Como o IP serve para identificar um criminoso na internet

31/10/2025

O advento da internet (estrutura) e web (aplicações) implicou na alteração das coordenadas simbólicas de referência, incluindo o domínio do processo penal, especialmente da prova digital, com desafios de entendimento e compreensão. O objetivo desta coluna, quando subscrita por mim, será o de apresentar os principais termos associados ao mundo digital.

Spacca

Em um mundo em que os dados e os metadados são intangíveis e omnilocais, em geral em código binário (0 e 1), a literacia digital (abrange aprendizagem, educação, conscientização, aquisição e atualização de competências digitais) se estabelece como uma condição de possibilidade para que profissionais do Direito possam compreender o estado da arte, permitindo atuar de modo informado e ético, mitigando o efeito do desconhecimento digital.

Neste ecossistema, o Protocolo de Internet (IP) é o suporte invisível que permite a comunicação e o funcionamento da rede, sendo entidade necessária na persecução penal digital, representada pelo código atribuído a um terminal (computador, celular ou outro dispositivo) para permitir sua identificação. Eis o tema a seguir.

IP

O IP é uma definição primária da Computação Forense e no Direito Processual Penal aplicado ao ambiente digital, porque atua como suporte básico da identificação e rastreamento de condutas ilícitas na rede. O exame do IP e dos nomes de domínio são o fundamento do exame pericial de local de internet.

É um protocolo de nível de rede que se encarrega do endereçamento e do roteamento de pacotes de dados, atribuindo a cada terminal (computador, smartphone etc.) um código único para permitir sua identificação.

Em linguagem figurada, o IP é o conjunto de regras que governa como os dados são enviados e recebidos através da web. Considere o IP como o sistema de correios da internet. Para que uma carta chegue ao destino correto, precisa de duas coisas: um endereço claro no envelope e um carteiro que saiba como navegar pelas ruas para fazer a entrega. O IP cumpre as duas funções para os dados digitais, com três funções principais:

> *a) Endereçamento: é a função de "endereço no envelope". O IP atribui um endereço numérico único, chamado de endereço IP, a cada dispositivo conectado a uma rede (computador, smartphone, smart TV etc.). É assim que outros dispositivos sabem para onde enviar os pacotes de dados;*
> *b) Roteamento: é a função do "carteiro". Quando você envia dados (p.ex., ao acessar um site), os dados são divididos em pequenos pacotes. O IP é responsável por guiar cada um dos pacotes através da complexa rede de roteadores e cabos que compõem a internet, determinando a rota mais eficiente para que eles cheguem ao seu destino; e*
> *c) Fragmentação: os dados viajam pela rede em pacotes. Diferentes partes da rede têm limites de tamanho diferentes para esses pacotes (MTU — Maximum Transmission Unit). Se um pacote for grande demais para uma determinada seção da rota, o IP tem a função de quebrá-lo em fragmentos menores e, em seguida, garantir que possam ser remontados na ordem correta quando chegam ao destino.*

Existem duas versões principais do IP m uso hoje:

> *a) IPv4 (version 4): é a versão mais antiga e ainda amplamente usada. Adota um esquema de endereçamento de 32 bits, o que permite cerca de 4,3 bilhões de endereços únicos (ex: 192.168.1.1). Devido ao crescimento explosivo da internet, o número de endereços IPv4 disponíveis está praticamente esgotado; e*
> *b) IPv6 (version 6): é a versão mais nova, projetada para substituir o IPv4. Utiliza um esquema de endereçamento de 128 bits, oferecendo um número de endereços praticamente ilimitado (aproximadamente 340 undecilhões). É condição da expansão da Internet das Coisas (IoT), em que bilhões de novos dispositivos (lâmpadas, geladeiras, carros, assistentes domésticos, drones etc.) precisam de seus próprios endereços IP.*

O IP trabalha em geral associado, compondo um conjunto de protocolos, sendo a combinação mais famosa a suíte TCP/IP. Cuida da parte do endereçamento e da entrega ("onde" os pacotes devem ir). O TCP (Transmission Control Protocol) trabalha em conjunto com o IP para garantir a confiabilidade da entrega, verificando se todos os pacotes chegaram, se estão na ordem correta e se não se perderam no caminho. Se um pacote se perde, o TCP solicita o reenvio. Em resumo, o IP é o protocolo que define o endereço de destino e traça a rota, enquanto outros protocolos como o TCP garantem que a "encomenda" chegue completa e sem danos.

A transição de um para o outro (do IPv4 para o IPv6) é uma consideração importante na perícia digital. Atualmente os provedores no Brasil utilizam ambos os protocolos (IPv4 e IPv6) simultaneamente. O modelo predominante é a coexistência ("pilha dupla" ou *dual-stack*), operando na mesma infraestrutura de rede. Embora o IPv4 ainda seja amplamente utilizado, o Brasil é um dos líderes mundiais na adoção do IPv6:

> *a) Mais de 50% do tráfego de internet no Brasil já roda sobre IPv6;*
> *b) Cerca de 89% dos usuários finais já têm acesso via IPv6;*
> *c) Os endereços IPv4 disponíveis para alocação no Brasil se esgotaram em 2020, obrigando que os provedores adotassem gradativamente o IPv6 para acomodar novos clientes e o crescimento da demanda;*
> *d) A tendência é a transição contínua, com o IPv6 se tornando o padrão principal, embora o IPv4 ainda deva coexistir por alguns anos. Para tornar precisa a diferença, a tabela abaixo especifica as diferenças:*

Atributo	**IPv4**	**IPv6**
Tamanho	Usa endereços de 32 bits.	Usa endereços de 128 bits.
Disponibilidade	É a versão mais antiga e mais comum. O número de endereços é limitado.	Foi introduzido para resolver o problema de esgotamento, fornecendo um número quase ilimitado de endereços IP.
Exemplo	200.128.154.202 (quatro *bytes* separados por pontos, cada um de 0 a 255).	FABD:249C:AA28:3673:85AC:DR66:C3C8:2FDF.

Importância da Porta Lógica de Origem no contexto IPv4

O compartilhamento de endereços IPv4 é conhecido tecnicamente como CGNAT (*Carrier Grade Network Address Translation*), modalidade em que múltiplos usuários podem estar utilizando o mesmo endereço de IP público. Nesse cenário, o endereço IP isolado não permite identificar e individualizar o usuário. Para a devida identificação, é necessário obter a informação sobre a "porta lógica" ou porta de acesso, compreendida como a "porta lógica de origem".

Por que a Porta Lógica é relevante? A informação sobre a porta lógica de origem é necessária quase sempre que um investigador precisa identificar um usuário específico por trás de um endereço IPv4 compartilhado. O motivo acontece por causa de uma tecnologia chamada NAT (Network Address Translation), a solução encontrada pelos provedores para lidar com a falta de endereços IPv4 disponíveis.

Vamos usar uma analogia:

> *a) O endereço IP Público (IPv4): pense nele como o endereço de um grande prédio de apartamentos. É o único endereço que o mundo exterior (um site, um servidor de jogos etc.) consegue ver;*
> *b) Os dispositivos na rede (seu celular, notebook etc.): pense neles como os moradores dos*

> *apartamentos dentro desse prédio;*
> *c) O problema: quando um crime digital é cometido (p.ex.: uma postagem caluniosa em uma rede social), o servidor da rede social registra o acesso vindo do "endereço do prédio" (203.0.113.45). A polícia, com uma ordem judicial, pergunta ao site: "Quem fez essa postagem?". O site responde: "Alguém do endereço 203.0.113.45 às 22h15". O problema é que centenas ou milhares de "moradores" (clientes do provedor) podem estar usando esse mesmo "endereço de prédio" (IP Público) naquele momento; e,*
> *d) A solução: A porta lógica funciona como o número do apartamento. O provedor de internet, que gerencia o "prédio", mantém um registro detalhado. O registro (log) diz: "Às 22h15, o morador do apartamento 54.321 usou nosso endereço público 203.0.113.45 para se conectar".*

Logo, o contexto da necessidade é: identificar o usuário final em redes que usam NAT. Para correlacionar o log externo (do site) com o cliente específico (do provedor), o investigador precisa de 3 informações:

> *a) Endereço IP de origem;*
> *b) Data e hora exata do evento (timestamp); e,*
> *c) Porta lógica de origem. Sem a porta lógica, é tecnicamente inviável (ou impossível) individualizar a conduta dentro de um universo de usuários compartilhando o mesmo IP.*

Em síntese, a porta lógica de origem é necessária, na fase de compartilhamento do IP (IPv4), para a individualização da navegação na internet passa a ser intrinsecamente dependente dessa informação, até que ocorra a migração para o IPv6. O fornecimento da porta lógica de origem é um simples desdobramento lógico do pedido de identificação do usuário por IP, conforme já estabeleceu o STJ no julgamento do REcp 1.784.156, Min. Marco Aurélio Bellizze, julgado em 05/11/2019, resumido no formato Irac (Issue, Rule, Application, Conclusion), uma metodologia utilizada para estruturar a análise de casos.

Elemento	Descrição
I – Issue (Questão)	Qual é a extensão da obrigação legal de um provedor de aplicações no Brasil, sob o Marco Civil da Internet (MCI), para fornecer dados que permitam a identificação de um usuário responsável por conteúdo ilícito, especificamente se essa obrigação inclui a Porta Lógica de Origem associada ao Endereço IP?
R – Rule (Regra)	O Marco Civil da Internet (Lei nº 12.965/2014), em seus arts. 5º, VII, e 15, estabelece o dever de guarda e fornecimento dos registros de acesso a aplicações de internet. Tais registros incluem o conjunto de informações referentes à data e hora de uso de uma determinada aplicação a partir de um determinado endereço IP.

A – Application (Aplicação)	Dada a realidade de esgotamento do IPv4 (CGNAT) e o compartilhamento de um mesmo endereço IP por múltiplos usuários, o endereço IP isolado não permite a individualização do usuário. Portanto, a fase de compartilhamento do IP torna a individualização da navegação intrinsecamente dependente da porta lógica de origem, até que a migração para o IPv6 se concretize. A determinação judicial para o fornecimento da porta lógica de origem é vista como um simples desdobramento lógico do pedido de identificação do usuário pelo IP.
C – Conclusion (Conclusão)	O STJ entendeu ser plenamente possível a determinação judicial para que o provedor de aplicações forneça tanto o endereço de IP quanto a Porta Lógica de Origem.

Provedores no Marco Civil da Internet

O provedor de conexão (que corresponde ao provedor de acesso) é o administrador de sistema autônomo que fornece o serviço de acesso à internet.

Aspecto	**Base Legal MCI, Lei 12.965/2014**
Objeto	**Registros de conexão**.
Definição	Art. 5º, VI: “registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”.
Prazo	Prazo de 1 (um) ano.
Condições	Manter sob sigilo, em ambiente controlado e de segurança. A responsabilidade pela guarda não pode ser transferida a terceiros (MCI, art. 13)

O Provedor de Aplicações de Internet é a pessoa jurídica que exerce a atividade de serviços de aplicações de internet (correio eletrônico, hospedagem e conteúdo) de forma organizada e com fins econômicos.

Aspecto	**Base Legal MCI, Lei 12.965/2014**
Objeto	**Registros de acesso a aplicações de internet**.
Definição	Art. 5º, VIII: “registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”.
Prazo	Prazo de 6 (seis) meses.
Condições	Manter sob sigilo, em ambiente controlado e de segurança (MCI, art. 15).

Estado da arte

A transição do IPv4 para o IPv6 é mais do que uma atualização técnica, justamente porque altera o suporte da principal evidência de conexão em uma rede: o endereço IP. Para um investigador, a diferença prática é comparável a passar de investigar um crime onde todos os suspeitos moram em um único e enorme prédio com um único endereço (IPv4 com NAT) para

um cenário onde cada suspeito tem sua própria casa com um endereço único e global (IPv6):

Aspecto	IPv4 (Desafio da Escassez)	IPv6 (Precisão da Abundância)
Atribuição Direta do Dispositivo	**Muito Difícil.** A maioria dos usuários está atrás de um NAT. Vários dispositivos (notebooks, TVs etc.) em uma casa ou empresa compartilham um único endereço IP público. O log de um servidor (p.ex: site acessado) registrará apenas o IP do roteador.	**Muito Mais Fácil.** Cada dispositivo pode ter seu próprio endereço IPv6 público e único. O log do servidor registrará o endereço específico do dispositivo que fez o acesso, não apenas o roteador da rede. Isso permite uma atribuição muito mais direta e precisa.
Correlação de Logs	**Complexa.** Para identificar um usuário específico por trás de um NAT, o investigador precisa correlacionar o log externo (do servidor) com os logs internos (do roteador da operadora ou da empresa), usando *timestamps* e números de porta. O processo é trabalhoso e os logs internos podem não estar disponíveis.	**Simplificada.** Como o endereço IPv6 é único para o dispositivo, o investigador pode correlacionar logs de diferentes fontes (servidor web, firewall, sistema de login) simplesmente procurando pelo mesmo endereço IPv6. A necessidade de correlacionar portas se torna menos crítica para a identificação.
Geolocalização Baseada em IP	**Imprecisa.** A geolocalização aponta para o provedor de internet ou para o ponto de presença (POP) da operadora, que pode estar a dezenas de quilômetros do usuário real. Você localiza o “prédio”, não o “apartamento”.	**Potencialmente Mais Precisa.** Embora ainda não seja um GPS, a geolocalização de um endereço IPv6 tende a ser mais granular, apontando para uma sub-rede mais específica. A precisão aumenta, permitindo focar a investigação em uma área geográfica menor.
Análise de Logs e Ferramentas	**Estabelecida.** Os endereços são curtos e em formato decimal (ex: 203.0.113.45). Todas as ferramentas forenses (SIEMs, parsers de log) estão totalmente adaptadas para analisar, buscar e visualizar esses endereços.	**Exige Adaptação.** Os endereços são longos, hexadecimais e podem ser abreviados (ex: 2001:db8::8a2e:370:7334). As ferramentas de análise precisam ser capazes de entender a sintaxe hexadecimal e as regras de abreviação para buscar e correlacionar endereços corretamente.

Rastreamento de Longo Prazo	**Instável.** Devido à natureza dinâmica (DHCP) e compartilhada (NAT) dos endereços IPv4, o mesmo IP pode ser atribuído a diferentes clientes em curtos períodos. Rastrear um ator ao longo de semanas pode ser difícil.	**Mais Estável, mas com ressalvas.** Um dispositivo pode manter o mesmo endereço IPv6 por muito tempo. **No entanto**, para proteger a privacidade, o IPv6 inclui mecanismos como *SLAAC Privacy Extensions*, que fazem com que um dispositivo use endereços temporários para conexões de saída. O investigador precisa saber diferenciar o endereço "estável" do dispositivo dos endereços "temporários".
Criptografia e Análise de Tráfego	**Opcional.** O IPsec (protocolo de segurança) pode ser implementado sobre o IPv4, mas não é parte integrante do protocolo. O investigador pode encontrar tráfego não criptografado com mais frequência.	**Integrada (IPsec).** O suporte ao IPsec é obrigatório na especificação do IPv6. Embora seu uso não seja mandatório, é muito mais comum. Significa que o investigador encontrará com mais frequência tráfego criptografado de ponta a ponta, dificultando a análise de conteúdo (Deep Packet Inspection) e focando a análise nos metadados da conexão (quem falou com quem e quando).

O lado positivo do IPv6 é a atribuição de um ato a um dispositivo específico se torna mais confiável. Em muitos casos, um endereço IPv6 em um log é uma evidência muito mais forte do que um endereço IPv4. No entanto, o desafio do IPv6 é que o investigador precisa lidar com novos complicadores, especialmente por agentes profissionais, como endereços temporários que ofuscam a identidade e o aumento do tráfego criptografado nativamente (IPsec), que impede a análise do conteúdo dos pacotes.

A realidade do mundo onlife (híbrido) é muito mais complexa porque se vive um mundo "dual-stack", em ambas as versões coexistem (IPv 4 e IPv 6). Em uma mesma investigação, o perito pode encontrar logs contendo endereços IPv4 de uma rede e endereços IPv6 de outra. É relevante que o investigador e suas ferramentas estejam aptos a analisar e correlacionar ambos os formatos de maneira fluida para não perder nenhuma pista. A velocidade das alterações é um desafio constante.

Conclusão

Diante da complexidade da rede e da crescente sofisticação dos crimes digitais, o endereço IP emerge como uma "impressão digital" relevante e um ponto de partida nas investigações, funcionando como um código único atribuído a um terminal para permitir sua identificação. No entanto, a mera busca por esse código, que é responsável por endereçar e rotear pacotes de dados, enfrenta desafios técnicos, como o uso de VPNs e IPs dinâmicos que mascaram a origem real, e limitações legais, exigindo autorização judicial para acesso a informações detalhadas.

Para que os profissionais do Direito e peritos digitais possam rastrear e identificar potenciais infratores, é condição de possibilidade a aquisição de competências digitais, incluindo o aprofundamento técnico sobre o IP (IPv4 e IPv6) e os mecanismos de endereçamento (porta

lógica), transformando a identificação do usuário em um desdobramento lógico e robusto da prova digital no contexto do processo penal onlife. Se você deseja que outros temas sejam abordados, escreva-me (*Instagram: @alexandremoraisdarosa*).

Fonte: https://conjur.jumps.com.br/2025-out-31/como-o-ip-serve-para-identificar-um-criminoso-na-internet/