Pathfinder

annotated IPv4 traceroutes

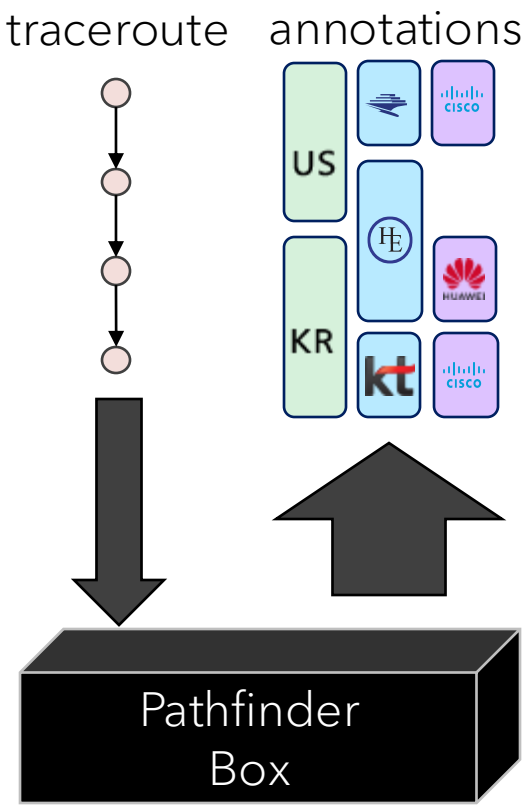
BRADLEY HUFFAKER

AIMS ‘25

What is Pathfinder?

Service that supports:

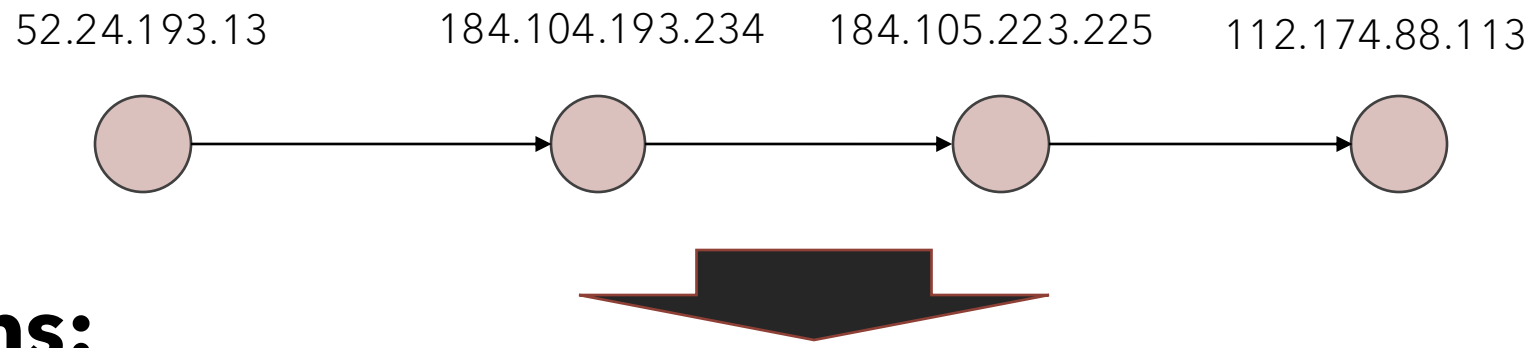
- Tagging (annotating) traceroutes
- Requesting traceroute execution
- Searching traceroutes by tag



Pathfinder Annotations:

Input:

- traceroute



Output Annotations:

- Country
- Organization
- Vendor

US USA

KR South Korea

UCSD

Hurricane Electric

kt Korean T.

Cisco

Huawei

Cisco

Annotations Sources:

	Passive			Active
	BGP Collectors (RIPE NCC, Route Views 6447)	**Geolocation Service** (digital element)	**WHOIS Servers** (AFRINIC, lacnic, ARIN, APNIC)	**Distributed Monitors** (ARCHIPELAGO)
Country		X	X	X
Autonomous Systems	X			
Organization			X	
Vendor				X

Traceroute Upload

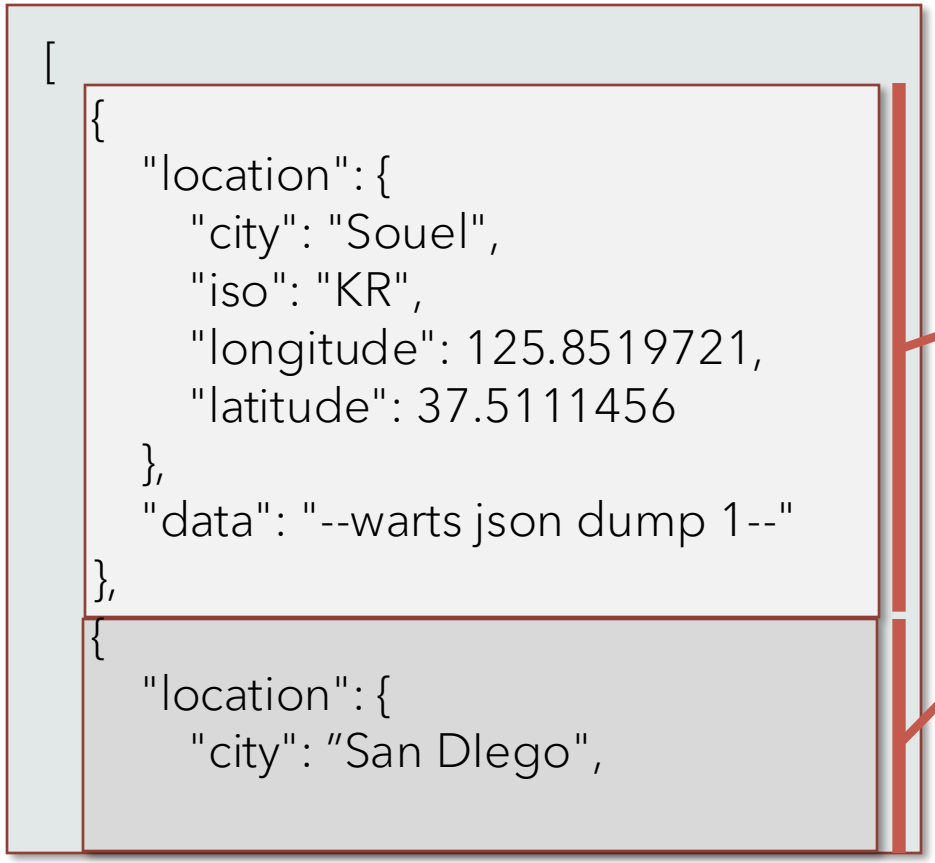
post request

Array of traceroutes

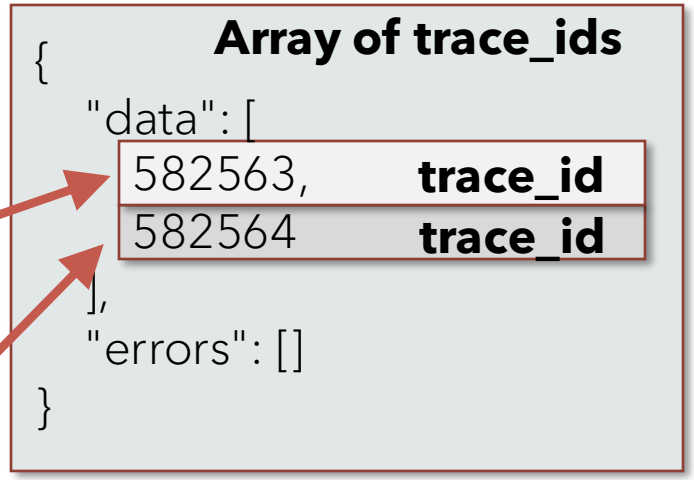
```
[
  {                                          single traceroute
    "location": {                            monitor location
      "city": "Seoul",
      "iso": "KR",
      "longitude": 125.8519721,
      "latitude": 37.5111456
    },
    "data": "--warts json dump 1--"          JSON/warts
  },
  {
    "location": {
      "city": ”San Dlego",
```

Traceroute Upload

post request



response



Traceroute Annotations

get request

```
{
   "data": [
     582563,
     582564
   ],
   "errors": []
}
```

http://api…/v2/traceroutes/582563

response

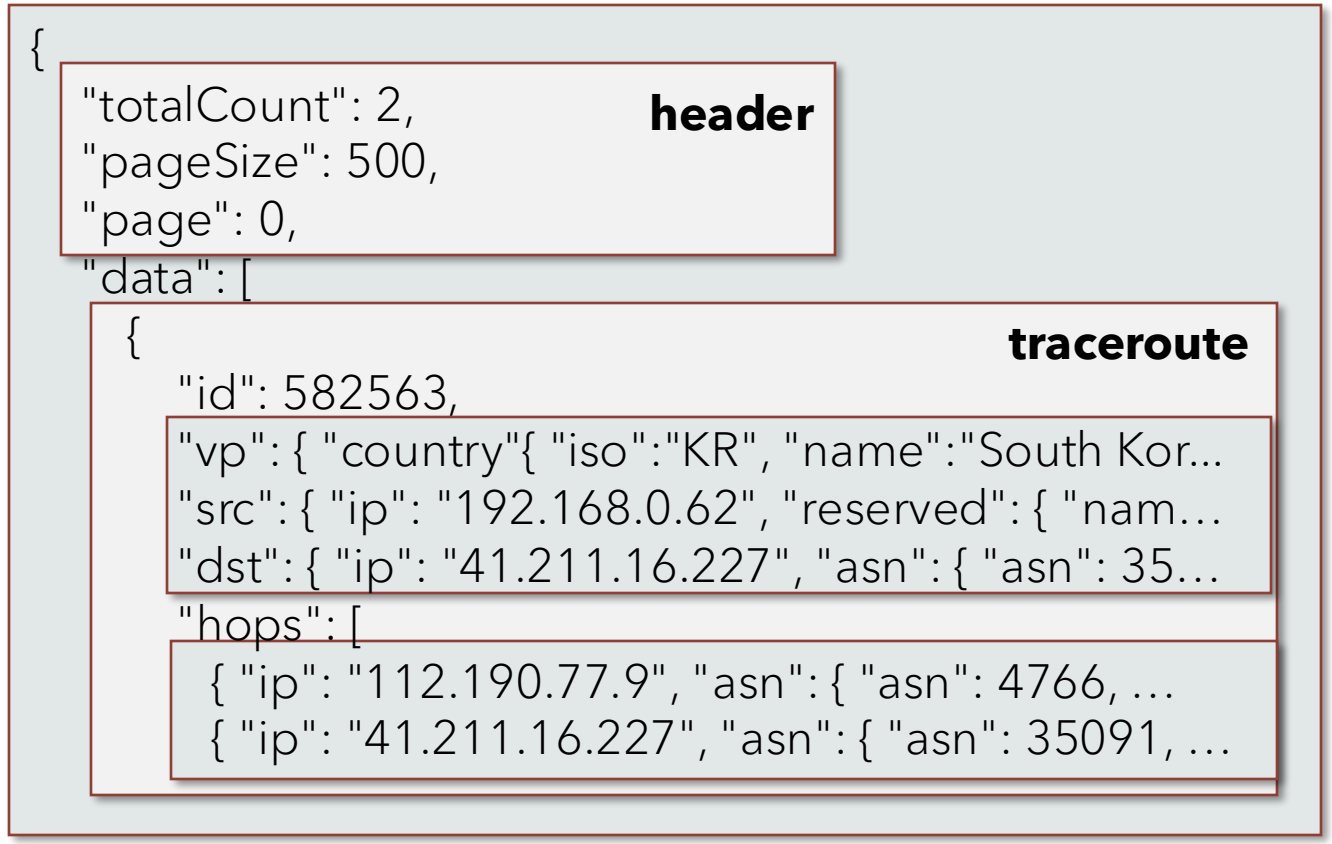
```
{
   "totalCount": 2,
   "pageSize": 500,
   "page": 0,
   "data": [
     {
        "id": 582563,
        "vp": {
           "country": {
              "iso": ”KR",
              "iso3": " KRS",
              "name": ”South Korea",
              "method": ”user",
        }
```

header

traceroute

Traceroute Annotations

response



annotations

vantage point
Source IP
Destination IP

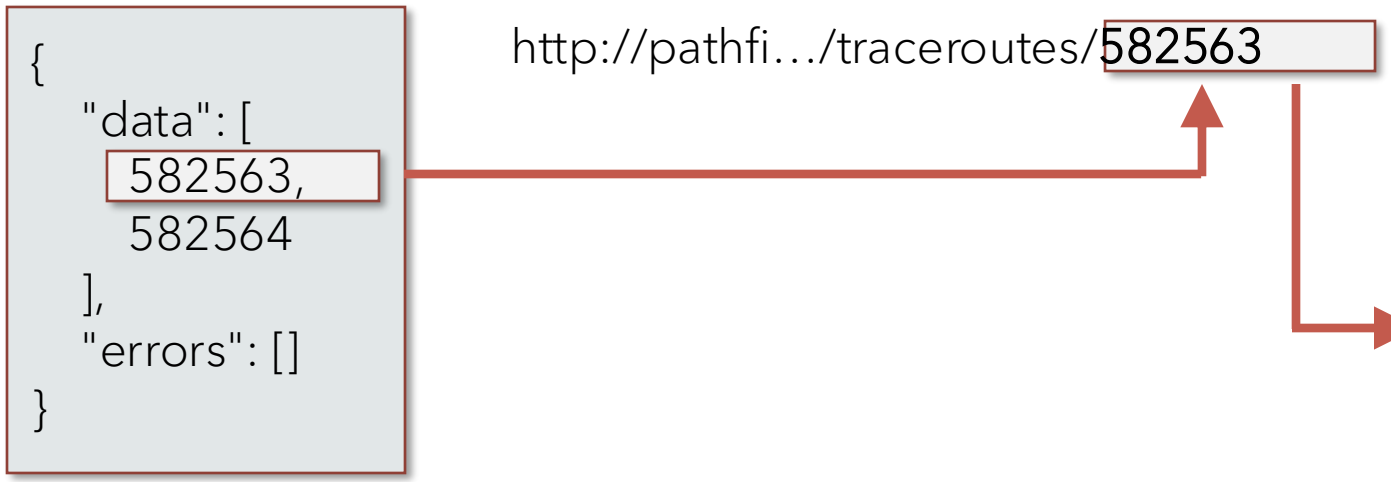
hops

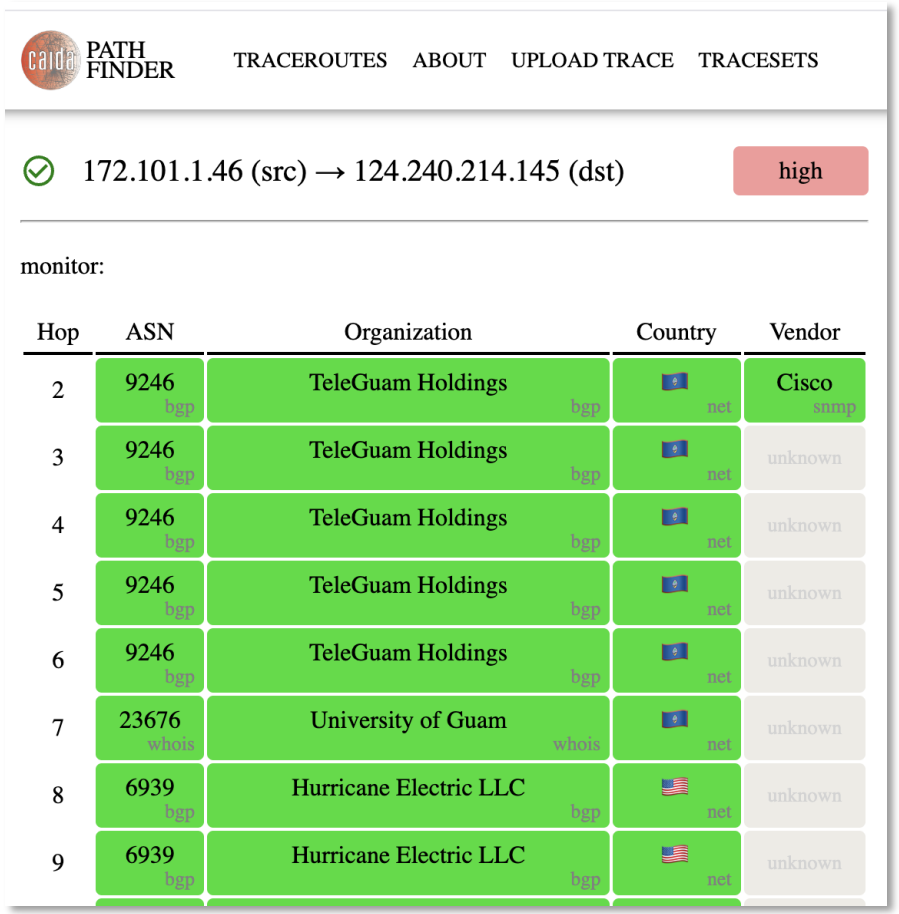
IP Annotations


```
{
  "ip": "112.190.77.9",
  "asn": {                                   AS
    "asn": 4766,
    "name": "Korea Telecom",
    "country": {
      "iso": "KR",
      "iso3": "KOR",
      "name": "South Korea",
      "threat": 3
    },
    "method": "bgp",
    "threat": 3
  },
  "country": {                               country
    "iso": "KR",
    "iso3": "KOR",
    "name": "South Korea",
    "method": "net",
    "threat": 3
  },
  "organization": {                          org
    "name": "Korea Telecom",
    "method": "bgp"
  },
  "vendor": {                                vendor
    "id": 25506,
    "name": "H3C",
    "country": {
      "iso": "CN"
    },
    "threat": 10,
    "method": "snmp"
  }
}
```

Traceroute Annotations

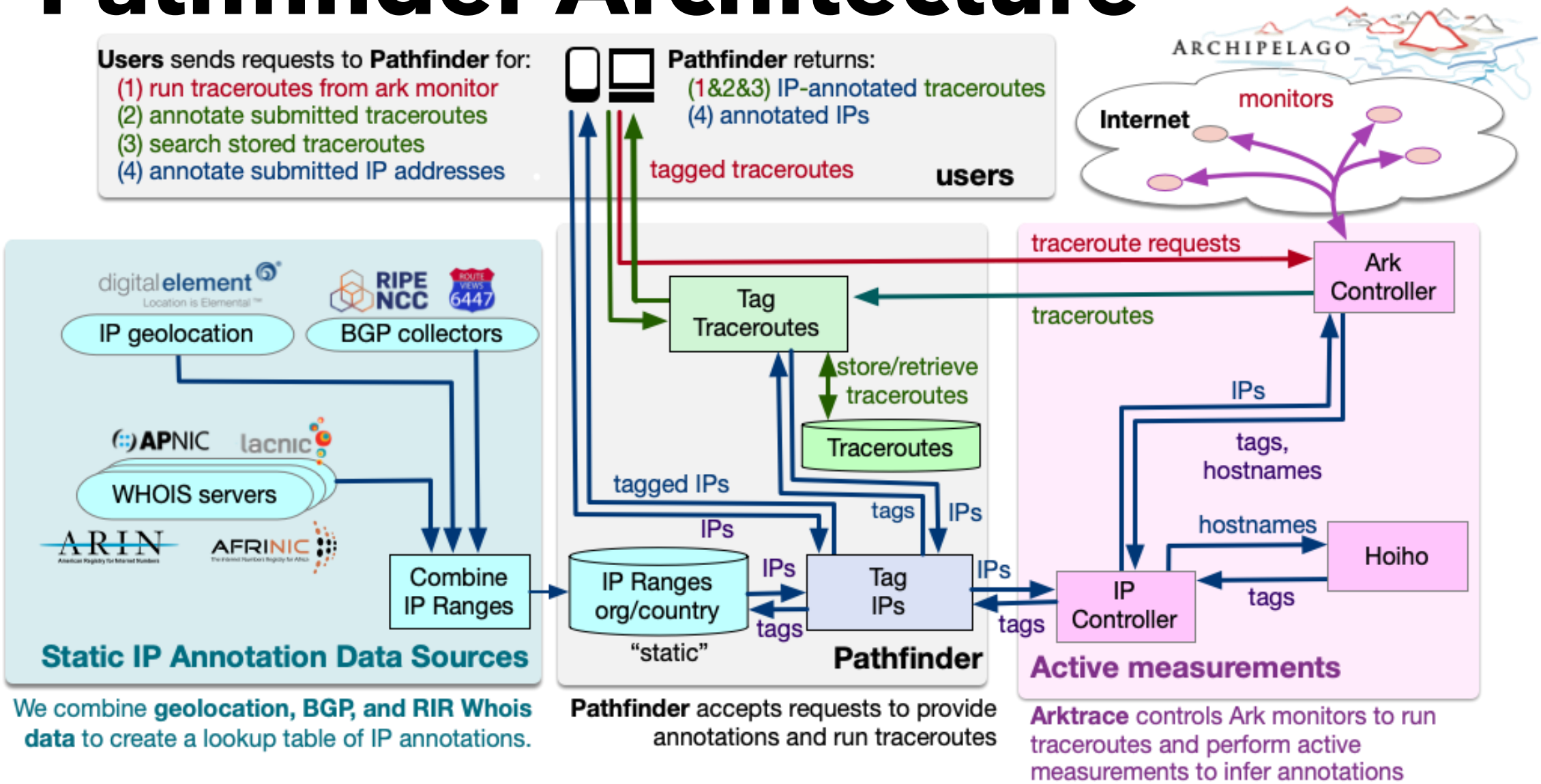
web UI



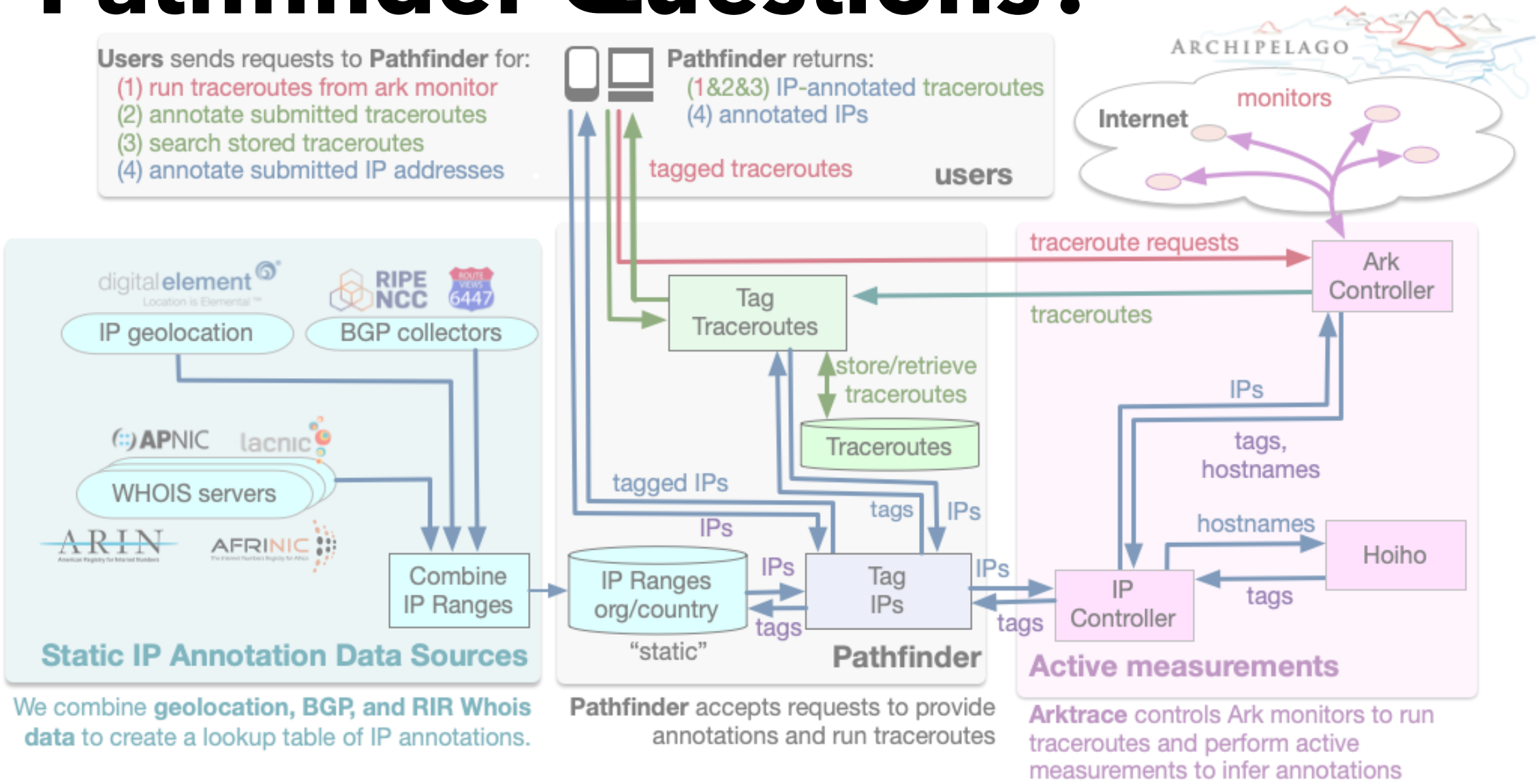


Hop	ASN	Organization	Country	Vendor
2	9246 bgp	TeleGuam Holdings bgp	net	Cisco snmp
3	9246 bgp	TeleGuam Holdings bgp	net	unknown
4	9246 bgp	TeleGuam Holdings bgp	net	unknown
5	9246 bgp	TeleGuam Holdings bgp	net	unknown
6	9246 bgp	TeleGuam Holdings bgp	net	unknown
7	23676 whois	University of Guam whois	net	unknown
8	6939 bgp	Hurricane Electric LLC bgp	net	unknown
9	6939 bgp	Hurricane Electric LLC bgp	net	unknown

Pathfinder Architecture



Pathfinder Questions?



We combine **geolocation, BGP, and RIR Whois data** to create a lookup table of IP annotations.

Pathfinder accepts requests to provide annotations and run traceroutes

Arktrace controls Ark monitors to run traceroutes and perform active measurements to infer annotations