Internet Protocol (IP) attribution is the attempt to identify a device ID or individual responsible for a [cyber attack](https://www.upguard.com/blog/cyber-attack) (e.g. [ransomware](https://www.upguard.com/blog/ransomware) or other [types of malware](https://www.upguard.com/blog/types-of-malware)) based on the origin of a network packet.

An IP address is given to a system for a period of time that enables them to exchange data to and from other devices on networks.

There are two major versions of IP today, IPv4 which has an address space of about 4 billion addresses and IPv6 which has about 340 undecillion, or 340 billion billion billion billion addresses. While 4 billion addresses sounds like a lot, IPv4 has been exhausted in many ways.

This has lead to a slow migration toward IPv6 addresses that most major networks and devices rely on today.

**Table of contents**

1. [Does IP attribution work?](https://www.upguard.com/blog/ip-attribution#work)
2. [Are IP addresses spoofable?](https://www.upguard.com/blog/ip-attribution#spoofable)
3. [How do cloud services and shared IP addresses affect IP attribution?](https://www.upguard.com/blog/ip-attribution#cloud-services-shared-ip)
4. [Is the value of malicious impersonation increasing?](https://www.upguard.com/blog/ip-attribution#malicious-impersonation)
5. [Conclusion](https://www.upguard.com/blog/ip-attribution#conclusion)
6. [How UpGuard can improve your security posture](https://www.upguard.com/blog/ip-attribution#upguard)

**1. Does IP attribution work?**

It's often said every device has a unique IP address assignment and that address can be reliably used as an identifier. This is not true.

The perpetuation of this myth continues to detract from the public's understanding of how the Internet works, both in terms of its underlying protocols and how it can be made secure.

Many believe that IP addresses are akin to fingerprints. However, there are key differences that need to be understood.

If humans could change their fingerprint from moment to moment, or even copy another person's fingerprint, there would be little value in finding and analyzing fingerprints. Fingerprints are useful for identifying malicious activity because they are unique and immutable.

If they weren't, we wouldn't be able to depend on them for forensic investigations.

Yet, this is exactly what happens in [cyber security](https://www.upguard.com/blog/cyber-security) [digital forensics](https://www.upguard.com/blog/digital-forensics) with the practice  of IP attribution to determine the geographical location, device or individual response for a cybercrime.

In short:

* There are common technologies that obscure who is tied to an IP address in real-time.
* There are many less transient signatures than IP addresses.
* Even if you can identify the device and its operating system, you may not be able to ascertain who was using it.
* Mobile devices and public networks like a guest wifi network allow unvetted access to the Internet, even if they protect against unauthorized access to more secure internal networks.
* The IP address space is large and can be defunct or repurposed.
* IP addresses can be shared.

A source IP is more accurately describe as the intended instructions of where to send a response to. There is nothing stopping the true sender of a network packet from marking the packet with an arbitrary or intentionally misleading IP address.

If sent with a random source IP, the sender cannot expect to receive a reply from the destination (as the destination server will attempt to send the reply to the random address instead of the true origin).

However, this design does allow many forms of routing which complete the communication without informing hosts of the true origin's IP address.

**2. Are IP addresses spoofable?**

IP addresses are easily faked or "spoofed". This concept is not new or secret, a quick Google will show thousands of pages. You can read more about it on [Wikipedia](https://en.wikipedia.org/wiki/IP_address_spoofing).

In fact, there are open source scripts available on GitHub showcasing [the concept](https://github.com/LetUsFsck/MagicPacketGenerator). As this project shows, the IP address originating a port scan “can also be faked.”

IP attribution is useful for non-security related trend analysis. And this remains true only because the majority of Internet traffic has no desire to obfuscate their originating IP address.

The situation changes when the purpose of attribution is to identify individual devices, especially for threat intelligence rather than general analysis of large amounts of varied traffic. Most people doing normal things on the internet have no reason to fake their IP address, and indeed it would cause problems for them if they did. Ironically, most of the people motivated to do it are precisely the miscreants that IP attribution efforts would be trying to catch.

**3. How do cloud services and shared IP addresses affect IP attribution?**

The growing adoption of cloud hosted services and other shared-IP platforms compound the issues with IP attribution even further.

Many cheap cloud computing services do not provide a unique IP address to the client. The same is true for small and medium businesses who may share address space with their internet service provider (ISP).

Hosts can and will use a single IP address for multiple clients. Routing magic, subnets, CIDR (Classless Inter-Domain Routing) and network address translation make this possible.

If actions are attributed to entities solely on the source IP address, then it is feasible a cloud hosted instance could be lumped in and categorized according to the actions of a nefarious neighbouring instance on the same physical host run by someone else.

Cloud services make it easy to rotate IPs, further increasing the likelihood of error in attribution.

**4. Is the value of malicious impersonation increasing?**

The most important reason to not rely on IP attribution is in relation to "Hack Back" legislation.

This idea is again in the news with [a new proposal from Representative Tom Graves](https://www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/) “that would allow companies to go outside of their own networks to identify their attackers and possibly disrupt their activities.”

If laws are ever passed allowing entities to return fire at perceived online attackers, IP addresses are likely to play a role in identifying who is pinned as the reverse target in [incident response](https://www.upguard.com/blog/incident-response-plan).

Security professionals need to educate the public regarding the ease of IP address manipulation. Allowing entities to hack back will be bad if it creates opportunities for malicious individuals to trick much larger entities into attack innocent, mimicked victim.

**5. Conclusion**

Just as [phishing](https://www.upguard.com/blog/phishing) and other forms of [social engineering](https://www.upguard.com/blog/social-engineering) mimicry have become common knowledge, IP address manipulation needs to be part of public vernacular and not just talked about in [information security](https://www.upguard.com/blog/information-security) circles.

IP attribution has many problems ranging from the complexities of multi-tenant cloud environments to the ease of IP spoofing.

The fundamental fact is a packet's sender IP is under the sender's control and is not something that can be relied upon like a fingerprint.

For low impact uses, IP attribution may be good enough but it isn't for security.

Imagine a future where IP attribution is central to security decisions and understand how dangerous it is due to fundamental mutability.

We don't want to incentivize bad actors to [exploit](https://www.upguard.com/blog/exploit) IP spoofing in the same way DDoS attacks have been.

In the best case scenario, IP attribution data would become useless. But the more troubling scenario is feasible where innocuous IPs are blacklisted and unsuspecting businesses are crippled due to their undeserved IP reputation.

**6. How UpGuard can improve your security posture**

There's no question that [cybersecurity is more important](https://www.upguard.com/blog/cybersecurity-important) than ever before. That's why companies like [Intercontinental Exchange](https://www.upguard.com/customers/ice-nyse), [Taylor Fry](https://www.upguard.com/customers/taylor-fry), [The New York Stock Exchange](https://www.upguard.com/customers/ice-nyse), IAG, First State Super, Akamai, Morningstar and NASA use UpGuard to protect their data and [prevent data breaches](https://www.upguard.com/blog/prevent-data-breaches).

We're experts in data breaches, in fact our [data breach research](https://www.upguard.com/breaches) has been featured in the [New York Times](https://www.nytimes.com/2018/07/20/business/suppliers-data-leak-automakers.html), [Bloomberg](https://www.bloomberg.com/news/articles/2019-06-27/ford-td-bank-files-found-online-in-cloud-data-exposure), [Washington Post](https://www.washingtonpost.com/news/the-switch/wp/2017/12/22/you-may-not-know-much-about-the-companies-exposing-your-personal-information-but-they-know-a-lot-about-you), [Forbes](https://www.forbes.com/sites/lconstantin/2017/07/17/cloud-storage-error-exposes-over-two-million-dow-jones-customer-records) and [Techcrunch.](https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/)

[UpGuard BreachSight](https://www.upguard.com/product/breachsight) can help combat [typosquatting](https://www.upguard.com/blog/typosquatting), prevent [data breaches](https://www.upguard.com/blog/data-breach) and [data leaks](https://www.upguard.com/blog/data-leak), avoiding regulatory fines and protecting your customer's trust through cyber security ratings and continuous exposure detection.

[UpGuard Vendor Risk](https://www.upguard.com/product/vendorrisk) can minimize the amount of time your organization spends managing third-party relationships by automating vendor questionnaires and continuously monitoring your [vendors](https://www.upguard.com/blog/third-party-vendor)' [security posture](https://www.upguard.com/blog/security-posture) over time while benchmarking them against their industry.

Each vendor is rated against 50+ criteria such as presence of [SSL](https://www.upguard.com/blog/ssl-certificate) and [DNSSEC](https://www.upguard.com/blog/dnssec), as well as risk of [domain hijacking](https://www.upguard.com/blog/domain-hijacking), [man-in-the-middle attacks](https://www.upguard.com/blog/man-in-the-middle-attack) and [email spoofing](https://www.upguard.com/blog/email-spoofing) for [phishing](https://www.upguard.com/blog/phishing).

Each day, our platform scores your vendors with a [Cyber Security Rating](https://www.upguard.com/blog/what-are-security-ratings) out of 950. We can even alert you if their score drops.

[Book a demo today.](https://www.upguard.com/cyber-risk/demo)