



QUICK REFERENCE GUIDE

IP ADDRESSES

INTRODUCTION

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

As we are navigating digital evidence obtained from various technology providers, including (but certainly not limited to) social media platforms, text messaging applications, P2P payment applications such as CashApp, online banks, and more, we often find ourselves staring at *large data sets* containing timestamps and IP addresses:

Timestamp (UTC)	IP Address
06-15-2025 04:31:10 UTC	2607:f8b0:4013:48ab:32d4:99ef:a231:7c10
06-15-2025 09:14:22 UTC	69.251.77.133
06-15-2025 12:45:55 UTC	2404:6800:4004:805:b7f3:2c40:aa1e:fc22
06-15-2025 17:03:37 UTC	2001:0db8:6e3a:5b1c:8e45:ab20:f02a:3bdc
06-15-2025 22:19:41 UTC	73.92.144.182
06-16-2025 02:11:53 UTC	2606:4700:4700:0000:8d4a:1182:a3be:7e29
06-16-2025 05:40:18 UTC	2c0f:fc89:8100:ff12:b34e:192b:11cc:4a09
06-16-2025 09:26:03 UTC	73.92.144.182
06-16-2025 14:59:10 UTC	73.92.144.182
06-16-2025 19:22:42 UTC	2001:0db8:abcd:12fa:7d3e:cc01:bb0e:9421
06-16-2025 23:47:05 UTC	2a02:6b8:0:1:5a3b:ee40:3492:6cd2
06-17-2025 03:36:29 UTC	69.251.77.133
06-17-2025 07:15:44 UTC	69.251.77.133
06-17-2025 10:41:33 UTC	2001:19f0:7001:0003:ac12:88ff:fe99:4422
06-17-2025 14:57:18 UTC	2406:da00:ff00:0:79a9:3c11:6eb1:bb77

Unfortunately, most investigators (with the exception of those with heavy technology training, a background in technology, or ICAC investigators) have limited training and experience on what we can do with IP addresses.

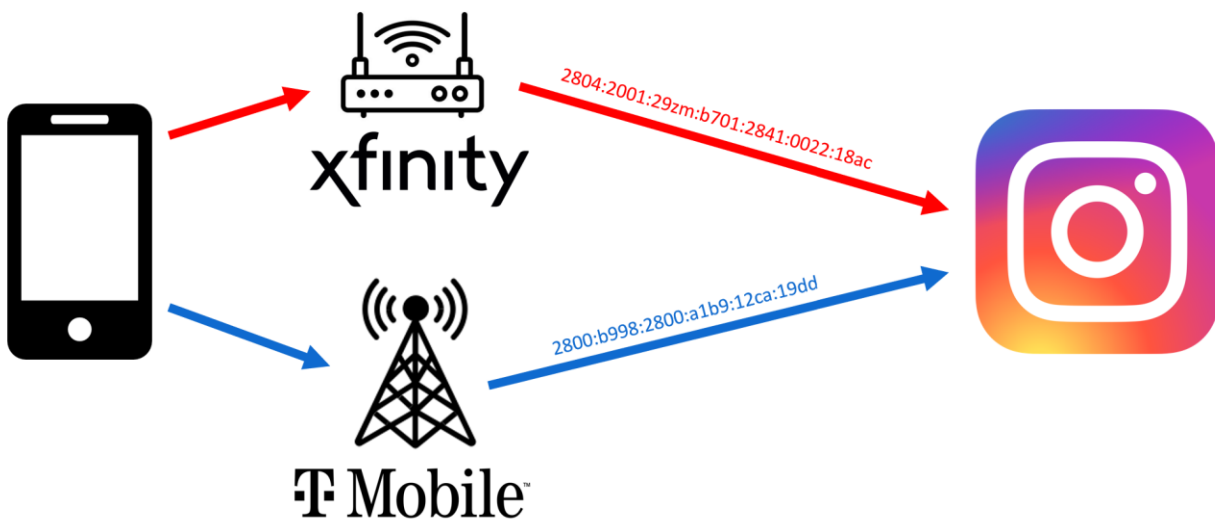
This short guide will cover, in a non-techy way, how to follow up on IP addresses we obtain during the course of our investigations and obtain additional valuable evidence.

WHAT IS AN IP (INTERNET PROTOCOL) ADDRESS?

An IP address (Internet Protocol address) is a unique identifier assigned to a device when it connects to a network, allowing data to be sent to and from that device across the internet. It works like a digital mailing address — telling the network where to deliver information, whether that's loading a website, sending an email, or streaming a video.

IP addresses can be assigned temporarily (**dynamic**) or stay consistent for longer periods (**static**), and they are often linked to an internet service provider (**ISP**) subscriber account.

IP addresses are collected and logged by almost every social media platform, application, and internet service that we might target with legal process. The length that providers maintain these records, and how often they collect IP addresses can vary.



Sometimes, in addition to an IP address, you'll see a **port number** listed (for example, 104.238.163.77:**443**). We should be actively asking for this in our legal process. While some social media platforms *always* provide it, others may not keep records of the ports or may only produce it when specifically ordered by legal process language (IE: Facebook).

While the IP address identifies the device or network connection, the port identifies the specific service, app, or type of traffic the device was using at that moment — like web browsing, messaging, or file sharing. Think of the IP address as the street address, and the port as the apartment number inside that building. In investigations, having both the IP and port can sometimes help providers or companies more accurately identify the exact user or device involved, especially on large networks where multiple users may share the same IP address at the same time.

WHY IP ADDRESSES ARE USEFUL TO LAW ENFORCEMENT

As we conduct digital investigations, IP addresses can be extremely valuable. We can take some investigative steps (resolving the IP address and following up with legal process to the Internet Service Provider) to get additional information.

Sometimes newer investigators think an IP address will tell us **who** is accessing a website or social media platform, and that's *not necessarily the case*. In reality, IP addresses can **help us identify the LOCATION where a person was accessing the internet to connect to a website or social media website from at a specific time**. We'll get more into that later in this document.

For investigators, **we can use that information** to further our investigations and:

- 1) **Identify Suspects:** They may be the listed subscriber who is paying the internet or cell phone bill, or they may be a family member, friend, or associate. Either way, identifying location(s) the suspect is accessing can help us to identify them or narrow down our list substantially.
- 2) **Tie Evidence to Suspects:** IP addresses are like a digital fingerprint – they *can* be changed (IE: Virtual Private Networks), but they are something that our suspects **cannot get rid of** once they've been captured by internet websites and social media platforms. As we search a social media account and locate mountains of incriminating evidence, we face the challenge of tying all of that illegal activity **to our suspect**. One of the easiest approaches is proving, through IP addresses, that at the time(s) the illegal activity occurred online – the IP addresses lead back to our suspect's residence, cell phone, girlfriend's house, etc.
- 3) **Locate Fugitives:** In cases where offenders are eluding law enforcement, particularly in violent crimes, pursuing IP addresses (particularly on an "exigent" basis when following up with Internet Service Providers) can help us identify location(s) where our fugitives may be residing at, "hiding out" at, or frequenting.
- 4) **Identify Locations of Particular Interest (IE: Stash Locations):** IP addresses can locate *more* than just a suspect's house – they can locate other locations of interest. Suspect workplaces, schools, apartment numbers within a large complex, and even potentially stash locations where a suspect keeps drugs or firearms. For example, if we know on 6/19/2025 at 2:50 AM our suspect posted a photograph of a kilo of cocaine on Instagram, and we see at 2:49 AM on the same day he connected to Snapchat using an IP that resolves back to Comcast, a subpoena or search warrant to Comcast can reveal where our suspect was when he posted that picture, and thus, the likely location where that kilo of Cocaine may be found.

IPv4 ADDRESSES VS. IPv6 ADDRESSES

IPv4 and IPv6 are two versions of IP addresses used to identify devices on a network.

IPv4 uses 32-bit addresses (e.g., 104.238.163.77), allowing about 4.3 billion unique addresses, which have become scarce as the internet has grown.

IPv6 uses 128-bit addresses (e.g., 2607:f8b0:4013:48ab:32d4:99ef:a231:7c10), offering an almost limitless number of addresses.

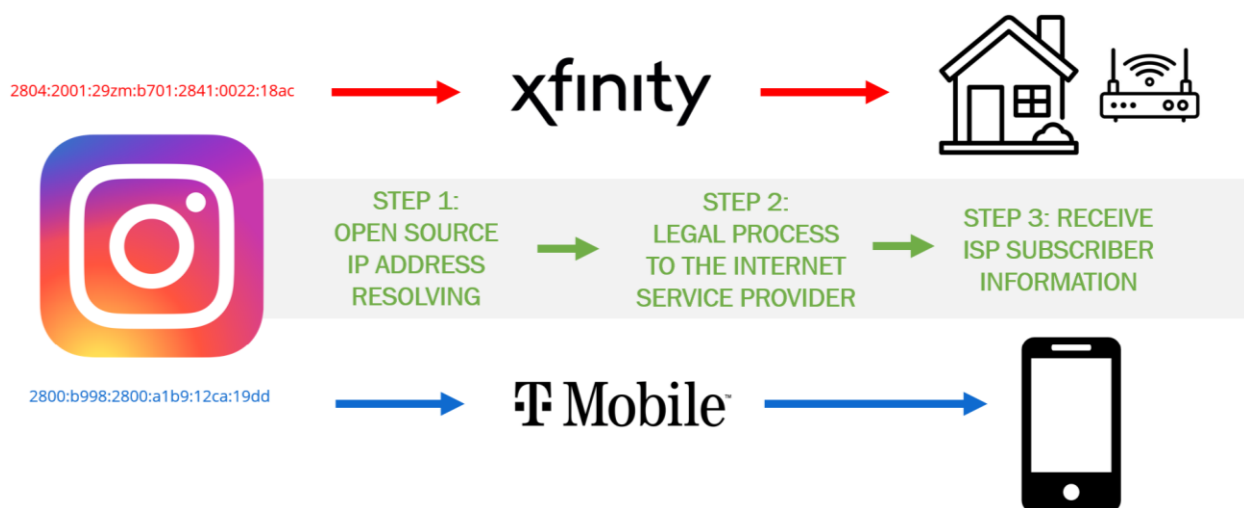
While IPv6 adoption is growing, many systems, providers, and devices still heavily rely on IPv4 or run both side-by-side ("dual stack").

For most forensic work, both can point to a subscriber or device, and the investigative process is essentially the same. What matters most is whether the provider keeps useful logs tied to either address format. In many legal process returns today, you'll see both formats; Investigators simply need to recognize them and treat them as unique identifiers.

STEP BY STEP: WORKING IP ADDRESSES BACKWARDS

A simple way of looking at it: **We actually work backwards** when we are following up on IP addresses with Internet Service Providers.

We will typically take the IP addresses we get from our provider(s), resolve them using an open source tool, and then serve legal process to the internet service providers or cellular carriers seeking additional information and records on the internet service:



RESOLVING IP ADDRESSES

When I say “Resolve” an IP address, all we are doing is an open-source query or search to take a string of numbers that tells us nothing at face value and identify who the internet service provider is (or who we should be providing legal process to). There are numerous tools and resources available to us to do this (see the next section).

IP Addresses can be resolved to one of essentially three “places,” as described below:

1) **Traditional Internet Service Provider**

This could be home internet (wired or wireless / WiFi), internet at a business such as Starbucks, or even public WiFi locations such as an airport or a courthouse. Examples of traditional ISPs include Comcast, Spectrum or Starlink.

2) **Cellular Providers**

Modern cellular providers such as AT&T, T-Mobile and Verizon operate cellular networks which allow users to access *mobile* data, connecting to the internet from their cell phones while moving and not connected to wireless internet. Most often, a suspect’s IP addresses will typically only resolve to **one** cellular provider, as they are likely connecting from the same phone on the same cellular network *every time*.

We will typically see quite a few IPs for cellular providers appear within the resolved IP address list, as these frequently change when people move around and connect to different cellular towers. We’ll talk about why that’s important later.

3) **Virtual Private Networks**

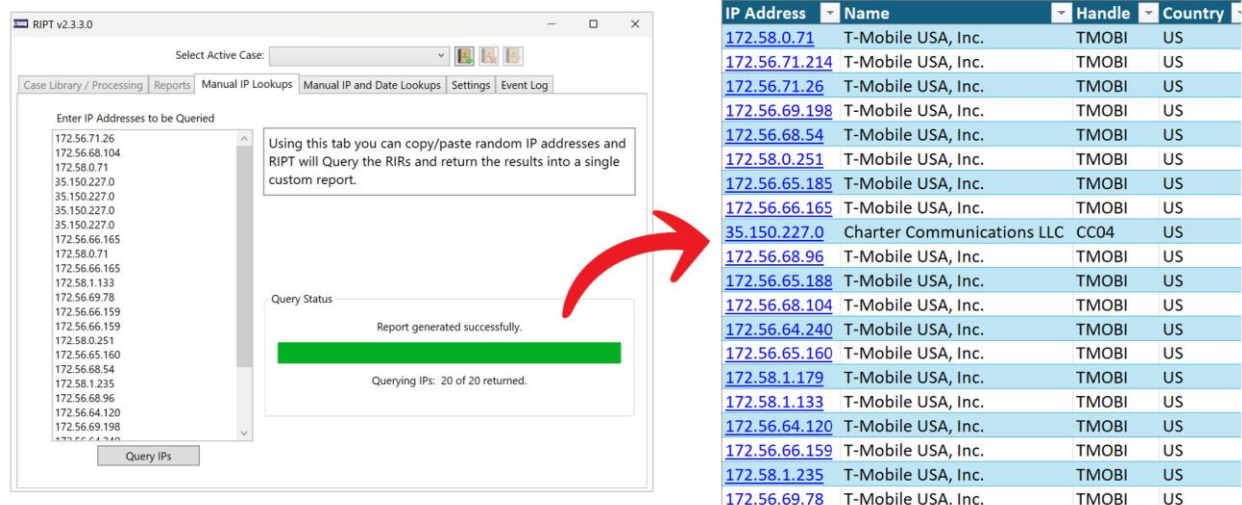
A common tactic suspects may use to conceal their IP addresses and try to protect their illicit online activity is to install or run a **virtual private network** (such as Proton VPN) on their phone(s) or computer(s).

Without getting overly technical, a VPN will connect to servers elsewhere in the world *before* connecting to internet websites or social media platforms. As we resolve IP addresses, it might appear that your suspect is quite the world traveler.

TOOLS / RESOURCES TO RESOLVE IP ADDRESSES

When it comes to resolving IP addresses, there's no "right" tool for the job, but there may be the "wrong" tools. Given that we'll likely use the information we obtain to author legal process and we are depending on it to be accurate, it's important that we're careful in selecting a tool that will be **reliable**.

My recommendation for law enforcement is to use a tool called **RIPT**, which is offered by the NDCAC through the law enforcement portal LEEP. RIPT is a free tool that can ingest hundreds of IP addresses at one time, quickly resolve them with up to date information from reliable sources, and produce an easy to review spreadsheet with the ISPs:



The screenshot shows the RIPT v2.3.3.0 application window. On the left, a list of IP addresses is entered for querying. A red arrow points from this list to a table on the right showing the results of the query. The table has columns for IP Address, Name, Handle, and Country.

IP Address	Name	Handle	Country
172.58.0.71	T-Mobile USA, Inc.	TMOBI	US
172.56.71.214	T-Mobile USA, Inc.	TMOBI	US
172.56.71.26	T-Mobile USA, Inc.	TMOBI	US
172.56.69.198	T-Mobile USA, Inc.	TMOBI	US
172.56.68.54	T-Mobile USA, Inc.	TMOBI	US
172.58.0.251	T-Mobile USA, Inc.	TMOBI	US
172.56.65.185	T-Mobile USA, Inc.	TMOBI	US
172.56.66.165	T-Mobile USA, Inc.	TMOBI	US
35.150.227.0	Charter Communications LLC	CC04	US
172.56.68.96	T-Mobile USA, Inc.	TMOBI	US
172.56.65.188	T-Mobile USA, Inc.	TMOBI	US
172.56.68.104	T-Mobile USA, Inc.	TMOBI	US
172.56.64.240	T-Mobile USA, Inc.	TMOBI	US
172.56.65.160	T-Mobile USA, Inc.	TMOBI	US
172.58.1.179	T-Mobile USA, Inc.	TMOBI	US
172.58.1.133	T-Mobile USA, Inc.	TMOBI	US
172.56.64.120	T-Mobile USA, Inc.	TMOBI	US
172.56.66.159	T-Mobile USA, Inc.	TMOBI	US
172.58.1.235	T-Mobile USA, Inc.	TMOBI	US
172.56.69.78	T-Mobile USA, Inc.	TMOBI	US

That's not to say that other websites don't exist that can do this – there's thousands of free websites, paid websites, and fancy paid tools. My other recommendations are:

ARIN (Official*)	https://www.arin.net
Domain Tools	https://whois.domaintools.com
MAXMIND	https://www.maxmind.com/en/geoip2-precision-demo

A relatively important consideration is that you'll likely be working with hundreds or thousands of IP addresses – so you'll prefer a tool that can run large lists of IP addresses at once as opposed to a "free" online website that only allows you to run one at a time.

Another important note – many free tools will give you an estimated **location**. Sometimes, with GPS coordinates or estimated addresses. **DO NOT trust these, they are notoriously wrong** and can be wildly inaccurate. Always follow up with the internet service providers.

HELP – MY SUSPECT’S IPS RESOLVED TO MULTIPLE ISPS?

This is one of the most common questions I get from investigators working their first investigation and resolving IP addresses.

In almost ALL cases involving IP addresses, we will see connections from multiple internet service providers (unless your suspect is a recluse and never leaves his mom’s basement). See the following table as an example of why this occurs:

Time	Location / Activity	Internet Service Provider
1200-0800	Suspect is at home	Starlink (Home WiFi)
0800-0830	Suspect drives to his local junior college	T-Mobile (Mobile Data)
0830-1100	Suspect is in class at junior college	Verizon Business (Public WiFi)
1100-1130	Suspect drives home	T-Mobile (Mobile Data)
1130-1320	Suspect is at home	Starlink (Home WiFi)
1320-1330	Suspect drives to work	T-Mobile (Mobile Data)
1330-2030	Suspect is at work at a local restaurant	Comcast (Work WiFi)
2030-2040	Suspect drives home	T-Mobile (Mobile Data)
2040-2359	Suspect is at home	Starlink (Home WiFi)

As depicted in the above example, throughout the day the suspect was moving around, as was his cellular device, and he accessed Instagram throughout the day. As such, when resolved, IP address records will show connections via Starlink, T-Mobile, Verizon Business, and Comcast Business intermittently throughout the day.

Sure, we could *just write* to the provider(s) that appear the most – but in the above example, why not write to *all of them*? We would be making an educated guess which ISP is likely his home internet (it could be Starlink or Comcast in that example if we didn’t know our suspect’s daily routine), not to mention T-Mobile can give you cellular records, Verizon Business would ultimately provide you intel that the suspect is a student at a local junior college (where we could obtain his class schedule), and Comcast would reveal where your suspect is employed. This could all be valuable intelligence for furthering your investigation.

LEGAL PROCESS TO INTERNET SERVICE PROVIDERS

Although these search warrants may seem *long, complicated, and technical* – they really aren’t difficult at all.

In essence, when writing to the internet service providers (ISPs), you’ll be copy and pasting the table of IP addresses and date/timestamps you have into the legal process and compelling the ISPs to **attempt to identify the subscribers and service locations** based on the IP addresses and timestamps you’re providing, as seen in the below example:

Starlink is to query all of the following target IP addresses to identify service location(s) / subscriber(s):

IP Address	Date / Timestamp (UTC)
2800:B219:C100:1992:102A:99CX:400C:2091:53AE	9/15/2024 at 05:10:52 UTC
2801:B219:C100:1600:104X:D702:0000:1021:915Z	9/15/2024 at 05:08:17 UTC
2800:B219:C100:1992:102A:99CX:400C:2091:53AE	9/15/2024 at 05:04:02 UTC
2801:B219:C100:1600:104X:D702:0000:1021:915Z	9/15/2024 at 05:00:01 UTC
2801:B219:C100:1600:104X:D702:0000:1021:915Z	9/15/2024 at 04:55:54 UTC
2802:B21C:D000:0192:102A:ASM2:400C:2091:88AS	9/15/2024 at 04:52:50 UTC
2800:B219:C100:1992:102A:99CX:400C:2091:53AE	9/15/2024 at 04:50:54 UTC
2801:B219:C100:1600:104X:D702:0000:1021:915Z	9/15/2024 at 04:44:11 UTC
2801:B219:C100:1600:104X:D702:0000:1021:915Z	9/15/2024 at 04:44:05 UTC

Two important considerations:

1) Provide ALL Available IP Addresses & PORTS (if available)

Many investigators will “short cut” this by grabbing just one or even few of the IP addresses that resolve to an ISP and calling it good. **Don’t!** *This is for two reasons:*

- The more data you give ISPs, the more likely it is that they’ll be able to identify a specific customer or subscriber. Many large ISPs share IP addresses amongst customers and may have difficulty identifying specific subscribers with limited information. That’s why providing numerous IP addresses, timestamps, and ports (if available) can make your chances of success increase.
- It’s likely that with a major ISP like “Comcast,” your suspect is connecting to multiple WiFi locations serviced by that ISP. For example, if your suspect frequently spends time and nights at his girlfriend’s house, and they both have Comcast, by providing Comcast with all the IP addresses they will likely be able to tell you that your suspect connected at both of those locations.

2) Provide DATE / TIMESTAMPS and DESIGNATE THE TIME ZONE (UTC? PST?)

We should be providing timestamps as UTC time so that it is standardized (most providers keep records in UTC anyways), but be sure to indicate this in your warrants. Eight hours can be a huge difference when trying to identify a subscriber.

LEGAL PROCESS TO CELLULAR CARRIERS

We will do the *exact same thing* we did for an ISP like Comcast, but to a cellular carrier.

In essence, when writing to the cellular carrier, you'll be copy and pasting the table of IP addresses and date/timestamps you have into the legal process and compelling the cellular carrier to **attempt to identify the subscribers and device (phone)** based on the IP addresses and timestamps you're providing.

If successful and a cellular carrier is able to identify your subscriber, you may be able to *literally* tie the internet activity to a phone in a suspect's pocket when you arrest them. You could also follow up with the carrier for phone pings or provider records, if needed.

It is particularly important with cellular carriers that you provide them with **ALL AVAILABLE IP ADDRESSES**. The difference in providing them with 25 IP addresses / timestamps versus 100 could be the difference in whether or not they can identify your subscriber. This, in part, is due to the fact that at any given time, hundreds or thousands of subscribers could be using the same mobile data IP address, on the same tower, at the same date and time. As we provide more IPs and timestamps, it will start to help them narrow down which phone is our suspects from the others through essentially link analysis (like a complex tower dump).

AT&T Wireless: Oh yea, and don't bother if it's AT&T Wireless. We've tried repeatedly, but AT&T Wireless claims they do not have the technology to resolve IP addresses to determine the device or subscriber. *It's strange* that T-Mobile and Verizon can though, isn't it?

DEALING WITH VIRTUAL PRIVATE NETWORKS

If your suspect is using a VPN, don't automatically assume you're *cooked*. It is true that most VPN providers have "no log" policies and either cannot comply with search warrants, or are intentionally located in countries where they won't comply with US search warrants. It is also true that some US based VPNs exist that can respond to legal process – but for obvious reasons, these tend *not* to be the VPNs used by our suspects.

Another truth: VPNs are a piece of technology that don't work 100% of the time. Brief disconnects from the VPN occur from time to time, and suspects may forget to activate a VPN after a phone dies or is restarted. We refer to these as "IP leaks," and this is our best chance of catching them slipping.

Check every IP address: While 99% might resolve to VPN servers that we can't do much with...if there are a few "leaks" (say, for example, 8 IP addresses resolve back to an ISP like Comcast?): You're in business.

THE TRUTH: THIS MAY NOT ALWAYS WORK

In theory, this should work 100% of the time. Unfortunately, this is not always the case. Every investigator will have varying degrees of success – *I'm sitting at about 65%*.

Below are some reasons this *may not work*:

- ✗ **AT&T Wireless:** They just claim they can't do it for some reason.
- ✗ **Dynamic IPs:** Most ISPs assign IP addresses dynamically — the same IP may belong to different customers at different times, sometimes changing multiple times per day.
- ✗ **NAT / CGNAT:** Multiple customers may share the same public IP at the same time. Without port and timestamp data, this can make identifying one user difficult or impossible.
- ✗ **ISP Time Source Variability:** Not all providers use synchronized or consistent time sources. Logs may reflect server time, local time, or universal time depending on the ISP.
- ✗ **Port Numbers May Help:** Some ISPs using CGNAT log port assignments along with IP addresses. Including port information (when available) can increase the accuracy of subscriber identification.
- ✗ **Timestamps Are Critical:** Even a small error in timestamp (minutes, seconds, time zone differences, daylight savings) can result in no match or a match to the wrong customer.
- ✗ **Log Retention Limits:** Many ISPs purge IP assignment logs after a certain period — sometimes as short as 30-90 days. Delays in legal process can result in records being unavailable.
- ✗ **Multiple Subscriber Returns:** Some ISPs may return multiple subscribers for the same IP/timestamp, especially if logs are ambiguous or CGNAT was used.
- ✗ **Subscriber ≠ User:** Even if a subscriber is identified, investigators still need to establish who was using the device or network at the relevant time — especially in shared households, businesses, or public Wi-Fi situations.
- ✗ **Delays in Producing Records:** While some ISPs will run these searches and produce records quickly, some may take weeks. Particularly in cases where we are trying to locate a fugitive – this delay will make it almost certain our suspect isn't at the same house they were at 3 weeks earlier. If your case justifies it, consider asking the ISP to do it on an "exigent" basis (violent fugitives wanted for serious crimes / public safety risks).



GBG Consulting, LLC. is proud to offer this “quick reference” guide to law enforcement to support their investigations involving IP addresses.

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!**