

# Network Forensics

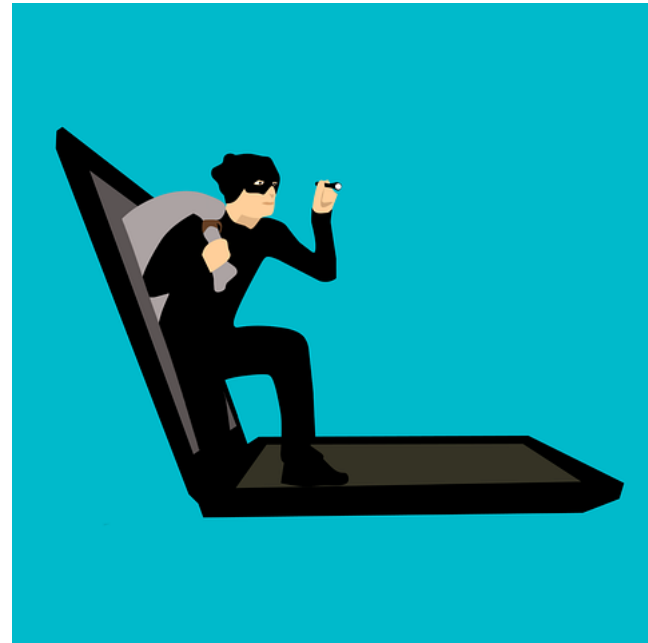
## Introduction

# Network Forensics Introduction

## Topics

- Concepts and terminology
- Networking fundamentals
- Network attacks
- Incident response

This is a broad introduction. Take some classes to learn some more! Plus practice on your own with free tools.



# Some Definitions

- **Forensics**: the application of scientific knowledge to legal cases
- **Computer forensics**: obtaining, preserving, and analyzing digital information from individual computers for use in a legal case
- **Network forensics**: obtaining, preserving, and analyzing digital information from networked devices and from wired or wireless network traffic, for use in a legal case

# Some Challenges

- On a network, evidence of criminality can be on multiple devices, spread across a large geographic area, and subject to the laws of multiple jurisdictions.
- The amount of data on a network that could have evidentiary value is vast.



# Who Are the Criminals?

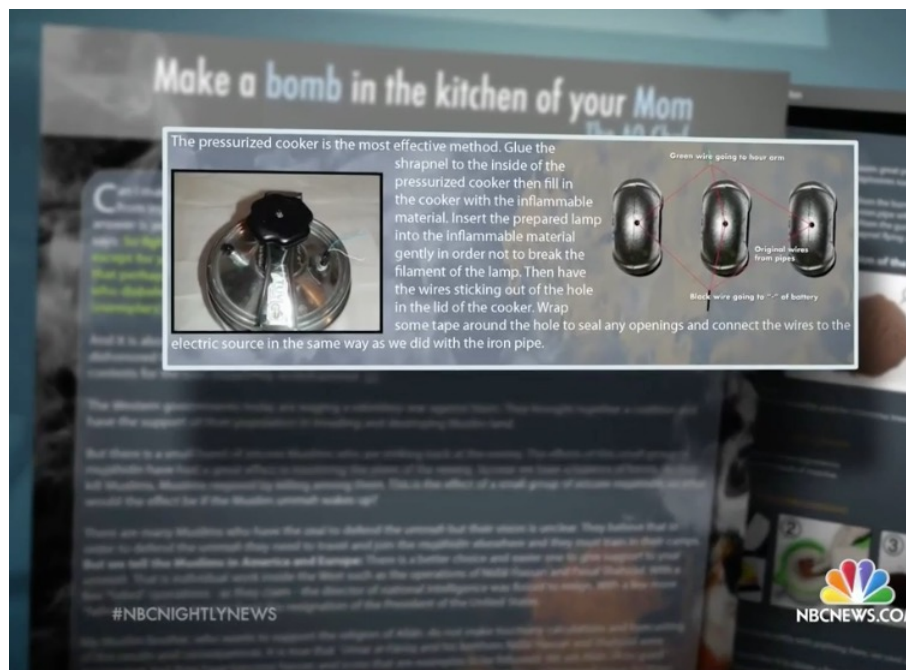
- Terrorists
- Child abusers
- Child pornographers
- Media thieves
- Corporate spies
- Illegal stock traders
- Scammers
- Murderers
- Thieves
- Disgruntled employees

# Why Collect Computer Evidence?

- Criminal cases
- Civil cases
- Corporate policy enforcement
- Protection from terrorists
- To help prove guilt (inculpatory evidence)
- To help prove innocence (exculpatory evidence)

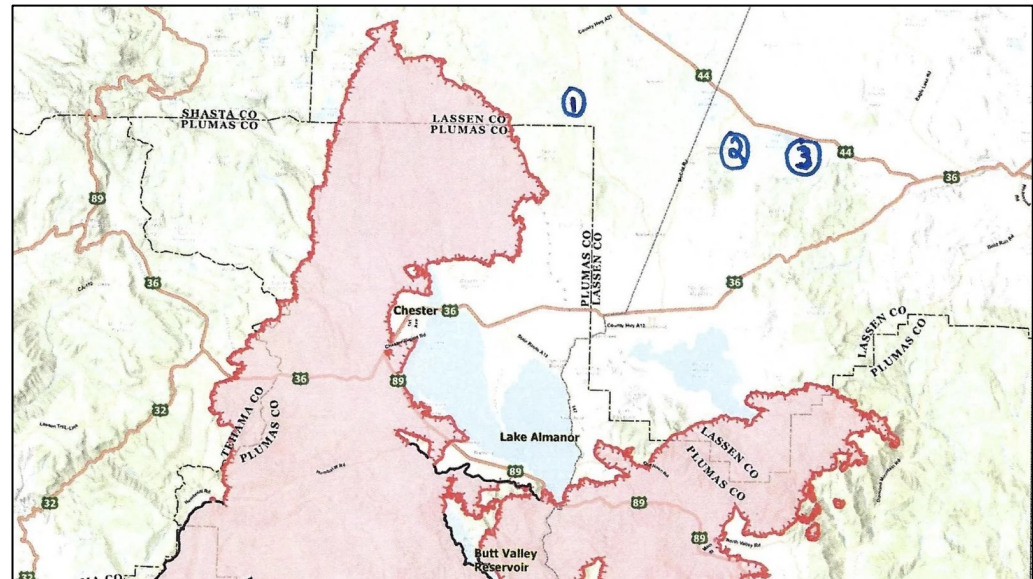
# Computer Forensics: Investigating Terrorism

- On March 19<sup>th</sup> 2015, FBI agents testified that investigators recovered documents with instructions on how to make pressure-cooker bombs on the laptop of Boston Marathon bomber Dzhokhar Tsarnaev.



# Computer Forensics: Investigating Arson

- In August 2021, Gary Maynard, a former college professor, was arrested for starting the Ranch Fire in Northern California.
- In July, a judge issued search warrants that allowed the U.S. Forest Service to require Verizon to track Maynard's phone and to disclose historical cell-site information for the phone.
- Maynard is suspected of setting numerous fires, all near the massive Dixie Fire (which he didn't set).



A map submitted with court papers shows the massive Dixie Fire, in red, along with three fires that U.S. Forest Service agents allege Maynard set. No. 1 marks the approximate location of the Moon Fire, which started on Aug. 5; No. 2 refers to the Ranch Fire, and No. 3 to the Conard Fire — both of which ignited on Aug. 7.

Source: <https://www.npr.org/2021/08/11/1026700103/former-college-professor-arson-charges-california-dixie-fire>



# Recovering Evidence

- The husband and wife team who carried out a deadly shooting spree in San Bernardino, CA 12/2/15 began erasing their digital footprint a day in advance of the attack, deleting email accounts, disposing of hard drives, and smashing their cell phones.
- Nonetheless, the FBI eventually managed to recover evidence from these devices using computer forensics techniques.

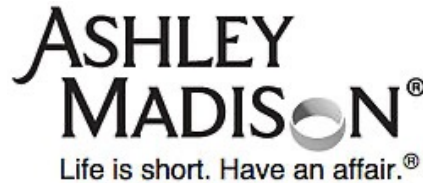
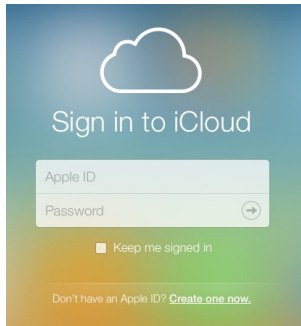


Victims of San Bernardino shootings



San Bernardino shootings investigators

# Recent Cyber-Attacks



# Critical Infrastructure Hacks

- U.S. government cyber security officials warn of an increase in attacks that penetrate industrial control systems.
- Industrial control systems are computers that control operations of industrial processes, including energy, water, oil, gas, and other critical infrastructure.



The image shows the cover of a document titled "Evolving Cyber Threats Against Critical Infrastructure Control Systems". The document is a "Classified Threat Briefing Campaign". It features the logos of the U.S. Department of Homeland Security and the U.S. Department of Justice. The text on the cover includes an overview and purpose section, stating that the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been responding to sophisticated cyber exploitation campaigns against U.S. critical infrastructure industrial control systems (ICSs). The document also mentions that the campaigns have involved two different sets of malware, both of which appear to be ICS focused. The characteristics of this activity include the use of ICS zero-day vulnerabilities, malicious ICS payloads, and specific targeting of the operations environment across a variety of sectors including energy, water, critical manufacturing, communications, and more. The document further states that to increase awareness of the threat and provide additional context, DHS ICS-CERT and FBI will conduct SECRET level classified briefings in select U.S. cities concerning this cyber activity and provide asset owners/operators with the capabilities to detect intrusions and develop mitigation strategies. Finally, it mentions that the regional classified (SECRET//REL TO USA, FVEY) briefing sessions will last approximately 2 hours and provide details about recent malicious cyber campaigns, techniques used by the threat actors, and strategies for mitigating risks and improving your cyber defensive posture.

**Evolving Cyber Threats Against  
Critical Infrastructure Control Systems**  
*Classified Threat Briefing Campaign*

**OVERVIEW and PURPOSE**

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been responding to sophisticated cyber exploitation campaigns against U.S. critical infrastructure industrial control systems (ICSs). These campaigns have involved two different sets of malware; both of which appear to be ICS focused. The characteristics of this activity include the use of ICS zero-day vulnerabilities, malicious ICS payloads, and specific targeting of the operations environment across a variety of sectors including energy, water, critical manufacturing, communications, and more.

To increase awareness of the threat and provide additional context, DHS ICS-CERT and FBI will conduct SECRET level classified briefings in select U.S. cities concerning this cyber activity and provide asset owners/operators with the capabilities to detect intrusions and develop mitigation strategies.

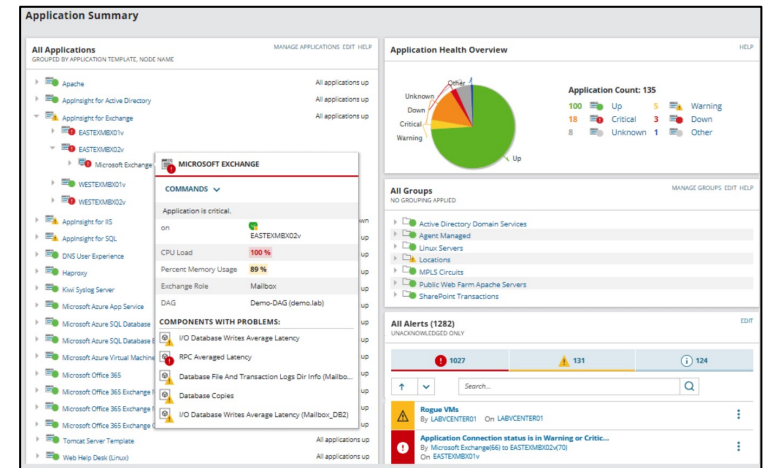
The regional classified (SECRET//REL TO USA, FVEY) briefing sessions will last approximately 2 hours and provide details about recent malicious cyber campaigns, techniques used by the threat actors, and strategies for mitigating risks and improving your cyber defensive posture.

# Nation State Attacks

- Attacks attributed to **Russia** backed hackers
  - **2015** Ukraine power grid attack
  - **2016** Interference in USA election
  - **2018** Attacks on network infrastructure devices such as routers, switches, and firewalls
  - **2020** US Federal Government breach
- 2017 WannaCry ransomware attributed to **North Korea**
- 2010 Stuxnet worm that targeted Iranian nuclear power plants, thought to be built by **USA** and **Israel**

# 2020 Attack on Feds and Others

- A major **cyberattack** suspected to have been committed by a group backed by the Russian government penetrated thousands of organizations globally including multiple parts of the US federal government, leading to a series of data breaches.
- First publicly reported on December 13, 2020, but the attack began as early as **March 2020**.
- A hacked version of **SolarWinds's Orion network management software**, widely used in government and industry, provided the initial entry point.



SolarWinds Software

# Attribution

- Cyber attribution is the process of tracking, identifying, and laying blame on the perpetrator of a cyberattack or other hacking exploit.



# Attribution Methods

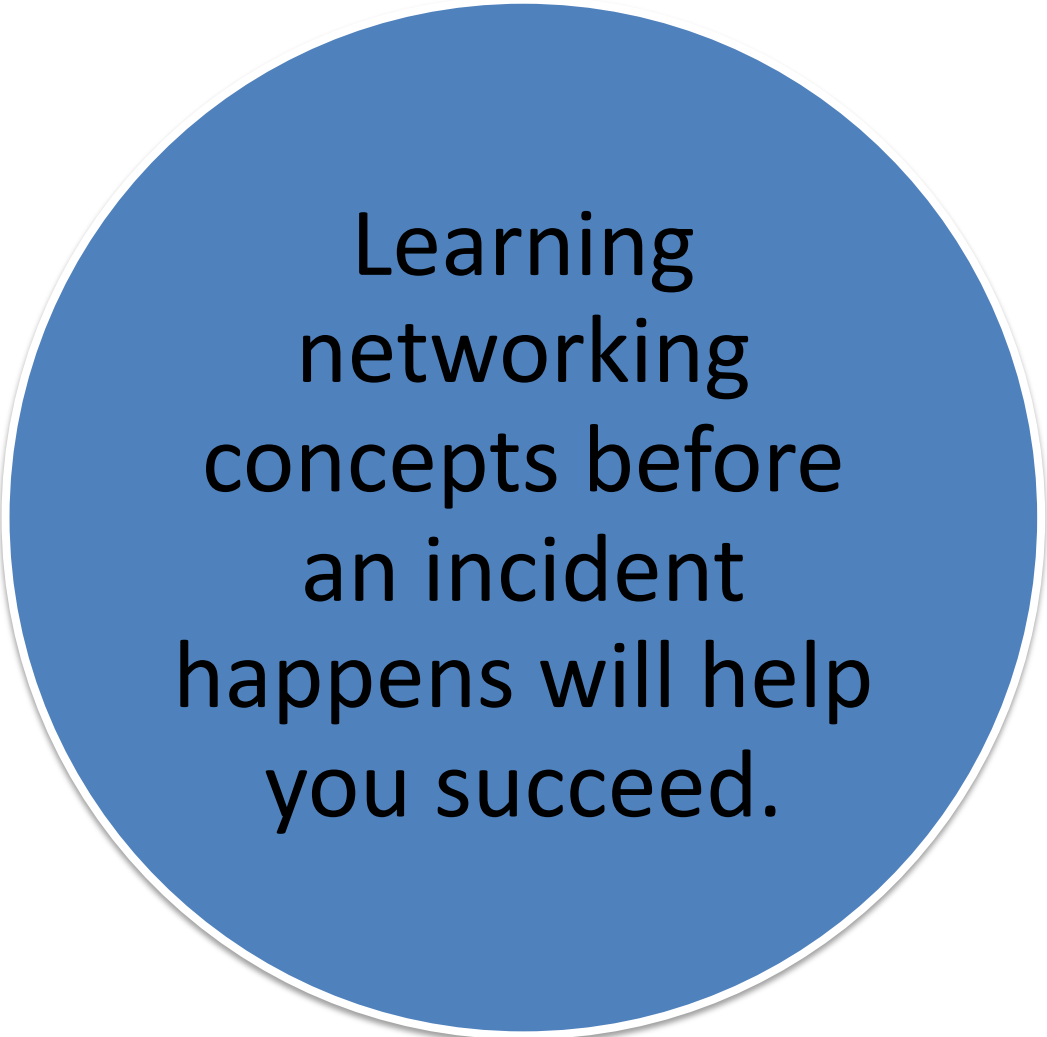
- Investigators analyze the motives, as well as the **techniques, procedures, and tactics (TPP)** used in an attack
  - Cyber attackers often have distinct and **recognizable styles** and methods.
  - Perpetrators often **reuse malware** components that they deployed in prior attacks.
- Investigators are often able to uncover information about the **programming language** used.
- Investigators also analyze any **metadata** connected to the attack, including **IP addresses, email data, hosting platforms, domain names, domain name registration** information, etc.

# How Would You Find the Culprits?

- What sort of evidence should you look for?
  - Is there **physical evidence**?
  - Can you find witnesses who will provide direct **testamentary evidence**?
  - Once you have a suspect, can you gather **circumstantial evidence** to prove your case?
  - Is there **digital evidence**?



# Network Forensics Introduction



Learning  
networking  
concepts before  
an incident  
happens will help  
you succeed.

# Networking Fundamentals

- Protocols
- Network types
- Packets and packet-switching
- IP addressing
- Routers
- Firewalls
- Intrusion Detection Systems

# Network Protocols

- Devices on a network communicate using protocols
  - Transmission Control Protocol (TCP)
  - Internet Protocol (IP)
  - HyperText Transfer Protocol (HTTP)
  - Domain Name System (DNS)
  - etc.
- A protocol is an agreed-upon set of rules and conventions that governs how devices on a network communicate

# Hypertext Transfer Protocol (HTTP)

- Client/server protocol used for web-browsing
- Uses simple ASCII-formatted requests and responses
- Behaves in a stateless manner
  - The server doesn't maintain information (state or status) about past client requests
  - The server can set cookies on the client's computer though which leaves behind lots of crumbs (evidence)



# Web Browsing Artifacts

- Index.dat files
  - Multiple files (hard to erase)
  - Assume that they never go away!
- Cookies
- Web caches
  - Temporary Internet files
- Web-browsing history files
- Windows Registry

# Web Browsing Artifacts (cont.)

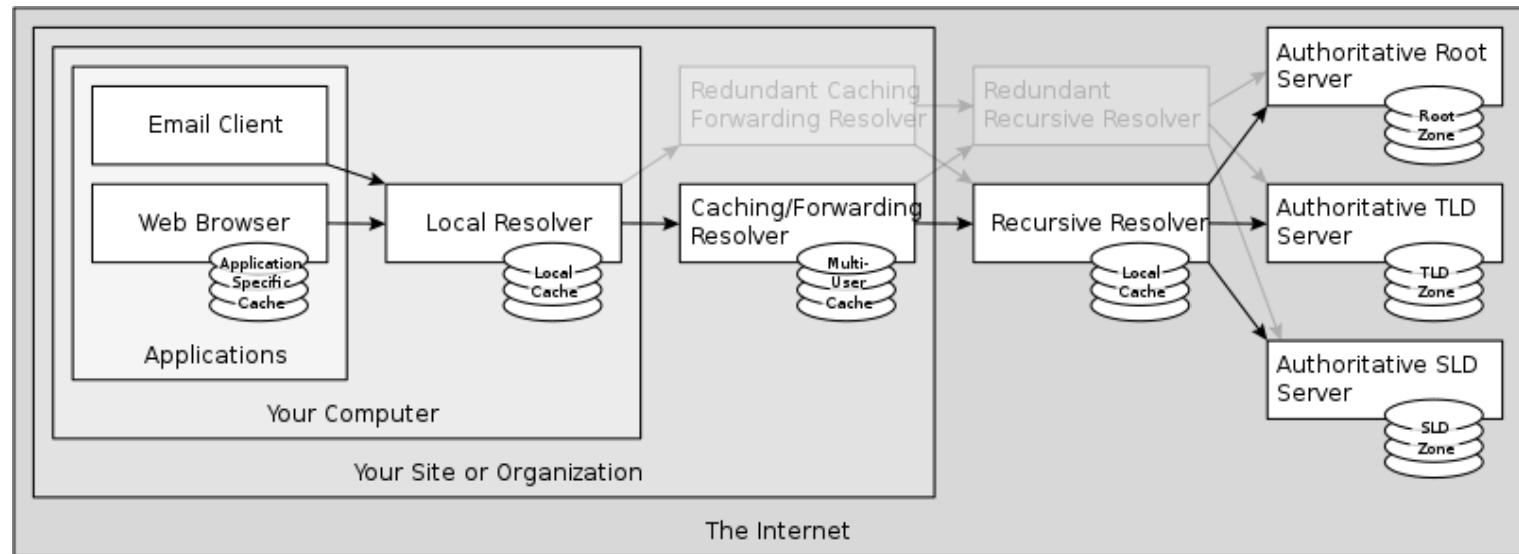
- Analyzing Web-browsing behavior may reveal
  - The user's name, SSN, address
  - Phone, credit card, bank account, driver's license number
  - Location, Google Maps searches
  - Purchase history
  - Travel history
  - Video downloads
  - Library record
  - Facebook uploads
  - Persistence: how often did the user search for strings and go to Web sites?

# Web Server Artifacts

- Web servers have logs that show
  - The IP address of each client
  - Date/time of day of access
  - Which browser the client used
  - What type of computer the client used
  - Cookies that the client sent
  - etc.

# DNS Server

- A Domain Name System (DNS) server maps names to specific IP addresses.



Source: [Wikipedia](#). Licensed under: [Creative Commons Attribution-Share Alike 4.0 International](#).



# DNS Top-Level Domains

## Original

.com

.org

.net

.edu

.gov

.mil

## Country

.ae

.am

.au

.br

.ch

.us

etc

## New

.biz

.adult

.app

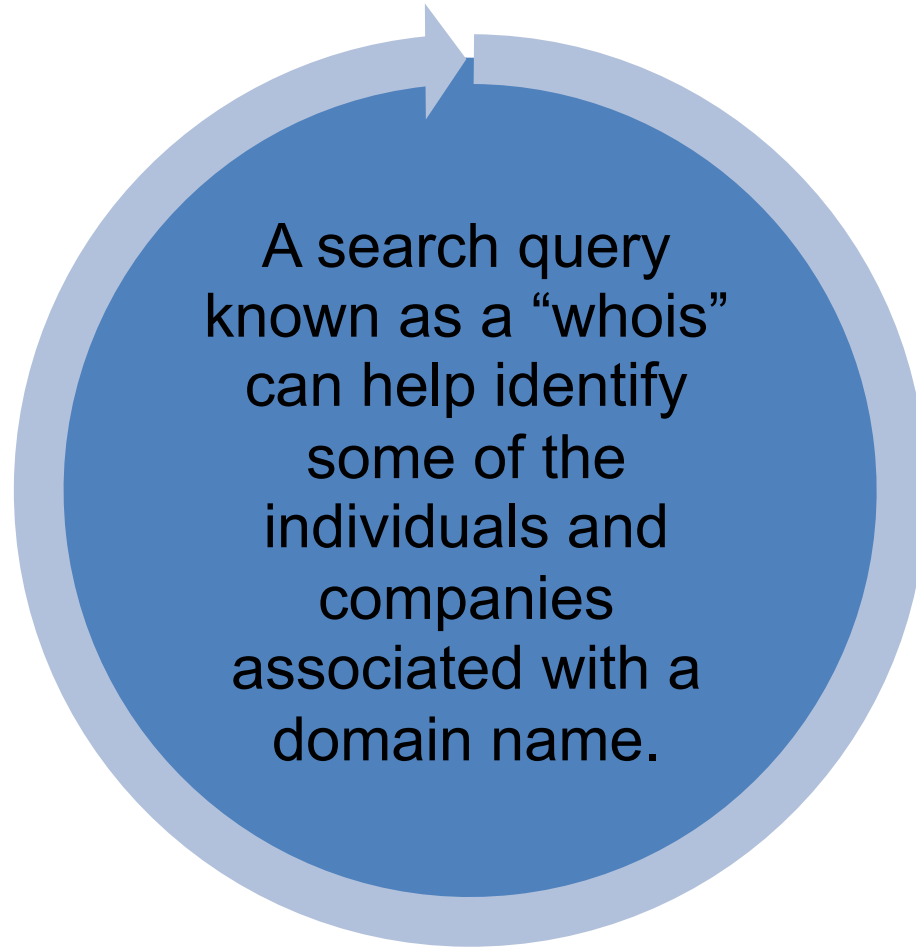
.buzz

.cash

.church

etc

# Whois



# Whois from Command Line

## **whois 66.241.68.18**

OrgName: Ashland Fiber Network  
OrgID: COFA  
Address: 90 N Mountain Ave / 20 E Main  
City: Ashland  
StateProv: OR  
PostalCode: 97520  
Country: US  
Referral: rwhois://rwhois.ashlandfiber.net:4321  
NetRange: 66.241.64.0 - 66.241.95.255  
CIDR: 66.241.64.0/19  
NetName: ASHLANDFN-1  
NetHandle: NET-66-241-64-0-1  
Parent: NET-66-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS0.ASHLANDFIBER.NET  
NameServer: NS1.ASHLANDFIBER.NET  
OrgTechPhone: +1-541-552-2222  
OrgTechEmail: systems@ashlandfiber.net

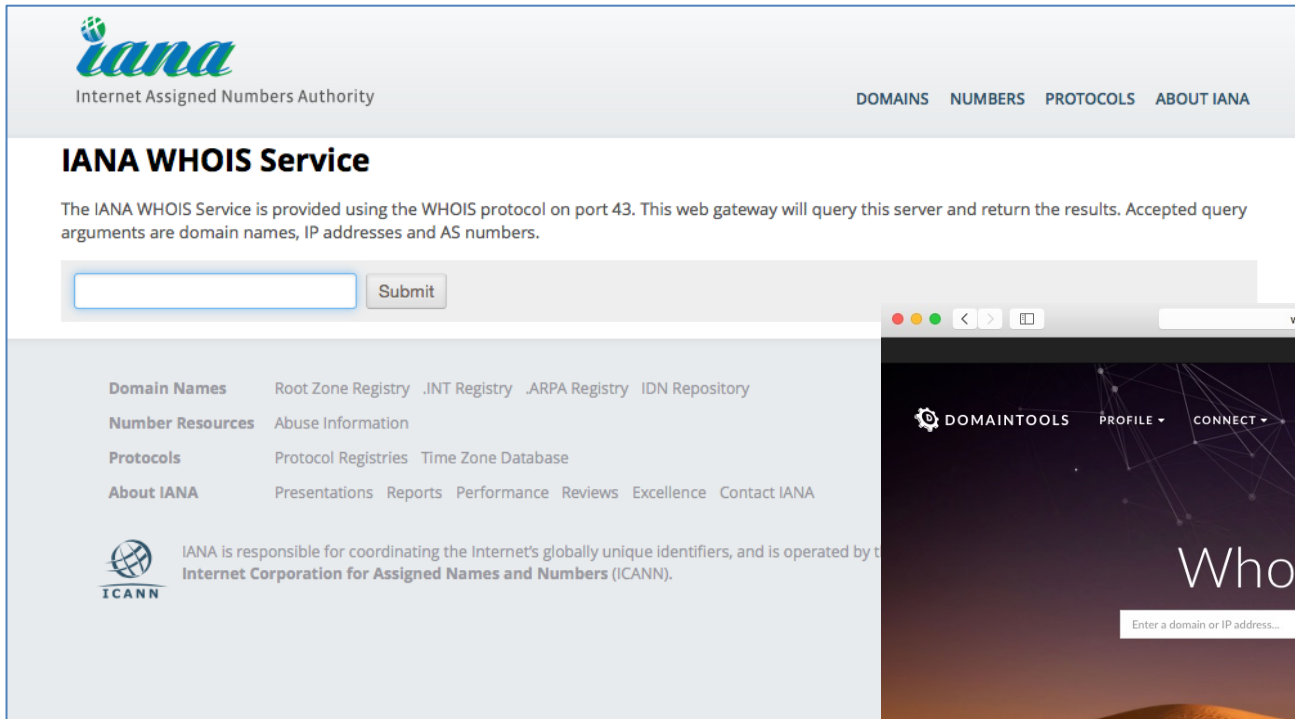
## **whois ashlandfiber.net**

Whois Server Version 2.0

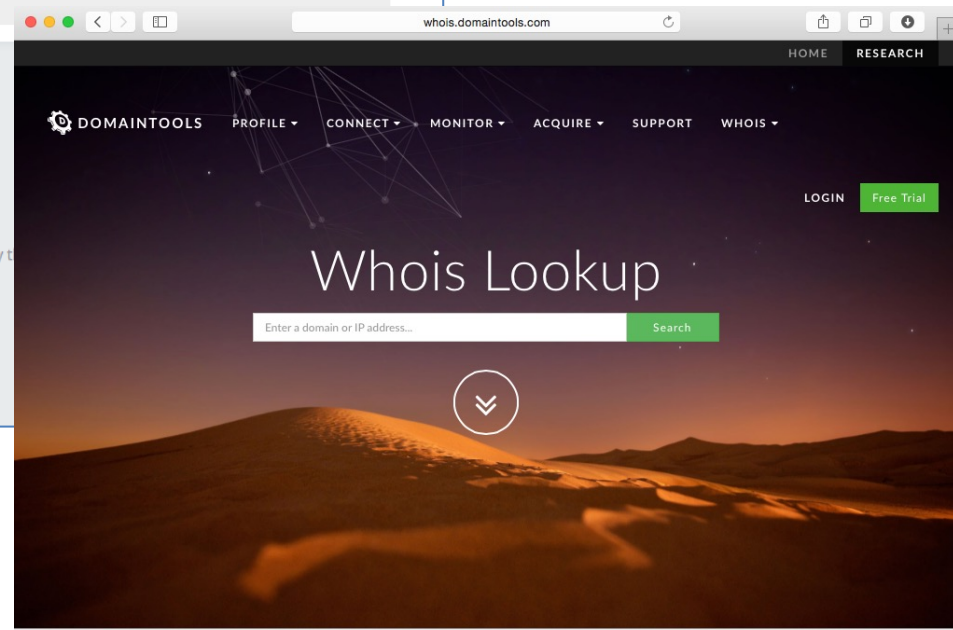
Domain names in the .com and .net domains  
can now be registered  
with many different competing registrars.  
Go to <http://www.internic.net>  
for detailed information.

Domain Name: ASHLANDFIBER.NET  
Registrar: NETWORK SOLUTIONS, LLC.  
Sponsoring Registrar IANA ID: 2  
Whois Server: whois.networksolutions.com  
Referral URL:  
<http://networksolutions.com>  
Name Server: NS.ASHLANDFIBER.COM  
Name Server: NS.ASHLANDFIBER.NET  
Name Server: NS0.ASHLANDFIBER.COM  
Name Server: NS0.ASHLANDFIBER.NET  
Status: ok <http://www.icann.org/epp#OK>  
Updated Date: 09-jan-2015  
Creation Date: 25-mar-1999  
Expiration Date: 25-mar-2019

# Whois on the Web



The screenshot shows the IANA WHOIS Service page. At the top left is the IANA logo (Internet Assigned Numbers Authority). To the right are navigation links: DOMAINS, NUMBERS, PROTOCOLS, and ABOUT IANA. Below the header is the section title "IANA WHOIS Service" followed by a paragraph explaining the service: "The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this server and return the results. Accepted query arguments are domain names, IP addresses and AS numbers." Below this is a search input field and a "Submit" button. A navigation menu follows with categories: Domain Names (Root Zone Registry, .INT Registry, .ARPA Registry, IDN Repository), Number Resources (Abuse Information), Protocols (Protocol Registries, Time Zone Database), and About IANA (Presentations, Reports, Performance, Reviews, Excellence, Contact IANA). At the bottom is the ICANN logo and a statement: "IANA is responsible for coordinating the Internet's globally unique identifiers, and is operated by the Internet Corporation for Assigned Names and Numbers (ICANN)."



The screenshot shows a web browser window displaying the "Whois Lookup" page on domaintools.com. The browser's address bar shows "whois.domaintools.com". The page has a dark theme with a background image of sand dunes at sunset. The navigation bar includes "HOME" and "RESEARCH". The main menu contains "DOMAINTOOLS", "PROFILE", "CONNECT", "MONITOR", "ACQUIRE", "SUPPORT", and "WHOIS". On the right side, there are "LOGIN" and "Free Trial" buttons. The main heading is "Whois Lookup" in a large white font. Below the heading is a search input field with the placeholder text "Enter a domain or IP address..." and a green "Search" button. A circular arrow icon is centered below the search field.

# Types of Networks

# Types of Networks

- Local Area Networks (LANs)
- Wide Area Networks (WANs)
- Metropolitan Area Networks (MANs)
- Intranets
- THE Internet
- Peer-to-Peer networks

# LANs

- Operate within a limited geographic area
- Allow many users to access high-bandwidth media
- Provide full-time connectivity to local services
- Connect physically adjacent devices via wired (e.g. Ethernet) or wireless technologies

# WANs

- Operate over large, geographically-separated areas
- Allow users all over the world to engage in real-time communication with other users
- Interconnect LANs
- Generally provide lower speeds than LANs



# Metropolitan-Area Networks (MANs)

- A MAN is a network that spans a metropolitan area such as a city or suburban area.
- A MAN usually consists of two or more LANs in a common geographic area.

# Intranets and the Internet

- An **intranet** is a set of LANs that are used for file sharing, printer sharing, collaboration, and so on, within a single private organization.
- The **Internet**, on the other hand, is a worldwide public WAN.
- Both intranets and the Internet use TCP/IP.

# Peer-to-Peer Networks

- Traffic flow is bidirectional and symmetric.
- Communicating entities transmit approximately equal amounts of information.
- There is no hierarchy. A computer can serve as both client and server.
- Each device is considered as important as each other device, and no device stores substantially more data than any other device.
- P-to-P networks are often used for file-sharing, especially sharing illegal files.

# Network Forensics Introduction

- Data on a network is divided into small chunks called **packets**.
- **Packet-switching** forwards each packet individually across a network (e.g. the Internet).

# A Typical Packet

```
▼ Ethernet II, Src: Apple_58:4f:69 (a8:20:66:58:4f:69), Dst: Apple_77:01:de (00:11:24:77:01:de)
  ▷ Destination: Apple_77:01:de (00:11:24:77:01:de)
  ▷ Source: Apple_58:4f:69 (a8:20:66:58:4f:69)
  Type: IP (0x0800)
▼ Internet Protocol Version 4, Src: 66.241.68.18 (66.241.68.18), Dst: 66.241.68.22 (66.241.68.22)
  Version: 4
  Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 471
  Identification: 0x4386 (17286)
  ▷ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  ▷ Header checksum: 0x0000 [validation disabled]
  Source: 66.241.68.18 (66.241.68.18)
  Destination: 66.241.68.22 (66.241.68.22)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▼ Transmission Control Protocol, Src Port: 60386 (60386), Dst Port: 80 (80), Seq: 1828147633, Ack: 3567726010, Len: 419
  Source Port: 60386 (60386)
  Destination Port: 80 (80)
```

# A Typical Packet (continued)

- A packet may have an Ethernet, IP, and TCP header.
- The Ethernet header includes source and destination MAC addresses.
- The Ethernet trailer includes a Cyclic Redundancy Check (CRC) to detect errors. The CRC is based on the remainder of a polynomial division of the contents of the packet.
- The IP and TCP layers also have source and destination info and checksums for error detection. The checksums are based on ones-complement arithmetic.

# Network Forensics Introduction

## IP Addressing

# Network Forensics Introduction

- Each *interface* on a network has a unique IP address.
- A *computer* typically has one active interface (an Ethernet wired interface or a Wi-Fi wireless interface.)
- A *router* has two or more active interfaces.
  - For example, a home router probably has one active Ethernet interface and one active Wi-Fi interface.
  - The router forwards packets from Wi-Fi to Ethernet and vice versa.
  - Each interface on the router has a unique IP address.



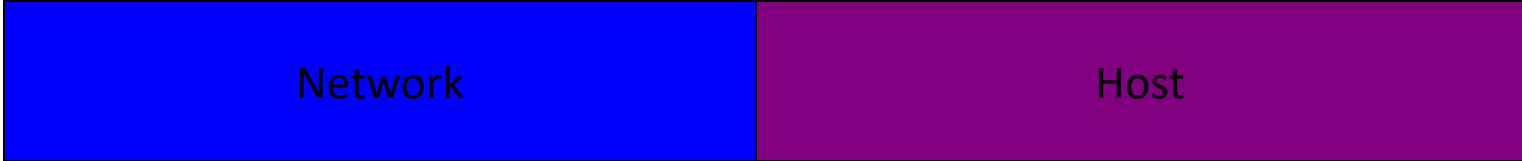
# Network Forensics Introduction

- IP addresses can be **static** or **dynamic**.
  - A static address doesn't change. In contrast, a dynamic address changes on a regular basis.
- IP addresses can also be **private** or **public**.
  - A private address isn't really private; it's just not used on the Internet. It's usually dynamically assigned.
  - A public address is used on the Internet. It can be dynamically assigned or statically assigned.

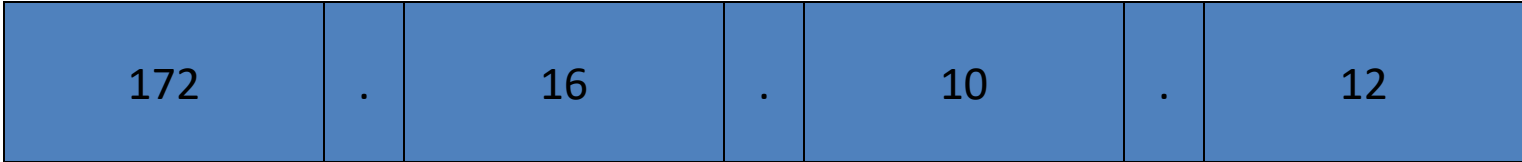
# IPv4 Addressing

- Each interface on a network is assigned a 32-bit IP address
- Examples
  - 10.0.0.1
  - 172.16.10.12
  - 192.168.11.1
- The address has a prefix and suffix
  - Network ID (prefix)
  - Host ID (suffix)

# IPv4 Addressing (continued)



← 32 Bits →



← 8 Bits 1 Byte →   ← 8 Bits 1 Byte →   ← 8 Bits 1 Byte →   ← 8 Bits 1 Byte →

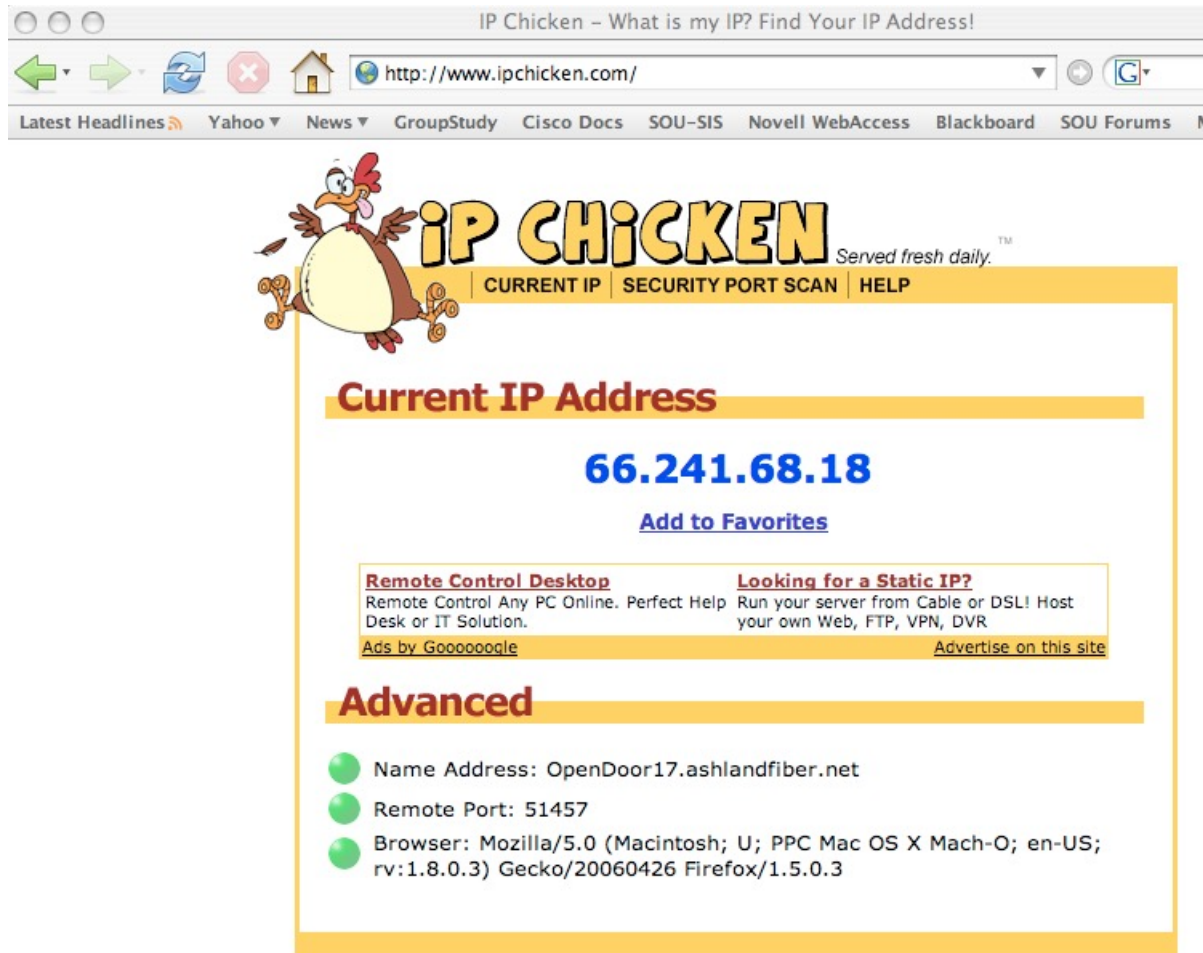
# Prefix Length

- An IP address is accompanied by an indication of the prefix length
  - Subnet mask
  - /Length in Classless Interdomain Routing (CIDR) notation
- Examples
  - 172.16.10.12 255.255.0.0
  - 172.16.10.12/16

# Your Own IP Address

- To see your own address, in a command prompt window, type
  - ipconfig (Windows)
    - or
  - ifconfig (Unix)
    - or
  - ip addr list (Linux)

# Your Own IP Address from the Internet's point of view



The screenshot shows a web browser window with the address bar containing <http://www.ipchicken.com/>. The page title is "IP Chicken - What is my IP? Find Your IP Address!". The navigation menu includes "Latest Headlines", "Yahoo", "News", "GroupStudy", "Cisco Docs", "SOU-SIS", "Novell WebAccess", "Blackboard", and "SOU Forums".

The main content area features a cartoon chicken logo and the text "iP CHICKEN Served fresh daily.™". Below this is a navigation bar with "CURRENT IP", "SECURITY PORT SCAN", and "HELP".

The "Current IP Address" section displays the IP address **66.241.68.18** in large blue text, with a link to "Add to Favorites".

The "Advanced" section lists the following information:

- Name Address: OpenDoor17.ashlandfiber.net
- Remote Port: 51457
- Browser: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.3) Gecko/20060426 Firefox/1.5.0.3

There are also links for "Remote Control Desktop" (with subtext "Remote Control Any PC Online. Perfect Help Desk or IT Solution.") and "Looking for a Static IP?" (with subtext "Run your server from Cable or DSL! Host your own Web, FTP, VPN, DVR").

# Address Location

IP Address Locator - Enter an IP address to find its location - Lookup Country Region City et

http://www.geobytes.com/lpLocator.htm?GetLocation

Latest Headlines Yahoo News GroupStudy Cisco Docs SOU-SIS Novell WebAccess Blackboard SOU Forums

**GEOBYTES**


[ Home ] [ Contact Us ] [ Support ] [ Forum ] [ Free Services ] [ Merchandise ] [ IP Address Locat

The following results were generated using **GeoSelect** version II.

Address to locate:

Country Code	US	Country	United States
Region Code	USOR	Region	Oregon
City Code	USORMEDF	City	Medford
CityId	10514	Certainty	97
Latitude	42.3017	Longitude	-122.8380
Capital City	Washington, DC	TimeZone	-08:00
Nationality Singular	American	Population	278058881
Nationality Plural	Americans	Is proxy	false
CIA Map Reference	North America	Currency	US Dollar
MapBytes Remaining	Free	Currency Code	USD

Search WHOIS data at: [RIPE](#) [ARIN](#) [APNIC](#) [LACNIC](#)


Flag 

[Click here](#) to find out why our data can differ from the WHOIS data.  
[Click here](#) for a description of each of the above fields.

**Distance to Nearby Cities**  
km, mi, City, Region, Country

0 0	Medford, OR, US
5 3	Phoenix, OR, US
16 10	Central Point, OR, US
19 11	Talent, OR, US
24 15	Jacksonville, OR, US
24 15	Eagle Point, OR, US
27 16	Ashland, OR, US
29 18	Gold Hill, OR, US
32 20	White City, OR, US
36 22	Shady Cove, OR, US
41 25	Rogue River, OR, US
41 25	Murphy, OR, US
42 26	Williams, OR, US
43 26	Butte Falls, OR, US
49 30	Trail, OR, US
49 30	Klamath River, CA, US
52 32	Seiad Valley, CA, US

Check out Geobytes other products including:  
[GeoSelect](#), [GeoNetMap](#), [GeoReport](#),  
[GeoPhrase](#), [GeoLyzer](#), [GeoRemote](#),  
[GeoDirection](#), [MapBytes](#)



# Network Attacks



# Network Attacks

- Hackers have many attack options at their disposal:
  - Denial of Service attacks
  - IP spoofing
  - Man-in-the middle attacks
  - Social engineering
  - Trojan horses
  - Keyloggers
  - Worms
  - Viruses

# Denial of Service Attacks

- A cyber-attack where the perpetrator seeks to make a computer or network service unavailable to its intended users by temporarily or indefinitely disrupting the service
- Typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

# Denial of Service Attacks

- A Distributed Denial of Service (DDoS) attack uses massive numbers of compromised computers to attack a lone system.
- The target of a DDoS attack can't deal with the volume of traffic and eventually buckles.

# IP Spoofing

- IP spoofing is when an attacker forges or “spoofs” a valid IP addresses to gain access.

# Man in the Middle Attack

- A Man-in-the-Middle-Attack is when the hacker inserts software between you and the entity you are communicating with in order to sniff the traffic or trick you into downloading malware.

# Social Engineering

- Social engineering happens when an unauthorized user finds a way to convince an authorized user to divulge sensitive information.
- Common social engineering attacks include hackers posing as employees, customers, or security consultants.

# Network Forensics Introduction

## Other malware:

- **Trojan horse:** a malicious software program that hacks into a computer by misleading users of its true intent
- **Keylogger:** a software program or hardware device that records everything a user types on a compromised computer
- **Worm:** a self-contained software program that spreads functional copies of itself to other computer systems
- **Virus:** a type of malicious software program that attaches itself to other software and replicates by reproducing itself

# Network Forensics Introduction

## Virus versus worm:

- **Viruses** require a host program or an already-infected operating system in order to run, cause damage, and infect other executable files or documents
- **Worms** are stand-alone malicious programs that can self-replicate and propagate via computer networks, without human help



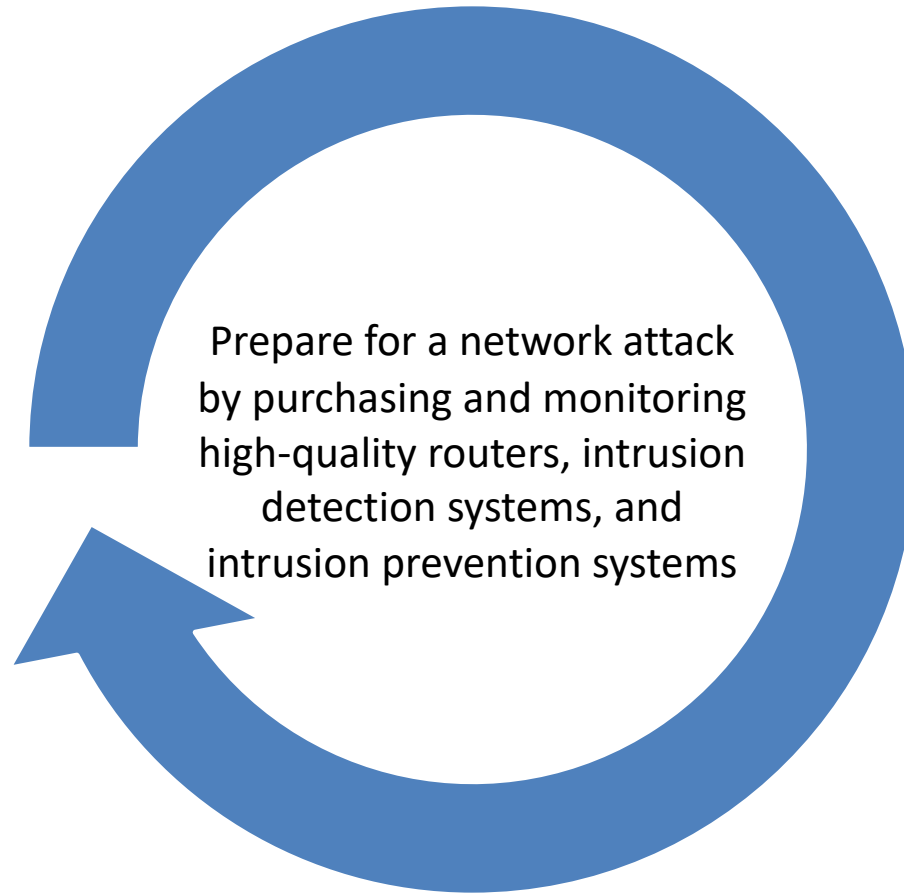
# Incident Response

# Network Forensics Introduction

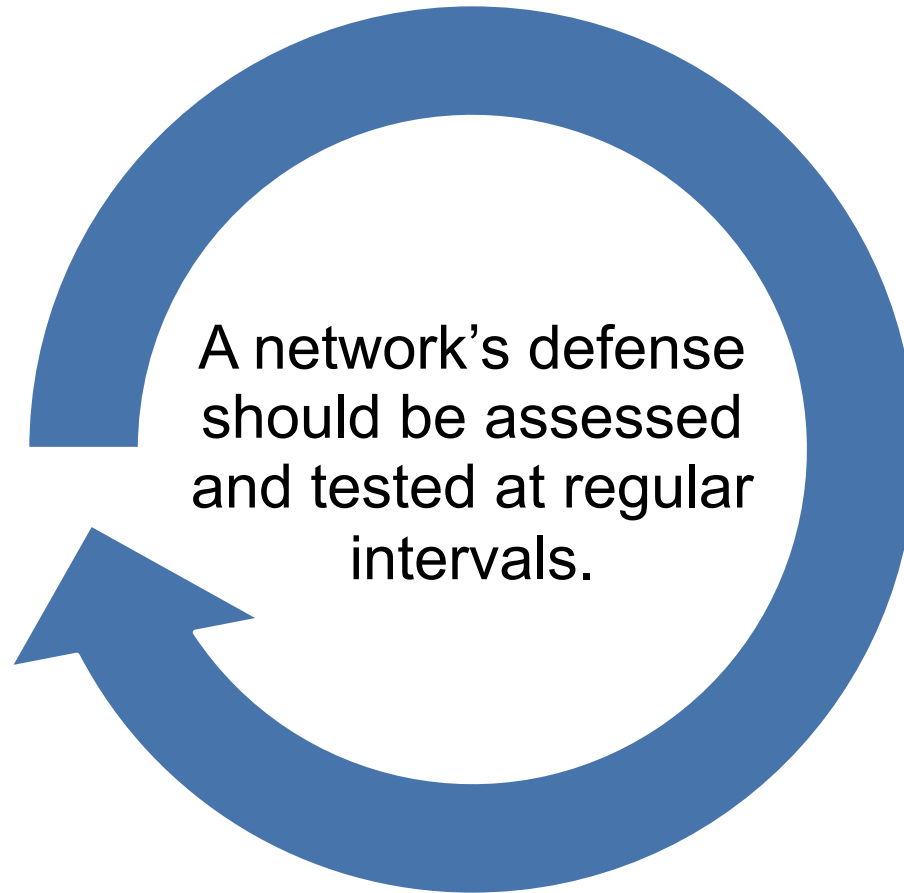
Phases for responding to an incident include:

- Preparation
- Prevention
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident review

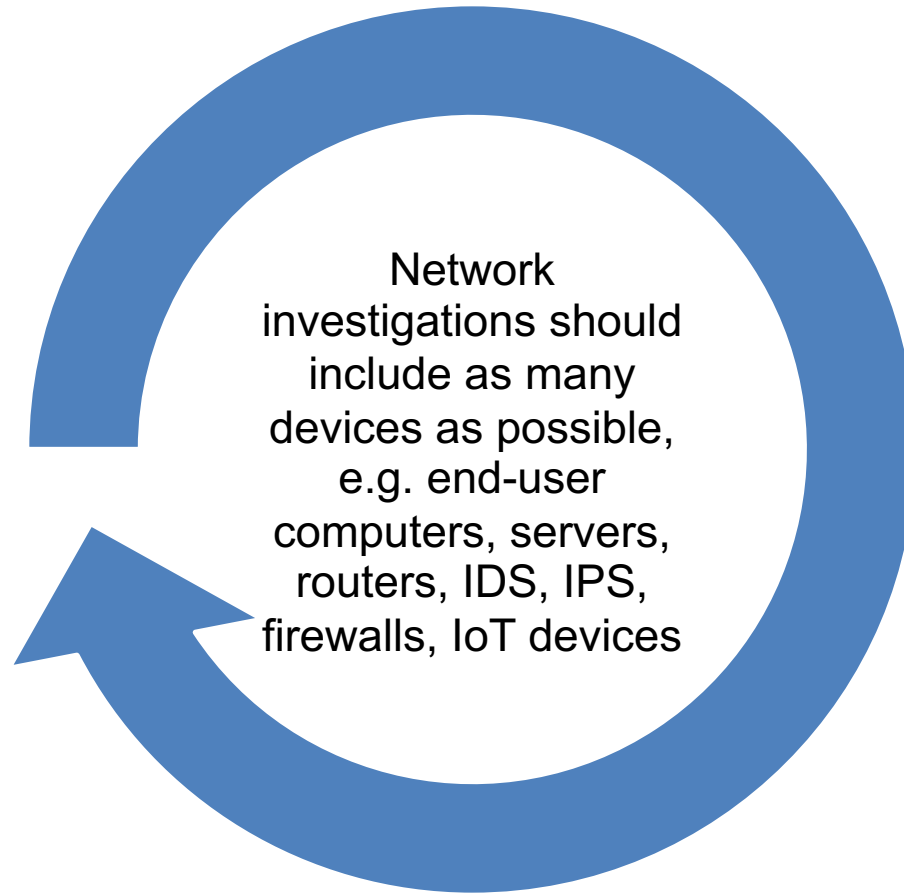
# Network Forensics Introduction



# Network Forensics Introduction



# Network Forensics Introduction



# Network Forensics Introduction

- Many devices and computers on a network produce logs of events and activities.
- These log files are a primary source of evidence.
- Devices:
  - **Routers** connect networks and direct data to their final destination, based on the destination IP address. Routers have packet-filtering capabilities.
  - A **firewall** acts as a filter for both inbound and outbound network traffic.
  - An **Intrusion Detection System (IDS)** detects attacks from both inside and outside the organization.
  - An **Intrusion Prevention System (IPS)** blocks malicious activity.
- Capture and analyze network traffic with a protocol analyzer (also known as a packet sniffer)

# Wireshark Protocol Analyzer

- Free, open-source sniffer and protocol analyzer
- Runs on Windows, Linux, OS X, etc.
- Captures from wired, wireless, Bluetooth, etc.
- Provides statistics regarding packet types, etc.
- Great for learning
- Also used in the “real world” to monitor network traffic

# Wireshark User Interface

The screenshot displays the Wireshark interface with three main panes. The Packet List pane at the top shows a table of captured packets. The Packet Details pane in the middle shows the hierarchical structure of the selected packet (Frame 10), including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The Packet Bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Size	Protocol	Info
1	0.000000	AppleCom_2a:a1:7a	Broadcast	42	ARP	Who has 66.241.68.28? Tell 66.241.68.28
2	0.000167	AppleCom_77:01:de	AppleCom_2a:a1:7a	60	ARP	66.241.68.28 is at 00:11:24:77:01:de
3	0.000246	66.241.68.18	66.241.68.28	77	DNS	Standard query A www.priscilla.com
4	0.000803	66.241.68.28	66.241.68.18	188	DNS	Standard query response CNAME www.opera.com
5	0.024912	AppleCom_2a:a1:7a	Broadcast	42	ARP	Who has 66.241.68.22? Tell 66.241.68.22
6	0.025048	AppleCom_77:01:de	AppleCom_2a:a1:7a	60	ARP	66.241.68.22 is at 00:11:24:77:01:de
7	0.025091	66.241.68.18	66.241.68.22	78	TCP	57005 > http [SYN] Seq=4244936253 Len=0
8	0.025280	66.241.68.22	66.241.68.18	78	TCP	http > 57005 [SYN, ACK] Seq=1931840696 Win=0
9	0.025356	66.241.68.18	66.241.68.22	66	TCP	57005 > http [ACK] Seq=4244936254 Ack=1931840697
10	0.025949	66.241.68.18	66.241.68.22	483	HTTP	GET / HTTP/1.1
11	0.026164	66.241.68.22	66.241.68.18	66	TCP	http > 57005 [ACK] Seq=1931840697 Ack=4244936254

Frame 10 (483 bytes on wire, 483 bytes captured)

- Ethernet II, Src: AppleCom\_2a:a1:7a (00:17:f2:2a:a1:7a), Dst: AppleCom\_77:01:de (00:11:24:77:01:de)
- Internet Protocol, Src: 66.241.68.18 (66.241.68.18), Dst: 66.241.68.22 (66.241.68.22)
- Transmission Control Protocol, Src Port: 57005 (57005), Dst Port: http (80), Seq: 4244936254, Ack: 1931840697, Len: 483
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n

0040 50 f1 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 P: GET / HTTP/1.1  
0050 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ..Accept-Language  
0060 65 3a 20 65 6e 0d 0a 41 63 63 65 70 74 2d 45 6e e: en..Accept-En  
0070 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de  
0080 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65 6e flate..User-Agen  
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozilla/5.0 (C  
00a0 4d 61 63 69 6e 74 6f 73 68 3b 20 55 3b 20 49 6e Macintosh; U; In  
00b0 74 65 6c 70 4d 61 63 70 4f 53 70 58 20 31 30 5f tel; Mac OS X 10

The Packet List pane displays a one-line summary of each packet captured.

The Packet Details pane displays the packet selected in the Packet List pane in more detail, with each layer decoded.

The Packet Bytes pane displays the packet selected in the Packet List pane in hexadecimal and ASCII.



# Network Forensics Commands

- ipconfig
- ipconfig /all
- ipconfig /displaydns
- ping
- tracert
- whois
- nslookup
- netstat
- route print
- arp -a
- nmap

# Summary

- Understanding network attacks and network forensics requires a solid understanding of how networks function.
- Evidence resides in network traffic and in logs from servers, routers, and firewalls.
- Protections from network attacks include firewalls, and intrusion detection and prevention systems.
- Incident response is an orderly process that involves preparation, detection and analysis, containment, recovery, and post-incident review.