8-6-2018

Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account

Ananya Yarramreddy
University of New Haven

Peter Gromkowski
University of New Haven

Ibrahim Baggili
University of New Haven, ibaggili@newhaven.edu

Publisher Citation

A. Yarramreddy, P. Gromkowski and I. Baggili, "Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, California, USA, 2018, pp. 186-196. doi:10.1109/SPW.2018.00034

This material is based upon work supported by the National Science Foundation under Grant No. 1748950.

Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account

Ananya Yarramreddy*, Peter Gromkowski*, and Ibrahim Baggili*
{ayarr1,pgrom1}@unh.newhaven.edu,
ibaggili@newhaven.edu
*Cyber Forensics Research & Education Group,
Tagliatela College of Engineering, ECECS,
University of New Haven, West Haven, CT 06516

***Abstract*—Our work presents the primary account for exploring the forensics of immersive Virtual Reality (VR) systems and their social applications. The Social VR applications studied in this work include Bigscreen, Altspace VR, Rec Room and Facebook Spaces. We explored the two most widely adopted consumer VR systems: the HTC Vive and the Oculus Rift. Our tests examined the efficacy of reconstructing evidence from network traffic as well as the systems themselves. The results showed that a significant amount of forensically relevant data such as user names, user profile pictures, events, and system details may be recovered. We anticipate that this work will stimulate future research directions in VR and Augmented Reality (AR) forensics as it is an area that is understudied and needs more attention from the community.**

***Index Terms*—Digital Forensics, Artifacts, Security, VR Applications, Virtual Reality, Steam, HTC Vive, Oculus Rift, VR Social Applications, Immersive VR.**

I. Introduction

VIRTUAL Reality (VR) is an emerging technology with promise to deliver new perspectives to a variety of applications. Most commonly, immersive VR facilitates a new generation of Human Computer Interaction (HCI). Advances in tracking technology have elevated user presence to a degree that blurs boundaries between virtual and physical realities [1]. Taking advantage of this, VR has found application in physiological and military practices. The adaptability of a Virtual Environment (VE) provides necessary conditions to treat phobias, or simulate a realistic training exercise [2]. In recent years, improvements in fabrication and reduced production costs have introduced VR devices into the consumer marketplace. Although new to the consumer market, VR has a significant history since its inception in 1969 [3]. Despite this, VR continues to occupy additional niches. One of which is a modern breed of social interaction.

Should VR systems follow the same meteoric rise as mobile device / social media usage, VR and Augmented Reality (AR) would become commonplace in day-to-day activities. The use of social applications has grown from 0.92 billion users in 2010 to 2.46 billion in 2017, a growth trend that is expected to continue [4]. Furthermore, the average individual spends 116 minutes daily on social applications [5]. Just as mobile phones have become another platform for social media, VR stands to be the next generation medium for communication. The latest craze of content sharing suits VR as users can coinhabit VEs and contribute content unique to immersion. When placed in an immersive VR environment, the user's view is completely obstructed from the real world due to the Head Mounted Display (HMD). This means the user cannot see anything around them except the VR environment. This visual obstruction provides an adversary with the opportunity to cause physical harm to an immersed VR user.

A recent study found that depth perception and balance were temporarily deteriorated in children immediately following 20 minutes of VR immersion [6]. Furthermore, VR may affect the psychological wellbeing of users given that they feel completely immersed into an environment. Immersion amplifies the consequences of cyber bullying and sexual harassment, where the misconduct "feels all too real" [7]. A legal precedence is yet to be set, however, VR wrongdoing remains in the middle ground between virtual and legitimate physical crimes [8].

In anticipation of a migration to virtual socialization, we intend to arm cyber forensic researchers and practitioners with the necessary tools and information to expedite investigations.

Our work is novel and makes the following contributions to the digital forensics community:

- This is the first account for immersive VR forensics.
- We present the first account for forensically relevant client-side and network-based artifacts generated by the HTC Vive and the Oculus Rift.
- We present the first account for forensically relevant network-based artifacts generated by the most widely used immersive VR social applications.
- We stimulate future research, and publicly share primary VR network datasets and system artifacts from our experiments here: https://www.unhcfreg.com/datasetsandtools.

Our work is limited to logically acquired artifacts residing on long term storage for room-scale immersive VR systems. We do not examine small scale VR devices, such as the Samsung Gear VR or the Pixel 2, nor investigate data in volatile memory. Being that this is the first account of artifact analysis of VR systems, our work aims to set direction for continued research.

The remainder of the paper is organized as follows: We discuss VR applications and related work in Section II. The methodology and apparatus used are discussed in Section III.

We present our findings for system artifacts in Section IV, followed by network analysis in Section V. We discuss our findings in Section VI and identify areas for future work in Section VII. Finally, we make concluding remarks in Section VIII.

II. Background Information and Related work

Artifacts acquired from VR social applications may serve as digital evidence in future cases, similar to current messaging applications used on mobile devices and computer systems.

High profile cases such as Brown and Nelthrope vs Kilpatrick have involved analysis of Short Message Service (SMS) resulting in pergery, evidence obtained long after the crime [9]. Cellular providers that retain SMS and subscriber information ease obtaining SMS activity, however, investigators may have limited time to retrieve these conversations [10]. Alternative messaging and social applications have become increasingly popular. For instance, Google Voice employs proprietary protocols in lieu of SMS, lowering costs associated with cellular providers. With the added features, security and low cost of third-party applications we can expect their continued growth.

Instant Messaging (IM) applications initially held popularity for adolescent socializing [11] and was later embraced in the workplace, increasing productivity and shortening interruptions [12]. An online presence introduced privacy concerns unique to IM applications, such as broadcasting the users status [13]. As shown by [14], examination of stand alone messaging applications held forensic importance even prior to mobile use. Techniques for examining PC based application artifacts are described for AOL instant messenger (AIM) [15], MSN Messenger 7.5 [16], and Yahoo Messenger 7.0 . Transition to web-based messaging relieved the necessity for registry keys and configuration files. Techniques for examining page files and swap space for various web messengers are described by [18] and Facebook Chat by [19].

Mobile phones have amplified user connectivity and have been extensively examined, however, frequent updates to Operating Systems (OS) and applications increase the difficulty of maintaining a database of artifacts [20], [21]. Android social applications were found to store identifying information and often archive messages, raising concerns about privacy, [22], [23]. Using Celebrite Universal Forensic Extraction Device (UFED), [24] were able to obtain call logs and messages from Android instant messaging applications WhatsApp and Viber. Furthermore, [25] examined third-party applications for the Apple iPhone and located information ranging from usernames to geo-location data.

Third party messaging applications have also grown in popularity, with WhatsApp reporting over 1 billion users in 2016 [26]. Poor authentication procedures in messaging alternatives are vulnerable to attack. Analysis of nine third party applications, including WhatsApp, revealed potential for account hijacking, spoofing, and unsolicited SMS's [27]. Moreover, traces of conversations, and even photographs, from social messaging applications were found to publicly remain unencrypted on servers [28]. Other work has also explored the decryption of voice traffic from applications such as WhatsApp [29].

The bargain and convenience of third party messaging applications are at the cost of security. Following in stride, cloud services pose a similar problem for secure communication [30].

As VR systems become increasingly available to the consumer, and content refined to complement existing means of communication, we expect an influx of virtual socialization. Such as each generation of messaging conceded flaws in infancy, VR is no exception, producing a wealth of artifacts. We have identified no prior work regarding the analysis of trace evidence remaining from VR social applications, nor VR systems in general.

A. Steam and SteamVR

The primary application distribution platform utilized in this study was Steam by the Valve Corporation. Steam provides services such as application acquisition and purchase, installation, multilayer matchmaking, support, automatic updating and socialization [31]. Users maintain an account which allows Steam to manage the user's applications, friends, and preferences. The features that Steam provide generally produce artifacts, many of which are redundantly stored on Steam Cloud Services.

Valve additionally provides support for VR systems and applications. The HTC Vive was co-developed with Valve and powered by SteamVR [32]. SteamVR is the hardware interface that initializes and drives the VR hardware. Although specifically designed for the HTC Vive, any VR system can utilize SteamVR, with added drivers, due to the OpenVR framework [33]. The nature of VR dictates that a great amount of information regarding the state of the system and the physical room be stored. This is used to calculate the location of tracked objects and provide player safety to obstacles in the room. The tracking devices, room configuration, and VR preferences are also stored in a collection of artifacts. This information is also stored via Steam Cloud Services, therefore, network traffic analysis may furnish forensically valuable artifacts.

In the following sections, we present the different social VR applications that were forensically explored in our work. We included these sections to inform readers not familiar with VR social applications and their features.

B. BigScreen

Bigscreen supports both the HTC Vive and Oculus Rift. It is a social VR application that allows VR immersed users to use their computers in the VE [34]. The application allows users not only to share their screens, but also to play Xbox One and PlayStation 4 games, YouTube videos, television, Netflix, and chat. Users are allowed to choose their own environment from a simple campfire to outer VEs.

Users can also sketch, doodle, and white board and customize the screen. The application allows multiple players in public and private rooms. The maximum number of players allowed in a public or private room is four, but the monitor

support is limited to three monitors (either physical monitors or virtual/emulated monitors). Like any other social application, the users can voice and video chat and share their computer screens with each other. One may think of BigScreen as a virtual Local Area Network (LAN) party.

C. Rec Room

[35] compares Rec Room to the likes of youth and recreation centers. The application allows users to engage in activities with other players, with more complex games in separate rooms. Players and their movements are represented through an avatar. Interactions between avatars have functionality, where groups can be formed through a handshake. At the time of writing, Rec Room offered six game rooms, such as Charades, Paintball, Soccer, etc.

Similar to other social VR applications, Rec Room allows players to customize their avatar and voice chat with other users. Additionally, this application allows users to conditionally filter interactions, muting or blocking other users. To further moderate socialization, private rooms prevent unwanted users from interfering or meddling with ongoing games. This feature is especially helpful for parental control.

D. AltspaceVR

AltspaceVR is one of the most popular social platforms for VR. Similar to the abovementioned applications, users can interact with others around the world, and play interactive games with friends day or night. This application lets users attend live events such as stand up comedies and music events.

According to [36], NBC news announced a new science series in VR. A couple took the next step and recited their vows on May 25, 2017 using Altspace VR. This application also allows user to voice chat and send messages to other users.

E. Facebook Spaces

[37], head of Facebook's social VR department, defined the Facebook Spaces application as an extension of who users are. Facebook Spaces not only allows users to chat and play games, but also allows customizing one's avatar based on their profile picture. Through Facebook Messenger, Facebook Spaces allows users to video or voice chat with friends and family who do not have a VR headset.

At the time of writing, Facebook Spaces was only available on the Oculus Rift and Oculus Touch.

III. Methodology

Applications were selected for testing by searching the Steam and Oculus stores for the keywords 'social', 'casual', and 'online co-op'. Candidate applications were then examined to confirm socialization as the primary purpose of the game. Although Steam does not disclose purchase statistics, we assumed that the user population would correlate to the quantity of user reviews. Applications that did not consistently have users present were not considered for evaluation. Selected applications and necessary drivers for the VR systems are presented in Table I.

An analysis of logical system artifacts and network traffic as a result of user activity was conducted. All testing was conducted in a controlled lab environment. Moreover, a sterile workstation was maintained to minimize irrelevant trace files and extraneous network traffic.

A. Apparatus

To facilitate multiplayer interactions in a controlled environment, two identical workstations were employed. The details of the computers are shown in Table 2. Additionally, this allowed for a known comparison of interaction between different VR systems (Figure 1). Testing was conducted utilizing both the HTC Vive and the Oculus Rift, the details of which are presented in Table 3.

B. Experimental Setup

Workstations were prepared by employing a factory reset and installing Steam and Oculus. An initial examination of the system was conducted to establish a baseline. The social application was then installed and a subsequent sweep of the system was conducted. User accounts solely for the purpose of testing were created for Steam and Oculus, in addition to new accounts for applications when required. A trial run was then conducted and Wireshark (version 2.4.1) was activated to capture network traffic.

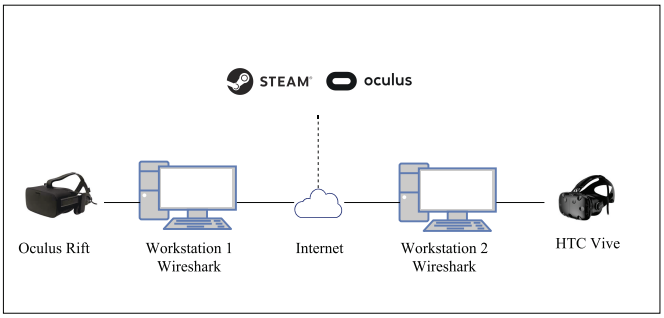

Fig. 1. Experimental Setup for Network Traffic Collection

C. User Activity Scenarios

Once the system was adequately prepared and network traffic collection was ongoing, the researchers commenced a series of activities. The social applications varied to some

TABLE I
Applications

Application	Version
Steam	1508273419
Oculus	1.20.02
SteamVR	1507941678
Bigscreen Beta	0.23.0
Rec Room	10
AltspaceVR	0.57.304
Facebook Spaces Beta	28.0.2507799

extent, thus trials were tailored to accommodate each. The activities conducted were analogous to that of a typical user experience. Performed events common to most applications were: joining and creating rooms, chatting, sharing content, and interacting with other users.

A detailed account of all activities performed was maintained and logged throughout the trials. For each, the event, application, time, user identity, and the identity of all other involved parties were recorded.

D. Analysis

Forensic examination of the collected data was conducted to determine if the activities performed on the VR social applications were stored on the system. The application files were compared to our baseline to identify traces resulting from the trial. Furthermore, a manual examination of all Steam, Oculus and social application logs was conducted for completeness. Evidence was typically found in a log intended for debugging. Network traffic was filtered to isolate only streams relevant to the social applications, Steam or Oculus. Manual examination of packet payloads was conducted to identify readily available information.

Details regarding the state of the system or user activity, uncovered from either artifacts remaining in long term storage or captured in network traffic, was recored.

IV. Summary of System Artifact Findings

A. Steam Artifacts

Multiple files related to the Steam application were found. Two folders were created: one in the program files (C:\ Program Files (86x)\ Steam) and another in the user's profile (C:\ Users\ Username\ AppData\ Local\ Steam). The first folder contained the appcache, backups, config files, controller data, logs, music, drivers, server details and userdata. The second folder contained the html cache details and Widevine modules. Widevine is the digital management system used by Steam to manage digital content.

The *httpcache* folder contained thousands of folders with details such as sites visited, HTTP responses and timestamps. The *stats* folder contained gaming statistics, such as achievements unlocked. The *appinfo* file contained the application id, application name, License type, application version and last updated information (Table IV, 1). The *config* folder contained the avatar preferences for each Steam profile and lighthouse data (Table IV, 2-4). Within the config directory, the lighthouse file contained the base station details, such as the last time Chaperone information was updated (Chaperone resembles the virtual boundaries of a user in a VE). Additional entries found in the lighthouse file contained the manufacturer details, master serial number, model number and tracking details, such as coordinates. The *vrappconfig* files indicate the launch time of different applications. The *chaperone_info* file contains the details of collision bounds, play area bounds and timestamp details (Table IV, 4).

Two authorization files were found hidden in the folder C:\ Program Files (86x)\ Steam and both could be used to bypass two-factor authentication. The *loginusers* file provided the account name, person name and timestamp of the most recent login (Table IV, 5). The directory C:\ Program Files (86x)\ logs holds the logs of the VR client and VR server, as well as application logs (Table IV, 1-11). The *connection_log.txt* file contained information regarding Steam connections, such as port details and number of connections established. The *content_log.txt* contained the logs of installed applications and included details such as IP addresses, Steam sites and timestamps (Table IV, 6). The *remote_connections* file contained timestamps and details of the system the Steam user utilized to log in(Table IV, 8).

The logs folder also contained the logs related to applications such as AltspaceVR, Bigscreen Beta, and Rec Room. These files contained splash screens with timestamps, which are used to load the settings of the applications. The file *vrserver.txt* contained the connections to lighthouse and also contained the logs of adding the base stations (Table IV, 17). The file *user_vr_vive.vcfg* contained the username associated with the Steam account, while the *localconfig.vdf* file contained the actual or given name of the Steam user.

Another Steam folder was created in the Documents folder of the system. This contained a number of SQLite and JPEG files related to the Steam applications. The SQL database files contained cookie-related details, such as cookie name, cookie expiry date and cookie value. Other located data files included details such as server sites, IP addresses, HTTP response codes, and date and timestsamps. Image files were located and examined, revealing that these files were cached from html pages previously accessed by Steam.

TABLE 3
Virtual Reality Devices

HTC Vive				Oculus Rift			
Device	**VID**	**PID**	**Firmware**	**Device**	**VID**	**PID**	**Firmware**
Hub	N/A	N/A	N/A	Rift	2833	0031	708/b1ae4f61ae
Hub Controller	0424	274D	N/A	Rift Audio	2833	0330	708/b1ae4f61ae
Bluetooth	N/A	N/A	211	Sensor x3	2833	0211	178/e9c7e04064ed1bd7a089
Watchman Board	28DE	2000	1462663157	Left Touch			f3c65f7a5f
Camera	0BB4	2C87	8590262295	Right Touch			f3c65f7a5f
Audio Device	0D8C	0012	3				
Main Board	0BB4	2C87	1.6				
Wireless Receiver 1	28DE	2101	C638F6E4EF				
Wireless Receiver 2	28DE	2101	90538B7D13				
Base Stations			436				

TABLE 2
SYSTEM DETAILS

Device	Details
Processor	Intel Core i7-6700 CPU
System Type:	64-bit OS, x64 processor
Graphics Card	NVDIA GeForce GTx 1070
Manufacturer	iBUYPOWER
Installed Memory (RAM)	8.00 GB

B. Bigscreen Beta System Artifacts

Bigscreen Beta was available for both the HTC Vive and the Oculus Rift, thus sterile accounts were created for testing both systems. Common activities such as creating rooms, joining existing rooms and chatting were performed on both. Data collection and analysis was then conducted for artifacts corresponding to both VR systems.

Artifact files were found stored in multiple locations on the system. The Steam-generated Bigscreen activity logs (vr-client_Bigscreen.txt) were stored in the previously discussed *Steam\logs* directory. The text file contained configuration settings for Bigscreen and responses from the vrserver. The file also contained the timestamps of application start time and end time, the System OS and version. No indicators of user activity were found in the file *vrclient_Bigscreen.txt*

```
(00:05:10.5236049): (00:05:13:239) Sending user state to new player =userid=user2
userName=labvr53 steamId=76561198437006377 oculusId= area=2 seat=0 isAdmin=False
environment=Living Room Day remoteUserSeatOrder=user2,,user1
(00:05:11.8586871): (00:05:14:574) Received user state =userid=user3 userName=Siena
steamId= oculusId=Dorkling area=0 seat=-1 isAdmin=False environment=
remoteUserSeatOrder=user3,,user1
00:05:12.6046693): (00:05:15:320) Received user state =userid=user1 userName=labvr5gffb
steamId=76561198435970010 oculusId= area=2 seat=2 isAdmin=True environment=Living
Room Day remoteUserSeatOrder=user2,,user1
(00:06:15.3093558): (00:06:18:024) Received user state =userid=user4 userName=grace
steamId= oculusId=DylanBennett area=2 seat=3 isAdmin=False environment=Living Room
Day remoteUserSeatOrder=user2,,user3,user4
```

Fig. 2. Big Screen Application Log

Application and user events were primarily logged in the directory SteamLibrary\ steamapps\ common\ Bigscreen\ Bigscreen_Data. Two log files, *output_log.txt* and *output_log2.txt*, were consistently produced in this folder. The *output_log2.txt* file contained the Interactive Connectivity Establishment (ICE) server responses and system display settings. The entry for HMD in *output_log.txt* indicated the type of VR headset (HTC Vive/Oculus Rift) the user had used. The *output_log.txt* file provided details of playback devices and audio output. The *output_log.txt* also contained the timestamps of scene initialization. As shown in Figure 2, the logs show user details and ID's, respectively. Given the Steam ID, profile details such as name, creation date, last login date, and location can be ascertained from a web database [38]. The log contained details of the virtual room, administrator, screen sharing information, environment chosen, and the seating order. All the social activities performed during testing are reflected in the logs, thus giving the chance to interpret and reconstruct the incident that occurred. Both log files were similarly produced when testing was replicated for the Oculus Rift, however, the corresponding directory was \ *Oculus*\ *Software*\ *Software*\ *bigscreen-bigscreen*\ *Bigscreen*\ *Bigscreen_Data*. The Bigscreen Beta development team produces these logs for the purpose of debugging user issues [39].

During testing, detailed accounts of activities were maintained to correlate the timestamps to relevant artifacts. Using the details of our activities as a baseline, the sequence of events is easily distinguishable within the logs. The scenario was constructed utilizing both the HTC Vive and the Oculus Rift, where the users created a room, joined a room, chatted, and shared videos. A general timeline of events is shown in Table V, with the corresponding log entry indicating the event. The remainder of this discussion will refer to Table V.

```
(00:00:00.0747036): CPU = Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
(00:00:00.0752047): Memory size = 8103
(00:00:00.0757062): GPU = NVIDIA GeForce GTX 1070
(00:00:00.3609628): SetPlaybackDevice index: 0 device Name=Speakers (3- USB
Audio Device) GUID=797236be-c20a-4b99-b1f5-924c3c871b64 connected=True
(00:00:00.3649738): SetPlaybackDevice index: 1 device Name=HTC-VIVE-4
(NVIDIA High Definition Audio) GUID=1a67552f-bc03-4994-84df-9b06508ebd53
connected=True
(00:00:00.3955549): SetPlaybackDevice index: 0 device Name=Speakers (3- USB
Audio Device) GUID=797236be-c20a-4b99-b1f5-924c3c871b64 connected=True
(00:00:02.7563296): OS = Windows 10  (10.0.0) 64bit
(00:00:02.7568308): OS = Windows 10
 (00:00:04.3218973): Plugin microphone input devices: [{ "type": "output",
"name": "HTC-VIVE-4 (NVIDIA High Definition Audio)", "default": "",
"audio_output_mirror_device": true},{ "type": "output", "name": "Realtek Digital
Output (Realtek High Definition Audio)", "default": "",
"audio_output_mirror_device": true},{ "type": "output", "name": "Speakers (3-
USB Audio Device)", "default": "", "audio_output_mirror_device": false},{ "type":
"input", "name": "Microphone (3- USB Audio Device)", "default": "Default",
"audio_output_mirror_device": false}]
```

Fig. 3. Artifact Containing System Information

Initialization of the application (Event 1), also signified by the creation of the log, was indicated by the date and time, followed by the Unity Version. This was of relevance given that all following timestamps are relative to this entry. The initialization procedure includes a survey of the system hardware and transfer of microphone and audio playback to the HMD. These log entries inform the investigator of the devices and software used. Figure 3 provides an example of hardware information discovered following a simulation with the HTC Vive.

Immediately following application initialization, the user was placed into a single player room (Event 2). Although explicitly stated in the log, the room can also be assumed to be single player from the lack of a room ID. In fact, the following event utilizes a room ID from when the user created a public, multiplayer room (Event 3). This attribute seems like a randomly generated tag for referencing the room and is independent of the room display name (not present in the logs). Public rooms populate in the application with a display name, however, private rooms may only be referenced via the room ID. No further authentication is required, thus this practice may be vulnerable to a Man-In-The-Middle (MITM) attack.

Event 4 shows the entry of the player *labvr53* into the room. Bigscreen does not route shared video and audio through their servers, instead it creates a peer-to-peer connection utilizing

TABLE IV
STEAM ARTIFACTS

	File Name	Location*	Content
1	appinfo.vdf	\Steam\appcache	App id, infostate, lastupated time, accesstoken (can be modified to rename the games as per the user locally to steam)
2	lighthousedb.json	\Steam\config	Manufacturer details, master serial number, model number, tracking coordinates
3.	vrappconfig files	\Steam\config\vrappconfig	Application launch times
4	chaperone_info.vrchap	\Steam\config	Collision and play area bounds
5	loginusers.vdf	\Steam\config	Steam ID, account name, user name, account creation date
6	content_log.txt	\Steam\logs	Contains information on every application downloaded, updated, or run through Steam.
7	connection_log.txt	\Steam\logs	Contains number of connections with Steam and port details.
8	remote_connections.txt	\Steam\logs	Logged communication between clients and port numbers.
9	broadcast_log.txt	\Steam\logs	Screenshot and video upload information for Steam broadcasting with timestamps.
10	cloud_log.txt	\Steam\logs	Log of information uploaded to the Steam Cloud, includes application names.
11	parental_log.txt	\Steam\logs	Parental control information.
12	runprocess_log.txt	\Steam\logs	List of applications run with ID's and start times.
13	streaming_log.txt	\Steam\logs	Streaming times and device information for Steam broadcasting
14	vrclient_vrcompositor.txt	\Steam\logs	Collision bounds, play area size
15	vrcompositor.txt	\Steam\logs	Collision bounds, display information
16	vrmonitor.txt	\Steam\logs	Device info, audio, video, bluetooth, startup, shutdown.
17	vrserver.txt	\Steam\logs	Vive info and its accessories activities, including startup display, communication

*Parent directory: C:\Program Files

ICE [1]. FMOD, a commonly used audio utility for applications created in Unity and Unreal, facilitated the transfer of microphone audio, the details of which are additionally included in the log [40]. Additionally, corresponding log entries are generated when audio and video streams are disposed of upon a user exiting the room (Event 5).

In addition to what is presented in Table V, Events 6 and 7, the joining of an ongoing party, are easily distinguishable given the large amount of simultaneous ICE offers and responses. Aside from the absence of an entry for room creation, we can ascertain the room was created by another user from the user state transactions. We can see from the Event 6 log, the user *Christy* is the administrator and the only user to specify the environment. Events 8 and 9 are indicated by the closure of all remaining data streams and are explicitly stated in the logs.

Although the contents of the data streams were not available in non-volatile memory, a reconstruction of major events is plausible through artifact analysis. Data relevant to the system state, as well as user information and activity, was found readily available and conveniently consolidated in log form.

[1]Interactive Connectivity Establishment (ICE) is a technique used in applications using video and voice to avoid communication through a central server as the central server introduces delay.

TABLE V
BIGSCREEN ACTIVITY AND ARTIFACTS

	Event	Log

1	Open Application	`12/12/2017 8:07:47 PM`
		`Unity version: 0.23.0`
		`UI version: 5.0`

2	Default Room Load	`(00:01.86): (00:08:214) Initializing scene` `(00:01.88): (00:08:234) Is in singleplayer room`

3	Create Room	`(00:51.12): (00:57:47) Reload scene, with user:`
		`user1 in room room-yhjdbg9b, enviro should be Living Room Day`
		`(00:51.48): (00:57:837) Is in multiplayer room`
		`(00:51.48): (00:57:838) Created room - Loading My User defaults`

4	New player enters room	`(01:01.37): ------------- NEW CONNECTION`
		`(01:01.37): (01:07:72) InitiatePeerConnection ... to user: user2`
		`(01:02.01): (01:08:36) NewUserJoinedRoom user2`
		`(01:05.58): Received user state =userid=user2 userName=labvr53`
		`(01:06.01): Sending user state to new player =userid=user1 userName=labvr54`

5	user2 Leaves Room	`(05:43.92): [UILog] user2 has left the room` `(05:43.93): (05:50:28) UI.DestroyPeerConnection`

6	Joining multiple player room	`(03:39.25): ------------- NEW CONNECTION`
		`(03:39.25): (03:42:43) InitiatePeerConnection ... to user: user2`
		`(03:39.25): (03:42:434) Is in multiplayer room`

7	Admin details	`(03:41.70): Received user state =userid=user3 userName=Christy`
		`steamId=76561198449315150 oculusId= area=0 seat=2 isAdmin=True`
		`environment=North Balcony remoteUserSeatOrder=,user3,user2`

8	Player Leaves Room	`(06:56.78): (07:03:13) UI.StopAllStreaming` `(06:57.78): (07:04:13) Reload scene, with user: user1 in room none`
9	Close Application	`(07:02.56): Exiter@OnApplicationQuit Successful`

TABLE VI
REC ROOM ACTIVITY AND ARTIFACTS

	Event	Log
1	Open Application	OpenVR initialized! UnloadTime: 1.798012 ms Connected to lighthouse:LHR-676305F7 Platform: STEAM, Hardware: VIVE Platform Profile Name: labvr53 Platform Tracking Mode: THREE_SIXTY_DEGREE
2	Failed Login attempts	RecNet login failed: Email is already in use
3	Login	Profile ID: 203970,Profile DisplayName: SteamingCrow Junior Profile: False SID: 1513369227130
4	Joining Dorm Room	Player joined activity "Dorm Room" with playerCount 1
5	Joining Rec Center	Player joined activity "Rec Center" with playerCount 7
6	Exit application	Releasing render texture that is set as Camera.targetTexture! OpenVR Shutdown

TABLE VII
ALTSPACEVR ACTIVITY AND ARTIFACTS

	Event	Log
1	Open Application	[1.496] Main: Init()... [2.917] Main: Loading version data... [2.921] Main: Authenticating unity... Device ID: 6d3d9d59-ccde-426d-9f8d-6f6ffd12493d Coherent Browser system initialized..|
2	Enter as Guest	Logged in as 780656450304212995 Guest52143385
3	Enter with username	Logged in as 823353831441039440 labvr53
4	Joining a room	[165.164] Connecting to Photon room 613940881048732244_16ed3ab11 Connect to: 54.214.112.182:5055 [166.040] Loading asset bundle https://dc1gsc5wc5y2l.cloudfront.net/environments/ GeometricCampfire/04/06/GeometricCampfire-040681f8.unity5... 100%
5	Playing Disc	[210.458] Started Travel to space disc-golf-lobby [250.936] Loading asset bundle https://dc1gsc5wc5y2l.cloudfront.net/environments/Disc/ df/22/Disc-df220b7f.unity5... 100%
6	Engaging in an activity	[319.936] Loading asset bundle https://dc1gsc5wc5y2l.cloudfront.net/environments/JungleMaze/ 00/b2/JungleMaze-00b24fbc.unity5... 100%
7	Leaving a room	[588.453] Started Travel to space experience-space-831179190551183822 Focus Changed from[SharedBrowser (WebBrowser)] to[] Left Room
8	Closing application	Quitting Unity

C. Rec Room Artifacts

Examination and analysis of both Steam and Oculus directories, as well as application specific folders, yielded a log similar to that of Bigscreen. For both systems, the file contained the profile name and platform and hardware information. Profile information specific to Rec Room was also found in *output_log.txt*. Events typical to the game were initiated, namely, entering the Rec Room, joining activities, chatting, and taking pictures and videos.

From this log, we were able to identify particular events and collect system information, as presented in Table VI. Upon application initialization, the user Steam ID is logged as well as a survey of hardware (Event 1). Rec Room requires an application specific profile and login, the details of which were found in the entries for Events 2 and 3. Note that Rec Room distinguishes between junior and adult users, the former of which is restricted from chatting and attending certain events [41]. Any transition between rooms or activities is likewise recorded in the logs (Events 4 and 5). Within rooms or activities, the user often records photos or videos; this media was found to be stored in the directory C:\ users\ username\ Documents\ Rec Room. Finally, the user can be observed to exit the application, as indicated by a release of resources and shutdown (Event 6).

The user activity and system information associated with this application were also conveniently located and consolidated, however, timestamps related to the log entries were not available. Given the sequence of events is preserved, an approximate time may be applied from related artifact modification timestamps.

D. AltspaceVR Artifacts

Examination of directories related to AltspaceVR, Steam and Oculus revealed a number of files containing relevant digital evidence. The most notable artifact, *output_log.txt*, was found in the default Steam application folder. In general, this output file contained the profile name, VE, and timestamped user activities, as shown in Table VII. The application was tested using both a user and guest account; the login identity of the user can be found in the entries shown for Events 2 and 3. The output file also provided the details of the games played by the user, such as a maze and disc game, as seen in Events 5 and 6. The user can be observed leaving the current activity in Event 7 and closing the application in Event 8. Though the gaming activities of the user have been logged

TABLE VIII
FACEBOOK ARTIFACTS

	File Name	Location**	Contents
1	output_log.txt	\facebook-vr-facebookvr\FacebookSpaces_Data	User name, activity log
2	fbrti_*.txt	\facebook-vr-facebookvr\fbrti_logs	Audio and video details
3	FBCaptureSDK.txt	\facebook-vr-facebookvr	Log of video codec and audio device details
4	*	\facebook-vr-facebookvr	User friends' profile pictures
5	avatar2	\facebook-vr-facebookvr\FacebookSpaces_Data \StreamingAssets\Avatar2\Win64	User profile picture

* File name generated from timestamp **Parent Directory: D:\Oculus Apps\Software

with timestamps, activities such as sending a friend request and chatting within the application were not found in this file.

The folder C:\ users\ username\ AppData \ LocalLow \ AltspaceVR \ Unity contained the unity logs of settings such as the config and platform rules, along with timestamps. This also contained the AltspaceVR Version and username.

E. Facebook Spaces Artifacts

Facebook, the parent company to Oculus, did not extend Facebook Spaces to Steam, thus testing was solely for the Rift. Files related to Facebook Spaces were found in the folder D:\ Oculus Apps \ Software. The commonly observed log file (Table VIII, 1) was found to contain the user name, room ID and activity details.

The second file, *fbrti_*.txt*, contained the logs of control information for RTP[2] sessions. The created file name indicated the date of recent login. The file also contained the encrypted username fragment and password of Session Traversal Utilities for NAT (STUN) connectivity. STUN is a tool used by ICE to discover the presence of a network address translator in case of remote hosts. From the fbrti_*.txt file we found that the agent is a lite implementation in terms of Session Description Protocol (SDP) connectivity. SDP is used for multimedia session initiation. The file also included the Real Time Control Protocol (RTCP) attributes. Further analysis yielded forensically interesting results. In addition to all the abovementioned details, it also contained the number of audio calls made, if video was used in the call and the number of peers interacted with. The RTP session information found in the file fbrti_*.txt can be used to intercept traffic and

[2]Real-time Transport Protocol (RTP) is used in applications involving streaming media for the purpose of delivering audio and video over IP networks. RTCP carries the control information of RTP protocol.

TABLE IX
BIGSCREEN ACTIVITY AND NETWORK ARTIFACTS

	Event	Packet Payload Contents
1	Open Application	"steamid": "76561198437006377" "personaname": "labvr53" "lastlogoff": 1508536942 "profileurl": "http://steamcommunity.com/profiles /76561198437006377/" "timecreated": 1508532419
2	List of public rooms	"type":"room-latest","rooms":"roomId":"room-s5gdod","name":"test","description":"test", "participants":"1","category":"Chat","environment":"Living Room", "roomId":"room-z2eqbkac","name":"dudes","description":"chill","participants":"2", "category":"Chat", "environment":"Cinema", "roomId":"room-ln779blt","name":"Merlin's Madness","description":"3D Movies yahh mannn", "participants":"1","category":"Movies","environment":"Home Theater" "roomId":"room-jpmizamc","name":"fr musique","description":"","participants":"1", "category":"Movies", "environment":"Cinema"
3	Joining Room named "test"	"type":"user-joined","userId":"user2","state":"name":"test","description":"testing", "participants":"2","private":"0","category":"Chat","created.name":"steve", "created.uuid":"199fb0b1-591a-95c8-2473-449f00598f1f", "created.time":"1508537907183","environment":"Living Room","version":"0.22.1", "user1.desktop":"SQZ0c-KvcX--dwPqA1GK","user1.name":"steve" [snip] üser1ː1508537907386,üser2ː1508538138179","admin":"user1", "user2.desktop":"E3s9T_fiEe2OO_EKA1G5","user2.name":"TestingVR", "user2.uuid":"1b550094-bf1d-0c9e-d478-1f08bfe4d481","roomId":"room-s5gdod0d"
4	Desktop sharing	"type":"ice","value":"1bigscreen_sdp_mline_indexvideobigscreen_sdp_midcandidate:4285824 1 udp 2122260223 192.168.0.12 62419 typ host generation 0 ufrag kN90 network-id 1 network-cost 50", "fromUser":"user1","SCID":"79a99ace-f9fc-7cde-a02a-70665be4f2e4"
5	New user joining	"type":"user-joined","userId":"user3","state":"admin":"user1","created.uuid": "199fb0b1-591a-95c8-2473-449f00598f1f","user1.desktop":"SQZ0c-KvcX--dwPqA1GK", "version":"0.22.1","user3.name":"guillaume37","description":"testing", "user3.desktop":"H9x9x7sV6ocTLL7PA1HD","name":"test","category":"Chat", "participants":"3", "user2.uuid":"1b550094-bf1d-0c9e-d478-1f08bfe4d481", "user3.uuid":"b72349fe-7186-7fef-71ed-e508b8c70e84","created.name":"steve", "user1.uuid":"199fb0b1-591a-95c8-2473-449f00598f1f","time": "üser1ː1508537907386,üser2ː1508538138179,üser3ː1508538251220

potentially eavesdrop on user calls. This makes the application potentially vulnerable to session hijacking and other attacks.

The third file located, *FBCaptureSDK.txt*, contained video and audio codecs, bit rates, frame timestamps and audio device names that were used. The profile pictures of the user's friends were saved in the default Oculus folder. All the files discussed above were created and stored in two different places in the system - one in the Oculus Apps default folder and one in the documents folder of the system.

V. Network Artifact Findings

Three of the four social applications tested employed a secure protocol. Our initial work did not focus on breaking security protocols. Low-hanging fruit packet inspection was not possible for network traffic collected from these applications, however, much of Bigscreen's communications were unencrypted.

During testing, various activities were performed to generate data in real time. The activity and corresponding details related to Bigscreen events were located and the corresponding logs listed in Table IX. Transport Control Protocol (TCP) streams relevant to Bigscreen were identifiable given the contents of the HTTP Get request. Streams that contained the strings 'steamid' and 'person name' were isolated using the filter "tcp.stream eq *x*". Details such as username, steam profile ID, last log off time and timestamp of profile creation were found in cleartext during the initialization of the application (Event 1). As discussed in Section IV-A, from this information we were able to retrieve profile photos and public details. Bigscreen uses the WebSocket protocol for client-server exchange. The WebSocket Protocol empowers two-path correspondence between a user running untrusted code in a controlled situation to a remote host that has selected in to interchanges from that code. The convention comprises of an opening handshake taken after by fundamental message surrounding, layered over TCP [42]. This protocol was filtered by using "tcp.stream eq 24" to intercept details of the room. Event 2 indicates the room details that were exchanged between the client and server and, in this case, the system and Bigscreen server. The room details include room ID, room name, number of participants per room, description and the environment chosen.

Event 3 shows the user joining a public room named "test". Details, such as room administrator and room creation time, are seen in cleartext. Besides a username, a unique user ID is associated with every user for authentication. A random identifier was associated with every user's desktop. Multiple offer requests were noticed with RTP streams, indicating a shared video, as seen in Event 4. However, the content of data streams were encrypted. A new update was exchanged every time a new room was created or a new user was added. Event 5 shows a new user, *guillaume37*, joining the room. Closing the application disconnects all the ICE connections and STUN sessions.

All data related to the Bigscreen application can be used to reconstruct events. As the data in the Bigscreen application is not encrypted, the application is potentially vulnerable to many attacks, such as MITM.

VI. Discussion

For all applications tested, we were successful in reconstructing the general course of events. Many of the events are tagged with precise timestamps, allowing an investigator to tie these events to auxiliary evidence. In all cases, the user identity was observable, providing non-repudiation to the system. Should investigators require proof of interaction with particular individuals, this was observable in Bigscreen, Rec Room and Facebook Spaces. Many of the in-game events a user would typically perform per application, were also inferable from the logs.

A consistency for name and location was found regarding the logs intended for debugging. This is likely an artifact of application development occurring in identical game engines (Unity). The similar manner in which the logs are constructed and stored is also advantageous to the forensic examiner.

Although the contents of the audio and video streams were not accessible due to encryption, the information uncovered in the network logs may allow an adversary to hijack or eavesdrop on the user sessions. A MITM attack against Bigscreen is certainly plausible given the lack of encryption, which could leak identifying information. With this information, an attacker will be able to inject themselves into a private room, as no further authentication is required.

VII. Future Work

Our selection of social applications is a snapshot of the current state of content available. The market share for virtual socialization has yet to converge, thus we expect continued competition and creation of social applications. As newcomers enter the ecosystem and resident applications update, continued cataloging of artifacts pertinent to digital investigators is warranted. For example, Bigscreen announced an update, *Big Room*, allowing an unlimited number of users at a time [43]. Features such as this may yield a large amount of identifiable information, however, changes in protocol and privacy improvements may nullify previous work.

Virtual socialization is not limited to the genre of applications our study encompassed. Both the HTC Vive and Oculus Rift include a microphone as a standard feature and many applications allow multiple players. The application is the vessel in which the players congregate and mingle; a possibility for a wide variety of applications, to include all multiplayer cooperative games. We cannot assume the activity of interest for a digital investigator will have occurred in a social application, thus further analysis of VR applications, regardless of genre is appropriate.

A recent update to Steam allowed user preferences, game progress, and system data to be backed-up to the Steam Cloud. Further analysis of the protocols and access privileges for this information may reveal additional points of data collection. The HMD, being a complex piece of hardware, may also maintain information regarding the system state post-use. Extracting the HMD state and location directly from the hardware may be advantageous should the workstation driving the VR system be unavailable due to evidence preservation.

To aid future VR investigations, we intend to create tools to rapidly extract and reconstruct events from artifacts discovered in this study. As a comprehensive catalog may not be plausible, a solution incorporating block hash matching, as described by [44] may relieve man hours associated with manual cataloging.

VIII. Conclusion

At the time of writing, there were no studies that have addressed the forensic analysis and recovery of activities performed through social VR applications on the HTC vive and Oculus Rift. Our work focused on the recovery of artifacts and traces related to use of social VR applications on two different platforms; HTC Vive and Oculus Rift. This study aimed to determine if the activities that were performed through these applications were stored and may be recovered from user's system/network. The tested social VR applications were Facebook Spaces, AltspaceVR, Steam, Rec Room and Bigscreen.

Our results showed that significant amount of data related to Bigscreen, Steam and Facebook Spaces may be recovered. No traces of Oculus application could be easily ascertained from the system.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1748950. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] M. V. Sanchez-Vives and M. Slater, "From presence to consciousness through virtual reality," *Nature Reviews Neuroscience*, vol. 6, no. 4, pp. 332–339, 2005.

[2] G. Riva, "Virtual reality: an experiential tool for clinical psychology," *British Journal of Guidance & Counselling*, vol. 37, no. 3, pp. 337–345, 2009.

[3] I. E. Sutherland, "A head-mounted three dimensional display," in *Proceedings of the December 9-11, 1968, fall joint computer conference, part I*. ACM, 1968, pp. 757–764.

[4] Statista, "Number of social media users worldwide 2010-2021," 2017. [Online]. Available: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[5] E. Asano, "How much time do people spend on social media? [infographic]," Jan 2017. [Online]. Available: https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic

[6] R. McKie, "Virtual reality headsets could put childrens health at risk," 2017. [Online]. Available: https://www.theguardian.com/technology/2017/oct/28/virtual-reality-headset-children-cognitive-problems

[7] J. C. Wong, "Sexual harassment in virtual reality feels all too real 'it's creepy beyond creepy'," 2016. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr

[8] M. A. Lemley and E. Volokh, "Law, virtual reality, and augmented reality," 2017.

[9] Brown and Nelthrope vs Kilpatrick, 2008. [Online]. Available: http://media.freep.com/documents/stefani042908/0429stefani.pdf

[10] Department of Justice, "Retention period of major cellular providers," August 2010, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

[11] R. E. Grinter, L. Palen, and M. Eldridge, "Chatting with teenagers: Considering the place of chat technologies in teen life," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 13, no. 4, pp. 423–447, 2006.

[12] R. K. Garrett and J. N. Danziger, "Im= interruption management? instant messaging and disruption in the workplace," *Journal of Computer-Mediated Communication*, vol. 13, no. 1, pp. 23–42, 2007.

[13] A. Kobsa, S. Patil, and B. Meyer, "Privacy in instant messaging: An impression management model," *Behaviour & Information Technology*, vol. 31, no. 4, pp. 355–370, 2012.

[14] J. Reust, "Case study: Aol instant messenger trace evidence," *digital investigation*, vol. 3, no. 4, pp. 238–243, 2006.

[15] M. Dickson, "An examination into aol instant messenger 5.5 contact identification," *digital investigation*, vol. 3, no. 4, pp. 227–237, 2006.

[16] M. Dickson, "An examination into msn messenger 7.5 contact identification," *digital investigation*, vol. 3, no. 2, pp. 79–83, 2006.

[17] M. Dickson, "An examination into yahoo messenger 7.0 contact identification," *digital investigation*, vol. 3, no. 3, pp. 159–165, 2006.

[18] M. Kiley, S. Dankner, and M. Rogers, "Forensic analysis of volatile instant messaging," *Advances in digital forensics IV*, pp. 129–138, 2008.

[19] N. Al Mutawa, I. Al Awadhi, I. Baggili, and A. Marrington, "Forensic artifacts of facebook's instant messaging service," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. IEEE, 2011, pp. 771–776.

[20] I. M. Baggili, R. Mislan, and M. Rogers, "Mobile phone forensics tool testing: A database driven approach," *International Journal of Digital Evidence*, vol. 6, no. 2, pp. 168–178, 2007.

[21] M. Al-Zarouni, "Mobile handset forensic evidence: a challenge for law enforcement," 2006.

[22] A. Azfar, K.-K. R. Choo, and L. Liu, "An android social app forensics adversary model," in *System Sciences (HICSS), 2016 49th Hawaii International Conference on*. IEEE, 2016, pp. 5597–5606.

[23] J. Farnden, B. Martini, and K.-K. R. Choo, "Privacy risks in mobile dating apps," *arXiv preprint arXiv:1505.02906*, 2015.

[24] A. Mahajan, M. Dahiya, and H. Sanghvi, "Forensic analysis of instant messenger applications on android devices," *arXiv preprint arXiv:1304.4915*, 2013.

[25] A. Levinson, B. Stackpole, and D. Johnson, "Third party application forensics on apple mobile devices," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011, pp. 1–9.

[26] N. Statt, "Whatsapp has grown to 1 billion users," 16 February 2016. [Online]. Available: https://www.theverge.com/2016/2/1/10889534/whats-app-1-billion-users-facebook-mark-zuckerberg

[27] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. R. Weippl, "Guess who's texting you? evaluating the security of smartphone messaging applications."

[28] D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of android social-messaging applications," *Digital Investigation*, vol. 14, pp. S77–S84, 2015.

[29] F. Karpisek, I. Baggili, and F. Breitinger, "Whatsapp network forensics: Decrypting and understanding the whatsapp call signaling messages," *Digital Investigation*, vol. 15, pp. 110–118, 2015.

[30] J. Ullrich, T. Zseby, J. Fabini, and E. Weippl, "Network-based secret communication in clouds: A survey," *IEEE Communications Surveys & Tutorials*, 2017.

[31] Valve Corporation, "Steam, the ultimate online game platform," Dec 4 2017, http://store.steampowered.com/about/.

[32] V. Corporation, "Htc vive on steam," Dec 4 2017, http://store.steampowered.com/app/358040/HTC_Vive/.

[33] J. Ludwig, "Openvr api documentation," 2017, https://github.com/ValveSoftware/openvr/wiki/API-Documentation.

[34] Bigscreen Inc, "Bigscreen," Dec 14 2017, http://bigscreenvr.com/.

[35] James Bricknell, "Rec room is the most fun you can have in vr," Nov 21 2017, https://www.vrheads.com/what-makes-rec-room-so-fun.

[36] AltspaceVR Blog, "nbc-news-announces-new-science-technology-series-vr/," June 6 2017, https://altvr.com/nbc-news-announces-new-science-technology-series-vr/.

[37] Rachel Franklin, "Facebook spaces: A new way to connect with friends in vr," Sep 16 2017, https://newsroom.fb.com/news/2017/04/facebook-spaces/.

[38] SteamID I/O, "Steamid i/o," 2017. [Online]. Available: https://steamid.io/

[39] Bigscreen Inc., "Bigscreen debug logs," 2017. [Online]. Available: http://bigscreenvr.com/help/faq/debuglog/

[40] Firelight Technologies, "Fmod," 2017. [Online]. Available: https://www.fmod.com/

[41] Rec Room Blog, "Help center," 2017, https://www.againstgrav.com/help-center/.

[42] I. Fette, A. Melnikov, "The websocket protocol," 2011. [Online]. Available: https://tools.ietf.org/html/rfc6455

[43] D. Shankar, "Hang out with tons of friends in the new big rooms update," 14 December 2017. [Online]. Available: https://blog.bigscreenvr.com/hang-out-with-tons-of-friends-in-the-new-big-rooms-update-f1540153a98b

[44] M. Kaya and M. Eris, "Hash based block matching for digital evidence image files from forensic software tools," *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 11, no. 10, pp. 1068–1071, 2017.