Today's Speakers:

Daniel B. Garrie, Executive Managing Partner, Law and Forensics; Special Master, Arbitrator, Forensic Neutral, JAMS

William Spernow, Chief Forensic Officer, Law and Forensics

Jeffrey Rosenfeld, Of Counsel, Blank Rome LLP

Forensics: What Lawyers Need to Know about Forensic Technology and Strategies to Litigate Data Privacy and Cybersecurity Breaches

Daniel B. Garrie, Esq.
Executive Managing Partner, Law & Forensics
Special Master, Neutral, Arbitrator, JAMS

William Spernow
Chief Forensic Officer, Law & Forensics

Jeffrey Rosenfeld,
Of Counsel, Blank Rome LLP

Disclaimer

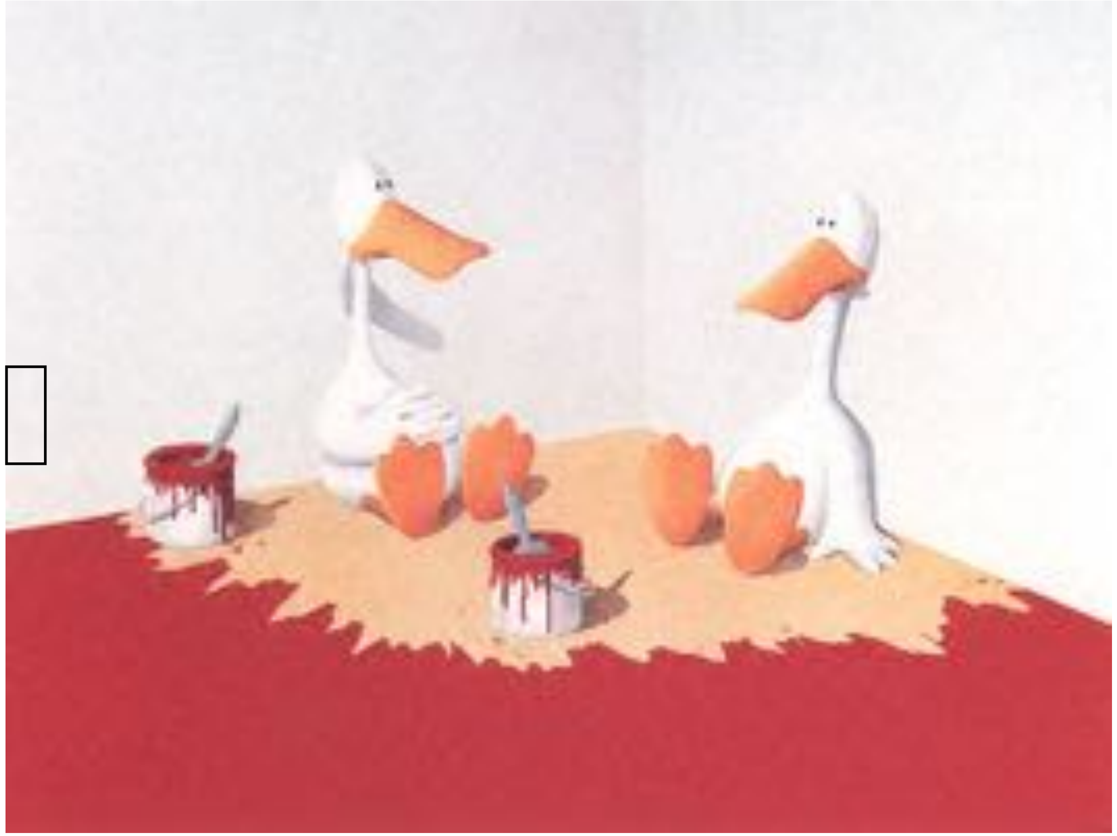
- This is not legal advice nor should it be considered legal advice
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients
- This presentation is offered for educational and informational uses only

Agenda

- Overview of Digital Forensic Evidence
- What is an IP Address
- What is an IP Port Number
- What is the Difference Between a Static and Dynamic IP v4 address
- How to find the IP Address of a Domain
- Questions

Overview of Digital Forensic Evidence

Forensic Evidence Dilemma



(Source: Author's private art collection,
M. Bedard / www.sitting-ducks.com)

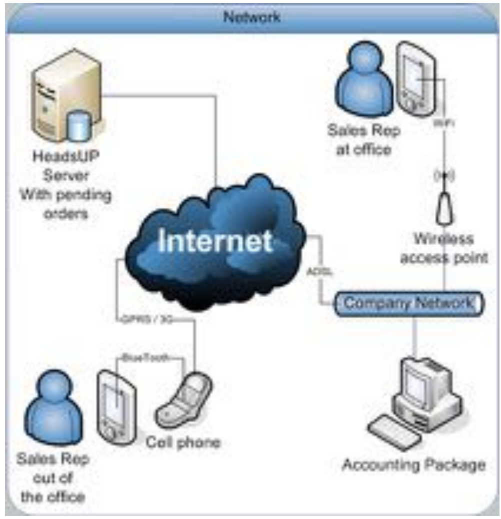
No Artifacts = No Evidence

Computer Data as Forensic Evidence

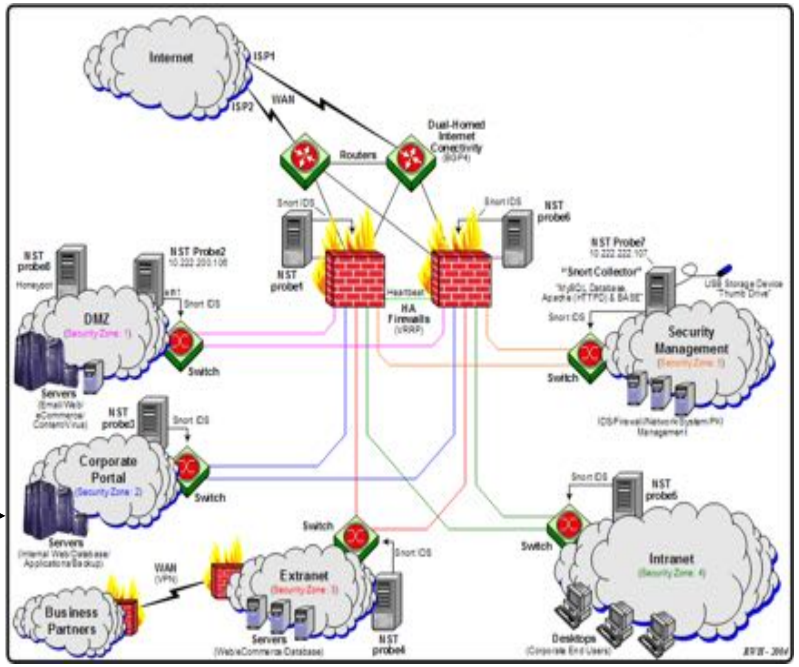
- Financial Fraud / Credit Card Theft
- Incident Response / Hacks / Trojans
- Intellectual Property Theft
- Identity Theft / Phishing / Spyware
- Internal Policy Violations
- Legal / Regulatory Compliance
- Civil eDiscovery Mandates (FRCP)

Types of Forensic Examinations

Standalone (single computer)



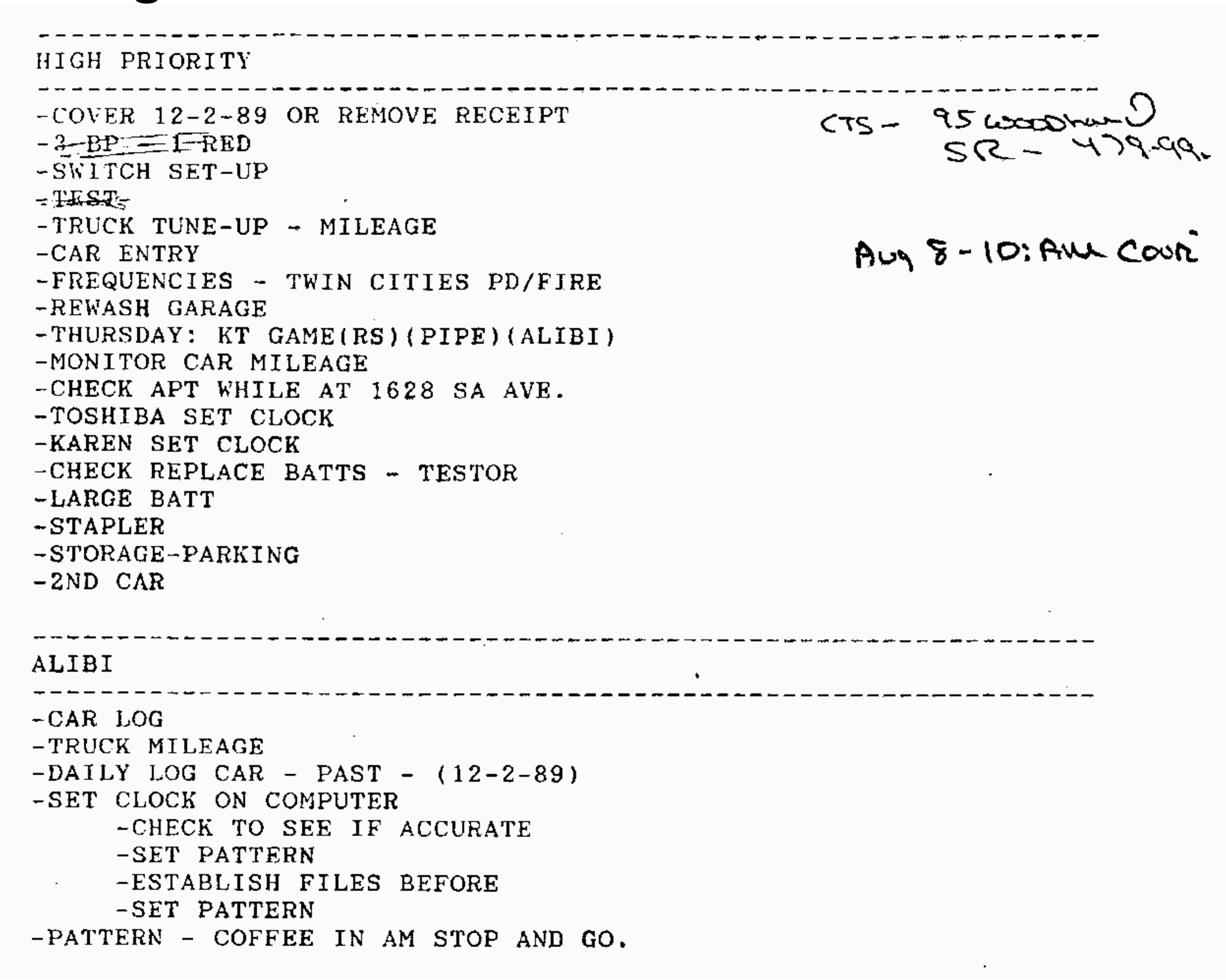
Network (packet traffic, e-mail spoofing, Web hacking, etc)



Internet
ISP1
ISP2
WAN
Dual-Homed Internet Connectivity (BGP4)
Routers
Snort IDS
NST probe1
Snort IDS
NST probe6
Heartbeat
HA Firewalls (VRRP)
NST probe8
Honeypot
NST Probe2 10.222.200.108
Snort IDS
DMZ (Security Zone: 1)
Switch
Servers (Email/Web/eCommerce/Content/Virus)
NST Probe7 10.222.222.107
"Snort Collector"
"MySQL Database Apache (HTTPD) & BASE"
USB Storage Device "Thumb Drive"
Snort IDS
Security Management (Security Zone: 5)
Switch
IDS/Firewall/Network/System/PKI Management
NST probe3
Snort IDS
Corporate Portal (Security Zone: 2)
Switch
Servers (Internal Web/Database/Applications/Backup)
Switch
Snort IDS
NST probe5
Switch
Intranet (Security Zone: 4)
Desktops (Corporate End Users)
WAN (VPN)
Business Partners
Extranet (Security Zone: 3)
Servers (Web/eCommerce/Database)
Snort IDS
NST probe4
RWH - 2004

Enterprise (business model, fraud, lawsuits, compliance, etc.)

Finding The Smoking Gun: Some Real Evidence



```
------------------------------------------------------------------
HIGH PRIORITY
------------------------------------------------------------------
-COVER 12-2-89 OR REMOVE RECEIPT
-~~2-BP = 1-~~RED
-SWITCH SET-UP
-~~TEST~~
-TRUCK TUNE-UP - MILEAGE
-CAR ENTRY
-FREQUENCIES - TWIN CITIES PD/FIRE
-REWASH GARAGE
-THURSDAY: KT GAME(RS)(PIPE)(ALIBI)
-MONITOR CAR MILEAGE
-CHECK APT WHILE AT 1628 SA AVE.
-TOSHIBA SET CLOCK
-KAREN SET CLOCK
-CHECK REPLACE BATTS - TESTOR
-LARGE BATT
-STAPLER
-STORAGE-PARKING
-2ND CAR

------------------------------------------------------------------
ALIBI
------------------------------------------------------------------
-CAR LOG
-TRUCK MILEAGE
-DAILY LOG CAR - PAST - (12-2-89)
-SET CLOCK ON COMPUTER
     -CHECK TO SEE IF ACCURATE
     -SET PATTERN
     -ESTABLISH FILES BEFORE
     -SET PATTERN
-PATTERN - COFFEE IN AM STOP AND GO.
```

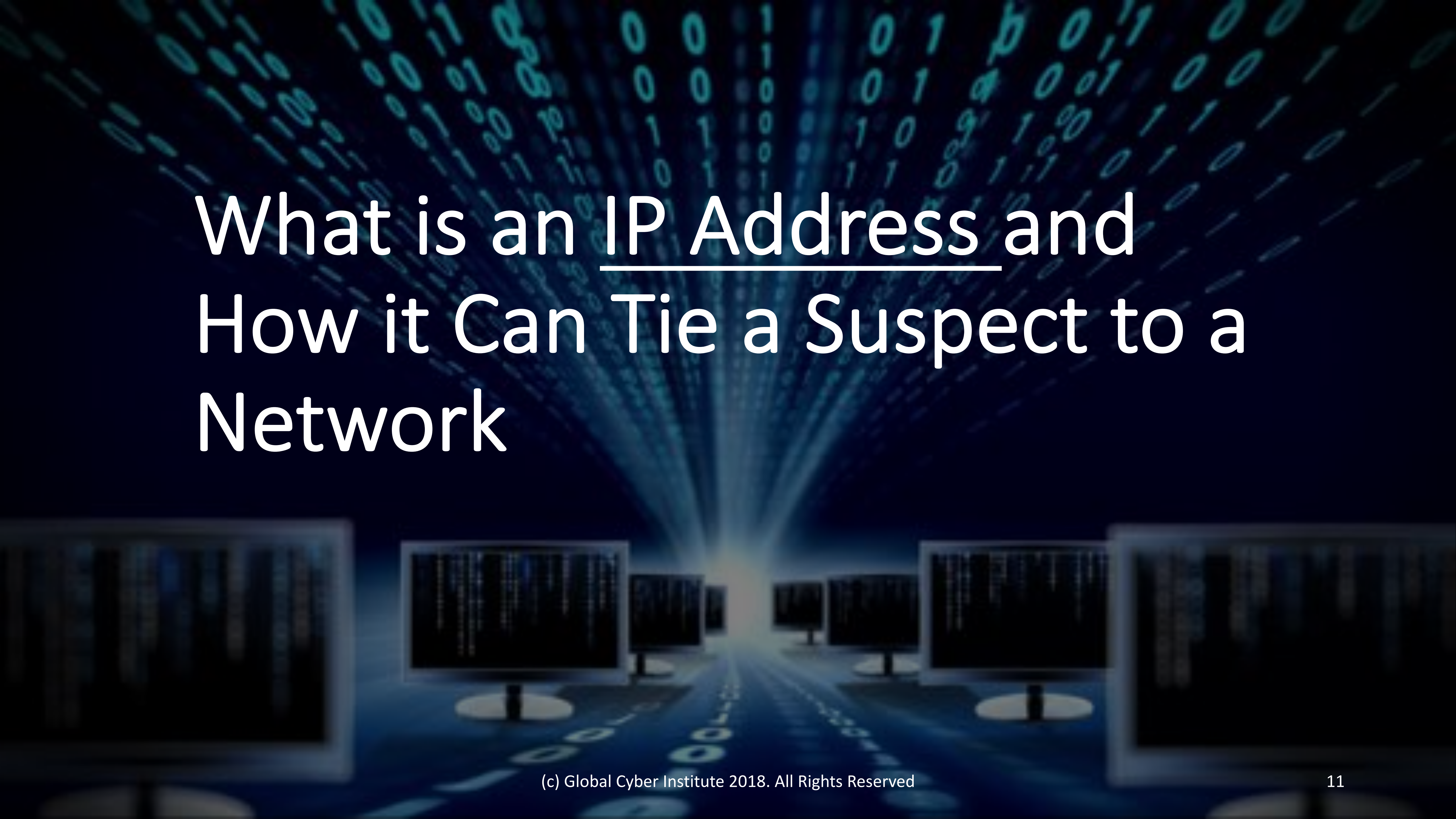
CTS - 95 Woodhead
SR - 479.99.

Aug 8-10: AM Cour

The original evidence was found in slack space. These are printouts of that evidence…

Standalone Forensics: The 4 Core Training Areas

1. Evidence Acquisition Techniques
2. Evidence Preservation Procedures
3. Analysis Methodologies
4. Court Presentation Skills

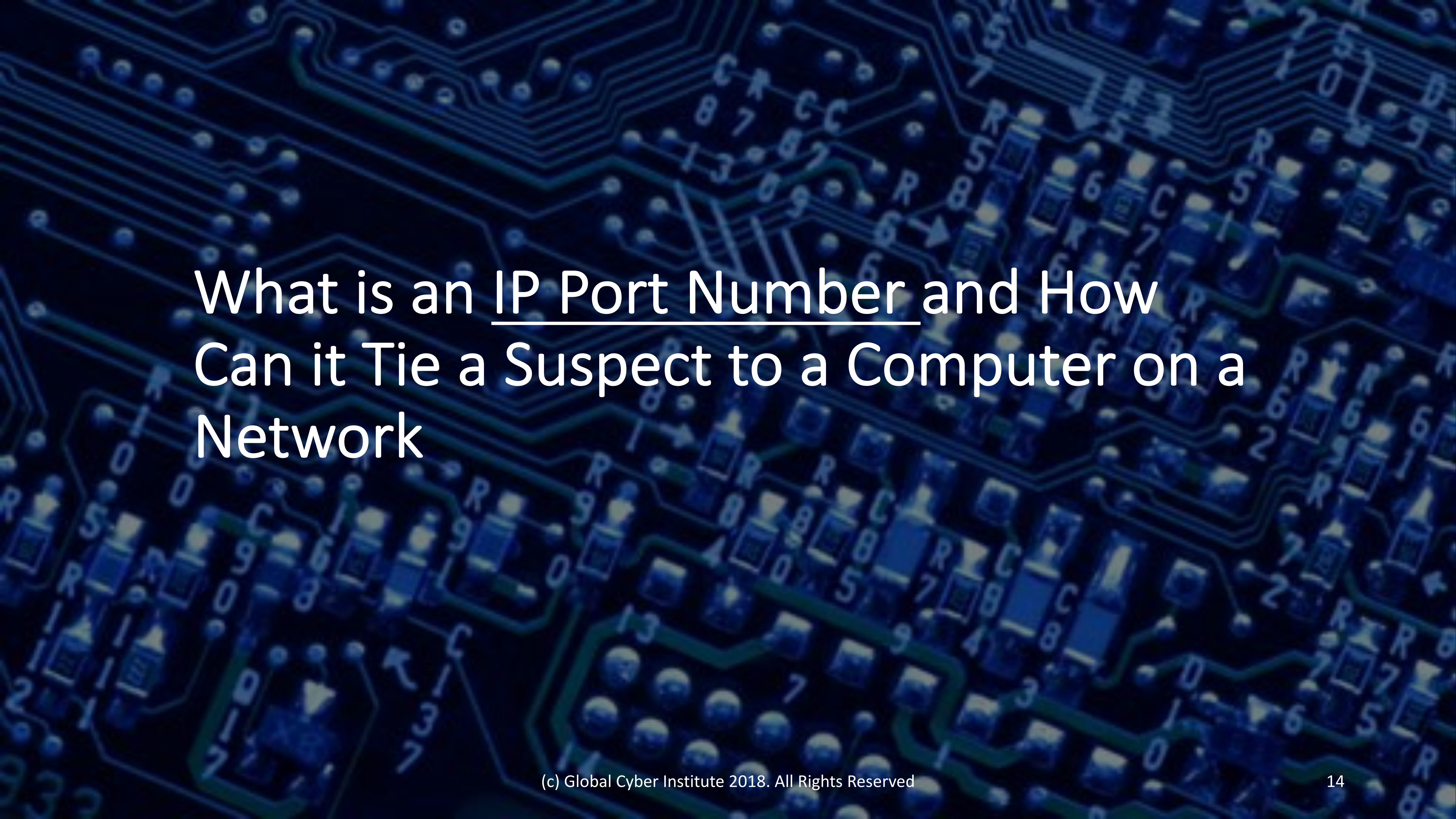


What is an IP Address and How it Can Tie a Suspect to a Network

Network IP v4 Address

- Purpose: Unique network identifier
- Format: AAA.BBB.CCC.DDD
- Low Range: 000.000.000.000
- High Range: 255.255.255.255
- Sample: 23.66.230.16 (foxnews.com)
- Max Possible Today: $(256)^4$ = 4,294,967,296
- Primary Types: Routable, Non-Routable, Static and Dynamic

Think of an IP Address as a License Plate Number

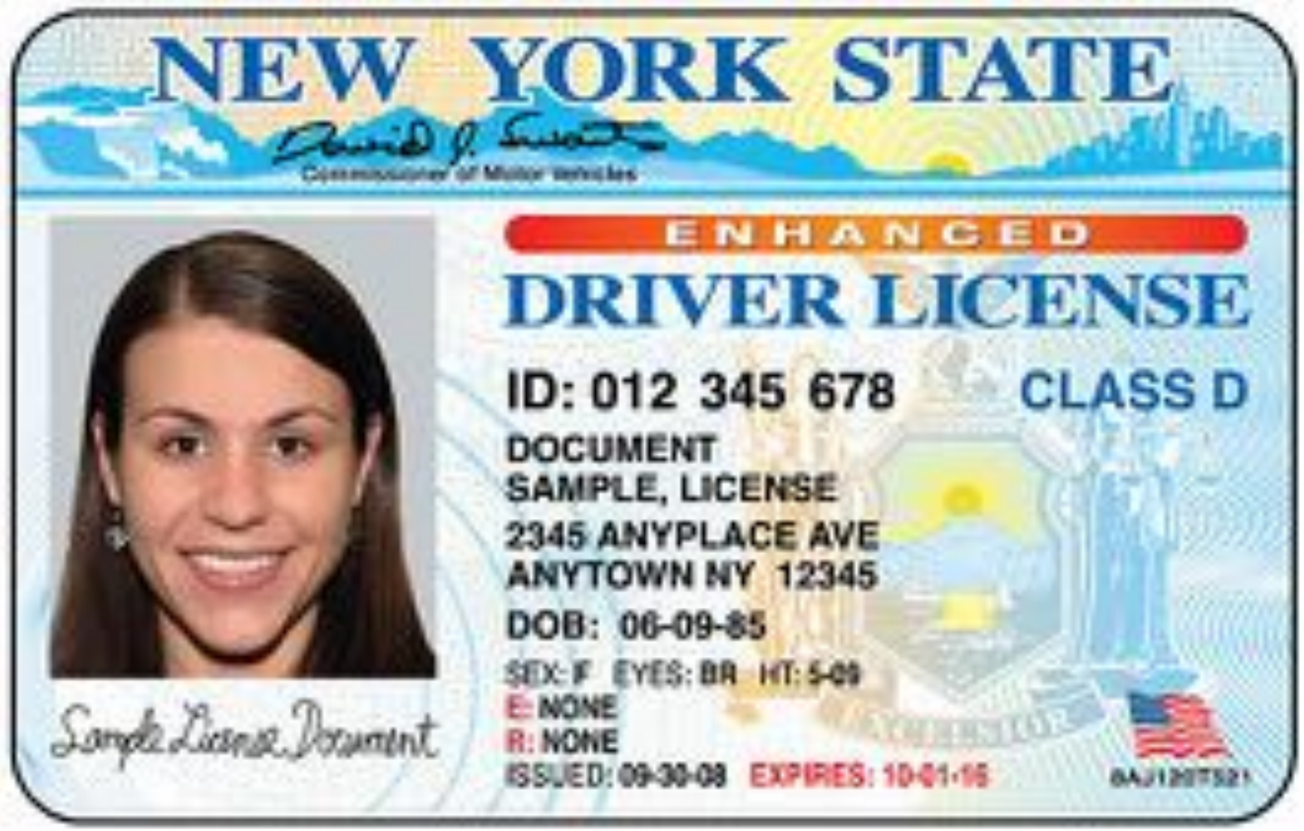


What is an IP Port Number and How Can it Tie a Suspect to a Computer on a Network

IP Port Numbers

- Purpose: Allow multiple access points into and out of a single IP address
- Format: Single number
- Low Range: 0
- High Range: 65,536
- Sample: Port 110 (get e-mail)
  Port 25 (send e-mail)
  Port 80 (Web site default)
- Max Possible Ports Per IP address: 65,536
- Primary Port Types: 0 → 1024 (per defined)
  1025 → 65,536 (open)

Think of a Port Address as a Driver’s License Number



NEW YORK STATE

Commissioner of Motor Vehicles

ENHANCED

DRIVER LICENSE

ID: 012 345 678 CLASS D

DOCUMENT
SAMPLE, LICENSE
2345 ANYPLACE AVE
ANYTOWN NY 12345

DOB: 06-09-85

SEX: F EYES: BR HT: 5-09

E: NONE

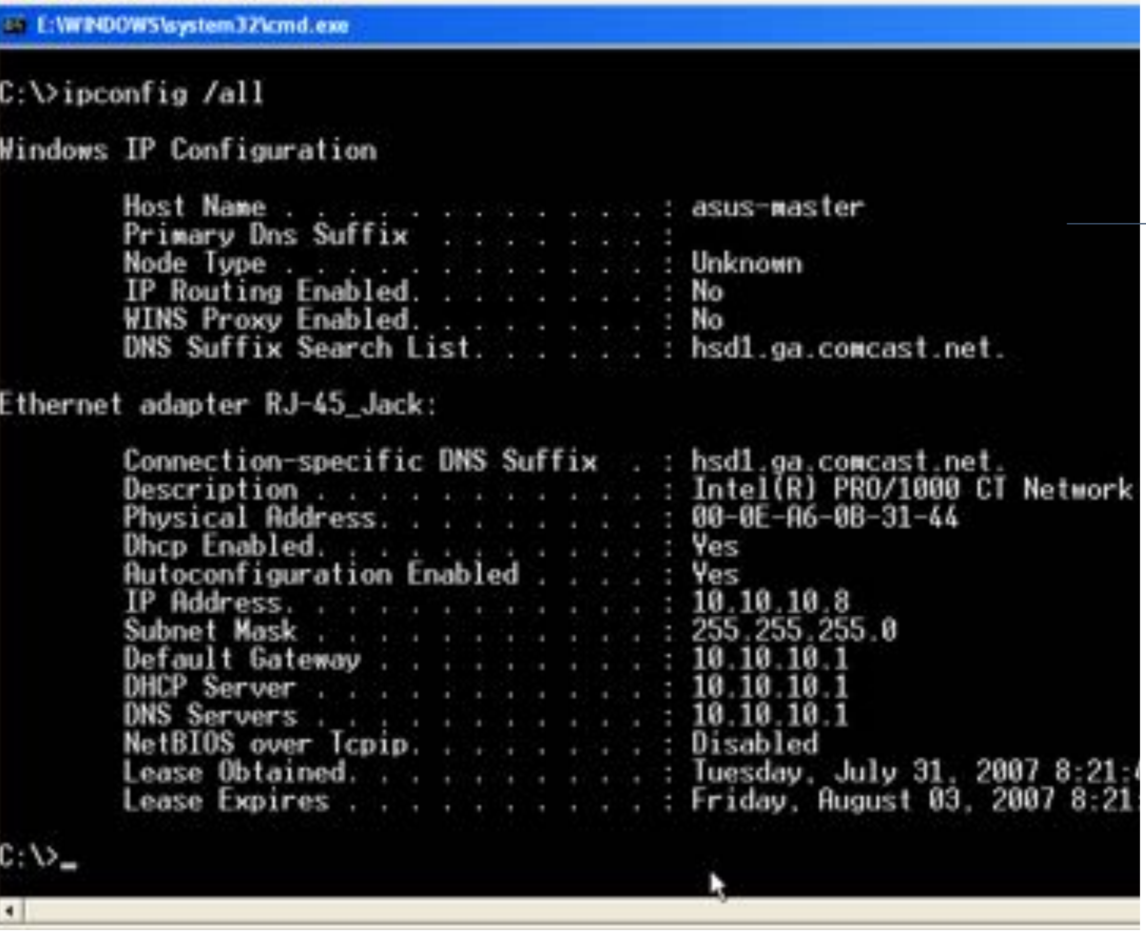
R: NONE

ISSUED: 09-30-08 EXPIRES: 10-01-16

8AJ120T521

Sample License Document

So, what is your MAC ID number and Network IP address?



```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : asus-master
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : hsd1.ga.comcast.net.

Ethernet adapter RJ-45_Jack:

        Connection-specific DNS Suffix  . : hsd1.ga.comcast.net.
        Description . . . . . . . . . . . : Intel(R) PRO/1000 CT Network
        Physical Address. . . . . . . . . : 00-0E-A6-0B-31-44
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.10.10.8
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.10.10.1
        DHCP Server . . . . . . . . . . . : 10.10.10.1
        DNS Servers . . . . . . . . . . . : 10.10.10.1
        NetBIOS over Tcpip. . . . . . . . : Disabled
        Lease Obtained. . . . . . . . . . : Tuesday, July 31, 2007 8:21:
        Lease Expires . . . . . . . . . . : Friday, August 03, 2007 8:21

C:\>_
```

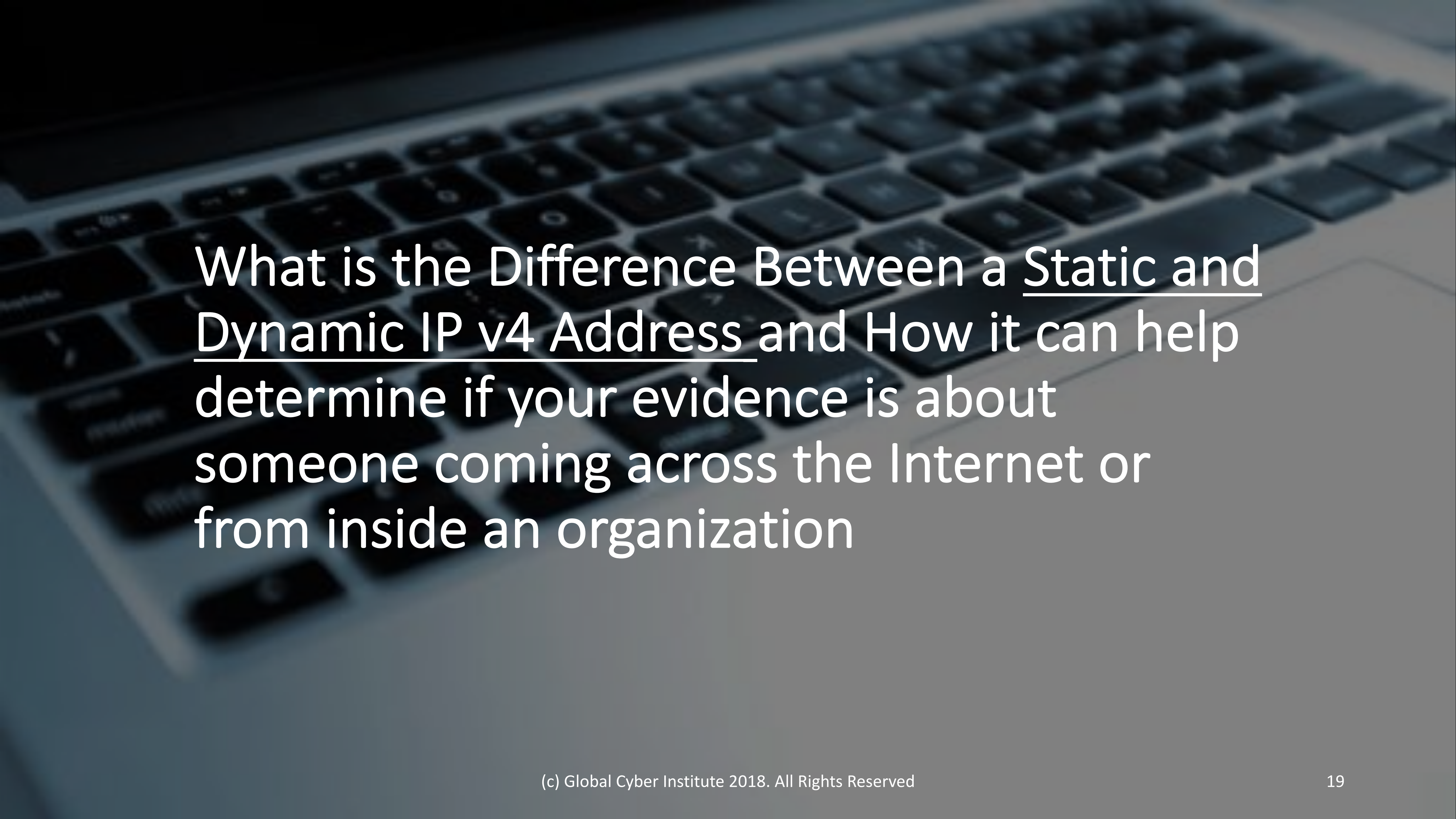
Lets Find Out..

- Windows Desktop
  - Start ➔ Run → type in CMD -> OK
- Windows opens up a DOS box
  - type in IPCONFIG /all press “Enter”
- Search for “Physical Address (aka MAC)” and “IP Address” on left hand side.
- The values you find are unique for your PC / Laptop / Server / Router / etc.

Questions You Should Be Asking Yourself…

- Where does the IP address come from?
- Who assigns it to the PC or Laptop?
- Once assigned, is it forever?
- How does the system know its unique?
- Can IP addresses be reused?

The answer to all these questions pivots on one single issue – is the IP Dynamic or Static?



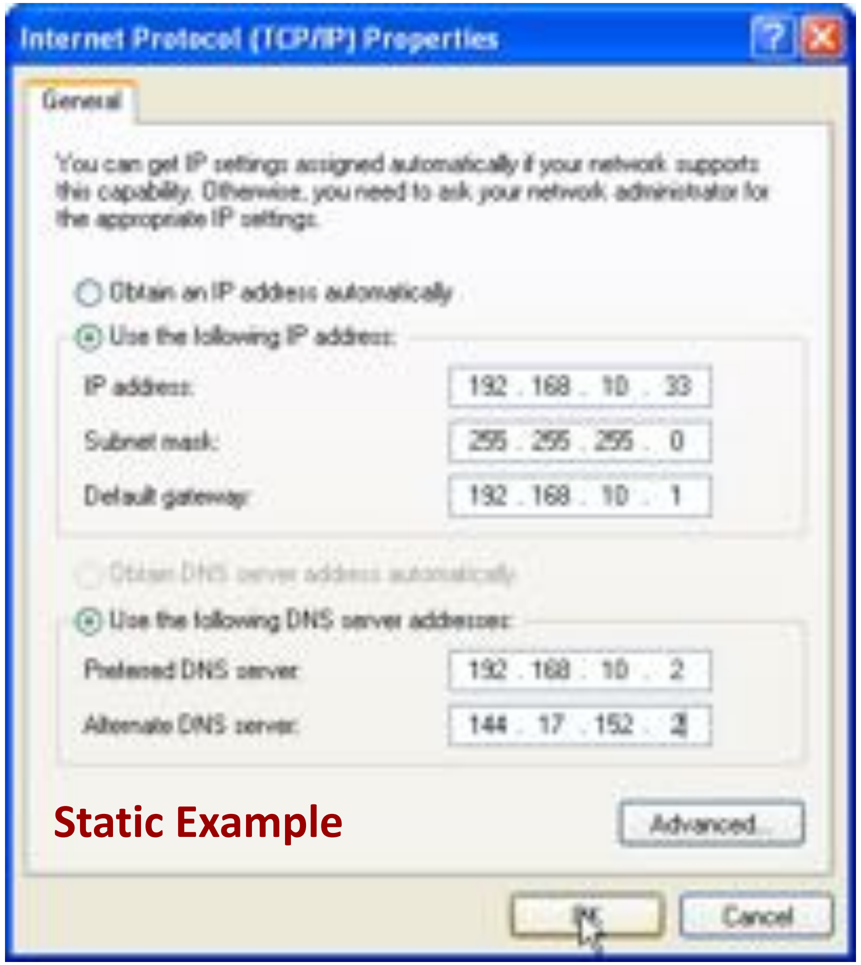
What is the Difference Between a Static and Dynamic IP v4 Address and How it can help determine if your evidence is about someone coming across the Internet or from inside an organization

Types of IP Addresses

- **Static** (makes for an easy investigation)
  - Created *manually* by User / Admin by typing it in to a network configuration form – can last forever. Ties suspect to a physical piece of evidence.
- **Dynamic** (complicates investigation)
  - Created *automatically* by the DHCP* service upon request during PC boot process – IP address assigned is leased for a set time period (which can be renewed). Logs are seldom kept. Over time different employees can have the same IP.

* Dynamic Host Configuration Protocol

Static vs. Dynamic


Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 33

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

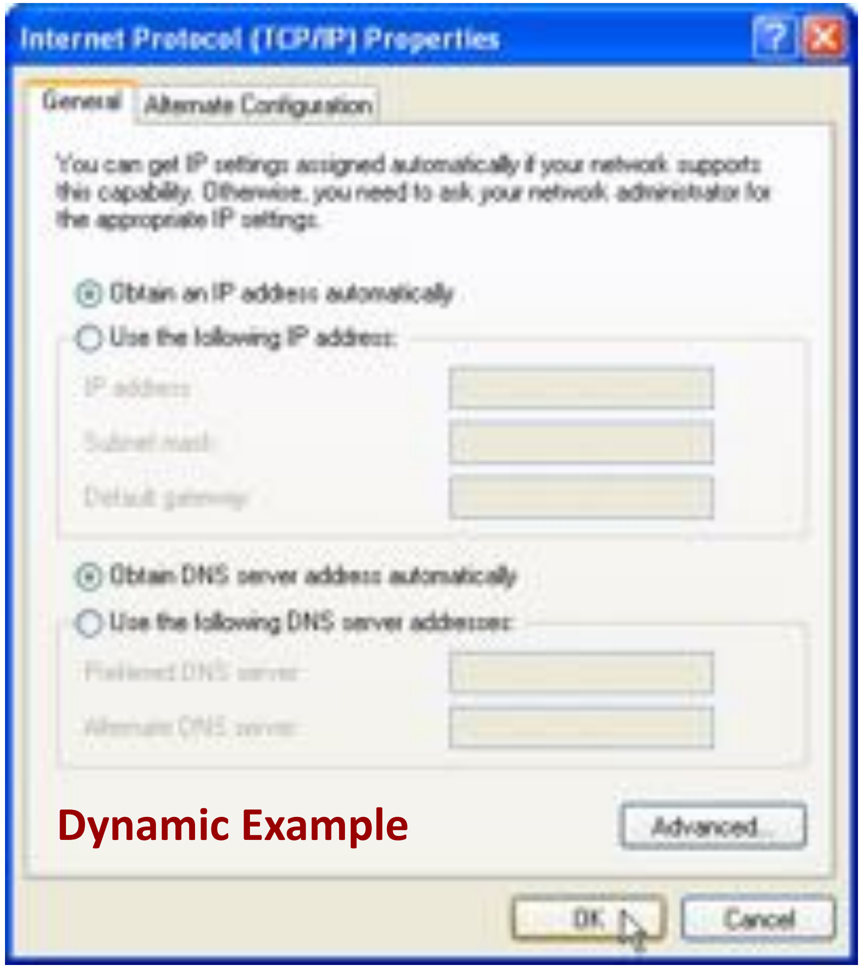
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 2

Alternate DNS server: 144 . 17 . 152 . 2

Static Example


Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

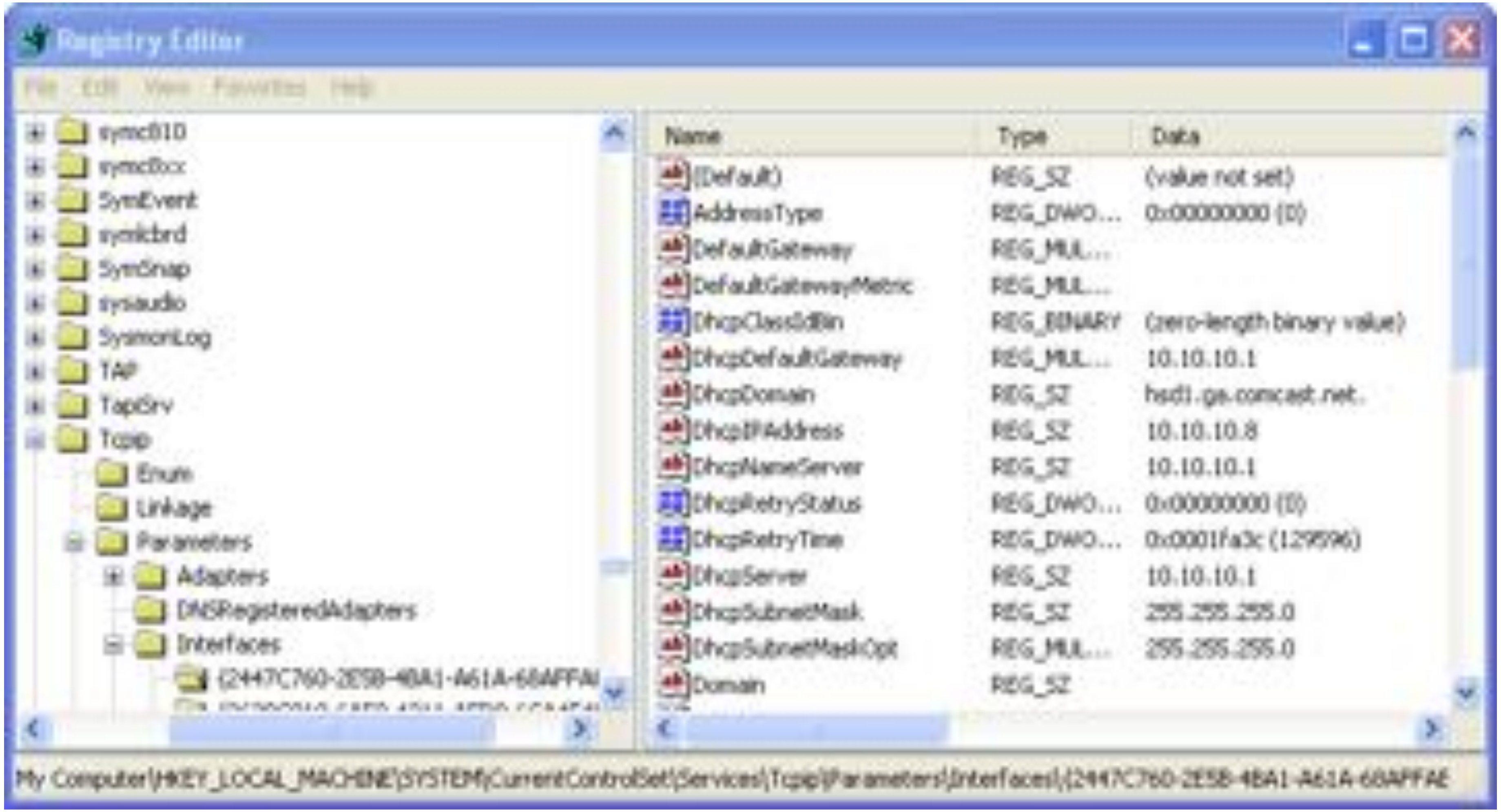
Preferred DNS server:

Alternate DNS server:

Dynamic Example

*Start → Settings → Network Connections → Local Area Connection → Properties →Internet Protocol (TCP/IP) → Properties

The Registry is Where This Information is Maintained



```
+ symc810
+ symc8xx
+ SymEvent
+ symlcbrd
+ SymSnap
+ sysaudio
+ SysmonLog
+ TAPI
+ TapiSrv
- Tcpip
    Enum
    Linkage
  - Parameters
    + Adapters
      DNSRegisteredAdapters
    - Interfaces
        {2447C760-2E58-4BA1-A61A-68AFFAE
```

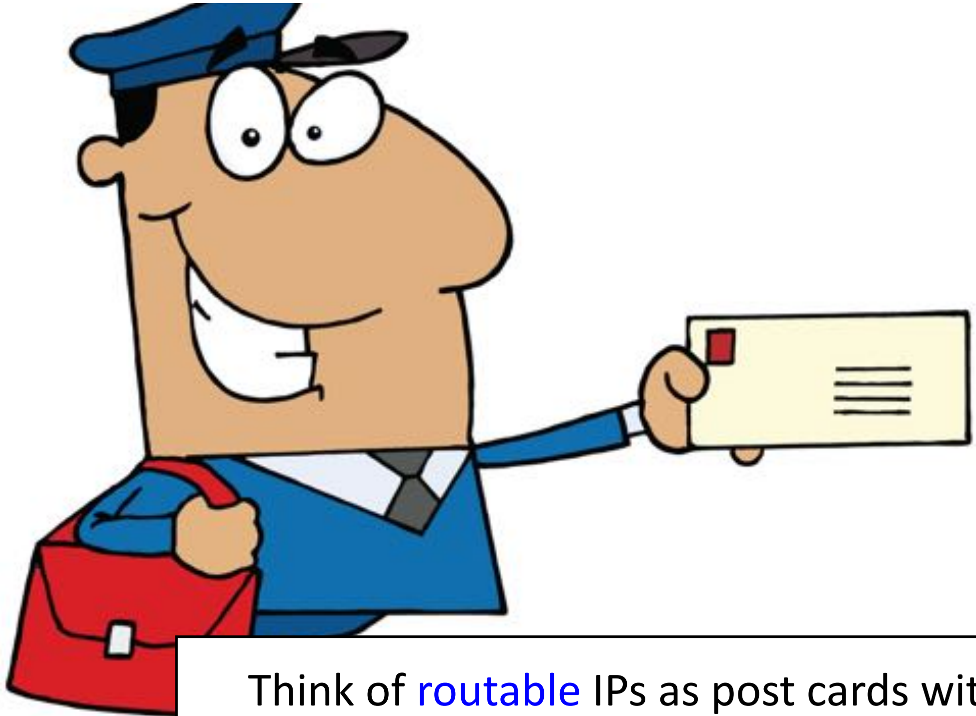
Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWO...	0x00000000 (0)
DefaultGateway	REG_MUL...	
DefaultGatewayMetric	REG_MUL...	
DhcpClassIdBin	REG_BINARY	(zero-length binary value)
DhcpDefaultGateway	REG_MUL...	10.10.10.1
DhcpDomain	REG_SZ	hsd1.ga.comcast.net.
DhcpIPAddress	REG_SZ	10.10.10.8
DhcpNameServer	REG_SZ	10.10.10.1
DhcpRetryStatus	REG_DWO...	0x00000000 (0)
DhcpRetryTime	REG_DWO...	0x0001fa3c (129596)
DhcpServer	REG_SZ	10.10.10.1
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMaskOpt	REG_MUL...	255.255.255.0
Domain	REG_SZ	

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2447C760-2E58-4BA1-A61A-68AFFAE

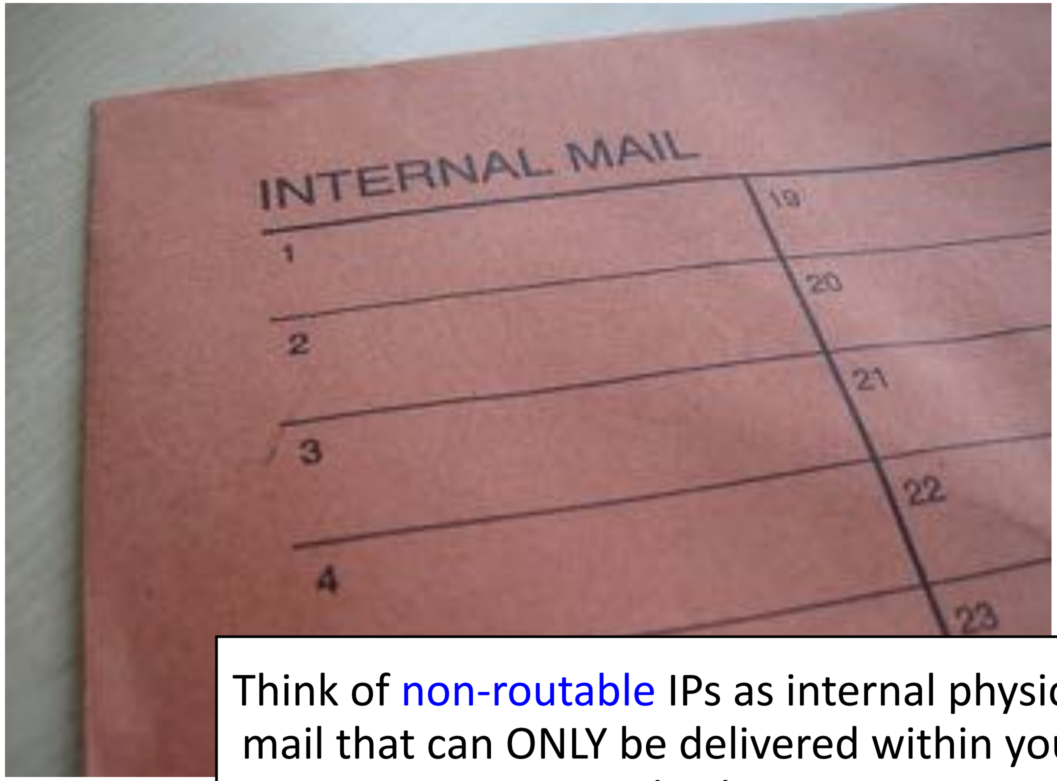
Is there a general rule that determines when to use static IPs vs dynamic IPs?

Yes, and that answer typically pivots on whether or not the IP needs to be routable or non-routable

Routable vs. Non-Routable



Think of routable IPs as post cards with stamps attached – they will be delivered by the Post Office (in this case to the Internet).



Think of non-routable IPs as internal physical mail that can ONLY be delivered within your organization.

Non-Routable “Private” IPs (local internal traffic ONLY!)

10.	0.	0.	0
↓	↓	↓	↓
10.	255.	255.	255

172.	16.	0.	0
↓	↓	↓	↓
172.	31.	255.	255

192.	168.	0.	0
↓	↓	↓	↓
192.	168.	255.	255

Are a subset of the maximum IPs possible in today’s world

Local Loopback Address

127.	0.	0.	0
↓	↓	↓	↓
127.	255.	255.	255

Nothing To Connect To

169.	254.	0.	0
↓	↓	↓	↓
169.	254.	255.	255

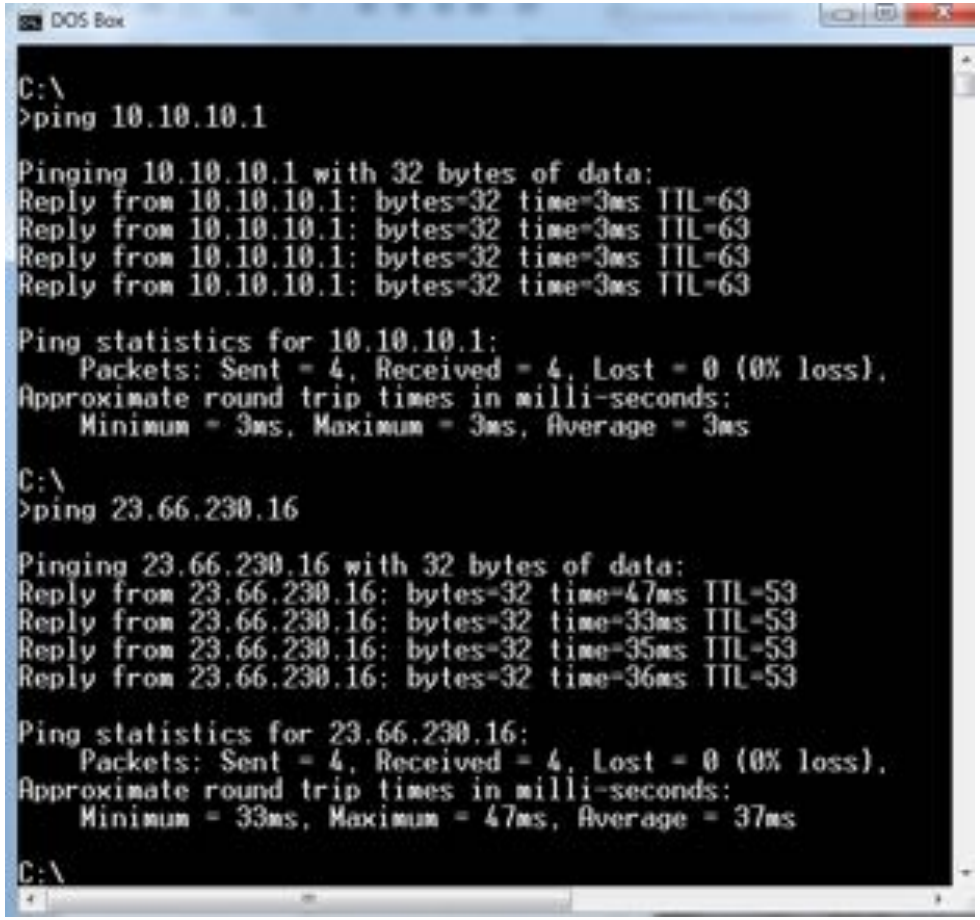
Source: http://www.rfc-editor.org/rfc/rfc3330.txt

Why Should I Be Concerned?

- **Non-routable** private IPs need to live behind something, a firewall or router for example, and are never connected directly to the Internet – they go thru some control point to reach the Net. Typically employees will all have non-routable **dynamic** IP addresses.
- In comparison, **routable** IPs are directly connected to the Internet. A public facing Web site, for example, typically needs a **static** routable IP address.

How to Find the IP Address of a Domain

How To Determine
If An IP Is "Live" Using PING*

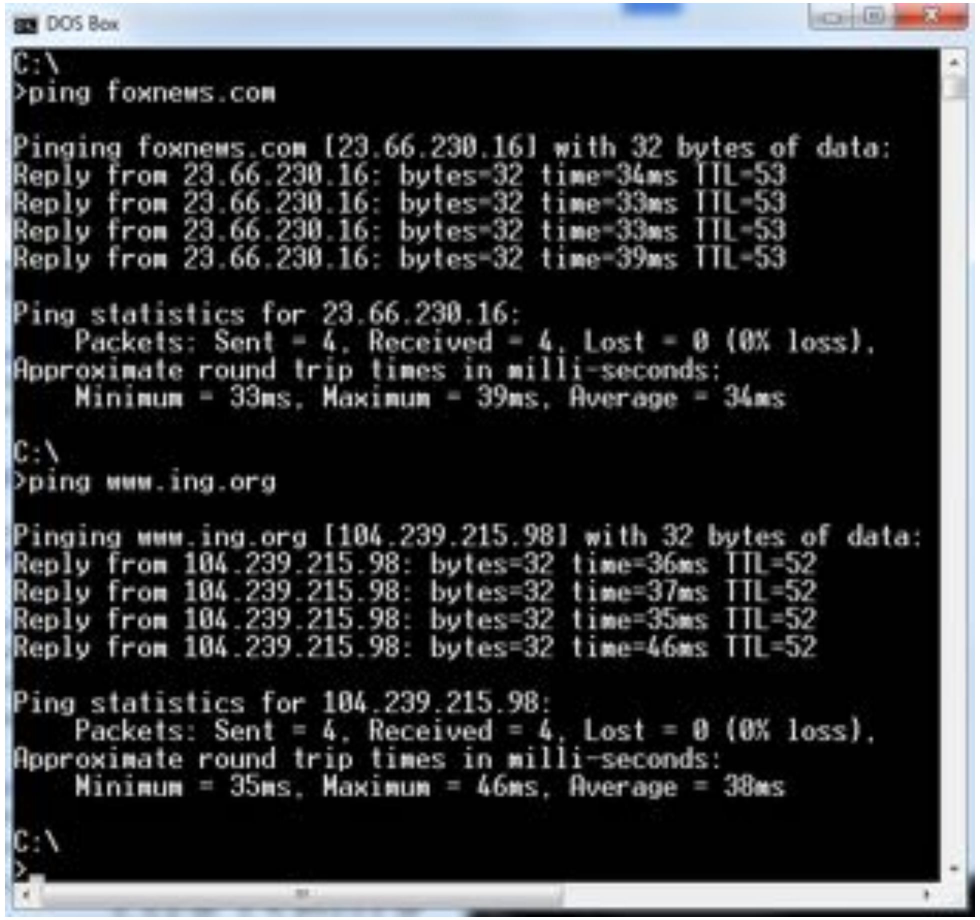


```
C:\
>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=3ms TTL=63
Reply from 10.10.10.1: bytes=32 time=3ms TTL=63
Reply from 10.10.10.1: bytes=32 time=3ms TTL=63
Reply from 10.10.10.1: bytes=32 time=3ms TTL=63

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\
>ping 23.66.230.16

Pinging 23.66.230.16 with 32 bytes of data:
Reply from 23.66.230.16: bytes=32 time=47ms TTL=53
Reply from 23.66.230.16: bytes=32 time=33ms TTL=53
Reply from 23.66.230.16: bytes=32 time=35ms TTL=53
Reply from 23.66.230.16: bytes=32 time=36ms TTL=53

Ping statistics for 23.66.230.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 47ms, Average = 37ms

C:\
```

Start ➔ Run ➔ Type in **CMD.EXE ➔** Click **GO**

*Packet InterNet Grouper utility created by Mike Muuss

How To Use PING When You Don’t Know The Actual IP, But Only The Name

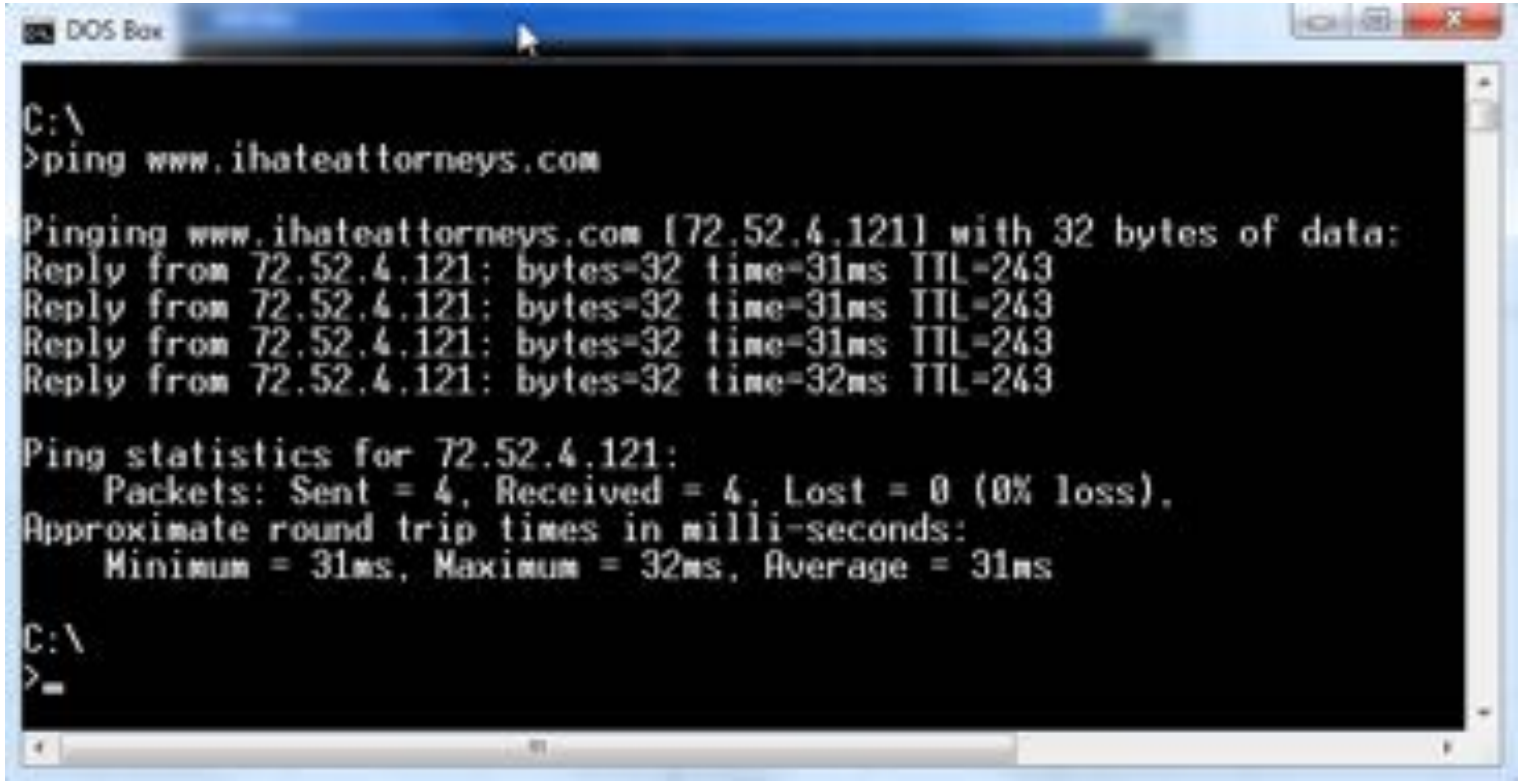


```
C:\
>ping foxnews.com

Pinging foxnews.com [23.66.230.16] with 32 bytes of data:
Reply from 23.66.230.16: bytes=32 time=34ms TTL=53
Reply from 23.66.230.16: bytes=32 time=33ms TTL=53
Reply from 23.66.230.16: bytes=32 time=33ms TTL=53
Reply from 23.66.230.16: bytes=32 time=39ms TTL=53

Ping statistics for 23.66.230.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 39ms, Average = 34ms

C:\
>ping www.ing.org

Pinging www.ing.org [104.239.215.98] with 32 bytes of data:
Reply from 104.239.215.98: bytes=32 time=36ms TTL=52
Reply from 104.239.215.98: bytes=32 time=37ms TTL=52
Reply from 104.239.215.98: bytes=32 time=35ms TTL=52
Reply from 104.239.215.98: bytes=32 time=46ms TTL=52

Ping statistics for 104.239.215.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 46ms, Average = 38ms

C:\
>
```

So, How Does It Know?

- How does your computer know that www.ing.org has an IP of 104.239.215.98?
- It goes out on the Internet and asks a universally accessible resource called a Domain Name Server (DNS) for a name to IP translation.

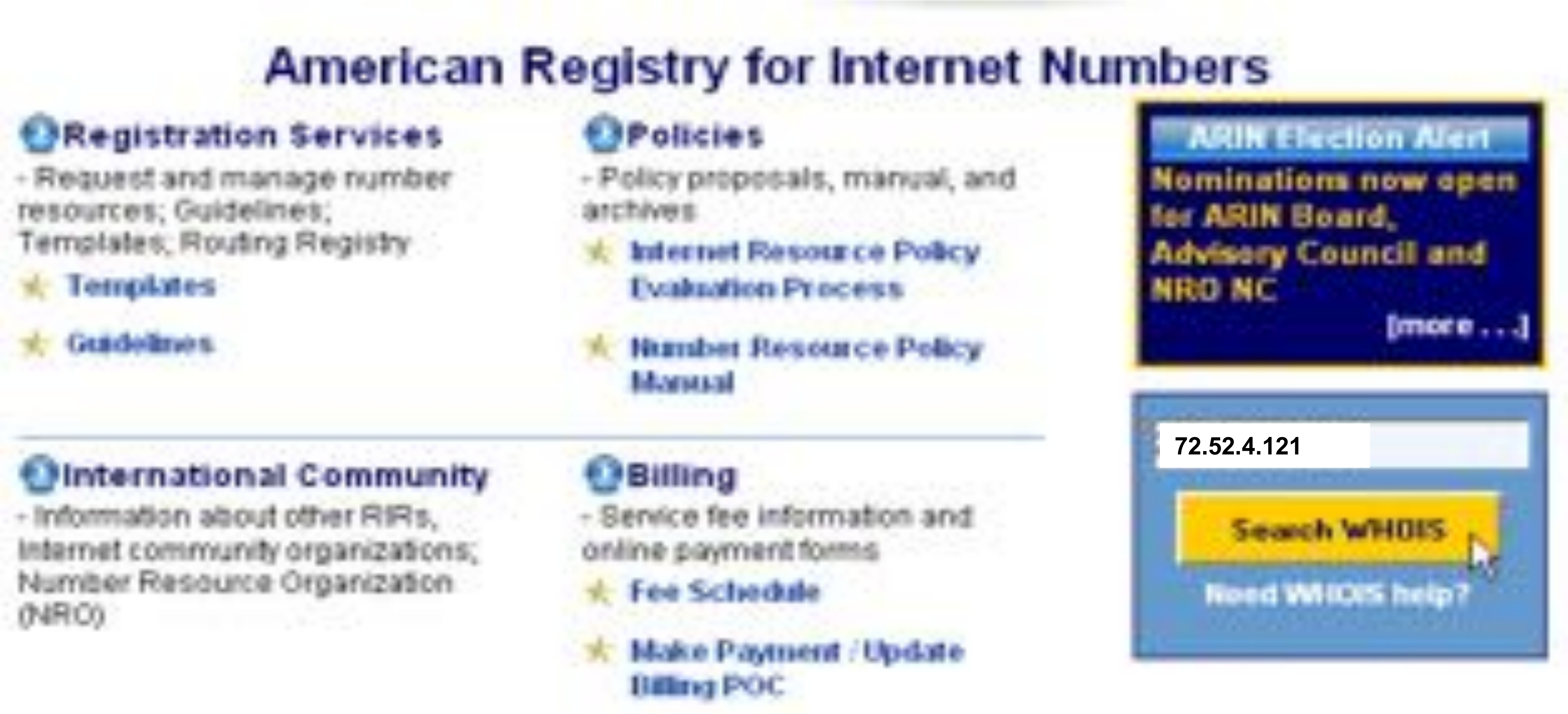
Who’s Responsible For This IP?



```
C:\
>ping www.ihateattorneys.com

Pinging www.ihateattorneys.com [72.52.4.121] with 32 bytes of data:
Reply from 72.52.4.121: bytes=32 time=31ms TTL=243
Reply from 72.52.4.121: bytes=32 time=31ms TTL=243
Reply from 72.52.4.121: bytes=32 time=31ms TTL=243
Reply from 72.52.4.121: bytes=32 time=32ms TTL=243

Ping statistics for 72.52.4.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 32ms, Average = 31ms

C:\
>_
```

Knowing what the IP is for www.ihateattorneys.com, we can go to www.arin.net and ask…

Using “www.arin.net” to Establish Ownership



American Registry for Internet Numbers

Registration Services

- Request and manage number resources; Guidelines; Templates; Routing Registry

★ Templates

★ Guidelines

Policies

- Policy proposals, manual, and archives

★ Internet Resource Policy Evaluation Process

★ Number Resource Policy Manual

International Community

- Information about other RIRs, Internet community organizations; Number Resource Organization (NRO)

Billing

- Service fee information and online payment forms

★ Fee Schedule

★ Make Payment / Update Billing POC

ARIN Election Alert

Nominations now open for ARIN Board, Advisory Council and NRO NC

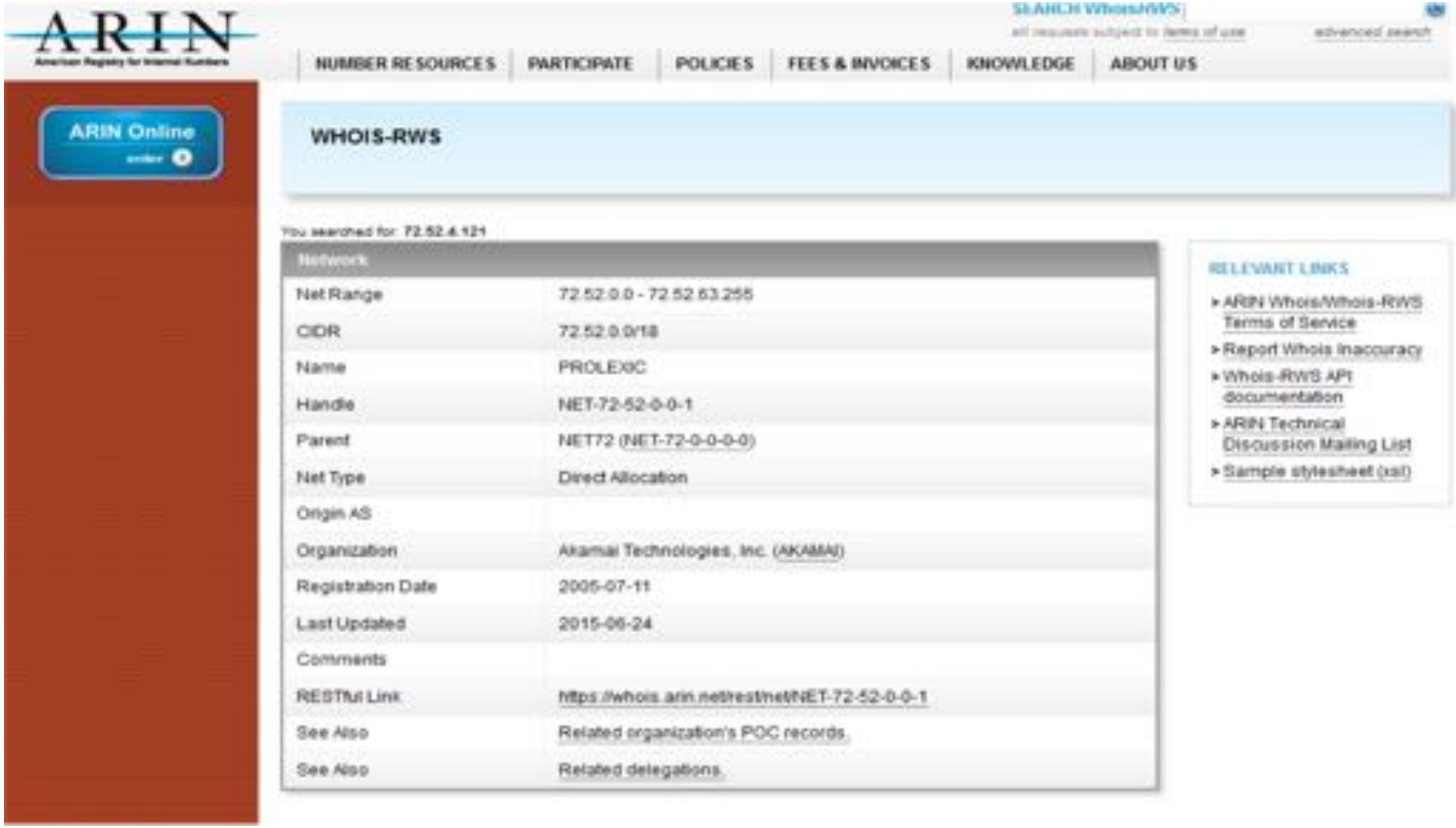
[more . . .]

72.52.4.121

Search WHOIS

Need WHOIS help?

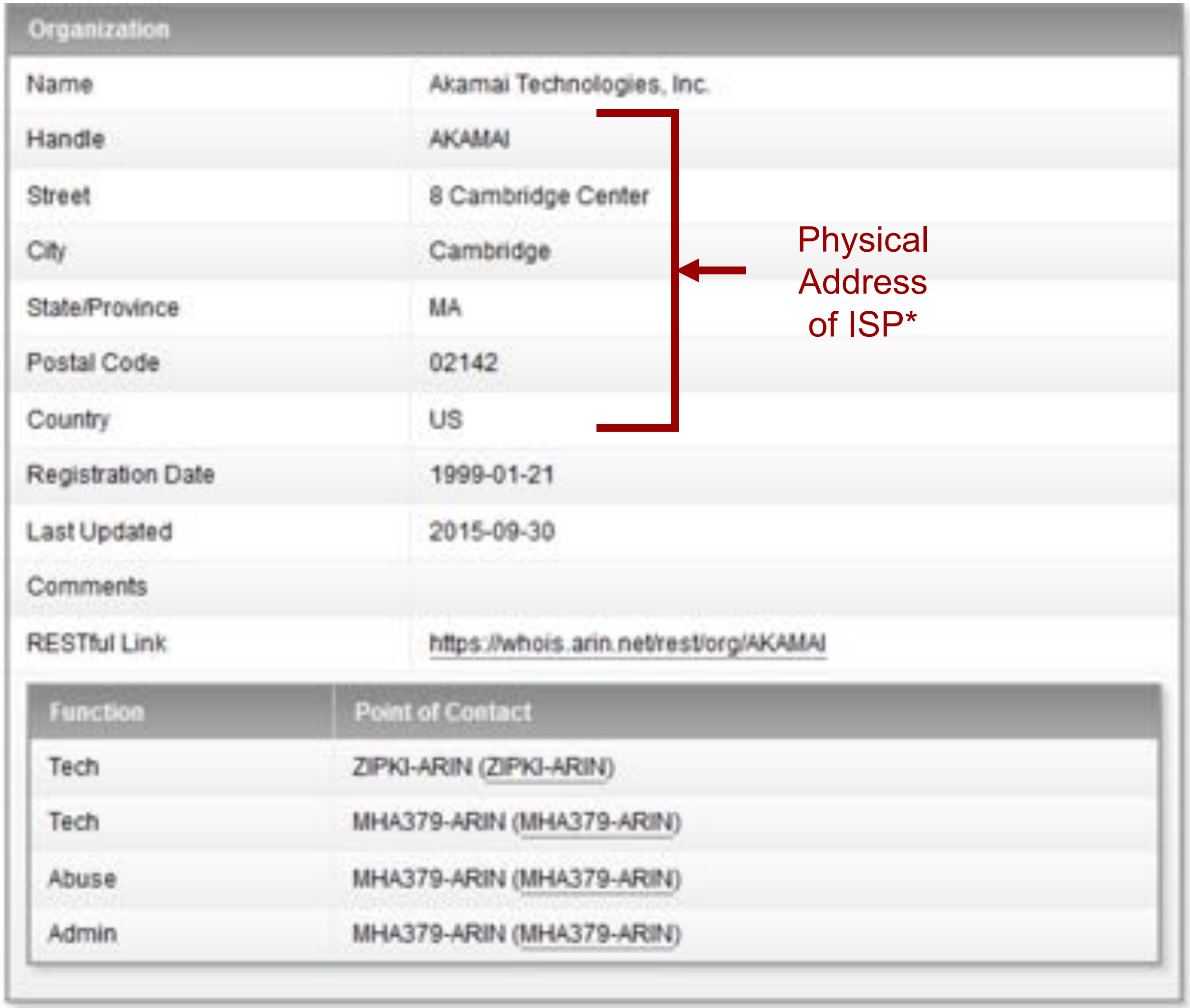
A Query to ARIN Produces These Results



WHOIS-RWS

You searched for: 72.52.4.121

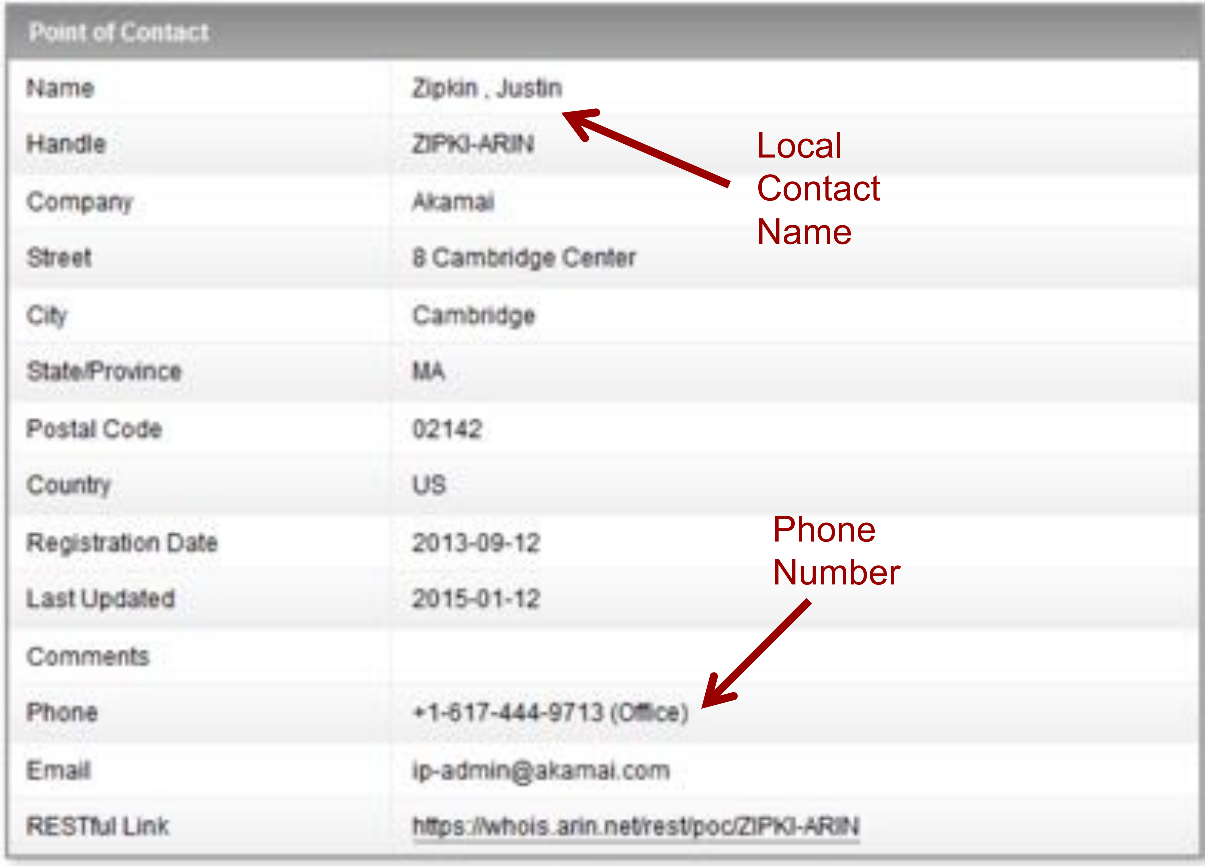
Network	
Net Range	72.52.0.0 - 72.52.63.255
CIDR	72.52.0.0/18
Name	PROLEXIC
Handle	NET-72-52-0-0-1
Parent	NET72 (NET-72-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Akamai Technologies, Inc. (AKAMAI)
Registration Date	2005-07-11
Last Updated	2015-06-24
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-72-52-0-0-1
See Also	Related organization's POC records.
See Also	Related delegations.



Organization	
Name	Akamai Technologies, Inc.
Handle	AKAMAI
Street	8 Cambridge Center
City	Cambridge
State/Province	MA
Postal Code	02142
Country	US
Registration Date	1999-01-21
Last Updated	2015-09-30
Comments	
RESTful Link	https://whois.arin.net/rest/org/AKAMAI

Function	Point of Contact
Tech	ZIPKI-ARIN (ZIPKI-ARIN)
Tech	MHA379-ARIN (MHA379-ARIN)
Abuse	MHA379-ARIN (MHA379-ARIN)
Admin	MHA379-ARIN (MHA379-ARIN)

Physical
Address
of ISP*

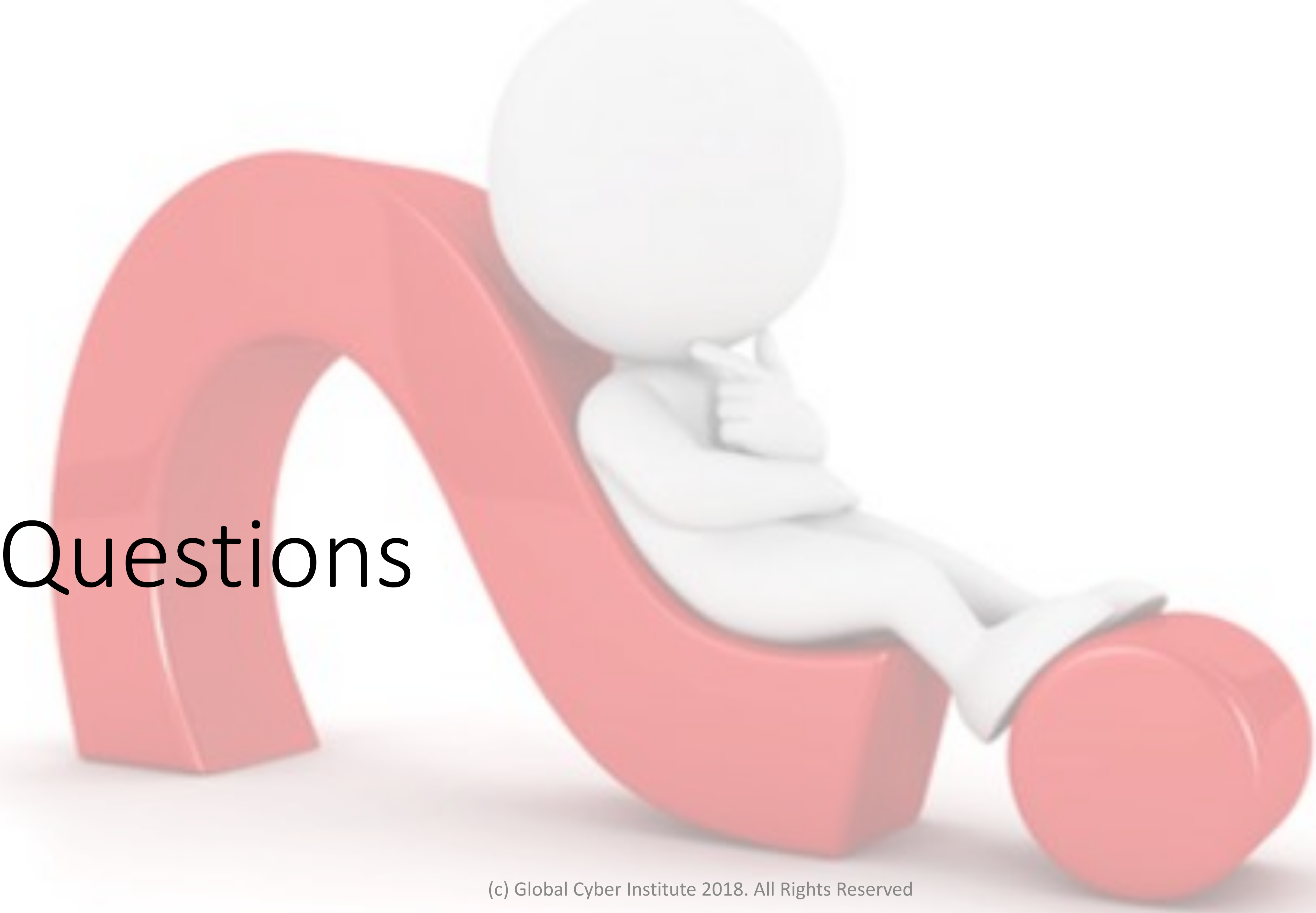


Point of Contact

Name	Zipkin , Justin
Handle	ZIPKI-ARIN
Company	Akamai
Street	8 Cambridge Center
City	Cambridge
State/Province	MA
Postal Code	02142
Country	US
Registration Date	2013-09-12
Last Updated	2015-01-12
Comments	
Phone	+1-617-444-9713 (Office)
Email	ip-admin@akamai.com
RESTful Link	https://whois.arin.net/rest/poc/ZIPKI-ARIN

Local Contact Name

Phone Number



Questions

(c) Global Cyber Institute 2018. All Rights Reserved

Contact Us

Daniel B. Garrie
Email: daniel@lawandforensics.com
dgarrie@jamsadr.com
Phone: 855-529-2466
Website: www.lawandforensics.com

William Spernow
Email: bill@lawandforensics.com
Phone: 855-529-2466
Website: www.lawandforensics.com

Jeff Rosenfeld
Phone: 424-239-3417
Email: JRosenfeld@BlankRome.com
URL: www.blankrome.com/people/jeffrey-rosenfeld

Daniel B. Garrie, Esq.
Law & Forensics -- Executive Managing Partner
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529 - 2466
M: (215) 280 – 7033
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is an Arbitrator, Forensic Neutral, technical Special Master at JAMS, available in Los Angeles, New York, and Seattle*;* Executive Managing Partner of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups, with locations in the United States, India, and Brazil; and adjunct Professor of Law at Cardozo School of Law. He is also a Partner at Zeichner Ellman & Krause, where he heads their global cyber security practice.

Mr. Garrie has built and sold several Internet security, e-commerce, and search technology startups. Prior to his time at Pulse Advisory, Daniel Garrie was the Worldwide Director of Electronic Discovery & Information Governance at Charles River Associates. He also works as a Strategic Partner for Quorumm Ventures and a Board of Governors member for the Organization of Legal Professionals. He is a nationally recognized educator and lecturer on various topics including computer software, cyber security, e-discovery, forensics, emerging internet and mobile technologies, and cyber warfare. He is the Editor in Chief of the Journal of Law & Cyber Warfare, a fellow at the Ponemon Information Privacy Institute, a distinguished neutral with CPR, and on the editorial board of the Beijing Law Review.

Mr. Garrie's scholarship in e-discovery, forensics, and cyber security is frequently cited by the bench and the bar, including: Arrivalstar v. US, US v. Briggs, Coast Professional, Inc. v. US, Genger v. TR Investors, LLC, John B. v. Goetz, and Northruop Grumman Computing Systems, Inc. v. US. Mr. Garrie is also frequently quoted by leading publications including the New York Times, Fortune, Forbes, and the Wall Street Journal on issues relating to cyber security and cyberwarfare.

William Spernow
Law & Forensics – Chief Forensic Officer

Contact:
W: (855) 529 - 2466
E: bill@lawandforensics.com
URL: www.lawandforensics.com

Bill is a consultant with Law & Forensics in the Atlanta area, specializing in forensic analysis, defense-in-depth enterprise level security projects, incident response events, reverse malware analysis, zero-day exploits and hacking activity.

Mr. Spernow spearheaded the development and implementation of several projects funded by the US Department of Justice providing hands-on training to Federal, State and local law enforcement in the area of Cyber Crime investigation. Over a previous five year period with the SEARCH Group he personally trained over 4,000 cyber criminal investigators. As the Assistant Director of the Computer Crime Section with the National White Collar Crime Center he managed their domestic and international digital evidence training program on forensic acquisition and analysis.

In addition to his training background, Mr. Spernow has extensive experience in Information Security at both the strategic and tactical levels gained from his practice in both the public and private sectors. He is quoted frequently in national and international publications regarding his expertise.

Jeffrey Rosenfeld
Blank Rome LLP— Of Counsel

Contact:
W: 424-239-3417
E: JRosenfeld@BlankRome.com
URL: www.blankrome.com/people/jeffrey-rosenfeld

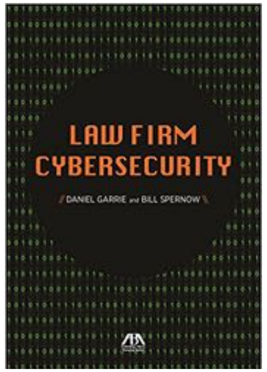
Jeffrey Rosenfeld's practice focuses on litigation involving corporate governance, entertainment, intellectual property, and bankruptcy. His clients include officers and directors of businesses in the technology, finance, and homebuilding industries, as well as actors, musicians, producers, authors, and other creative talent. Jeffrey also represents high-profile individuals and businesses facing cybersecurity and personal security threats.

Jeffrey is involved in all aspects of litigation and alternative dispute resolution, from factual investigations, depositions and expert witness preparation through summary judgment and trial. He incorporates the strategic use of e-discovery, and co-authored a chapter in an e-discovery treatise on the use of special masters in litigation.

Jeffrey has been repeatedly listed in *Super Lawyers* as a Southern California "Rising Star." He is also a member of Phi Beta Kappa.

Additional Reading

BOOKS



Law Firm Cybersecurity

Plugged In: Guidebook to Software and the Law

Software and the Law: Digital Forensic Investigations and E-Discovery

Dispute Resolution and e-Discovery

ARTICLES

Hacked? Don't Waste Time Pointing Fingers

Authenticating Social Media Evidence

Using Forensic Neutrals in Large Commercial Disputes