Background

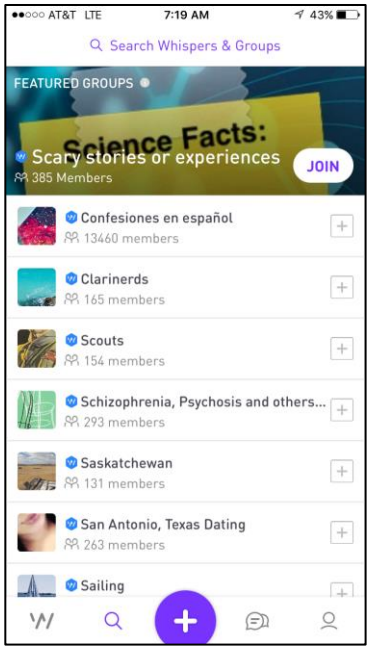
WhisperText LLC was co-founded in 2011 by CEO Michael Heyward and Brad Brooks, who also is the co-founder and the CEO of TigerText. Their mobile app, Whisper, launched in March 2012, and in December of 2015 the company announced that they had 20 million active users in 187 countries, doubling the number of users that it had six months prior to that (O'Brien). As of January 9, 2017 the app description in the Apple App Store and Google Play for Android devices states that there are 30+ million users every month. According to Whisper's website:

> Whisper is the largest online platform where people share real thoughts and feelings, forge relationships and engage in conversations on an endless variety of topics—without identities or profiles. Whisper content and stories reach hundreds of millions of people each month across platforms. Whisper is spearheading a movement that believes that happiness starts with being your real self. Whisper is backed by venture investors including Sequoia Capital, Lightspeed Venture Partners, Thrive Capital, Shasta Ventures, Trinity Capital, and CAA Ventures. ("Whisper Press" 2016)

What Is Whisper?

According to the application's law enforcement guidelines, Whisper:

Allows users to communicate without providing or disclosing their identities by posting content for public viewing and sending private messages. Most content on Whisper is posted publicly, so the public, including law enforcement, can view it at any time. Whisper is unlike other services because Whisper users do not register for unique Whisper accounts and do not generally provide to Whisper their names, email addresses, phone numbers, or similar identifying information. Because of the nature of Whisper's service, Whisper does not have information about users' names, email or physical addresses, phone number, or payment accounts. Whisper does assign a non-unique display name to each user. Multiple users may be assigned the same display name and users can change their assigned display name at any time and as many times as they like. ("Whisper Legal" 2016)



Whisper can be accessed via web browser, http://whisper.sh, where the public can view whispers that contain text entered by users which is superimposed onto randomly generated pictures from Whisper. Users can also select pictures for their whispers by choosing from Whisper-generated images and animated gifs, selecting "camera" to take a new picture, or choosing an image already stored on their mobile device. Via web browser, the public can view whispers grouped by topic or can use the search feature to look for particular keywords, but that is the extent of the website's capabilities. The only way to post, reply, chat, see other replies, or view location information such as city and state is by downloading the Whisper app to a mobile device.

***Additional features*:**

Groups: A user can select the "Group" button at the top of the app upon login and have the option to "Create a Group" where they get to pick the group name, background image for the group, and add a description for the group. They could also select "Add My School," which allows them to see or post whispers for that school once they arrive on campus. The school will be unlocked when they select "I'm on campus" and the request has been submitted. This feature uses the location services of the mobile device to ensure users aren't picking schools they haven't been to, and it appears once a school is selected, the user does not have the option to add a different school until the previous one is removed. Finally, a user can "Find a Group" by searching based on keyword, which will display the group name and current amount of members in the results.

Popular: The "Popular" button at the top of the app provides a listing of the most popular whispers, presumably generated by the number of "hearts" and/or replies each whisper has. After selecting a whisper, users can view information about it including the poster's display name, city/state/country (if available), approximate time/date of posting (i.e. hours/days/weeks from the current time), the number of "hearts" it has, the number of replies it has, and the content of those replies. Users can also reply to a whisper or initiate a chat with the poster. Other options are to "share whisper," "invite user to group," or "flag whisper."

Nearby: The "Nearby" button at the top of the app provides a listing of whispers close to a user's location. This feature works only if location services on the user's mobile device are enabled. This feature provides the same capabilities and options for interacting with a whisper as the "Popular" feature.

Latest: The "Latest" button at the top of the app provides a listing of the most recent whispers, typically shown by minutes since posting in relation to the current date and time. This feature provides the same capabilities and options for interacting with a whisper as the "Popular" feature.

At the bottom of the app, users can view whispers, search for whispers based on keywords, add a whisper, and view their chats and favorited whispers; or see their own previously posted whispers, the number of "hearts their whispers have, and the replies to their whispers. Their chats, replies, previous whisper information, "hearts", and replies to their whispers can be protected by a PIN. It appears once that is entered the user does not have to reenter it until the app is completely closed and reopened.

Importance to Law Enforcement

Whisper's purported anonymity and non-unique display names can make it challenging for law enforcement to obtain the information needed for potential investigations. Obtaining information based on username alone may not be possible due to the ease of changing display names. There are other digital artifacts that could potentially assist within an investigation and lead to an arrest. Illegal activity through Whisper has been documented in various cases such as a case in Woodbury, Minnesota in which a 25-year-old sex offender was soliciting a 15-year-old girl for sex, as well as requesting her to send nude pictures. Police in Bolton, Massachusetts were able to arrest a teenage girl for making a threat to her school on Whisper stating she was "gonna pull a columbine…before I graduate."

Investigative Information

Information Obtained from Whisper

Whisper is located at 69 Windward Avenue, Venice, CA 90291. Legal process can be served through email at law@whisper.sh or Facsimile: 310-421-9200. Law Enforcement requests must include:

- The user's Whisper display name.
- An image of the user's public Whisper post, the precise text of the particular Whisper with respect to which information is sought, or the unique URL for the public Whisper about which the legal process is seeking information.
- The specific information (e.g., usage data) that is requested and its relationship to your investigation.
- The date by which a response is requested.
- Whisper will not disclose user information or content to a U.S. governmental entity unless it is presented with a valid subpoena, court order, search warrant, or other legal process issued by a United States court or that entity.

- Whisper responds to preservation requests issued under 18 U.S.C. § 2703(f). Preservation requests must identify the Whisper and information to be preserved with specificity.

  Because Whisper display names are not unique, it is not possible to identify a particular user account by a display name alone and therefore Whisper cannot guarantee that it will be able to identify any particular user based solely on information pertaining to a public Whisper.

  If there is a life-threatening emergency Whisper states that it may disclose information or content to U.S. governmental entities without receiving legal process when they believe, in good faith, that an emergency involving a danger of death or serious physical injury to any person requires disclosure without delay.

  If a U.S. governmental entity believes that such an emergency exists, it should provide to Whisper the following information, in writing, via the contact information provided below:
  1. A summary of the emergency;
  2. An explanation of how the emergency involves a danger of death or serious physical injury that requires disclosure of the records sought without delay;
  3. An explanation of how the requested communications relate to the emergency; and
  4. An explanation of why the emergency precludes the entity from obtaining legal process.

  In addition, Whisper requires the following information to verify that the emergency request is from a U.S. law enforcement authority:
  - Requesting Agency name;
  - Requesting Agent name; and
  - Requesting Agent and Agency work contact information, such as a governmental email address, phone number, fax number, or mailing address.

According to Whisper's law enforcement guidelines the following data is available:

> "Whisper stores content posted for public viewing and usage data, including session times and location information, in accordance with its Privacy Policy and Terms of Use. Location information may not be available, for example, when it is not transmitted to Whisper. Whisper may retain for a limited time certain IP addresses associated with a device that accessed Whisper, but Whisper is not able to match posted content with an exact IP address." ("Whisper Legal" 2016)

But according to the Privacy Policy located at http://whisper.sh/privacy, users are notified of the information collected and used by Whisper, which appears to indicate there may possibly be more information for law enforcement to recover, and that includes:

Information you provide to us:

- *Account Information:* When you use our mobile application, a username will be randomly assigned to you that you may change or delete at any time. Your username is publicly displayed when you interact with the Services, such as when you post a whisper or send a chat message to another user. Please keep in mind that if your username contains your real name or is the same as how you identify yourself on other online services, people who see it may determine your identity. We may also ask you for, or you may choose to provide, additional information, such as age or gender, that will be associated with your Whisper account.
- *User Content:* When you interact with the Services, we collect the information and content you create. For example, we collect the text and/or image content of your whispers, replies, and chat messages. All whispers and replies are public and are publicly displayed (for information about deletion of whispers, please see "Your Choices" below). They may be viewed, shared and modified by our users, us and others for commercial or personal purposes (consistent with the rights and licenses in our **Terms of Use**). Please keep in mind that if you include information that could identify you in the text or image of a whisper, people who see it may determine your identity. Whisper does not post chat messages publicly but, as with any message that you send via any service, the recipient might do so.
- *Other Information:* You may provide other information directly to us. For example, we may collect information when you fill out a form, update your account, interact with the Services, apply for a job at our company, communicate with us via third-party social media sites, request customer support or otherwise communicate with us.

OTHER INFORMATION WE COLLECT WHEN YOU USE THE SERVICES

- *Location Information:* Many features of the Services will not work unless you provide us with some information about your location. If you consent to the collection of location information (e.g. if you permit your mobile device to send us your latitude and longitude), we will collect and use this information both while you are directly using the Services and in the "background" (i.e. at times when you are not directly using the Services), so that we can tailor your interactions and experiences with the Services and to provide more relevant advertising to you on our Services and other websites and mobile applications. For example, we or our advertising partners may show you whispers from people around you or places you frequently visit, notifications of things happening around you in real time, or advertisements from businesses near your location. If you do not permit your mobile device to provide us with location information, or location information is not available from your device for technical reasons, we may use your IP address or information about the Wi-Fi SSID from which you access the Services to determine an approximate geographic location for your device. For more details about how you may control the collection of location information, please see "Your Choices" below.
- *Usage Information:* We collect information about your use of the Services, including

access times, pages and whispers viewed, user and whisper interactions (e.g. hearts, flags and replies) and other information about your interactions with us, the Services and other users. We use this information to, among other things, personalize your experience, provide and improve the Services, and monitor and analyze use of the Services.

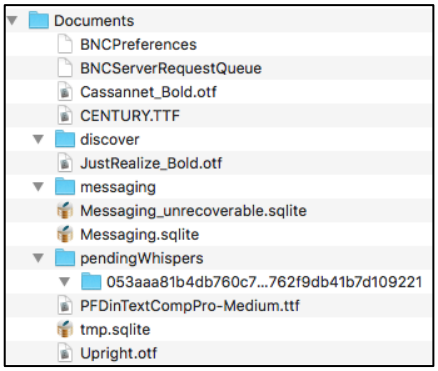
- *Device Information:* We collect information about the device you use to access our Services, which may include the hardware model, operating system and version, browser type and language, IP address, unique device identifiers and mobile network information. Among other things, we use this information to customize the Service for your device, to provide customer service and support, to deliver the products and services you request, to deliver notifications, for user safety, and for analytics and authentication.
- *Information Collected by Cookies and Other Tracking Technologies:* Like most websites and applications, we and our service providers use cookies, web beacons and other technologies to collect information. Cookies are small data files stored on your hard drive or in device memory that help us and our service providers to, among other things, improve our Services and your experience by seeing which areas and features of our Services are popular. For more information about cookies, and how to disable them, please see "Your Choices" below.
- *Log Information:* We collect information in our log files when you use the Services. This includes, among other things, your browser and device type, language, access times, pages viewed, your IP address, and the URL you visited before navigating to our websites. We use log information to provide, understand, and improve our Services. ("Whisper Privacy" 2016)

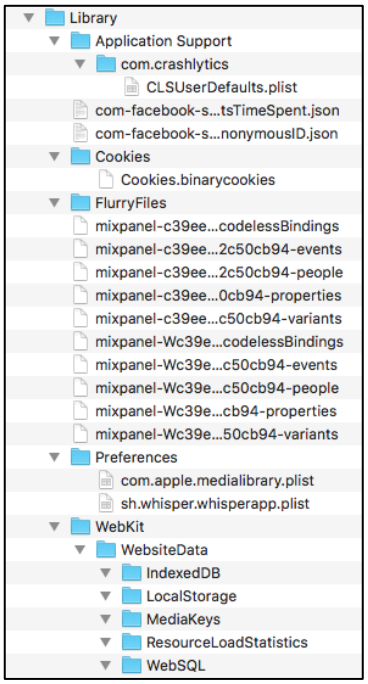
Information Retrieved from an iOS Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the Whisper application version 7.4.9 on an Apple iPhone 6 model MG4X2LL/A running iOS version 10.2. The test machine was an Apple MacBook Pro running MacOS Sierra. A logical extraction of the device was completed using BlackBag Technologies Blacklight 2016 Release 3. A search of the results and keyword search for the word "Whisper" located many artifacts during the examination. The files and folders of interest were exported then viewed manually with database and property list viewers.

- *Clients.plist* with the path of /root/Library/Caches/location/ had three values of interest recorded in Mac Absolute Time, and they included:
    - FenceTimeStarted – this appeared to be the last time that the app was opened.
    - LocationTimeStopped – this appeared to be the last time that the app was closed.
    - SignificantTimeStopped – this appeared to be the last time the user double-clicked the home button and manually swiped it to close it from running in the background.

- *Consolidated.db* with the path of /root/Library/Caches/Locationd/ contained a table of interest:
    - *Fences*: This table had a column called "BundleId" which had a value of sh.whisper.whisperapp in four different rows. These rows showed values of "10,100,500,1000" and there were two other columns, "Name" and "Distance," where every row had the same latitude and longitude of the last location where the Nearby button was selected when using the app.
- *DataUsage.sqlite* with the path of /wireless/Library/Databases/ contained a table of interest:
    - *zprocess*: A column in that table called "zprocname" had a value of whisper/sh.whisper.whisperapp and two corresponding columns titled "zfirsttimestamp" which appeared to have first time program was executed recorded in Mac Absolute Time, and "ztimestamp" which appeared to have last time program was executed, also recorded in Mac Absolute Time.
- *sh.whisper.whisperapp* was a folder with the path of /mobile/Applications/ sh.whisper.whisperapp/ that contained two subfolders, "Documents" and "Library."





- *Messaging.sqlite* with the path of /mobile/Applications/sh.whisper.whisperapp/Documents contained multiple tables of interest which included:
    - *zconversation*: This table appeared to contain the age (zage), approximate location (zdistanceorlocation), gender (zgender), and display name

(zpartnernickname) of the parties the user chatted with. It also included the user's display name (zrecommender), and some dates and times (zstartdate) and (ztimestamp) of the chats.

- *zfeed*: This table appeared to contain information about groups the user encountered either by searching groups or searching for a keyword to narrow down to a particular group. Columns included how many people liked the group (zheartcount), how many whispers the group had (zwhispercount), the last time a whisper was posted to the group (zlastwhisperpostedtimestamp), the name of the group (zdisplayname), a description of the group (ztribedescription), various url's for images related to the group, the search term used in finding a group (zquery), and if the group was a school had the address (zaddress).
- *zfeeditem*: This table appeared to contain information about whispers the user encountered. There was how many times people liked the whisper (zheartcount), how many times people replied to the whisper (zreplycount) timestamp (ztimestamp), url to the background image (zimageurlstring), the text superimposed on the image (ztext), distance away from the user if they used Nearby button in miles (zdistancequantity and zdistanceunits), the approximate location of the poster (zlocation), the posters display name (znickname), the feed it was posted to (zpostedtofeedname), and other various url's to images for the post.
- *zmessage*: This table appeared to contain the chats between the user and other parties. The column "zmine" indicated if the user sent the message with the value of "1" or if they received it with the value of "0." It also showed if it was read (zread), sent (zsent), the date and time (ztimestamp), and the actual content of the message (ztext).
- *znotification* table: This table appeared to show when notifications were sent (ztimestamp) to the user and what kind of notification it was (ztype).

- *sh.whisper.whisperapp.plist* with the path of /mobile/Applications/sh.whisper.whisperapp/Library/Preferences contained multiple items of interest including but not limited to the "BITStoreUpdateLastStoreVersion" which appeared to be the version number, as well as the date and time the "user_pin_validated."

In a second test on a machine running Windows 8.1 Enterprise 64-bit and a logical extraction of the device was completed using MSAB's XRY v. 7.2 64-bit. A search of the results and keyword search for the word "Whisper" using XRY Reader 6.19.0 located many artifacts during the examination and XRY categorized keyword hits into various categories. The files found appeared to be the same ones that Blacklight found in its extraction. One of the biggest differences is that the hits to the word "Whisper" that Blacklight identified in *DataUsage.sqlite* with the path of /wireless/Library/Databases/ did parse out actual data usage information. XRY

went a little further by matching up the information from multiple tables in the database and was able to produce usage statistics of the time used, Traffic In (Cellular), and Traffic Out (Cellular) in the "Event Log" category which would otherwise have to be manually converted. Other databases, property lists, pictures, and videos were exported to confirm the contents matched those found with Blacklight, and they did. The one key difference was that, when the files were found and the path was examined, it was not exactly as found in Blacklight. For example, a file was found in Blacklight and had a path of /mobile/Applications/sh.whisper.whisperapp/Documents/, but when it was found in XRY the "Path" column showed

/private/var/mobile/Containers/Data/Application/sh.whisper.whisperapp/Documents/. Depending on the tool used to examine the device there could be a slight difference in paths according to how the tool interpreted that data, but the information from Blacklight such as the content of in the databases, property lists, etc. still was the same. There did not appear to be any extra information of interest found that was not recovered by Blacklight.

Information Retrieved from an Android Device

The NW3C Cybercrime Section downloaded, installed, and used the Whisper application version 7.4.8.1261 on a Samsung Galaxy S7 model SM-G930U running Android version 6.0.1 Marshmallow. The test machine was an Apple MacBook Pro running MacOS Sierra. A logical extraction of the device was completed using BlackBag Technologies Blacklight 2016 Release 3. A search of the results and keyword search for the word "Whisper" located many artifacts during the examination. The files and folders of interest were exported then viewed manually with database and property list viewers.

- *c.db* with the path of /apps/sh.whisper/db/ contained two tables of interest:
    - *c* table: This table appeared to contain chats between the user (sid) and other individuals (pid). It also had the content of the message (Im), the date and time sent (ts), the age in the other individual's profile (profile_age), and that person's listed gender (profile_gender).
    - *m* table: This table also had the content of the chat (text) and the date and time of sending (ts).
- *w.db* with the path of /apps/sh.whisper/db/ contained two tables of interest:
    - *n* table: This table appeared to contain the type (type) of notification sent to the user, the message sent with it (message), and the date and time it was sent (ts).
    - *w* table: This table appeared to contain whispers the user viewed. It had the poster's display name (user), date and time stamp (ts), url's where the images were stored (url), the city and state of the poster (location), the text the user entered (text), how many likes the whisper received (hearts), how many replies the whisper received (replies), what group it was posted to (to_place_display_name), and only five replies (replies_list) to the whisper even if there were more. It should be noted that multiple logical extraction were

performed over a week long period, and whispers that were in the database on Jan 4, 2017 were not located on Jan 9, 2017. Many attempts were made to replicate the purging of the database or to determine why entries are missing but none have been found. The app was killed as a background running process, and the phone was even shut off then turned back on, but all whispers from earlier in the day still appear in the database. It is unclear if it is purged after so many days or if there is a limit to how many entries the database will store. In order to get the most accurate information an extraction should be done as soon as possible without opening the app possibly overwriting data.

- *me* was a folder with the path of /apps/sh.whisper/f/ that had files without extensions, but they were identified as .jpg image files with a hex editor and had the image of the whisper that the user posted.
- *app_whisper* was a folder with the path of /apps/sh.whisper/r/ that had files with the extensions of .0 or .1, and the .1 files appeared to be the whispers with animated gif's as their background. If these files were opened with a media player the examiner could see the whisper with text and background animated gif. The .0 files with the same name appeared to have identifying information about the images/videos.
- *sh.whisper_preferences.xml* with the path of /apps/sh.whisper/sp/ appeared to contain the latitude (lattitude_prefs_key) and longitude (longitude_prefs_key) of the last location used for Nearby button. It also contained the users display name (nickname), identified if the pin is turned on (pin_exists), and what the four-digit PIN is (PIN).

In a second test on a machine running Windows 8.1 Enterprise 64-bit and a logical extraction of the device was completed using MSAB's XRY v. 7.2 64-bit. A search of the results and keyword search for the word "Whisper" using XRY Reader 6.19.0 located many artifacts during the examination and XRY categorized keyword hits into various categories. XRY listed the installed app as "Whisper" and the package name as "sh.whisper." Also the files found appeared to be the same ones that Blacklight found in its extraction. Multiple databases, property lists, pictures, and videos were exported to confirm the contents matched those found with Blacklight, and they did. The one key difference was that when the files were found and the path was examined it was not exactly as found in Blacklight. For example, a file was found in Blacklight and had a path of /apps/sh.whisper/f/, but when it was found in XRY the "Path" column showed /data/data/sh.whisper/files/ and the "Misc" column showed /apps/sh.whisper/f/. In order to clarify the path a little further the phone was connected to an Apple MacBook Pro and the adb (Android Device Bridge) command was used to connect to the phone and view a listing of the folder structure. ABD reported the path to be /data/data/sh.whisper/files/ proving that depending on the tool used to examine the device there could be a slight difference in paths according to how the tool interpreted that data. While it was the "Misc" column as opposed to the "Path" column from XRY that matched the "Browser" view from Blacklight the content of in the databases, property lists, etc. still was the same. There did not appear to be any extra information of interest found that was not recovered by Blacklight.

Feedback

For additional information or suggestions please contact cyberalerts@nw3c.org

Sources

O'Brien, Sarah A. "Whisper: 20 million people are sharing secrets on this anonymous social app." CNNMoney. December 11, 2015. Accessed January 6, 2017. http://money.cnn.com/2015/12/11/technology/whisper-20-million-users-privacy/.

"Whisper Legal." Whisper. 2016. Accessed January 6, 2017. http://whisper.sh/legal.

"Whisper Press." Whisper. 2016. Accessed January 6, 2017. http://whisper.sh/press.

"Whisper Privacy." Whisper. 2016. Accessed January 6, 2017. http://whisper.sh/privacy.

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

©2016. NW3C, Inc. d/b/a the National White Collar Crime Center. All rights reserved.