



QUICK REFERENCE GUIDE

VOIPS / TEXTING APPS

INTRODUCTION

This quick reference handbook is designed to accompany the various **Social Media Investigations Courses** instructed by GBG Consulting, LLC. and Tradecraft Training.

Typically, when we use our preferred tool (TraX, CellHawk, Etc.) to look up a phone number being utilized by a suspect in a case we're working, we expect to see a major carrier: **Verizon Wireless, T-Mobile or AT&T Wireless.**

But from time to time, we may get an unexpected result we don't fully understand:

**LAW ENFORCEMENT**
Phone Carrier Lookup Tool

PHONE NUMBER

(707) 238-1190

SEARCH

CARRIER RESULTS

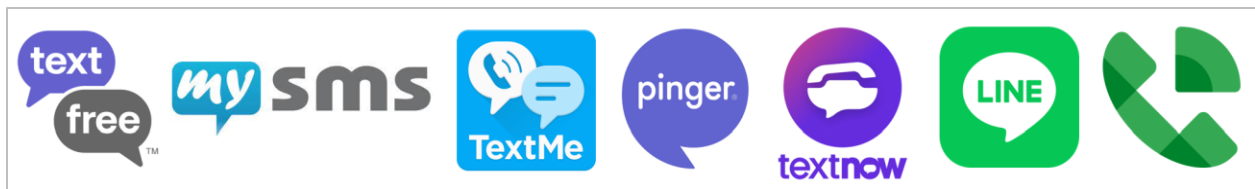
RESULTS FOR CARRIER SUBSCRIBER	(707) 238-1190 Bandwidth.com Unknown
--------------------------------	---

An unfortunate reality: Sometimes, law enforcement investigators who are unfamiliar with Text Messaging Applications and VOIP Applications may “walk away” instead of continuing to pursue that phone number.

The truth? These numbers tend to be associated with VOIPs or Text Messaging applications, and many of these providers have **tons of data / information / evidence** for investigators if we follow through with our investigation into these numbers.

Criminals involved in all facets of crime may use these text messaging applications as opposed to spending money on a “burner” phone (pre-paid phone). This includes drug and firearm traffickers using them to communicate with customers, scammers using them to communicate with victims, human trafficking suspects using them to communicate with customers or “johns,” and even sex crime offenders using them to communicate with and exploit juveniles. As such, learning how to investigate and pursue records from these providers is **necessary** for 21st century investigations.

INFORMATION ON TEXT MESSAGING APPS / VOIPS



You may or may not recognize some of the logos above, but they represent some of the most commonly used Text Messaging or VOIP applications available today. It’s important to recognize, however, that the above image only contains seven applications, and there are several dozen.

These applications are **mobile** or **web based** applications which allow users to create temporary phone numbers, not linked to an actual cellular provider, to communicate via text message and phone call with other real cell phones. Some are free, others may be paid services (such as Burner).

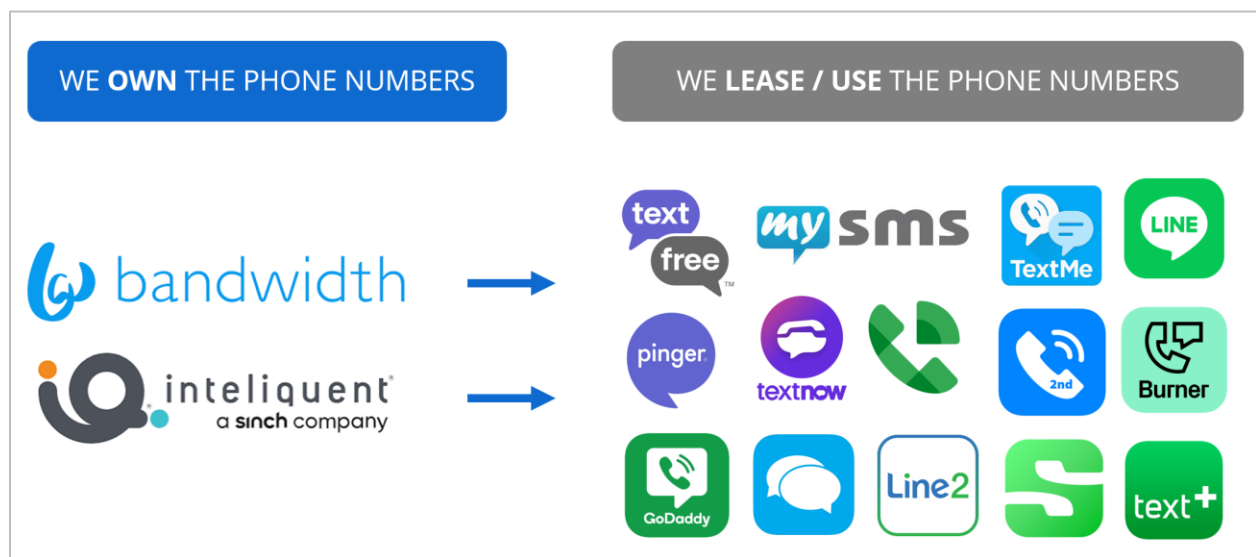
Law enforcement should recognize that these are **not** traditional cell phone numbers: They do not rely on cellular tower coverage, but instead they rely on **internet access**. They can be accessed and utilized from cellular data or wireless internet (WiFi).

In the same regard, all data transmitted through these applications must go through the service provider’s **servers**, and that’s why it’s so paramount that we investigate them when the opportunity presents itself – these applications are likely keeping significant information and evidence for us if we seek to obtain it with legal process.

IDENTIFYING THE TEXT MESSAGING APPLICATION

Typically, if a phone number does not return to a known carrier, it will return to one of the two major companies that lease phone numbers to VOIPs and Text Messaging Applications: Either **Bandwidth.com** or **Sinch / Inteliquent**.

It's important to recognize that these companies simply *own* the phone numbers and **lease them** to the numerous available VOIP and text messaging platforms. In most cases, Bandwidth.com or Sinch / Inteliquent has little to no useful information for us.



Our Mission: Investigators have to work through these companies to identify the application which is “leasing” the phone number, and which our suspect is using, so that we know where to send our legal process and where our evidence may be. Here’s how:

BANDWIDTH.COM

Identifying the platform for Bandwidth.com numbers is **easy** and **DOES NOT** require any legal process or extra work, but it may take some time.

Investigators should email uslawenforcement@bandwidth.com seeking assistance. This email should come from an official government email, and should (at a minimum) include the phone number, the date it was known to be used by the suspect (as sometimes these numbers may move between platforms), and a statement to the nature of your investigation (IE: I am investigating this number related to a sexual exploitation case).

Within a few days, oftentimes quicker, investigators can expect a response from Bandwidth.com identifying the platform using the phone number at the date specified.

INTELIQUENT / SINCH

First, it's worth mentioning that Inteliquent apparently owns numerous other companies. Sometimes, your phone carrier lookup tool may not say "Inteliquent" directly. It may say any of the following companies. These are still *all* Inteliquent.

- Inteliquent
- Sinch
- Sinch AB
- CLX Communications
- Broadvox, LLC
- Onvoy Spectrum, LLC.
- Onvoy Inc.
- Voyant Communications
- ANPI Business
- Layered Communications
- Vitelity
- Neutral Tandem
- ***& There May Be Others...***

There are two different ways law enforcement can identify the carrier from Inteliquent:

1. **Subpoena or Search Warrant**

Law enforcement can serve legal process to Inteliquent seeking this information.

2. **Access Inteliquent's Law Enforcement Portal**

Visit Inteliquent's website at <https://www.sinch.com/legal/lea-portal/> to create an account with their Law Enforcement Portal. The process will take 3-5 days (or longer) so do it *before* you need the information. Once your account is setup, you can simply login and look up numbers, getting the results without delay.

WRITING LEGAL PROCESS TO THE VOIP PROVIDER

Now that you've identified the provider, you can look up how to serve them with legal process on the Search.org ISP list or check your resources such as KLoveing for templates, law enforcement guides, or additional information as each carrier is slightly different.

It varies from provider to provider what they retain, but we may be able to obtain:

- **Subscriber Information:** Usernames, emails, phone numbers, and similar records.
- **Device Information:** Identifying device IDs, makes, models, and operating systems.
- **IP Address Records:** Logs of IP addresses used by suspects to access the VOIP.
- **Contact Lists:** Records of any "contacts" saved by suspects within the apps.
- **Call Logs:** Logs of any calls made through the VOIP / Application.
- **Text Message Logs:** Logs of any messages sent through the VOIP / Application.
- **Text Message Content:** The actual content (text) of messages sent / received.
- **Text Message Attachments:** Multimedia (photos / videos) sent or received.
- **Voicemails:** Records of voicemails left for the target accounts.

It's incredibly important that we **do not** serve VOIP Providers or Text Messaging Applications with traditional cell provider warrants which ask for things like "Timing Advance Records, Call Detail Records, etc." because these applications **do not** possess those records or refer to these items the way traditional carriers do.

Here's what we **can NOT** typically do with VOIPs / Texting Applications:

- Obtain Cell Records / Locations (*although a few possess limited location data*).
- Set up a "PING" to geolocate the device with the application installed.

If you truly need to "PING" the phone or obtain cell records and location data, we can **attempt** to identify the phone that the application is installed upon and obtain cell records from the actual cellular carrier by working the **IP Address Records**. In summary, resolve the IP addresses to identify the internet service providers (and hopefully cellular carrier). Then, write legal process to that cellular carrier (if it is not AT&T Wireless) with the IP Addresses and Timestamps, asking them to identify the subscriber and produce records. This *may* or *may not* work (mixed success) but is always worth trying. [*For more information, refer to the Quick Guide on Chasing IP Addresses.*](#)

ISSUES YOU MAY ENCOUNTER

Deleted Accounts:

If your suspect learns they are being investigated, they can easily "delete" their accounts with many of these providers. Many providers will immediately wipe the records from their servers with limited opportunity for recovery, so consider sending a **preservation letter**!

Canadian Providers:

Many of these applications and VOIP services are operated out of Canada. We've experienced mixed results with serving them legal process: Some accept US legal process without hesitation and produce records, and some may have some hoops to jump through.

Overseas Providers:

A few of these applications may be operated overseas, and cooperation with US legal process may vary. Research the particular application for additional information.

IP Address Issues:

Suspects may use virtual private networks to mask their IP Addresses, or sometimes we may only obtain IPv4 addresses which are more difficult for cellular carriers to resolve. Refer to the "Quick Guide on Chasing IP Addresses" for additional suggestions.

Burner / Pre-Paid Phones:

We have regularly seen that from time to time, these applications may be installed by suspects on pre-paid phones as an added layer of protection / shielding.



GBG Consulting, LLC. is proud to offer this “quick reference” guide to law enforcement to support their VOIP / Texting Applications.

GBG Consulting, LLC. provides quality social media and technology-based investigation training to law enforcement investigators, analysts, and prosecutors. Below are some of the courses we offer:



PLUG
Investigations



SOCIAL MEDIA
INVESTIGATIONS



CHASING
DIGITAL MONEY



LOCATING FUGITIVES
UTILIZING SOCIAL MEDIA



SNAPCHAT
INVESTIGATIONS



CAL ECPA
1546 PC FOR INVESTIGATORS

VISIT OUR WEBSITE FOR INFORMATION ON HOSTING TRAINING!

WWW.GBGCONSULTING.ORG



TRADECRAFT TRAINING
FOR LAW ENFORCEMENT PROFESSIONALS

We proudly partner with **Tradecraft Training, LLC.** to provide **WEBINAR BASED** training on the classes above for students. Tradecraft Training also offers great classes by other industry experts and instructors on technology based topics. **Check out their website at www.tradecrafttraining.org to see upcoming classes, or register for a course!**