch: 28862638016 - 6416 - 54471603

Name: **f_000022**
Description: existing file
Type: png
Type status: newly identified
Type descr.: Portable Network Graphics
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 121 KB
Created: 28/05/2018 03:14:12 +1
Modified: 28/05/2018 03:14:12 +1
Record changed: 28/05/2018 03:14:12 +1
Accessed: 28/05/2018 03:14:12 +1
Attr.: XA
1st sector: 40,260,032
ID: 101192
Int. ID: 123570
Int. parent: 112963
Unique ID: 12-123570
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 92 KP
Report table: Notable documents
Comment: [Me] Elegy twitch profile image from the twitch.tv player.

Name: **f_000025**
Description: existing file
Type: jpg
Type status: newly identified
Type descr.: JPEG
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 46.9 KB
Created: 28/05/2018 03:16:59 +1
Modified: 28/05/2018 03:16:59 +1
Record changed: 28/05/2018 03:16:59 +1
Accessed: 28/05/2018 03:16:59 +1
Attr.: XA
1st sector: 40,194,928
ID: 101257
Int. ID: 123635
Int. parent: 112963
Unique ID: 12-123635
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 0.3 MP
Report table: Notable documents
Comment: [Me] Kermit.jpg Image sent from the attacker displayed in the cache.

Name: **f_000027**
Description: existing file
Type: jpg
Type status: newly identified
Type descr.: JPEG
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 62.3 KB
Created: 28/05/2018 03:18:50 +1
Modified: 28/05/2018 03:18:50 +1
Record changed: 28/05/2018 03:18:50 +1
Accessed: 28/05/2018 03:18:50 +1
Attr.: XA
1st sector: 41,222,984
ID: 109695
Int. ID: 132139
Int. parent: 112963
Unique ID: 12-132139
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 0.3 MP
Report table: Notable documents
Comment: [Me] Ducky image that was sent to the victim via private message.

discordvictim2

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw]
Date added: 28/05/2018 22:26:20
Hash: n/a
Description
Total capacity: 34,359,738,368 bytes = 32.0 GB
Bytes per sector: 512
Sector count: 67,108,864

Partitioning style: MBR
Disk signature: 7C0177B1
Unpartitionable space: 2,048 Sectors

Partition 1
Sectors 2,048 - 206,847
Partition table: Sector 0
NTFS

Partition 2
Sectors 206,848 - 67,106,815
Partition table: Sector 0
NTFS

Unused inter-partition space:
Sectors 0 - 2,047 (1.0 MB)
Sectors 67,106,816 - 67,108,863 (1.0 MB)
= 2.0 MB

Partition 1

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw], Partition 1
Date added: 28/05/2018 22:26:21
Hash: n/a
Description File system: NTFS
Name: System Reserved
Total capacity: 104,857,600 bytes = 100 MB
Sector count: 204,800
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 19,418 = 76% free
Total clusters: 25,599
NTFS version: 3.1
Volume flags: 0x0000
Serial No.: 78240B14 (hex)
Serial No.: 140B2478 (hex, rev)
Serial No.: 336274552 (dec, rev)

Partition 2

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw], Partition 2
Date added: 28/05/2018 22:26:21
Hash: n/a
Description Windows Installation
Domain: WORKGROUP
Computer name: OLIVER-MDL3HDER
Owner: John Doe
Version: Windows 7 Professional
Time zone: 0 min
Installation date: 04/05/2018 20:24:57 +0
Number of accounts: 2

File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 3,495,830 = 42% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)
Serial No.: 2618238392 (dec, rev)

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_discordattacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Cache	Local Cache, contains links to Kermit image that has been uploaded t	2018-05-28 03:19:10 BST	2018-05-28 03:19:10 BST	2018-05-28 03:19:10 BST	2018-05-28 01:28:19 BST	168	
Notable Item (Notable)	/img_discordattacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Local Storage/https_discordapp.com_0.localstorage	Unable to open file on Autospy's in built SQL Viewer.	2018-05-28 03:21:04 BST	2018-05-28 03:21:04 BST	2018-05-28 01:28:35 BST	2018-05-28 01:28:35 BST	8192	9bcdd149f2973bcb55b1b6b084d21802
Notable Item (Notable)	/img_discordattacker.raw/vol_vol3/Users/John Doe/AppData/Roaming/discord/Local Storage/https_www.google.com_0.localstorage	Autospy is unable to read this file.	2018-05-28 01:37:22 BST	2018-05-28 01:37:22 BST	2018-05-28 01:37:21 BST	2018-05-28 01:37:21 BST	3072	aadb29b82a893571 9bb2f822017d4901
Notable Item (Notable)	/img_discordattacker.raw/vol_vol3/Users/John Doe/Pictures/kermit.jpg	Kermit image found in Cache on desktop of attacker's machine.	2018-05-28 03:15:45 BST	2018-05-28 03:15:55 BST	2018-05-28 03:15:55 BST	2018-05-28 03:15:55 BST	143304	79dfc0fcb6526e93fd2ec89f792219e2
Notable Item (Notable)	/img_discordattacker.raw/vol_vol3/Users/John Doe/Pictures/ducks.jpg	Ducks image sent to victim via private message.	2018-05-28 03:18:21 BST	2018-05-28 03:18:21 BST	2018-05-28 03:18:33 BST	2018-05-28 03:18:33 BST	512783	718ff5a3b471ec42ed841ebf1443ee2

Chrome Cache

Created by using ChromeCacheView

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Content Encoding	Cache Nam
0ecbb6c3-fecb-4016-8115-aa467b7c36ed-profile_image-300x300.jpg.png	https://images-ext-1.discordapp.net/external/NBcZ5uwYdm0FSWMIkYUThVcLKAIyDJdRiVhRdaSiXzw/https/static-cdn.jtvnw.net/user-default-pictures/0ecbb6c3-fecb-4016-8115-aa467b7c36ed-profile_image-300x300.jpg	image/png	71,890	28/05/2018 03:12:50	28/05/2018 03:13:35	05/10/2017 22:57:46	28/05/2019 03:13:35	cloudflare	HTTP/1.1 200		f_000020
elegy-profile_image-8d875f34e3a4d014-300x300.png	https://images-ext-1.discordapp.net/external/D-nx5cuVwuYj1nNLYLD2xe-EwcV7ZHZE5sViAaLYqXY/https/static-cdn.jtvnw.net/jtv_user_pictures/elegy-profile_image-8d875f34e3a4d014-300x300.png	image/png	124,341	28/05/2018 03:14:01	28/05/2018 03:14:57	06/05/2018 02:20:05	28/05/2019 03:14:57	cloudflare	HTTP/1.1 200		f_000021
width=400&height=185.jpg	https://media.discordapp.net/attachments/450482283099455490/450482646636822528/kermit.jpg?width=400&height=185	image/jpeg	16,303	28/05/2018 03:16:25	28/05/2018 03:17:14	28/05/2018 03:17:12	28/05/2019 03:17:14	cloudflare	HTTP/1.1 200		data_3 [1335
width=784&height=363.jpg	https://media.discordapp.net/attachments/450482283099455490/450482646636822528/kermit.jpg?width=784&height=363	image/jpeg	49,252	28/05/2018 03:17:26	28/05/2018 03:17:58	28/05/2018 03:17:12	28/05/2019 03:17:58	cloudflare	HTTP/1.1 200		f_000022
width=400&height=250.jpg	https://media.discordapp.net/attachments/450461385437085719/450483184753442816/ducks.jpg?width=400&height=250	image/jpeg	30,929	28/05/2018 03:18:49	28/05/2018 03:19:21	28/05/2018 03:19:20	28/05/2019 03:19:21	cloudflare	HTTP/1.1 200		f_000023
width=657&height=410.jpg	https://media.discordapp.net/attachments/450461385437085719/450483184753442816/ducks.jpg?width=657&height=410	image/jpeg	63,820	28/05/2018 03:19:10	28/05/2018 03:19:42	28/05/2018 03:19:20	28/05/2019 03:19:42	cloudflare	HTTP/1.1 200		f_000024

DiscordVictim

Examiner(s), organization, address:
Oliver George Bryant
Report generated by X-Ways Forensics 18.1 SR-8
Case file: E:\XWays\DiscordVictim.xfc
Creation time: 28/05/2018 21:55:03
Log time zone: +01:00 GMT Daylight Time

Report tables:
Notable documents

Evidence objects:
discordvictim2
Partition 1
Partition 2

Notable documents (7 items)

Name: **Cache**
Description: existing directory
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord
Parent name: discord
Size: 10.3 MB
Created: 28/05/2018 02:32:57 +1
Modified: 28/05/2018 03:18:50 +1
Record changed: 28/05/2018 03:18:50 +1
Accessed: 28/05/2018 03:18:50 +1
Attr.: X
1st sector: 28,624
ID: 90577
Int. ID: 112963
Int. parent: 112079
Unique ID: 12-112963
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
File count: 44
Report table: Notable documents
Comment: [Me] Twitch.tv images saved in the cache from a twitch.tv profile, The image ducky.jpg sent via a private message was displayed in the cache and kermit.jpg was also sent in a public chat. All the links are publically accessible with no authentication methods required to view the content.

Name: **Cookies**
Description: existing file
Type: sqlitedb
Type status: confirmed
Type descr.: Google Chrome cookies
Category: Internet
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord
Parent name: discord
Size: 7.0 KB
Created: 28/05/2018 02:32:59 +1
Modified: 28/05/2018 03:20:55 +1
Record changed: 28/05/2018 03:20:55 +1
Accessed: 28/05/2018 02:32:59 +1
Attr.: XA
1st sector: 18,690,832
ID: 90585
Int. ID: 112971
Int. parent: 112079
Unique ID: 12-112971
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Report table: Notable documents
Comment: [Me] Twitch.tv cookie shows that user accessed Twitch.tv.

Name: **https_discordapp.com_0.localstorage**
Description: existing file
Ext.: localstorage
Type: localstorage
Type status: not verified
Type descr.: localstorage
Category: Other/unknown type
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 8.0 KB
Created: 28/05/2018 02:47:02 +1
Modified: 28/05/2018 03:20:28 +1
Record changed: 28/05/2018 03:20:28 +1
Accessed: 28/05/2018 02:47:02 +1
Attr.: XA
1st sector: 135,128
ID: 90620
Int. ID: 113006
Int. parent: 113002
Unique ID: 12-113006
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] email: cccudiscordt3@protonmail.com, locale: US-Eng, Channels: 450461385437085716, 450461385437085719, 450482283099455490

Name: **https_player.twitch.tv_0.localstorage**
Description: existing file
Ext.: localstorage
Type: localstorage
Type status: not verified
Type descr.: localstorage
Category: Other/unknown type
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Local Storage
Parent name: Local Storage
Size: 3.0 KB
Created: 28/05/2018 03:12:45 +1
Modified: 28/05/2018 03:14:58 +1
Record changed: 28/05/2018 03:14:58 +1
Accessed: 28/05/2018 03:12:45 +1
Attr.: XA
1st sector: 36,320,592
ID: 101173
Int. ID: 123551
Int. parent: 113002
Unique ID: 12-123551
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: °1
Report table: Notable documents
Comment: [Me] Content marked as mature sent to Jane Doe. Resume Times/Epoch: 28862638016 - 6416 - 54471603

Name: **f_000022**
Description: existing file
Type: png
Type status: newly identified
Type descr.: Portable Network Graphics
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 121 KB
Created: 28/05/2018 03:14:12 +1
Modified: 28/05/2018 03:14:12 +1
Record changed: 28/05/2018 03:14:12 +1
Accessed: 28/05/2018 03:14:12 +1
Attr.: XA
1st sector: 40,260,032
ID: 101192
Int. ID: 123570
Int. parent: 112963
Unique ID: 12-123570
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 92 KP
Report table: Notable documents
Comment: [Me] Elegy twitch profile image from the twitch.tv player.

Name: **f_000025**
Description: existing file
Type: jpg
Type status: newly identified
Type descr.: JPEG
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 46.9 KB
Created: 28/05/2018 03:16:59 +1
Modified: 28/05/2018 03:16:59 +1
Record changed: 28/05/2018 03:16:59 +1
Accessed: 28/05/2018 03:16:59 +1
Attr.: XA
1st sector: 40,194,928
ID: 101257
Int. ID: 123635
Int. parent: 112963
Unique ID: 12-123635
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 0.3 MP
Report table: Notable documents
Comment: [Me] Kermit.jpg Image sent from the attacker displayed in the cache.

Name: **f_000027**
Description: existing file
Type: jpg
Type status: newly identified
Type descr.: JPEG
Category: Pictures
Evidence object: discordvictim2, Partition 2
Path: \Users\Jane Doe\AppData\Roaming\discord\Cache
Parent name: Cache
Size: 62.3 KB
Created: 28/05/2018 03:18:50 +1
Modified: 28/05/2018 03:18:50 +1
Record changed: 28/05/2018 03:18:50 +1
Accessed: 28/05/2018 03:18:50 +1
Attr.: XA
1st sector: 41,222,984
ID: 109695
Int. ID: 132139
Int. parent: 112963
Unique ID: 12-132139
Owner: Jane Doe S-1-5-21-1362272797-2432772758-3627158256-1001
Link count: 1
Pixels: 0.3 MP
Report table: Notable documents
Comment: [Me] Ducky image that was sent to the victim via private message.

discordvictim2

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw]
Date added: 28/05/2018 22:26:20
Hash: n/a
Description
Total capacity: 34,359,738,368 bytes = 32.0 GB
Bytes per sector: 512
Sector count: 67,108,864

Partitioning style: MBR
Disk signature: 7C0177B1
Unpartitionable space: 2,048 Sectors

Partition 1
Sectors 2,048 - 206,847
Partition table: Sector 0
NTFS

Partition 2
Sectors 206,848 - 67,106,815
Partition table: Sector 0
NTFS

Unused inter-partition space:
Sectors 0 - 2,047 (1.0 MB)
Sectors 67,106,816 - 67,108,863 (1.0 MB)
= 2.0 MB

Partition 1

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw], Partition 1
Date added: 28/05/2018 22:26:21
Hash: n/a
Description File system: NTFS
Name: System Reserved
Total capacity: 104,857,600 bytes = 100 MB
Sector count: 204,800
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 19,418 = 76% free
Total clusters: 25,599
NTFS version: 3.1
Volume flags: 0x0000
Serial No.: 78240B14 (hex)
Serial No.: 140B2478 (hex, rev)
Serial No.: 336274552 (dec, rev)

Partition 2

Internal designation: [F:\Discord\Discord Victim\discordvictim2.raw], Partition 2
Date added: 28/05/2018 22:26:21
Hash: n/a
Description Windows Installation
Domain: WORKGROUP
Computer name: OLIVER-MDL3HDER
Owner: John Doe
Version: Windows 7 Professional
Time zone: 0 min
Installation date: 04/05/2018 20:24:57 +0
Number of accounts: 2

File system: NTFS
Total capacity: 34,252,783,616 bytes = 31.9 GB
Sector count: 66,899,968
Bytes per sector: 512
Bytes per cluster: 4,096
Free clusters: 3,495,830 = 42% free
Total clusters: 8,362,495
NTFS version: 3.1
Volume flags: 0x0000
Volume GUID: {FCD8BFEE-DDE3-4231-A0AD-C07A0B8F778D}
Serial No.: B8250F9C (hex)
Serial No.: 9C0F25B8 (hex, rev)
Serial No.: 2618238392 (dec, rev)

Discord Victim Autopsy Analysis

Tag	File	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cache/f_00001f	elegy twitch.tv image	2018-05-28 03:14:00 BST	2018-05-28 03:14:00 BST	2018-05-28 03:14:00 BST	2018-05-28 03:14:00 BST	124341	9380a0ddd6af608bd44e06c11b7290ce
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cache/f_000022	Elegy Twitch.tv image	2018-05-28 03:14:12 BST	2018-05-28 03:14:12 BST	2018-05-28 03:14:12 BST	2018-05-28 03:14:12 BST	124341	9380a0ddd6af608bd44e06c11b7290ce
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cache/f_000025	Kermit.jpg sent from John to Jane on the public channel.	2018-05-28 03:16:59 BST	2018-05-28 03:16:59 BST	2018-05-28 03:16:59 BST	2018-05-28 03:16:59 BST	47975	6b169744792 1d2bb9e4139d948b2e51f
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cache/f_000026	The ducky image sent to Jane from John in the private channel.	2018-05-28 03:18:46 BST	2018-05-28 03:18:46 BST	2018-05-28 03:18:46 BST	2018-05-28 03:18:46 BST	30929	ae071387f561c8fd0cfcecc113ad7a05
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cache/f_000027	Ducky image sent from John to Jane.	2018-05-28 03:18:50 BST	2018-05-28 03:18:50 BST	2018-05-28 03:18:50 BST	2018-05-28 03:18:50 BST	63820	373b90136b13a22478bee023ce9a4708
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Local Storage/https_discordapp.com_0.localstorage	Unable to view contents on Autopsy.	2018-05-28 03:20:28 BST	2018-05-28 03:20:28 BST	2018-05-28 02:47:02 BST	2018-05-28 02:47:02 BST	8192	d33b3607e303296948 1bf60f4cf6b785
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Local Storage/https_player.twitch.tv_0.localstorage	Unable to view database in Autopsy.	2018-05-28 03:14:58 BST	2018-05-28 03:14:58 BST	2018-05-28 03:12:45 BST	2018-05-28 03:12:45 BST	3072	3c9b7292a3c13d3f09cd445eddc82d6f
Notable Item (Notable)	/img_discordvictim2.raw/vol_vol3/Users/Jane Doe/AppData/Roaming/discord/Cookies	Twitch.tv cookie stored inside the cookies section of the client indicating twitch.tv player has been used.	2018-05-28 03:20:55 BST	2018-05-28 03:20:55 BST	2018-05-28 02:32:59 BST	2018-05-28 02:32:59 BST	7168	460f740e74d5de2e9d22f7bedebbbe76

Chrome Cache

Created by using ChromeCacheView

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Content Encoding	Cache Name	
royalrumble	https://api.twitch.tv/api/channels/royalrumble	application/json	351	28/05/2018 03:13:04	28/05/2018 03:13:56			nginx	HTTP/1.1 200		data_1 [77312]	max-age=
channel=royalrumble&player=facebook&autoplay=1&auto_play=1.htm	https://player.twitch.tv/?channel=royalrumble&player=facebook&autoplay=1&auto_play=1	text/html	1,019	28/05/2018 03:13:07	28/05/2018 03:13:41	25/05/2018 19:27:30		AmazonS3	HTTP/1.1 200	gzip	data_1 [70656]	public, m
elegy-profile_image-8d875f34e3a4d014-300x300.png	https://images-ext-1.discordapp.net/external/D-nx5cuVwuYj1nNLYLD2xe-EwcV7ZHZE5sViAaLYqXY/https/static-cdn.jtvnw.net/jtv_user_pictures/elegy-profile_image-8d875f34e3a4d014-300x300.png	image/png	124,341	28/05/2018 03:13:55	28/05/2018 03:14:58	06/05/2018 02:20:05	28/05/2019 03:14:58	cloudflare	HTTP/1.1 200		f_00001f	public, m
channel=elegy&player=facebook&autoplay=1&auto_play=1.htm	https://player.twitch.tv/?channel=elegy&player=facebook&autoplay=1&auto_play=1	text/html	1,019	28/05/2018 03:14:01	28/05/2018 03:15:00	25/05/2018 19:27:30		AmazonS3	HTTP/1.1 200	gzip	data_1 [82944]	public, m
elegy-profile_image-8d875f34e3a4d014-300x300.png	https://static-cdn.jtvnw.net/jtv_user_pictures/elegy-profile_image-8d875f34e3a4d014-300x300.png	image/png	124,341	28/05/2018 03:14:11	28/05/2018 03:15:07	06/05/2018 02:20:05	18/05/2018 19:21:25		HTTP/1.1 200		f_000022	max-age=
width=400&height=185.jpg	https://media.discordapp.net/attachments/450482283099455490/450482646636822528/kermit.jpg?width=400&height=185	image/jpeg	16,303	28/05/2018 03:16:39	28/05/2018 03:17:14	28/05/2018 03:17:12	28/05/2019 03:17:14	cloudflare	HTTP/1.1 200		data_3 [1335296]	public, m
width=770&height=357.jpg	https://media.discordapp.net/attachments/450482283099455490/450482646636822528/kermit.jpg?width=770&height=357	image/jpeg	47,975	28/05/2018 03:16:58	28/05/2018 03:17:16	28/05/2018 03:17:12	28/05/2019 03:17:15	cloudflare	HTTP/1.1 200		f_000025	public, m
width=400&height=250.jpg	https://media.discordapp.net/attachments/450461385437085719/450483184753442816/ducks.jpg?width=400&height=250	image/jpeg	30,929	28/05/2018 03:18:47	28/05/2018 03:19:21	28/05/2018 03:19:20	28/05/2019 03:19:21	cloudflare	HTTP/1.1 200		f_000026	public, m
width=657&height=410.jpg	https://media.discordapp.net/attachments/450461385437085719/450483184753442816/ducks.jpg?width=657&height=410	image/jpeg	63,820	28/05/2018 03:18:51	28/05/2018 03:19:25	28/05/2018 03:19:20	28/05/2019 03:19:25	cloudflare	HTTP/1.1 200		f_000027	public, m
dd920c06a01e5bb8b09678581e29d56f.mp3	https://discordapp.com/assets/dd920c06a01e5bb8b09678581e29d56f.mp3	audio/mpeg	17,922	28/05/2018 03:19:39	28/05/2018 03:15:47	24/03/2018 09:01:08		cloudflare	HTTP/1.1 200		f_000024	public