IMPOSING RISK AND CONSEQUENCES ON CYBER ADVERSARIES

Domain Name System (DNS) and The Onion Router (TOR)

David M. Martin, GSE
Unit Chief
FBI Cyber Division
Cyber Technical Analysis Unit

FBI CYBER

DNS Primer

DNS – What is it?

- DNS: “Domain Name System”
- Maps names of servers on the Internet to numeric IP addresses
- Works similarly to the way phone directories map names to phone numbers

Phone Book

J. Doe 202-324-3000

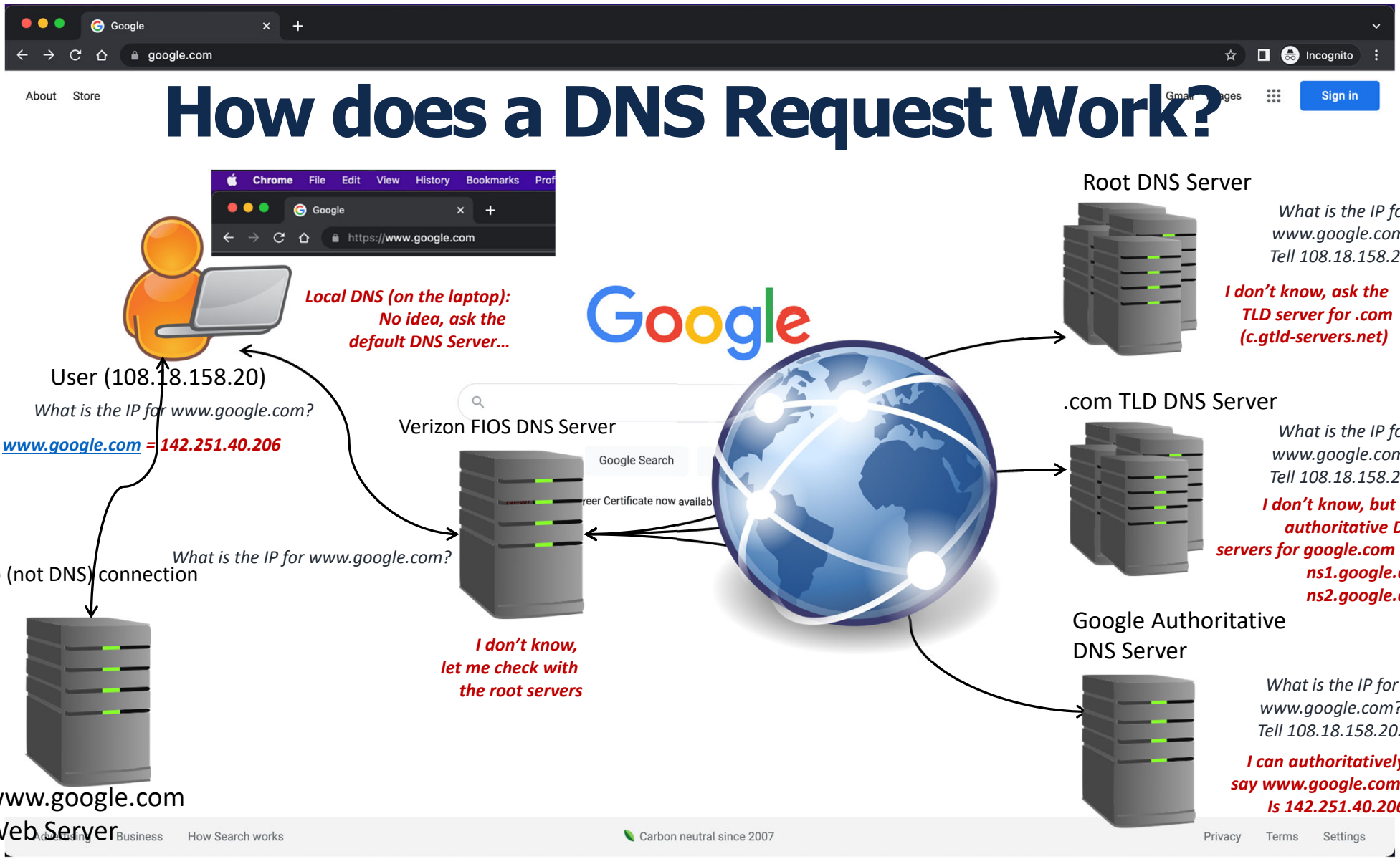
A. Smith 312-555-5555

DNS

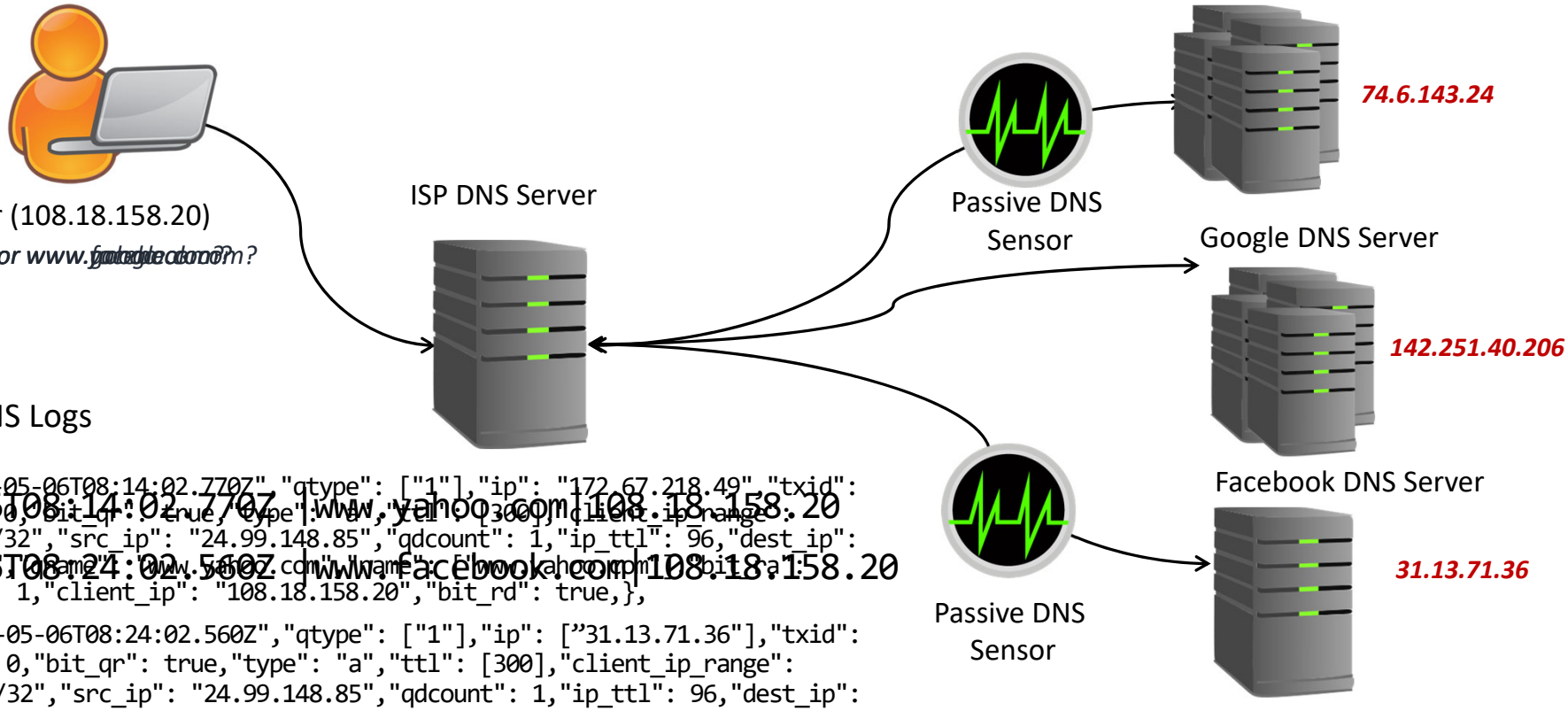
www.google.com 142.251.40.164

www.yahoo.com 74.6.231.20

How does a DNS Request Work?



Passive DNS



Passive DNS Logs

2022-05-06T08:14:02.770Z|www.yahoo.com|108.18.158.20

2022-05-06T08:24:02.560Z|www.facebook.com|108.18.158.20

{"date": "2022-05-06T08:14:02.770Z","qtype": ["1"],"ip": "172.67.218.49","txid": 57016,"rcode": 0,"bit_qr": true,"type": "a","ttl": [300],"client_ip_range": "108.18.158.20/32","src_ip": "24.99.148.85","qdcount": 1,"ip_ttl": 96,"dest_ip": "108.18.158.20","qname": "www.yahoo.com","name": ["www.yahoo.com"],"bit_ra": true,"ancount": 1,"client_ip": "108.18.158.20","bit_rd": true,},

{"date": "2022-05-06T08:24:02.560Z","qtype": ["1"],"ip": ["31.13.71.36"],"txid": 57127,"rcode": 0,"bit_qr": true,"type": "a","ttl": [300],"client_ip_range": "108.18.158.20/32","src_ip": "24.99.148.85","qdcount": 1,"ip_ttl": 96,"dest_ip": "108.18.158.20","qname": "www.facebook.com","name": ["www.facebook.com"],"bit_ra": true,"ancount": 1,"client_ip": "108.18.158.20","bit_rd": true,},

TOR Primer

TOR (The Onion Router)

- Open network designed to enable anonymity on the Internet
  - Operated by the TOR Project, a non-profit internet privacy organization
  - Runs through computers operated by volunteers
- Each connection is routed through a different, random set of computers
  - Often in different countries
- The TOR Project publishes a list of all TOR exit nodes
  - Data is available back to February 2010

Tor Network Basics