

Intro Cybercamp



DIGITAL FORENSICS

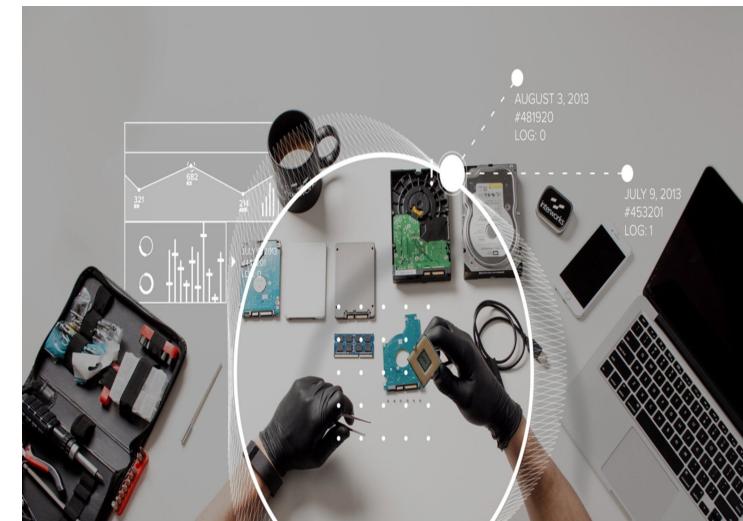


The Role of Digital Forensics

Digital forensics is a forensic science where experts look at digital information contained on PCs, digital storage media, and mobile and smart devices to help

- a) solve crimes
- b) find information about a person or company
- c) analyze a hacker's intrusion into a network

The experts who do digital forensics are often called "analysts" or "investigators".



Why Digital Forensics?

Everything we do online leaves a footprint. In public and private legal disputes this footprint is compiled and frequently used as evidence. Though the digital forensics field was once as wild and disorganized as early Silicon Valley, today experts are highly trained and follow rigorous protocols. These guidelines help protect law enforcement agencies from evidence contamination and help corporations fend off cyber attacks.

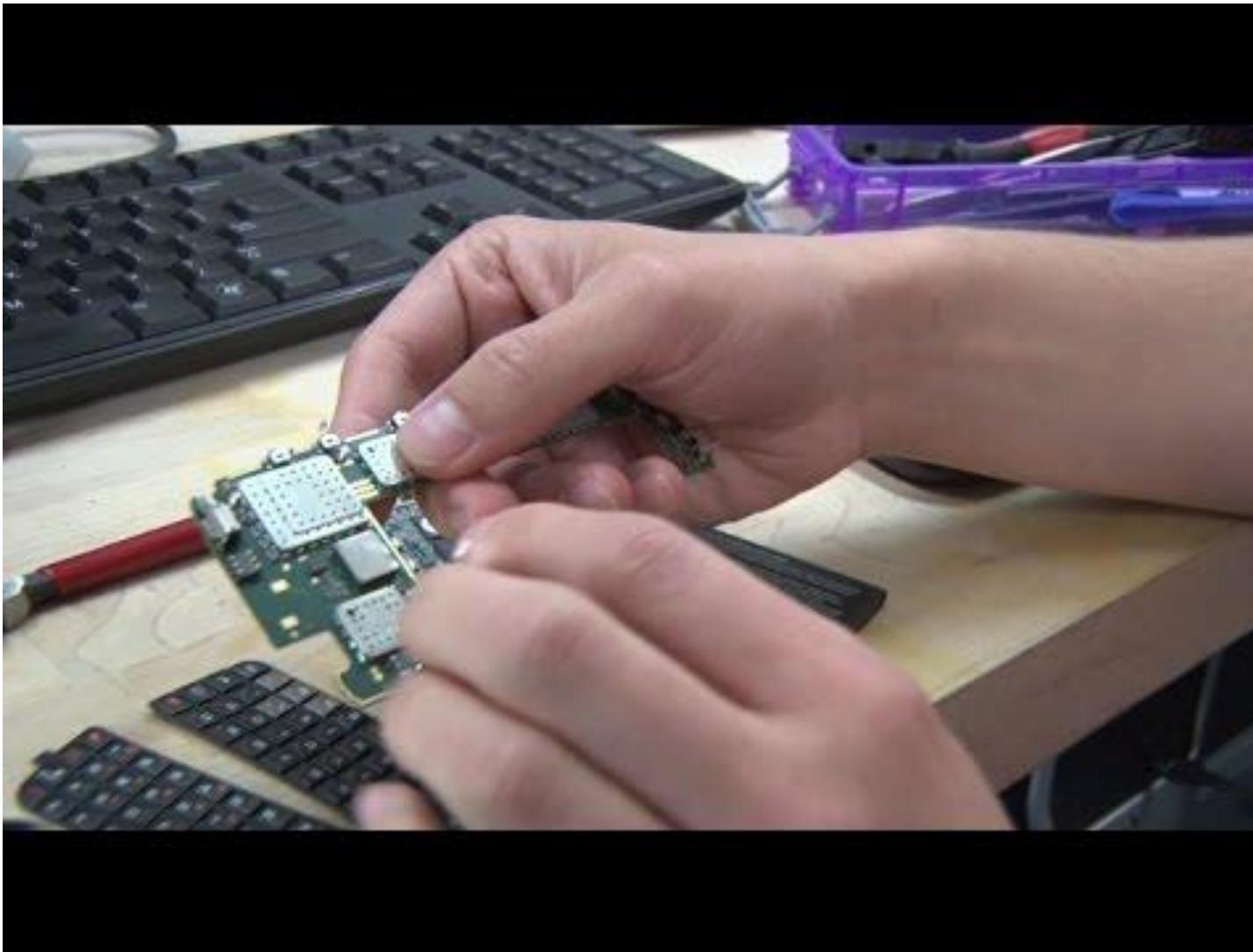


Why Digital Forensics?

For example, just opening a computer file changes the file -- the computer records the time and date it was accessed on the file itself. If detectives seize a computer and then start opening files, there's no way to tell for sure that they didn't change anything. Lawyers can contest the validity of the evidence when the case goes to court.



Inside a Digital Crime Lab



Careers in Digital Forensics

In most cases, computer forensic experts are referred to as Computer Forensic Analysts (or Technicians). There are a few different career paths that are fairly common for computer forensic experts. In general, computer forensic experts enter the field either from an information technology (IT) or law enforcement background. Both trajectories have their advantages.



Careers in Digital Forensics

An IT professional who comes to computer forensics will have the advantage of deeper knowledge of computer systems and technical experience. On the other hand, law enforcement officers who decide to specialize in computer forensics will come to the field with a more thorough understanding of the laws of evidence, which can certainly be helpful in criminal as well as civil cases.



Careers In Digital Forensics

A lot of different types of companies need digital forensic analysts.

Average Salary of Digital Forensic Analyst Jobs



Jobs
Near Oakland, CA

Analyst Past 3 days Full-time Examiner Investigator Director

Digital Forensics Analyst, Career
Pacific Gas and Electric Company
Concord, CA
via LinkedIn
Over 1 month ago Full-time

Digital/Computer Forensics Technician - Entry Level
TransPerfect
San Francisco, CA
via Glassdoor
3 days ago Full-time

Digital Forensic Analyst
Facebook
Menlo Park, CA
via CyberSecJobs.com
Over 1 month ago Full-time

→ 39 more jobs

The Autopsy Digital Forensics Tool



What is Autopsy?

- A Digital forensics tool
- Used by law enforcement, military, and corporate examiners to investigate what happened on a computer.



What is Autopsy?

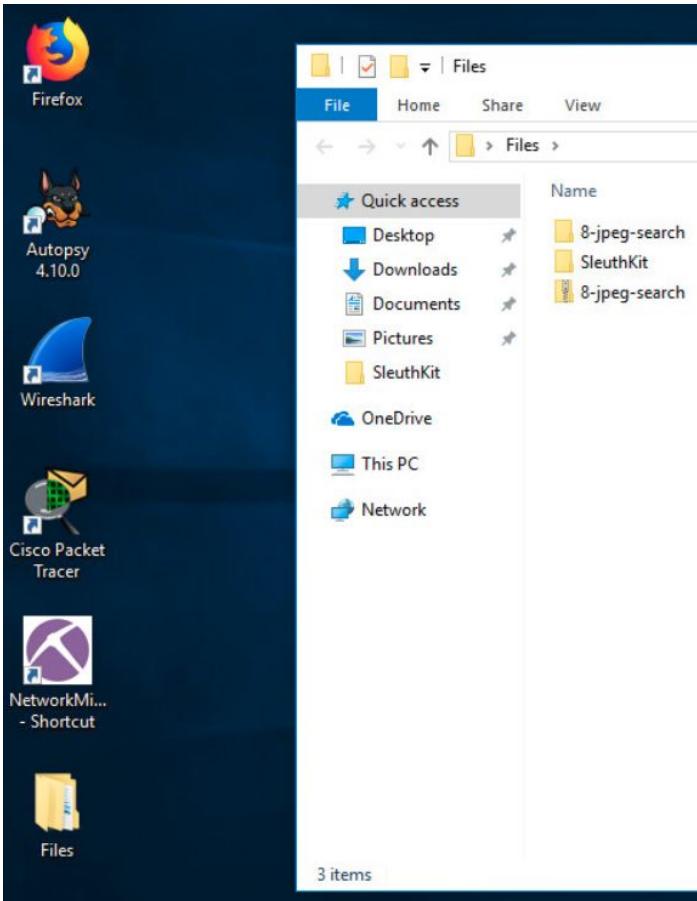
- Why are we learning this tool?
- You will use Autopsy to complete the CTF



Image Files to Use in Autopsy



Files are located on the Desktop



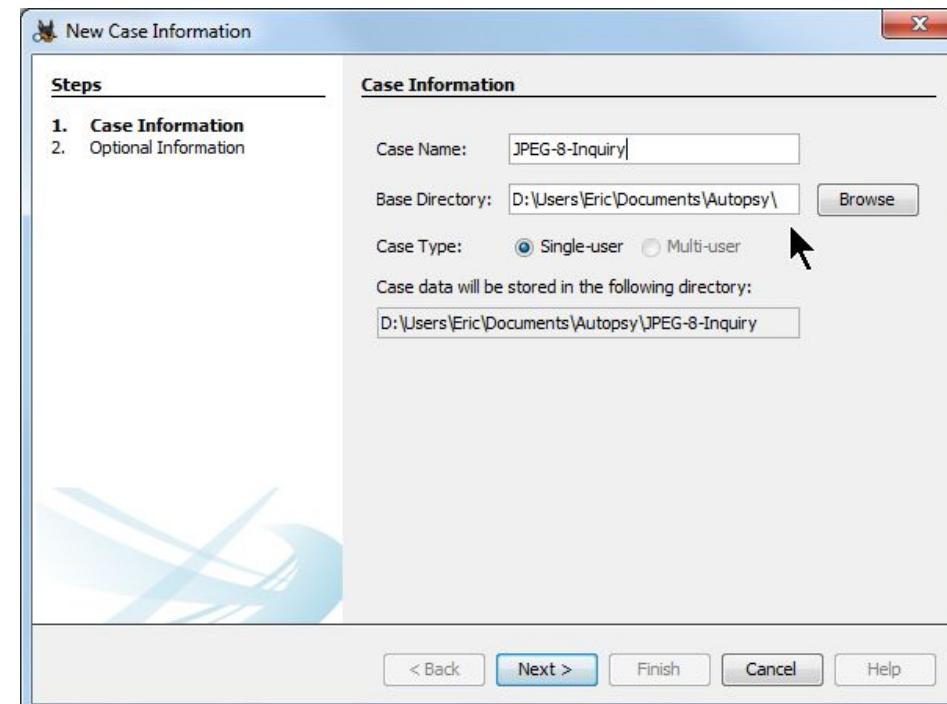
Create a Case

- Launch Autopsy
- Click New Case



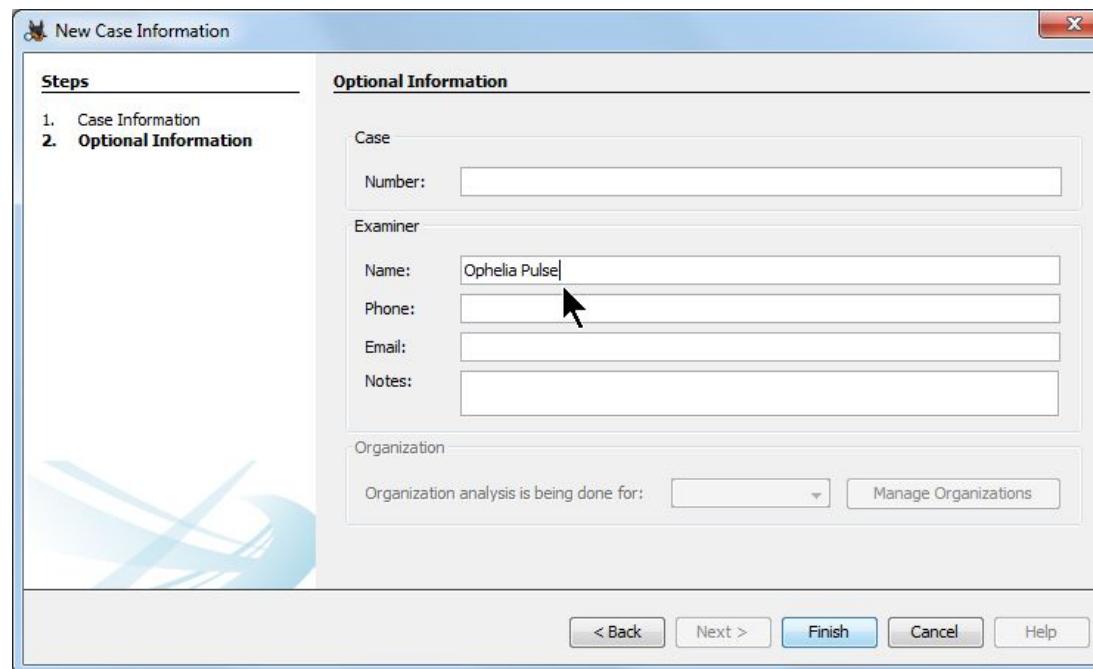
Enter Case Name & Base Directory Folder

- Enter Case Name:
 - **JPEG-8-Inquiry**
- Enter Base Directory:
 - Browse and make the folder "Autopsy" in your Documents folder.
- Click **Next**



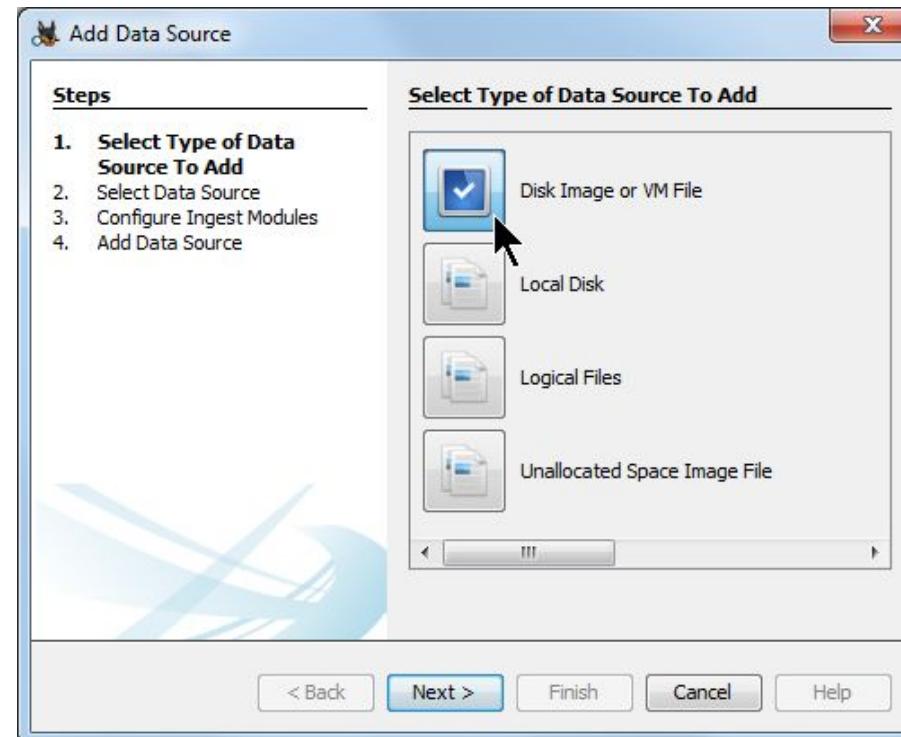
Enter your name

- Enter your name
 - In real life, you would also enter a Case Number and other information.
- Click Finish



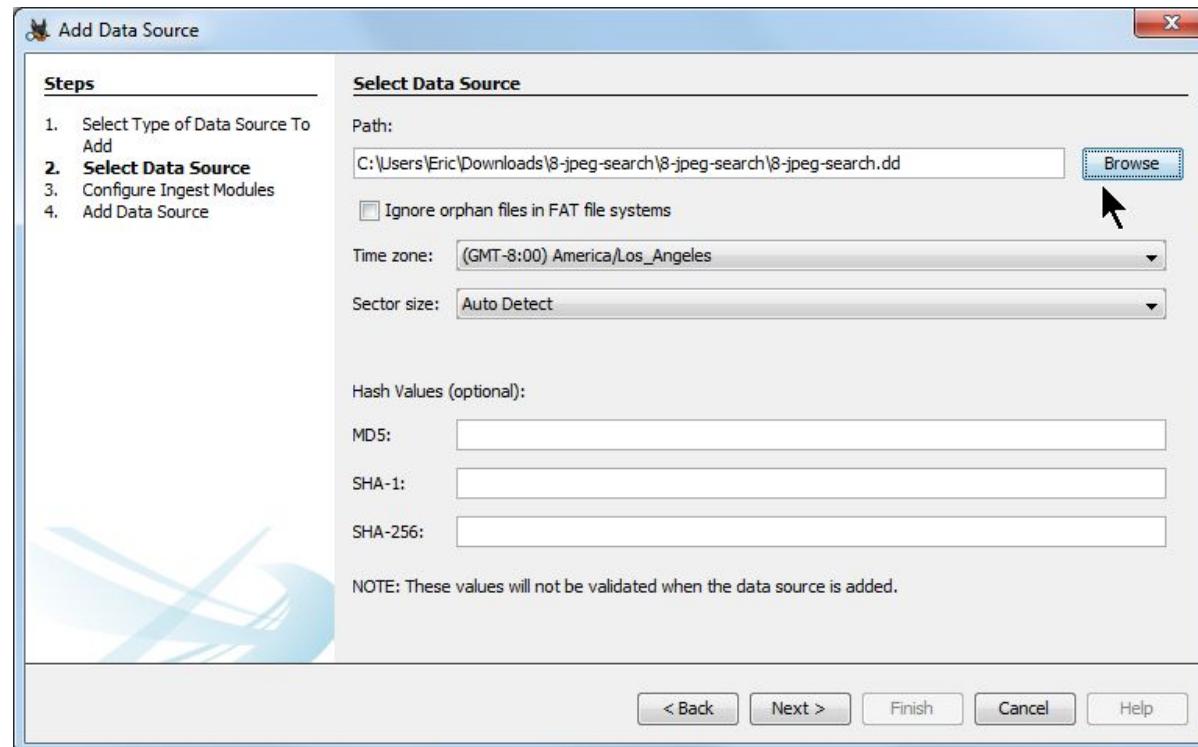
Add a Data Source

- **Click Disk Image or VM File**
 - A disk image is file containing a complete exact copy of a whole computer drive. Use it instead of reading the original drive.
- **Click Next**



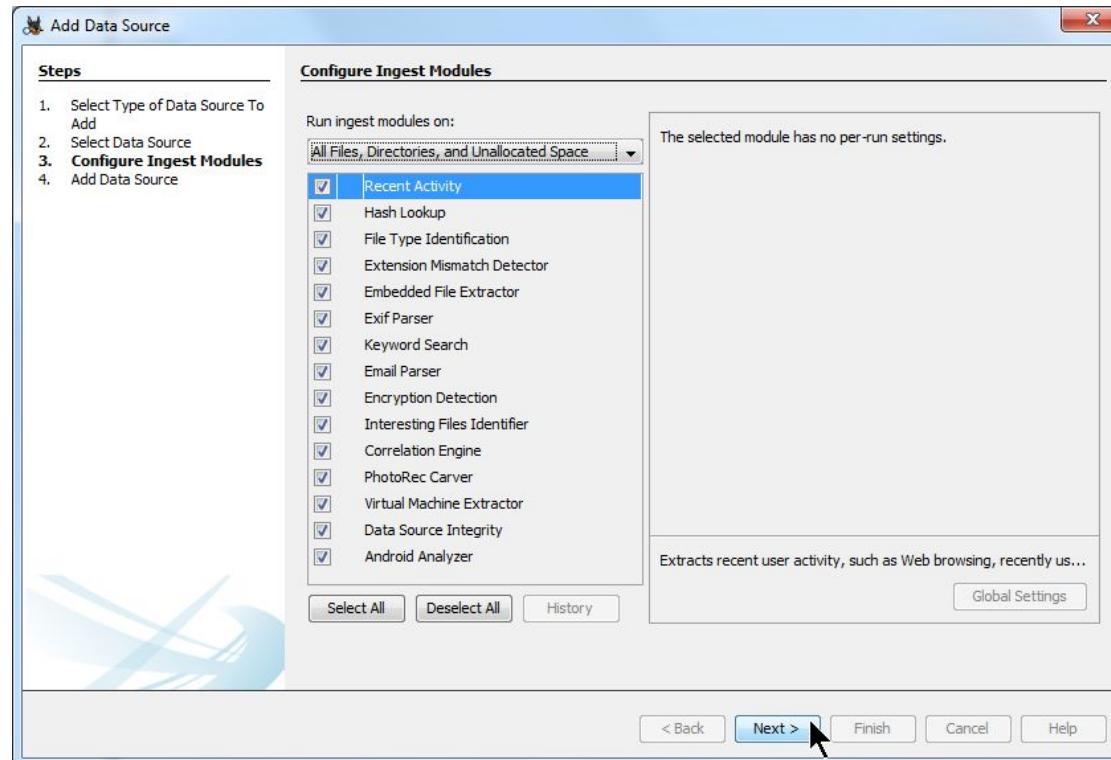
Select the Drive Image

- Browse to **8-jpeg-search.dd** and open it.
 - "Hash Values" are a kind of measurement. If a file changes, its calculated hash value changes. Use hash values to legally verify that your examination did not change the drive image.
- Click **Next**



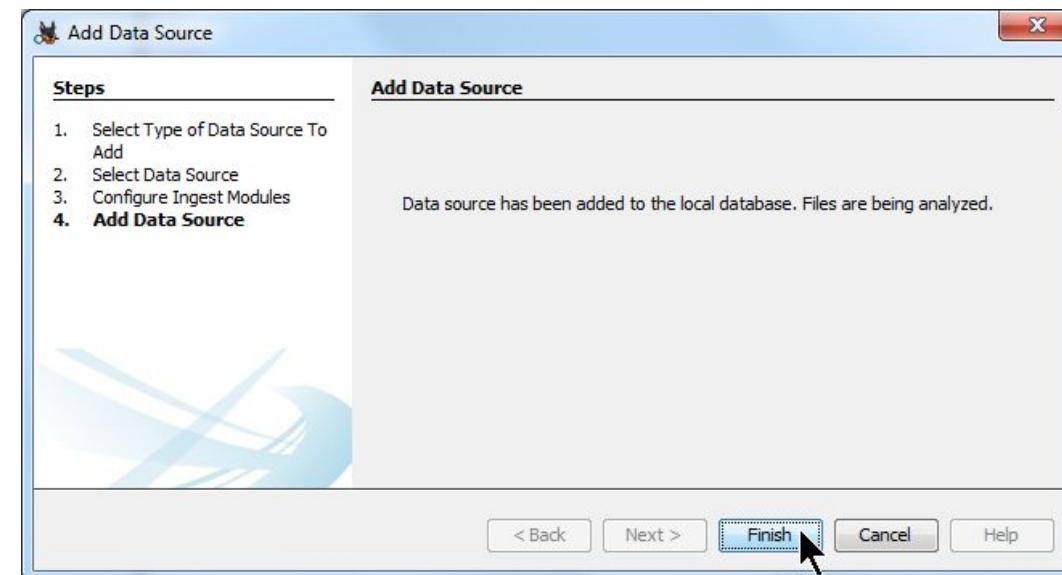
Select Ingest Modules

- Leave all the Ingest Modules checked, and click **Next**.
 - Ingest modules analyze the data in a data source. They perform all of the analysis of the files and separate out their contents. Examples include hash calculation and lookup, keyword searching, and web artifact extraction.



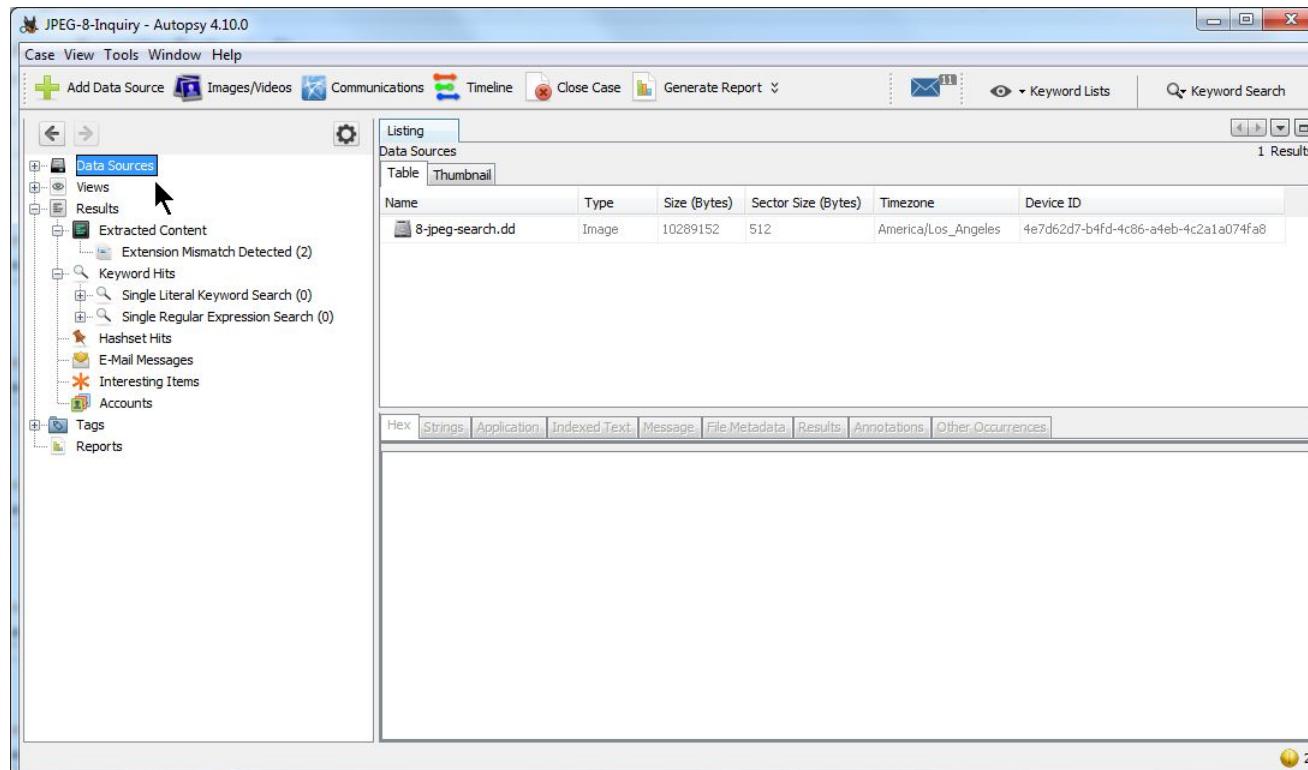
Finish Data Source

- Click Finish



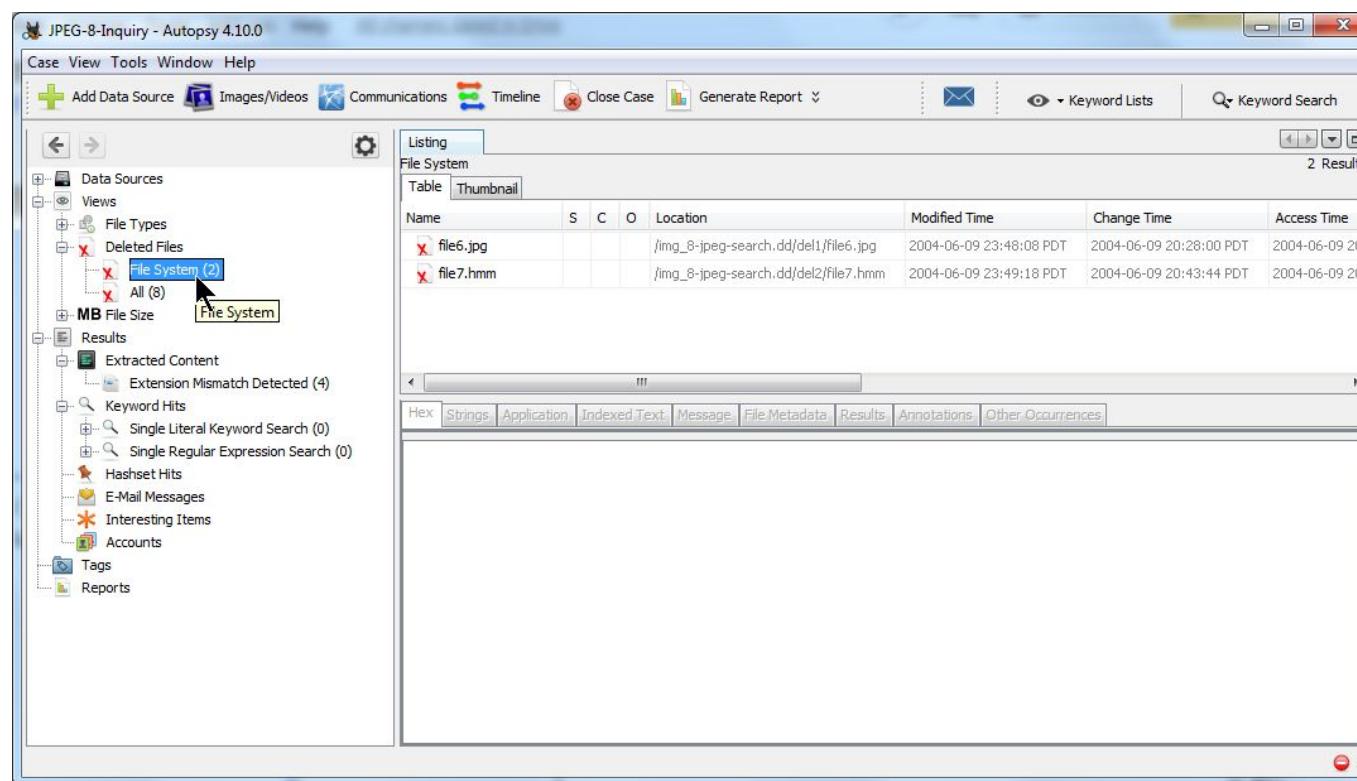
Autopsy Workspace

- Autopsy automatically analyses your drive image, and then displays the results.



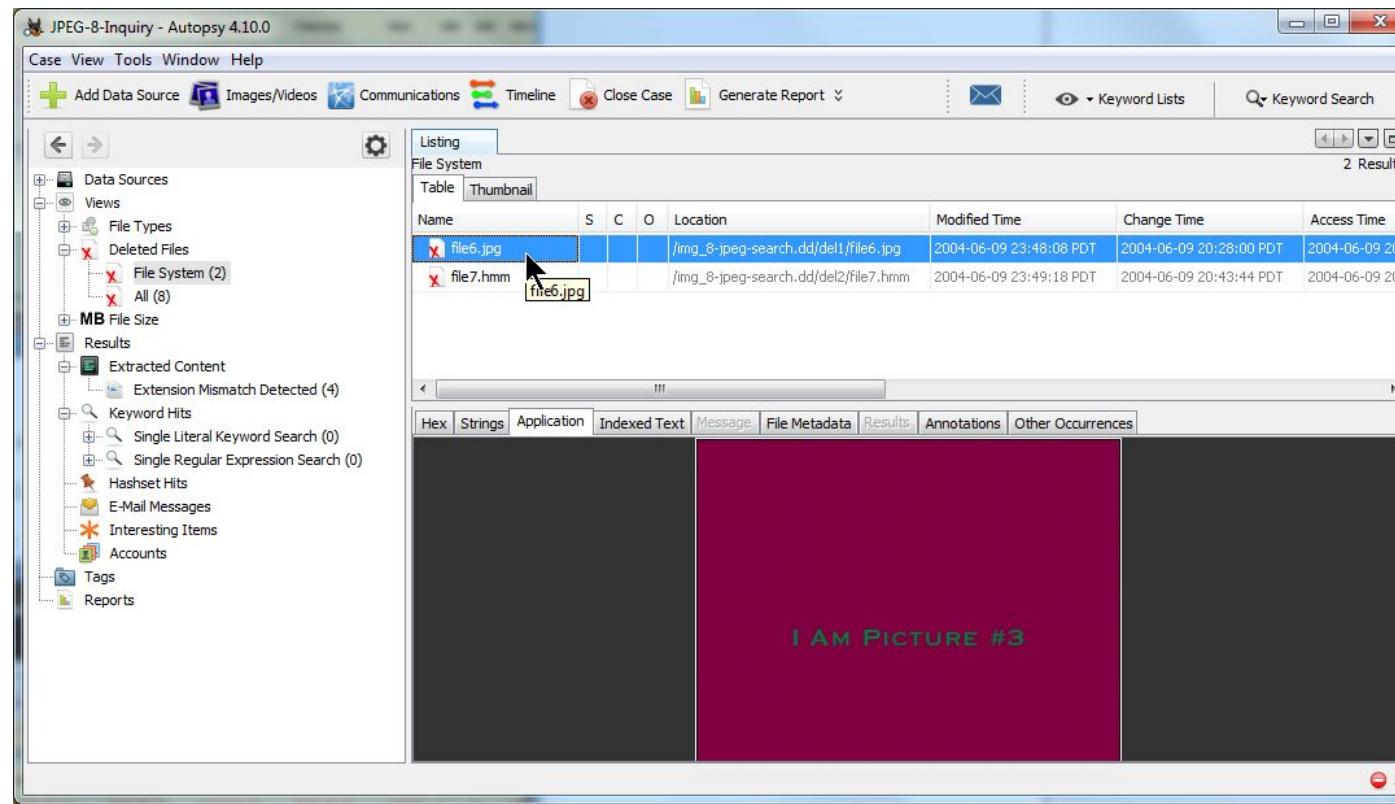
Show Deleted Files

- Click the + sign to expand Views
- Expand Deleted Files
- Click File Systems



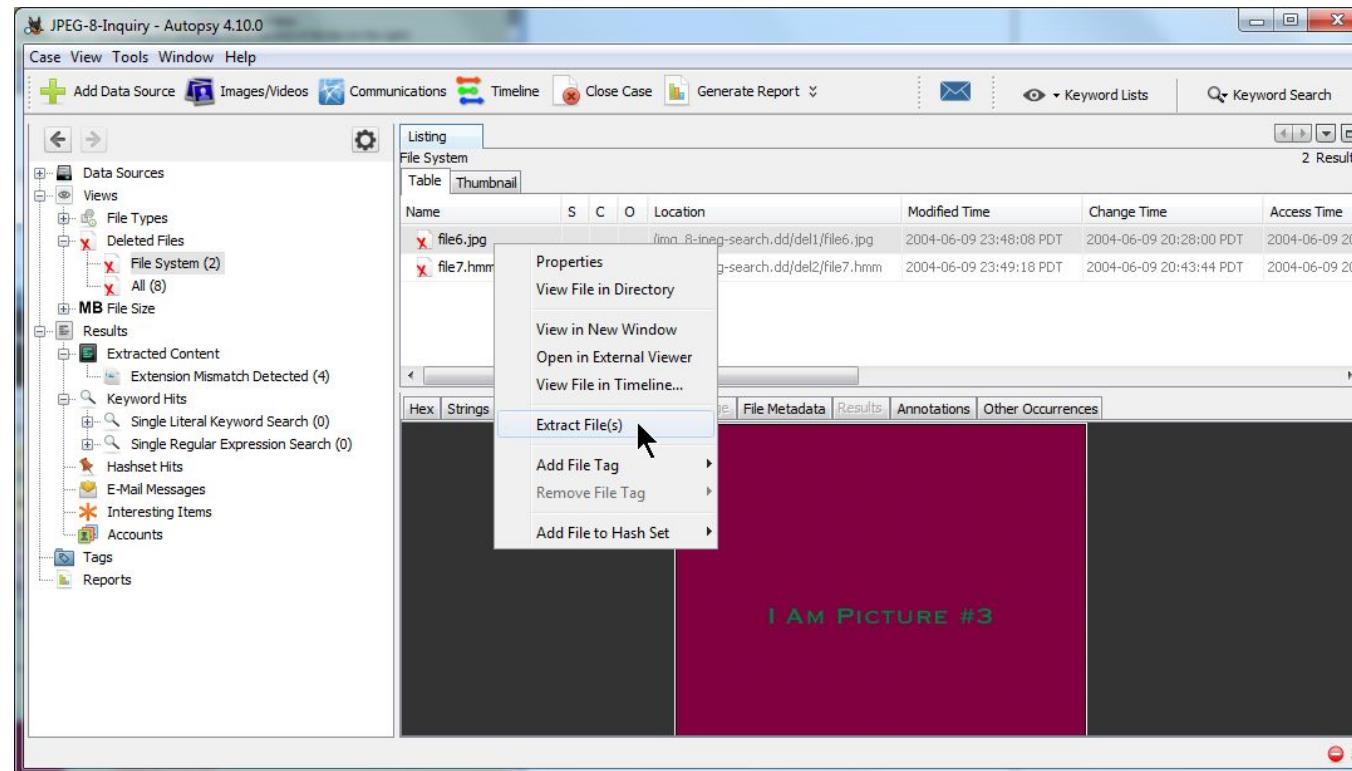
Preview Deleted File

- Click on the file named **file6.jpg**
- The bottom frame displays a thumbnail of the JPEG.



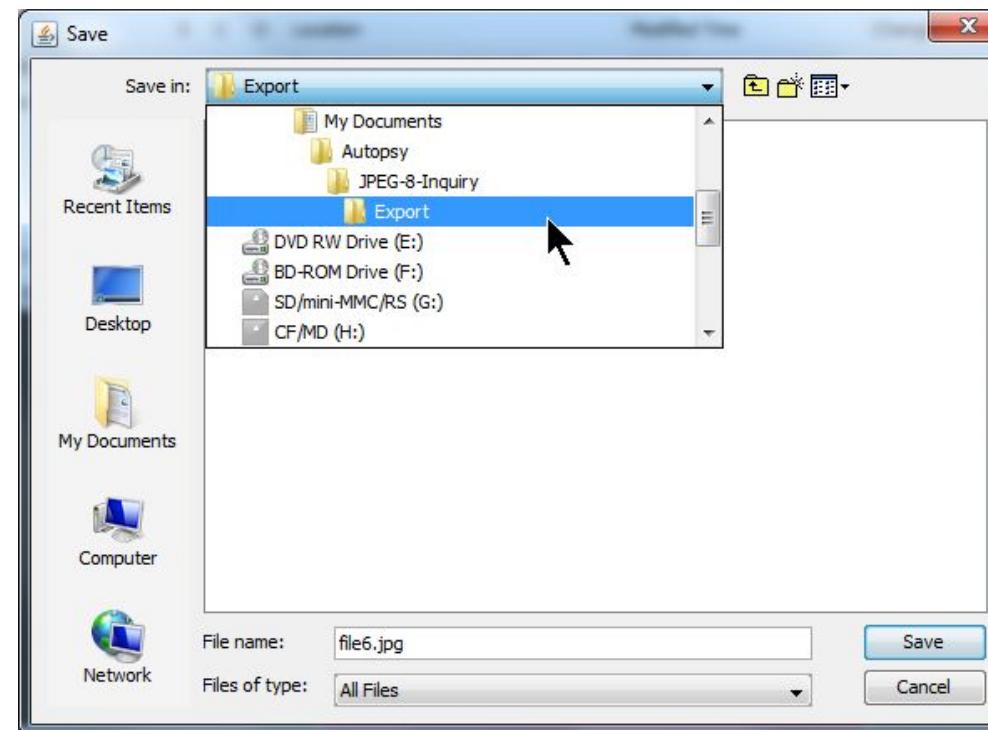
Extract (Export) a File

- Right-click file6.jpg
- Click Extract File(s)



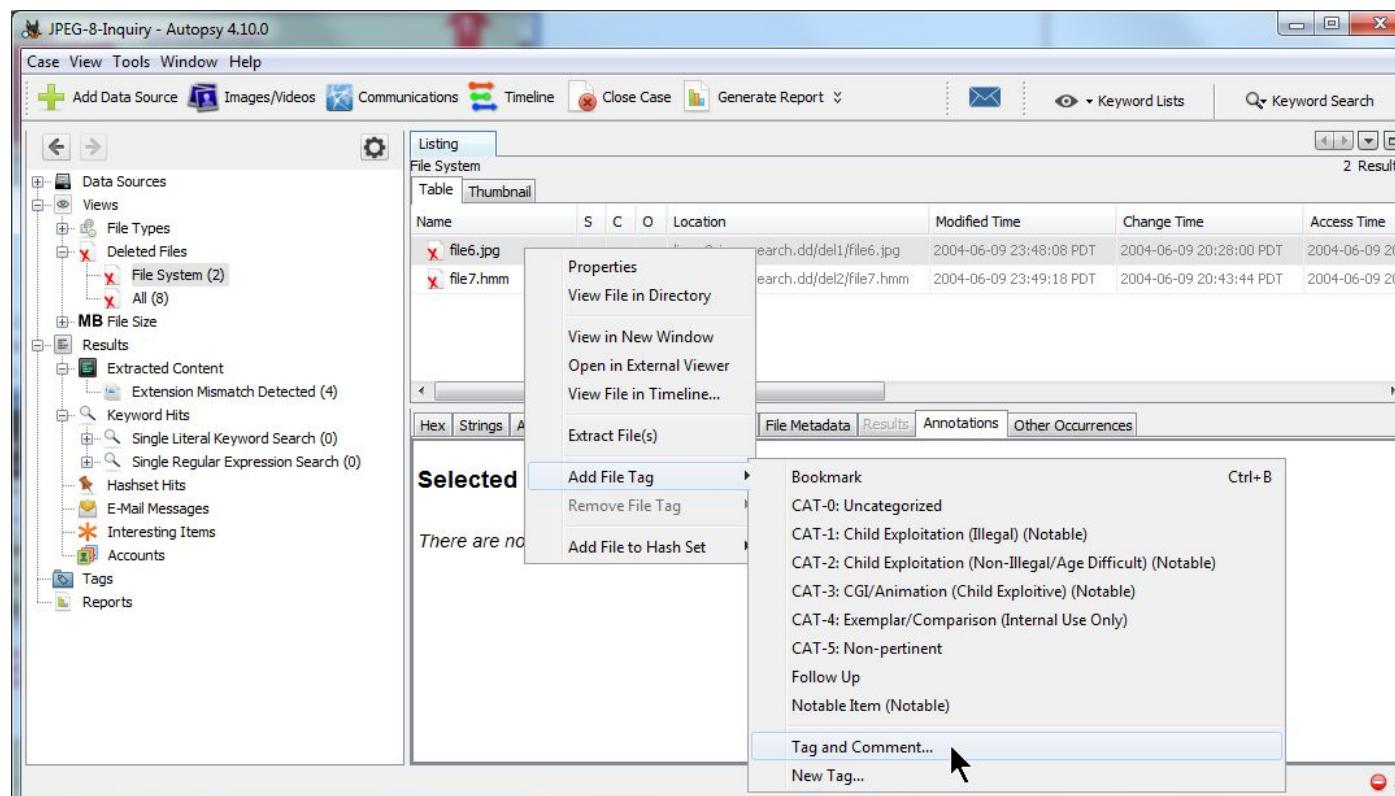
Save the Exported File

- Save **file6.jpg** into the **Export** folder of your **JPEG-8-Inquiry** case folder.
- Autopsy displays a dialog box with "File(s) extracted." Click the OK button.



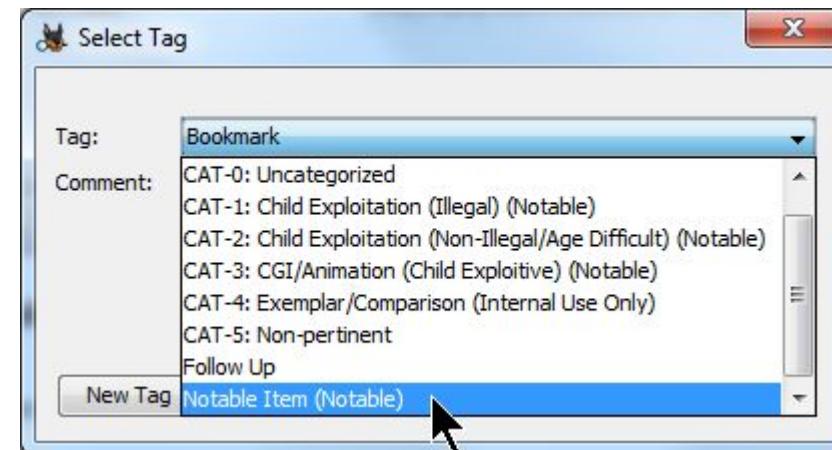
Add a Note

- Right-click file6.jpg
- Click Add File Tag
- Click Tag and Comment...



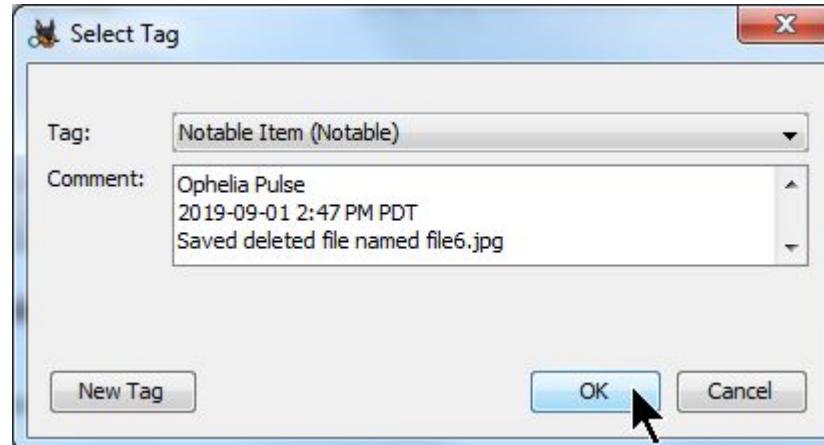
Tag Category

- In the Tag: drop-down list, select **Notable Item**



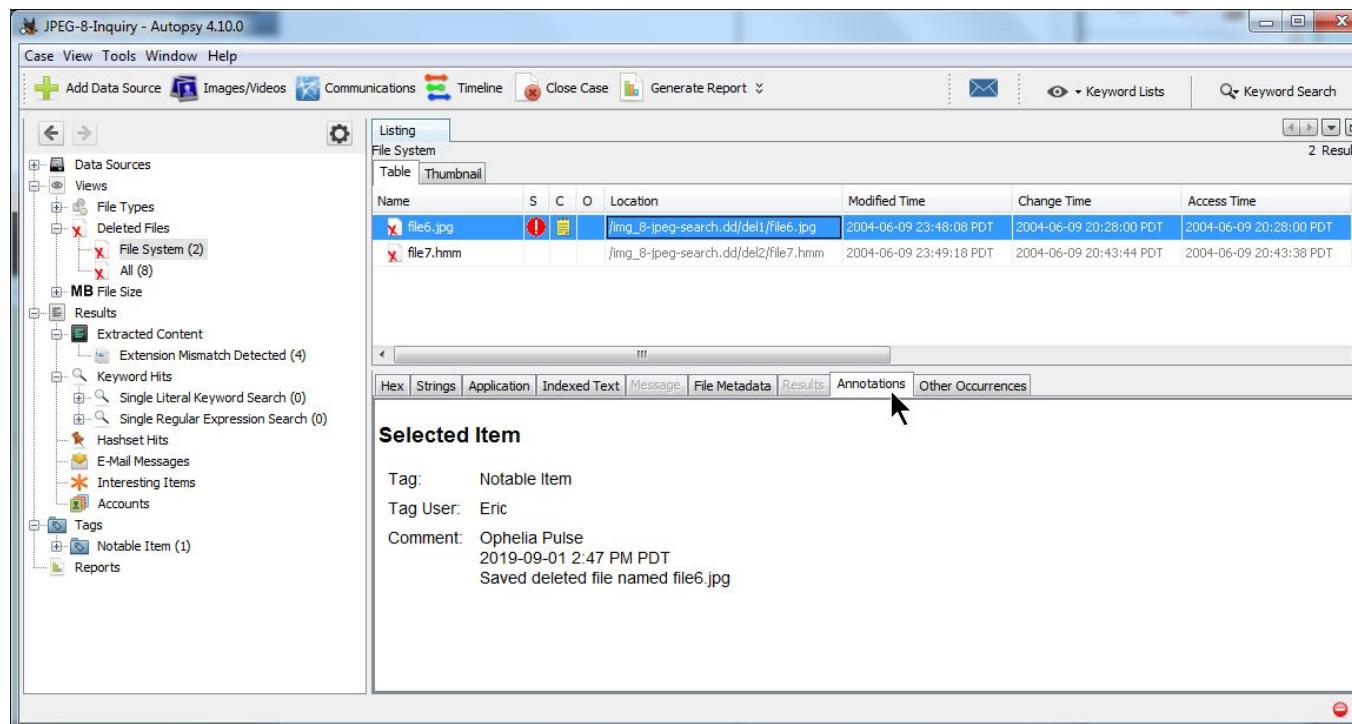
Write a Comment

- Add the following information in **Comment**:
 - Your Actual Name, Current Date and Time, and a Comment
- Click the **OK** button.



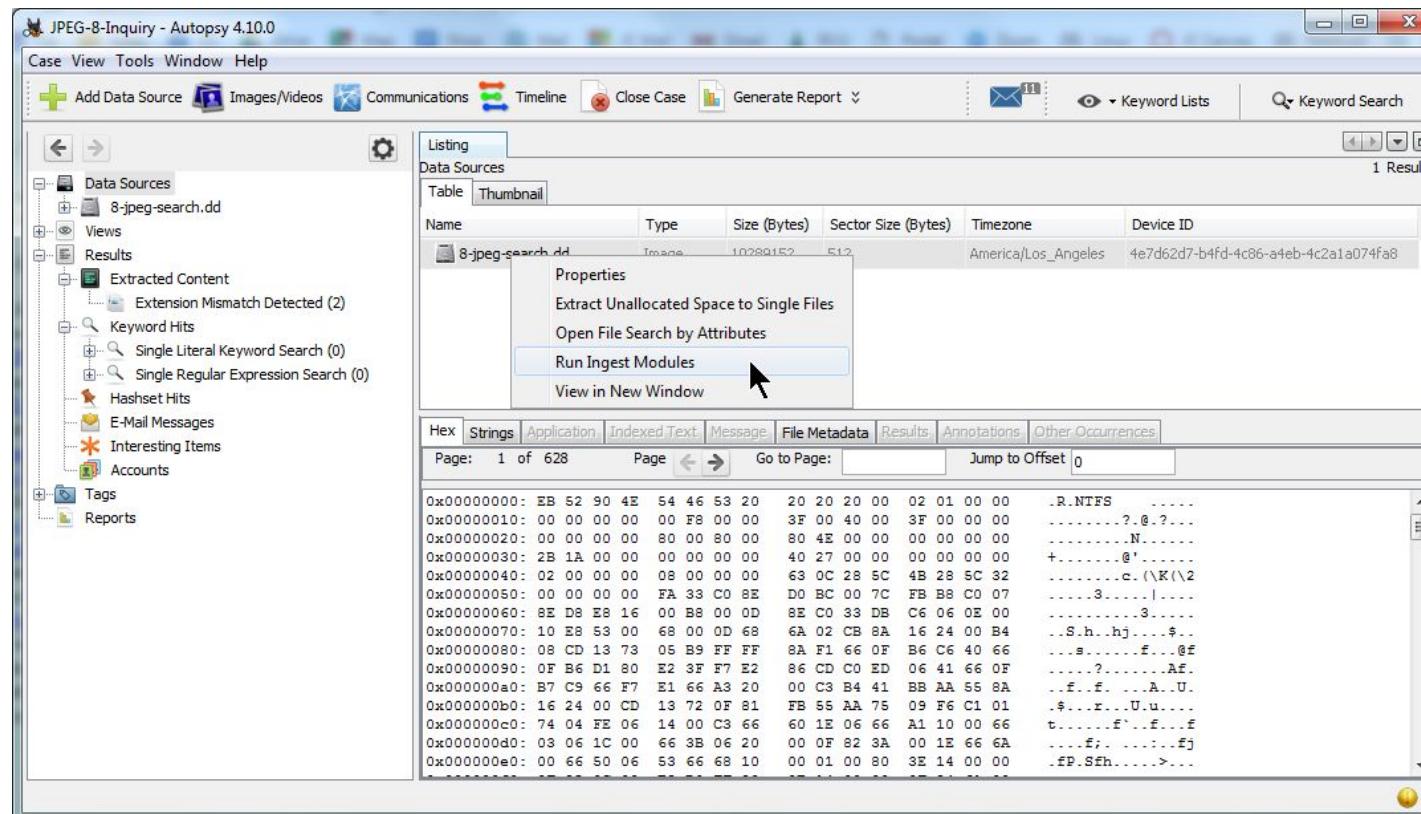
View Tag Information

- Click **file7.hmm**
- Click back to **file6.jpg**
- Click **Annotations** to view your tag



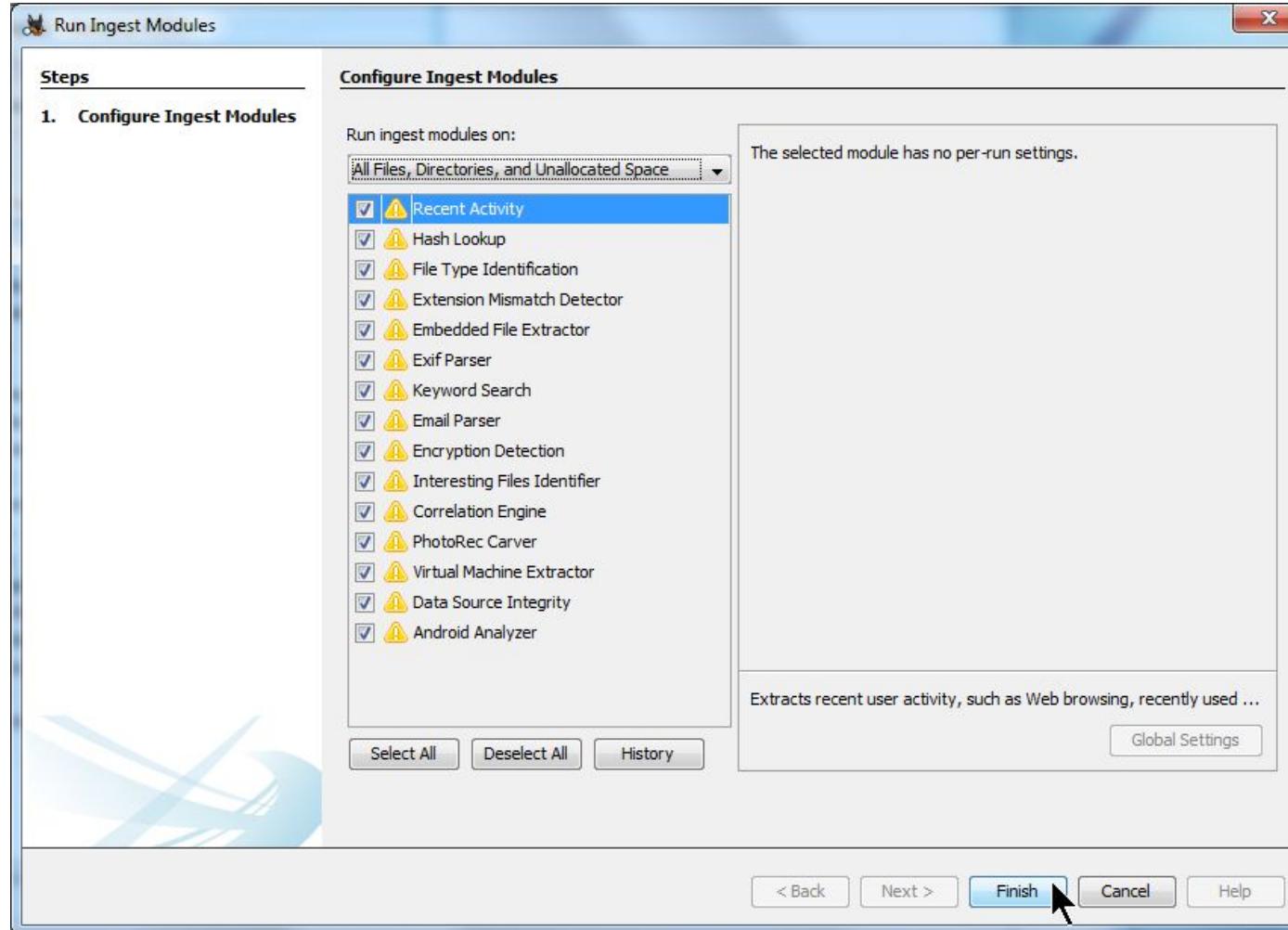
Checking Drive Image Integrity: Run Ingest Modules Again

- Click Data Sources
- Right-click 8-jpeg-search.dd
- Click Run Ingest Modules



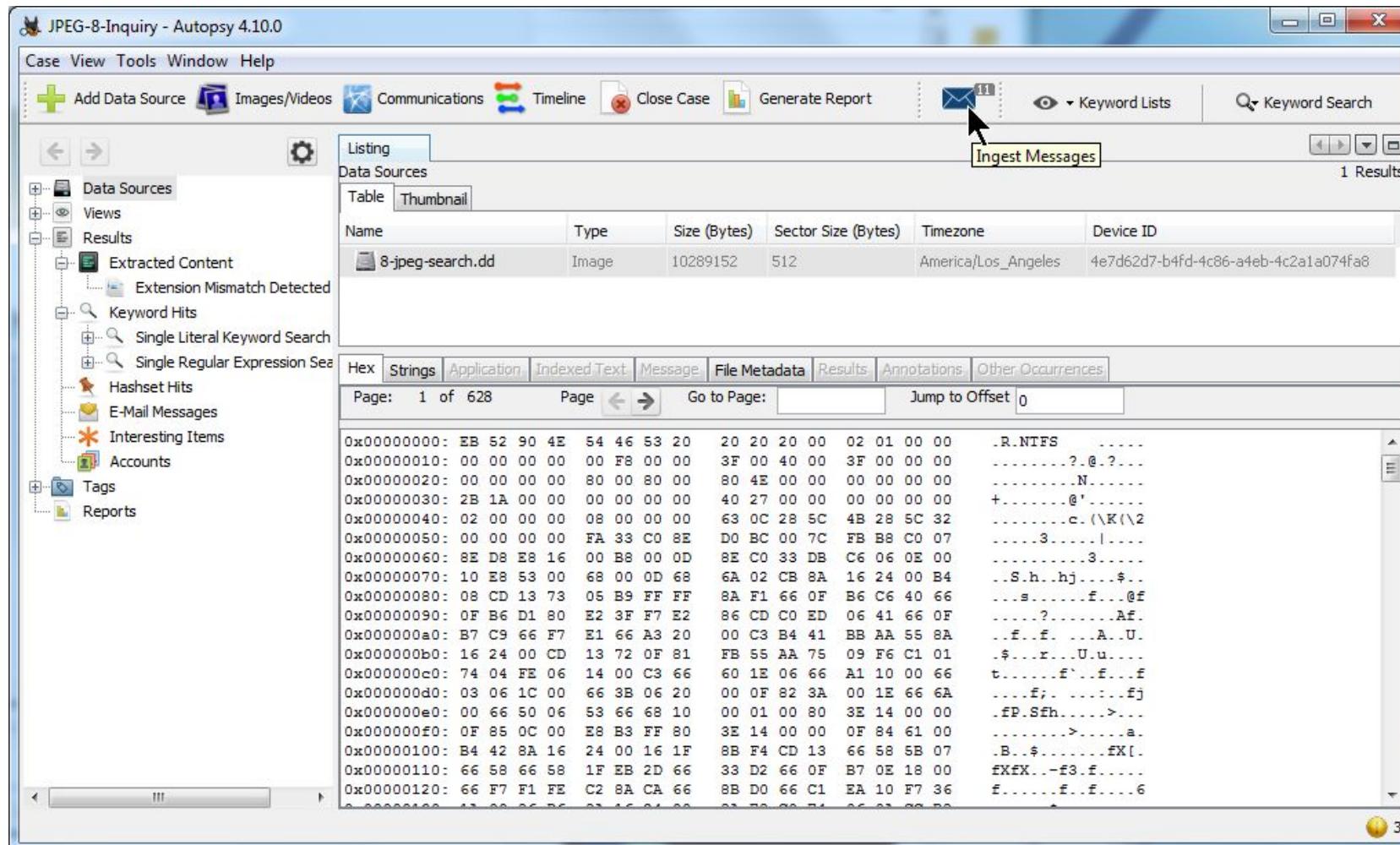
Run Ingest Modules

- Click Finish to run all Ingest Modules



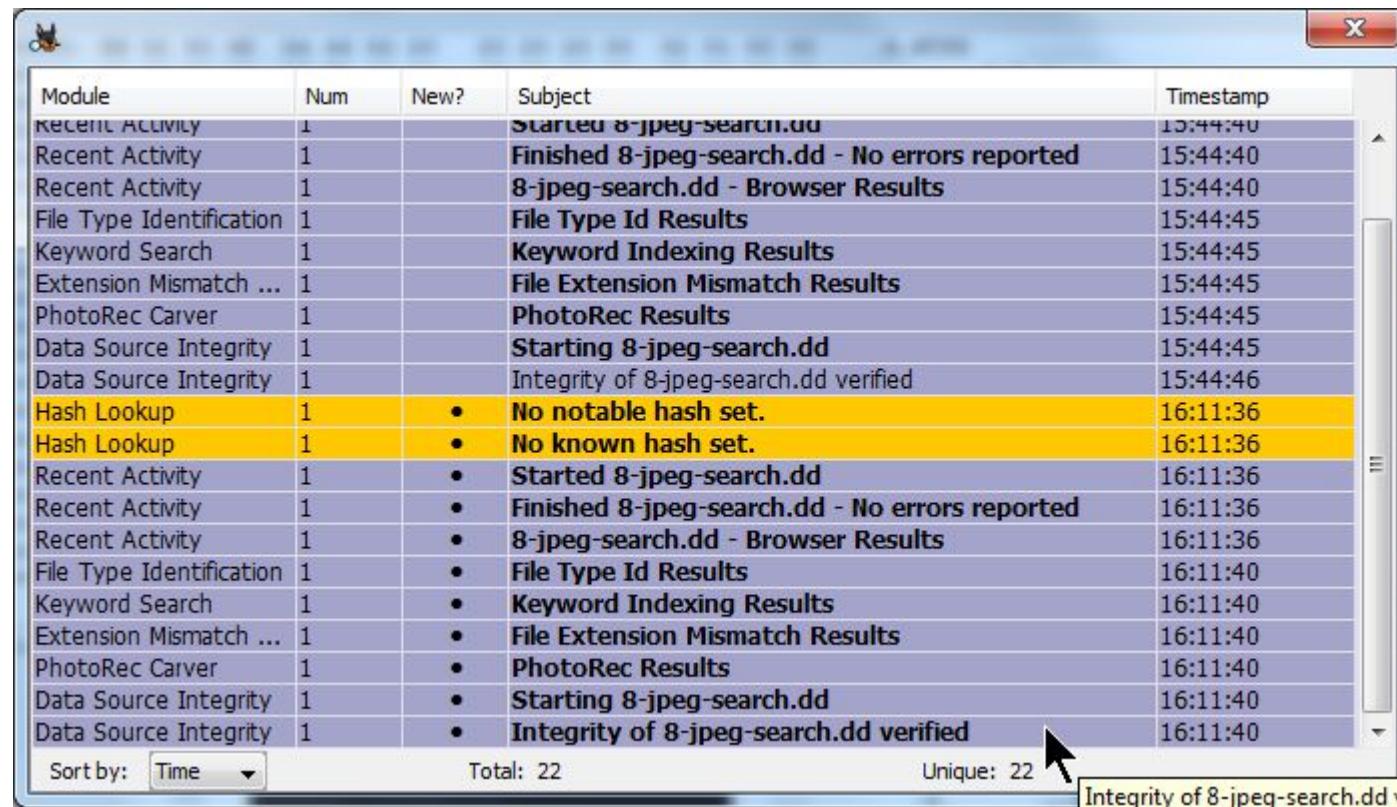
Open Ingest Messages

- Click the blue envelope to open Ingest Messages



Open Image Integrity Message

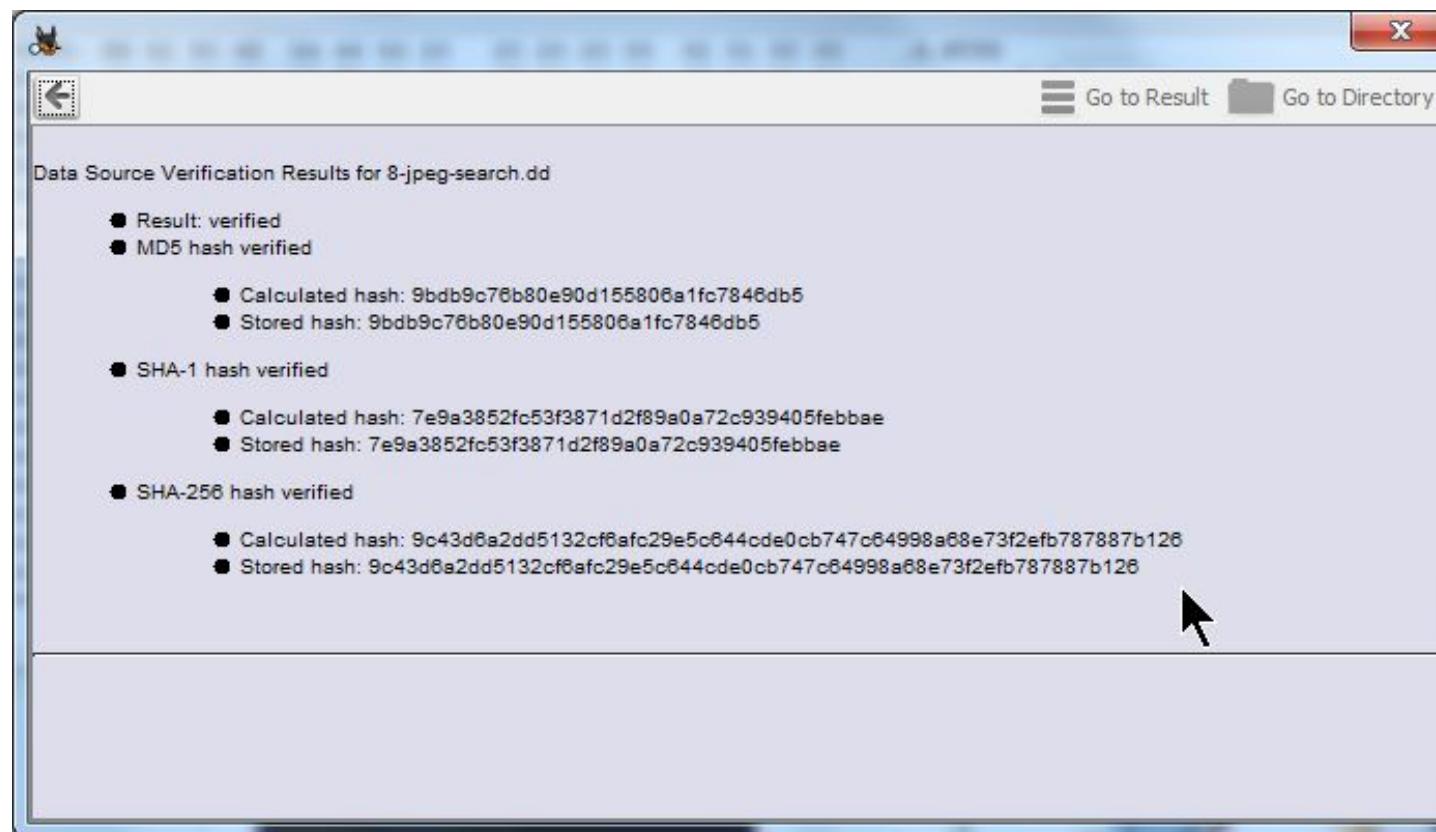
- Click last message: **Integrity of 8-jpeg-search.dd verified**



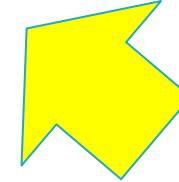
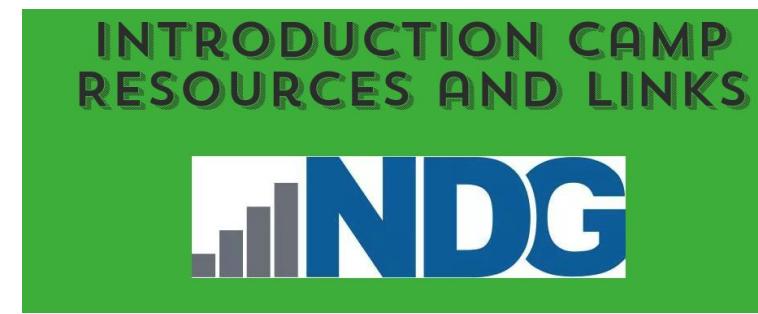
Module	Num	New?	Subject	Timestamp
RECENT ACTIVITY	1		Started 8-jpeg-search.dd	15:44:40
Recent Activity	1		Finished 8-jpeg-search.dd - No errors reported	15:44:40
Recent Activity	1		8-jpeg-search.dd - Browser Results	15:44:40
File Type Identification	1		File Type Id Results	15:44:45
Keyword Search	1		Keyword Indexing Results	15:44:45
Extension Mismatch ...	1		File Extension Mismatch Results	15:44:45
PhotoRec Carver	1		PhotoRec Results	15:44:45
Data Source Integrity	1		Starting 8-jpeg-search.dd	15:44:45
Data Source Integrity	1		Integrity of 8-jpeg-search.dd verified	15:44:46
Hash Lookup	1		• No notable hash set.	16:11:36
Hash Lookup	1		• No known hash set.	16:11:36
Recent Activity	1		• Started 8-jpeg-search.dd	16:11:36
Recent Activity	1		• Finished 8-jpeg-search.dd - No errors reported	16:11:36
Recent Activity	1		• 8-jpeg-search.dd - Browser Results	16:11:36
File Type Identification	1		• File Type Id Results	16:11:40
Keyword Search	1		• Keyword Indexing Results	16:11:40
Extension Mismatch ...	1		• File Extension Mismatch Results	16:11:40
PhotoRec Carver	1		• PhotoRec Results	16:11:40
Data Source Integrity	1		• Starting 8-jpeg-search.dd	16:11:40
Data Source Integrity	1		• Integrity of 8-jpeg-search.dd verified	16:11:40

Open Image Integrity Message

- Do the image integrity hash measurement strings match?
- Make sure you didn't legally compromise the drive image
- Close the window when done



Netlab Login



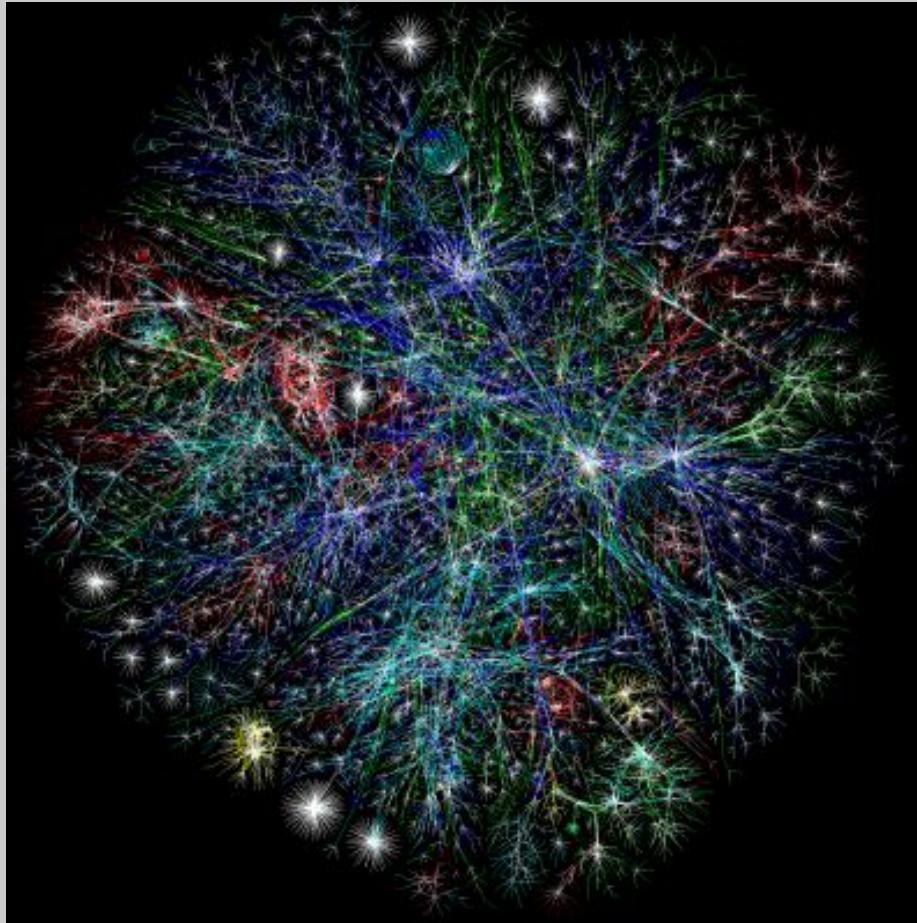
1. Log in to Netlab baycyber.net/intro
2. Click on the large “NDG” logo to access Netlab
3. Create a Team Reservation for
Cyber_Camp_2019_Forensic Access
(same Netlab as tomorrow’s Wireshark exercise)
4. Use the Autopsy reference guide

Forensics CTF

- Go to baycyber.net/intro
- Go to Day 3 “Digital Forensics and Networking”
- Click on “Digital Forensics CTF”
- Create a login and play

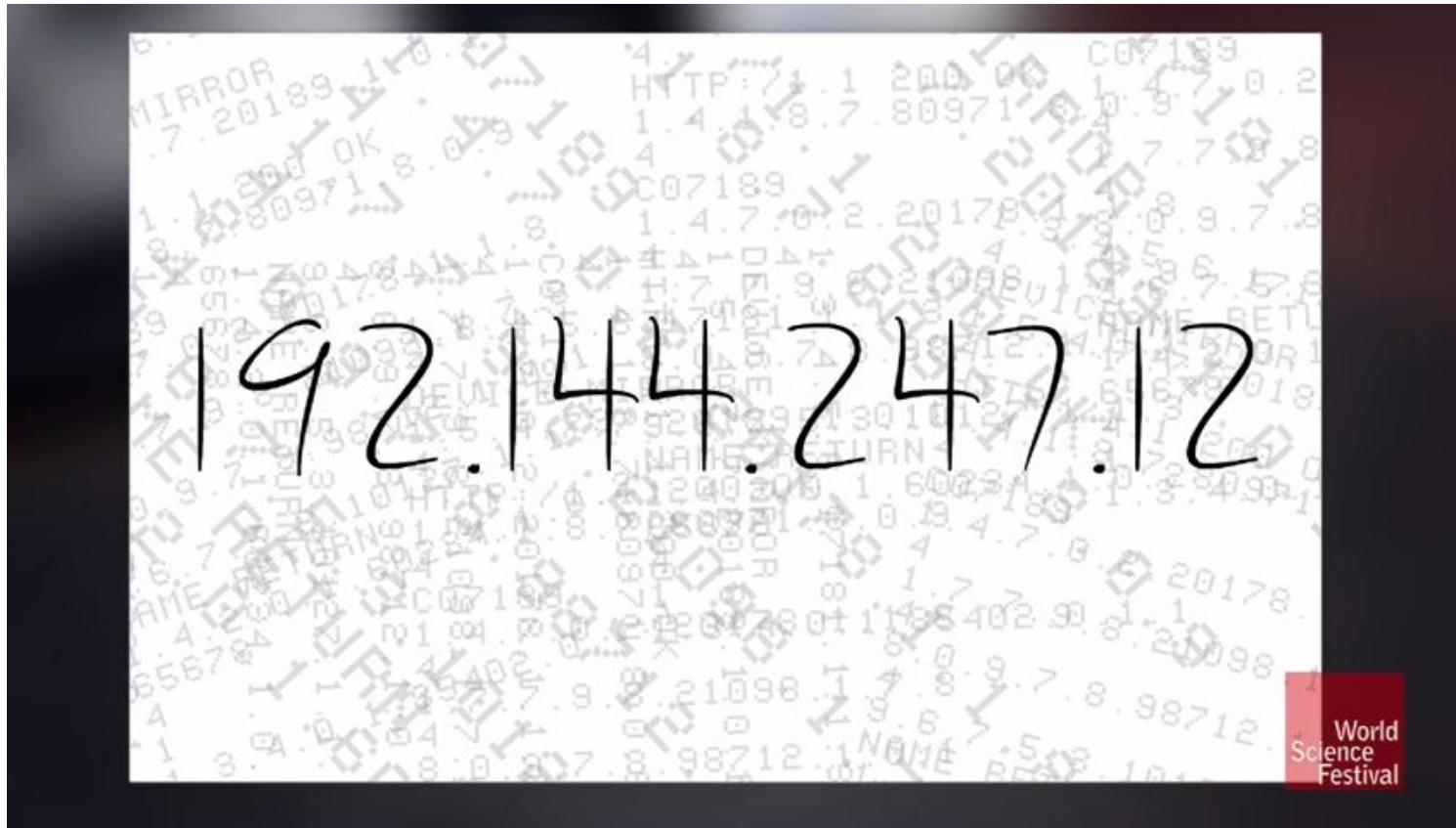


Networking & The Internet



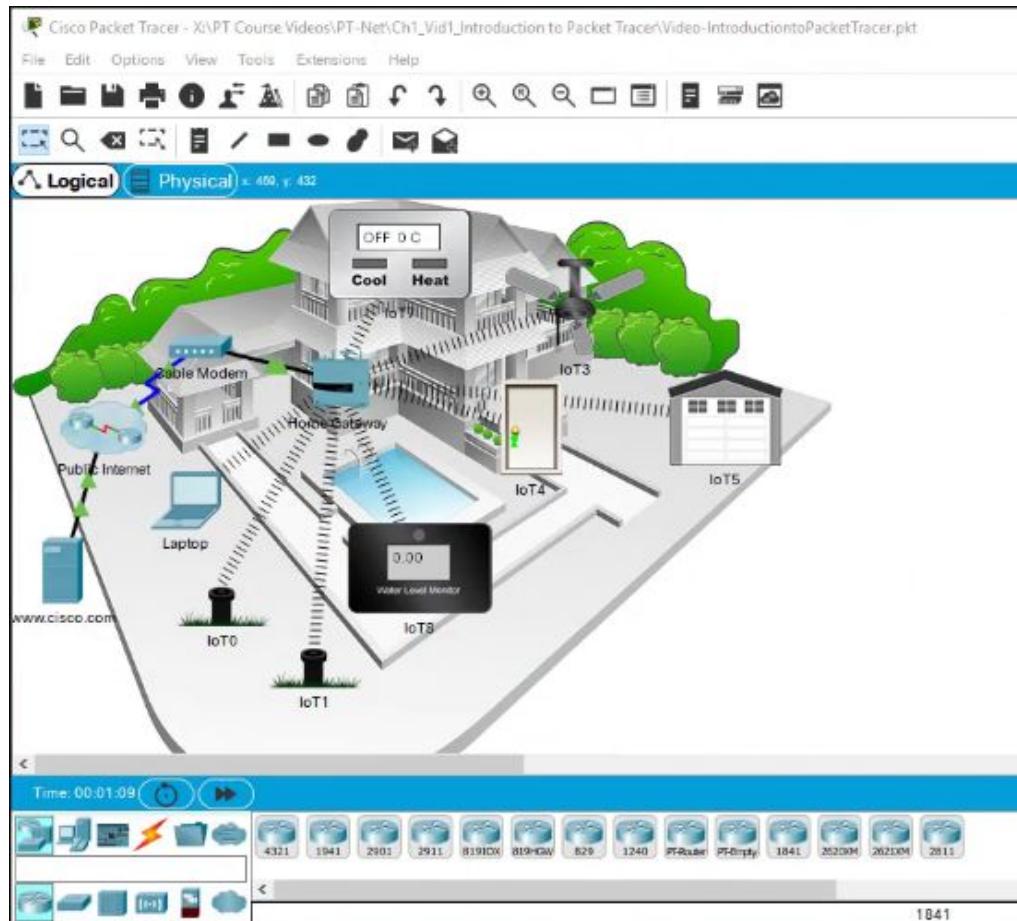
How Does the Internet Work?

Video: Internet Overview



What is Packet Tracer?

Packet Tracer lets you draw and run a simulated network on screen.



Packet Tracer Online Course

Enroll or sign in here:



My NetAcad

I'm Teaching

I'm Managing

Courses I've Enrolled In

		In Progress
Exploratory		
Introduction to Packet Trac...		
Introduction to Packet Tracer		

Cisco Virtual Academy

Networking using
Packet Tracer





Home

Modules

Discussions

Grades

Assignments

Quizzes

Courses



Calendar



Inbox



Introduction to Packet Tracer 0419 g

If this is your first time in the course, click [here](#) for more information.



- Chapter 1**
Introduction to Packet Tracer
- Chapter 2**
The User Interface
- Chapter 3**
Simulation Mode
- Chapter 4**
Packet Tracer Physical View and File Assessment Types
- Chapter 5**
IoT Components in Packet Tracer
- Chapter 6**
Creating and Controlling a Small Smart Home Network
- Chapter 7**
Packet Tracer Environment Controls
- Chapter 8**
Creating and Programming Objects in Packet Tracer



Chapter 1

Overview of Packet Tracer

[Video to Overview](#)

Download and Install Packet Tracer

How to install Packet Tracer for home use

The screenshot shows a video player interface. At the top, a navigation bar displays 'Chapter 1' and 'Introduction to Packet Tracer' followed by a series of numbered steps: '1.1 Introduction to Packet Tracer', '1.1.2 How do I Setup Packet Tracer?', and '1.1.2.1 Download and Install Packet Tracer'. A close button is located in the top right corner. The main content area features a collage of images related to networking, such as people, trees, and circuit boards. Below this collage, a video thumbnail has a black overlay with the text 'Video - Download and Install Packet Tracer'. The video player includes standard controls like play, pause, volume, and a progress bar indicating '3:33'. To the right of the video, a sidebar titled 'Download and Install Packet Tracer' contains a list of reasons why students use the tool, followed by a detailed description of its use in Cisco Networking Academy courses, and a call-to-action to click play for a walk-through.

Chapter 1
Introduction to Packet Tracer

1.1 Introduction to Packet Tracer

1.1.2 How do I Setup Packet Tracer?

1.1.2.1 Download and Install Packet Tracer

Download and Install Packet Tracer

Students commonly use Packet Tracer to:

- Prepare for a certification exam.
- Practice what they learn in networking courses.
- Sharpen their skills for a job interview.
- Examine the impact of adding new technologies into existing network designs.
- Build their skills for jobs in the Internet of Things.
- Compete in Global Design Challenges (take a look at the 2017 PT 7 Design Challenge on Facebook).

Packet Tracer is an essential learning tool used in many Cisco Networking Academy courses.

Click Play in the video for a [detailed walk-through](#) of the [Packet Tracer download and installation](#).

Video - Download and Install Packet Tracer

3:33

About Wistia

Report a Problem

Comment and thumbs up

Share

Like

Next

Previous

44

Host Devices

Host: Any Kind of computer that uses the network. Also called “End Devices”

“Client” and “Server” are jobs that a host can have.

- **Clients** are devices that ask for content.
- **Servers** are devices that provide content



Desktop Computer



Smartphone



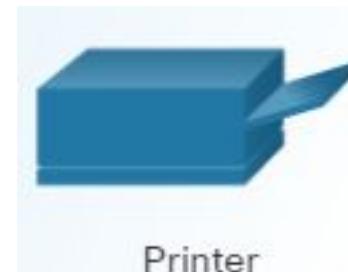
Laptop Computer



Server



IP Phone

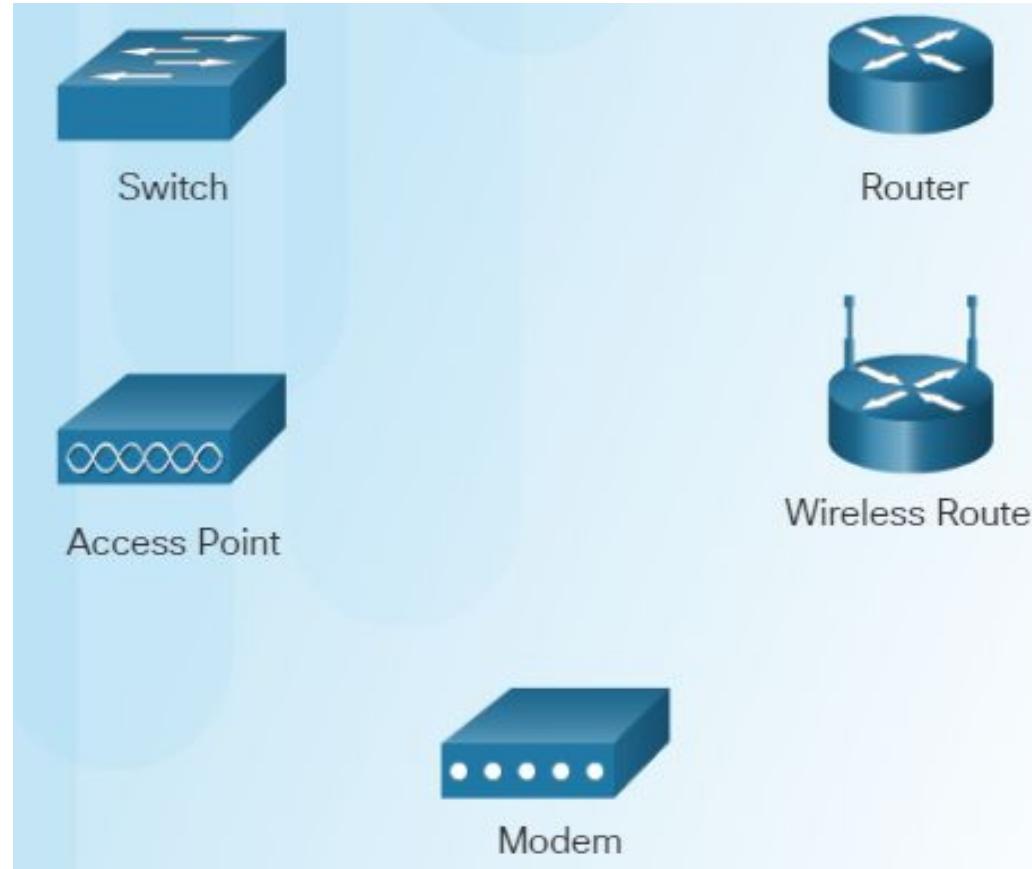


Printer

Intermediary Devices

Intermediary Devices: interconnect Host devices

They Provide Network Connectivity and manage data flow through the network



Home Network Equipment

A home network normally has a single gateway device combining four jobs:

- **Modem** - Outside connection: converts (modulates & demodulates) outside cable or DSL.
- **Router** - Connects Internet with inside network.
- **Switch** - A set Ethernet ports to make a wired LAN (Local Area Network).
- **Wifi: wireless access point (WAP)** as part of the LAN



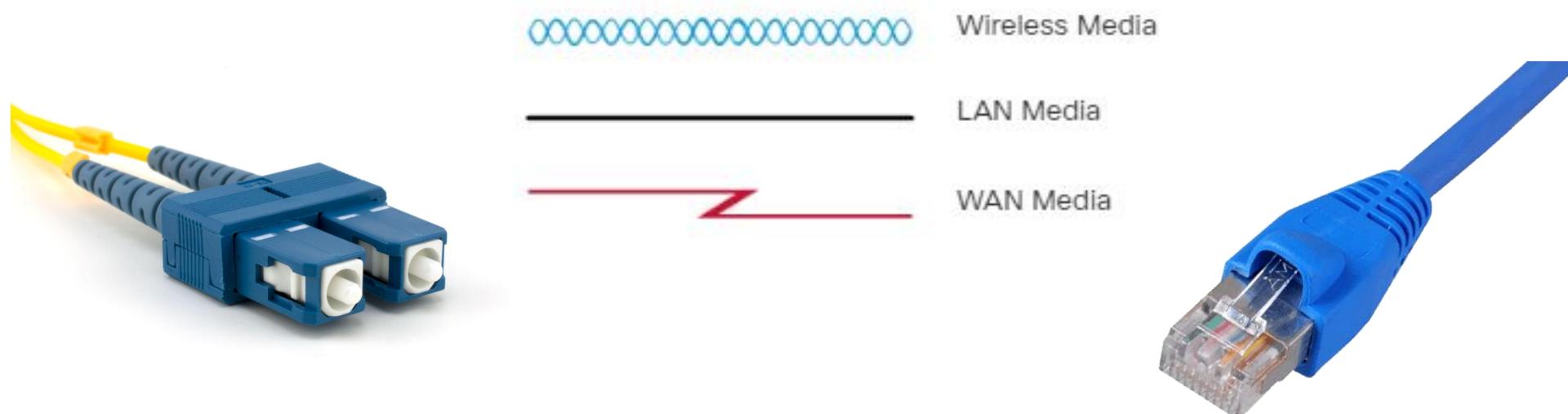
Network Media

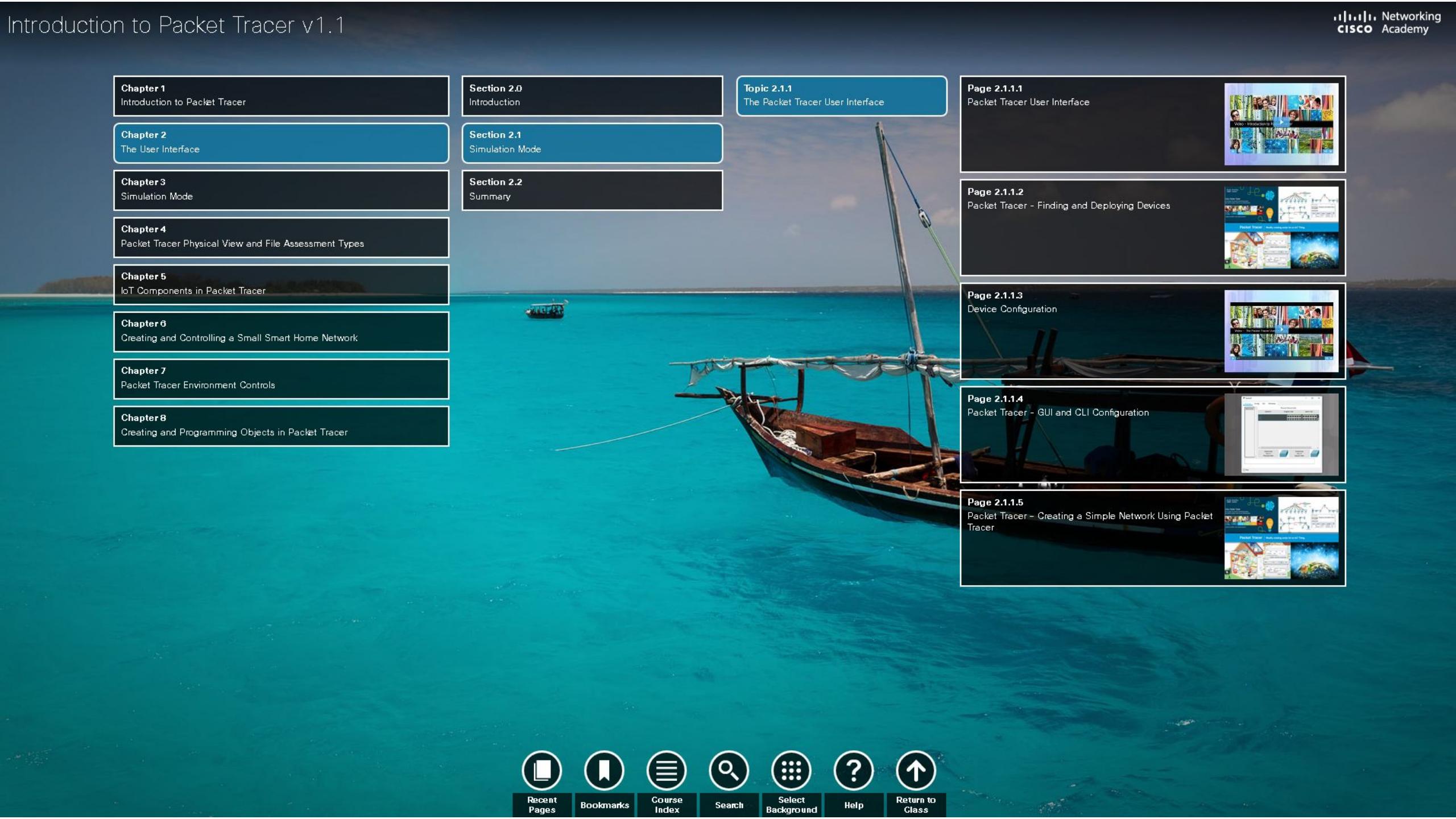
Network Media: Provides the channel over which the message travels from source to destination. The actual path that data, as electrical signals, travels between devices.

Example: Wireless, Optical, Copper

Straight through: Unlike Devices - Router To Switch, Switch to Computer

Cross Over: Like Devices- Router To Router, Switch to Switch



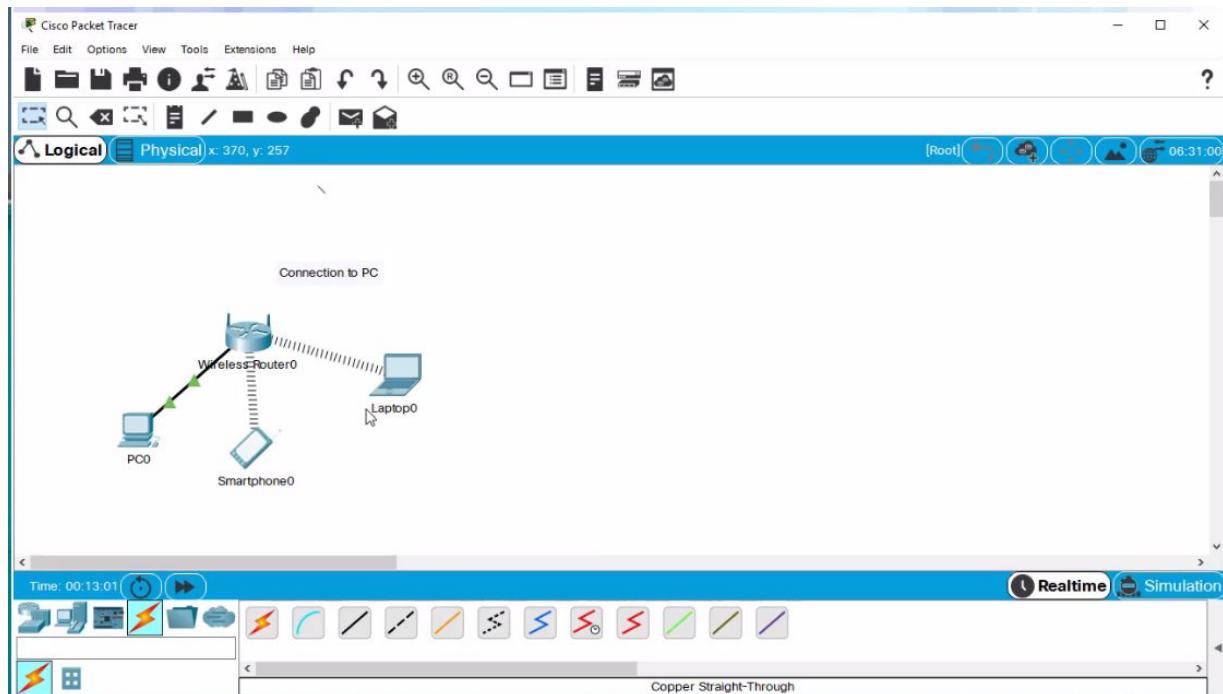
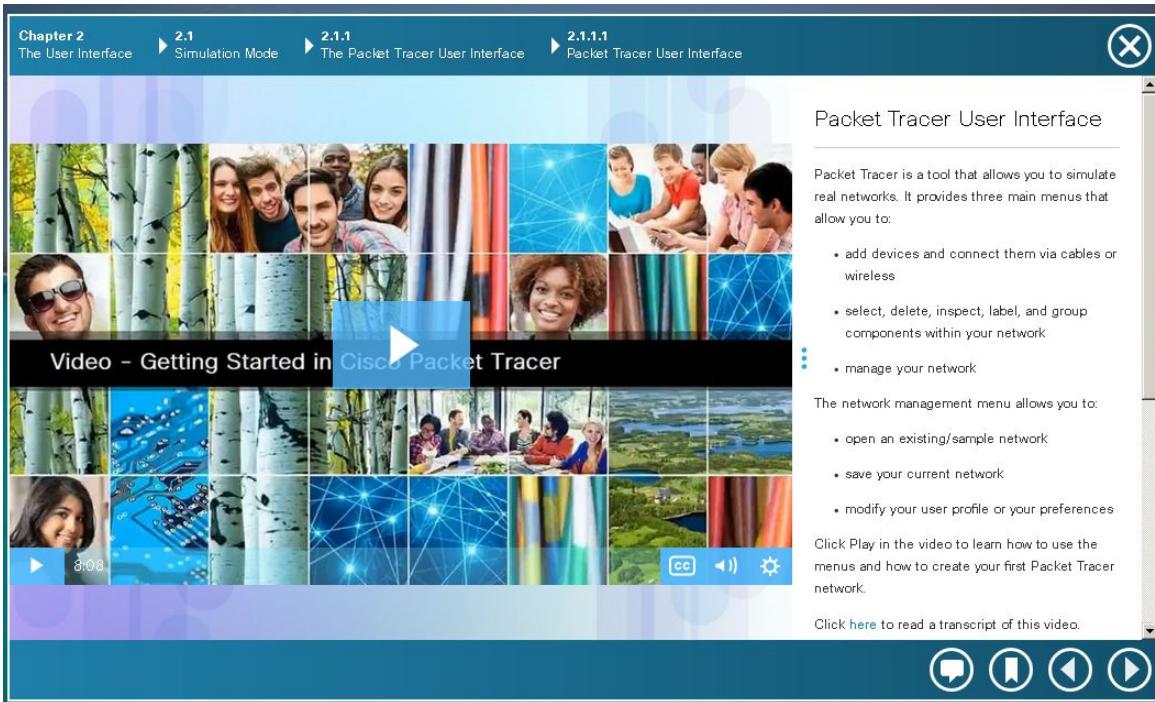


The main content area features a large, traditional wooden sailboat with a single mast and a small sail, positioned in the center of a bright blue ocean. The sky above is a clear, pale blue with a few wispy white clouds. In the background, a distant, low-lying island with lush green vegetation is visible under the sun.

Chapter 1 Introduction to Packet Tracer	Section 2.0 Introduction	Topic 2.1.1 The Packet Tracer User Interface
Chapter 2 The User Interface	Section 2.1 Simulation Mode	Page 2.1.1.1 Packet Tracer User Interface
Chapter 3 Simulation Mode	Section 2.2 Summary	Page 2.1.1.2 Packet Tracer - Finding and Deploying Devices
Chapter 4 Packet Tracer Physical View and File Assessment Types		Page 2.1.1.3 Device Configuration
Chapter 5 IoT Components in Packet Tracer		Page 2.1.1.4 Packet Tracer - GUI and CLI Configuration
Chapter 6 Creating and Controlling a Small Smart Home Network		Page 2.1.1.5 Packet Tracer - Creating a Simple Network Using Packet Tracer
Chapter 7 Packet Tracer Environment Controls		
Chapter 8 Creating and Programming Objects in Packet Tracer		

Packet Tracer User Interface

2.1.1.1 Video: Getting Started in Packet Tracer View and follow along with the video in page 2.1.1.1



Packet Tracer - Finding and Deploying Devices

Do both 2.1.1.2 exercises: **Deploying Devices & Deploying and Cabling Devices**

The screenshot displays the Cisco Packet Tracer software interface. At the top, a navigation bar shows the progression from Chapter 2 User Interface to 2.1.1.2 Packet Tracer - Finding and Deploying Devices. The main window features a network diagram with various devices like PCs, switches, and routers connected to an Internet port. To the right, a detailed configuration window titled "PT Activity 00002: Packet Tracer - Configuring a Zone-Based Policy Firewall (ZPF) Addressing Table" is open, showing an addressing table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	GE1	192.168.1.1	255.255.255.0	N/A
RR1 (GE2)	GE1	192.168.1.2	255.255.255.0	N/A

Below the main window, there's a "Devices" panel showing a list of network components and a "Links" panel for managing connections between them. A large globe graphic representing a global network is visible in the background.

Packet Tracer - Finding and Deploying Devices

Since Packet Tracer simulates networks and network traffic, the physical aspects of these networks also needs to be simulated. This includes actually finding and deploying physical devices, customizing those devices, and cabling those devices. After the physical deployment and cabling is done, then it is time for configuration of the interfaces used to connect the devices.

Finding a device to deploy requires looking in the Device-Type Selection Box. The Device-Type Selection Box works on the concept of categories and sub-categories as shown in the figure.

The top row of icons represents the category list consisting of: [Networking Devices], [End Devices], [Components], [Connections], [Miscellaneous], and [Multiuser]. Each category contains at least one sub-category group.

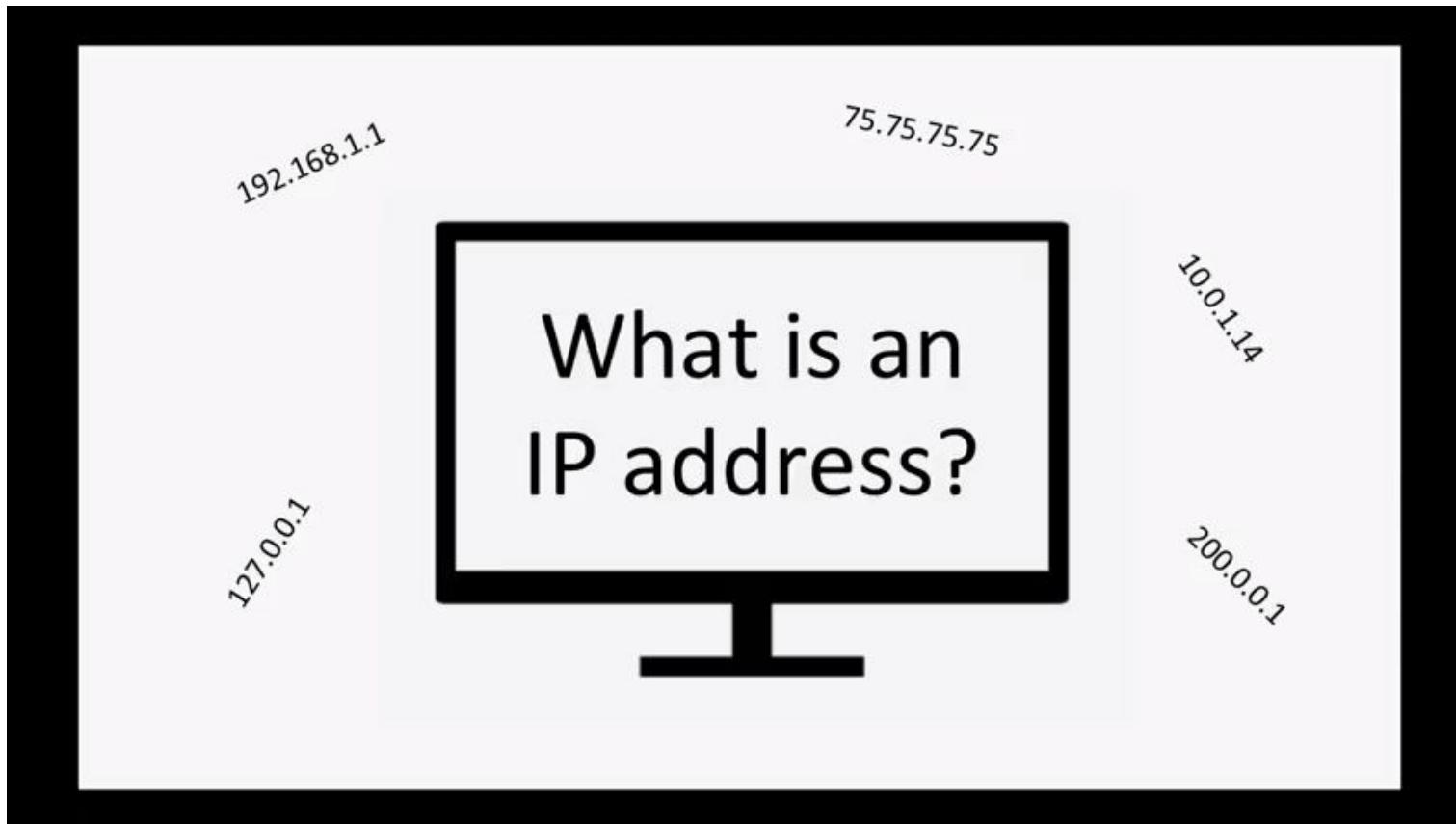
[Packet Tracer - Deploying Devices Instructions](#)
[Packet Tracer - Deploying Devices Packet Tracer File](#)
[Packet Tracer - Deploying and Cabling Devices Instructions](#)
[Packet Tracer - Deploying and Cabling Devices Packet Tracer File](#)

The Internet - Packets, Routing, & Reliability



Video - IP Addresses

What is an IP Address?



Exercise 1: What's My IP Address?

1. Open up a web browser and navigate to: WhatIsMyIP.com
2. You'll notice that the IP address you get from this web service is different from the address given in your command prompt.
3. The address you see displayed on this webpage is your **public IP address**.



Exercise 2: Where does this address go?

IP addresses are used to locate hosts on the Internet.

Enter IP address **172.217.0.46** into your web browser's address bar.

Where does it take you?

IP (Internet Protocol) Version 4 address

- Address number of a computer (or device) on the Internet or local network
- Shown as 4 numbers (max 255), separated by periods
- For example: **192.168.1.12**
- But really, it's 32 binary digits (bits), like this:
11000000.10101000.00000001.00001100



IPv4 Addressing: Subnet Mask

- Splits the IP address into ***network*** and ***host*** portions
- Shown in dotted decimal
 - But in binary, it's a row of 1's (network) followed by a row of 0's (host).
- For example, **255.255.255.0:**
11111111.11111111.11111111.00000000



IPv4 Addressing: Subnet Mask Example

- For example, **255.255.255.0**:
11111111.11111111.11111111.00000000
- ... splits our address **192.168.1.12**:
11000000.10101000.00000001.00001100
- ... into *network* **192.168.1.0**:
11000000.10101000.00000001.00000000
- ... and *host* (individual computer) **12**:
00000000.00000000.00000000.00001100

IP (Internet Protocol) Version 6 address

IPv6 (IP version 6) Address

- Because we are running out of IPv4 addresses, the Internet is slowly moving to IP version 6 (IPv6)



128 bit IPv6 Address Format:

2001:0DB8:CAFE:0200:0000:0000:0000:0008

- 8 “hextets,” 4-digit hexadecimal values separated with colons
- Number of addresses: $2^{128} =$
340,282,366,920,938,463,463,374,607,431,768,211,456
(340 undecillion)



Packet Tracer: Device Configuration

Chapter 2 The User Interface ► 2.1 Simulation Mode ► 2.1.1 The Packet Tracer User Interface ► 2.1.1.3 Device Configuration X



▶

7:44

CC

Speaker

Settings

Device Configuration

Once your network has been created, it is time to configure the devices and components. Packet Tracer has the capability to configure the different intermediate and end devices that make up your network. To access the configuration interface of any devices first click on the device that you wish to configure. A popup window will appear displaying a series of tabs. Different types of devices have different interfaces.

Click Play in the video to learn how to configure devices and components in your simulated network.

Click [here](#) to read a transcript of this video.

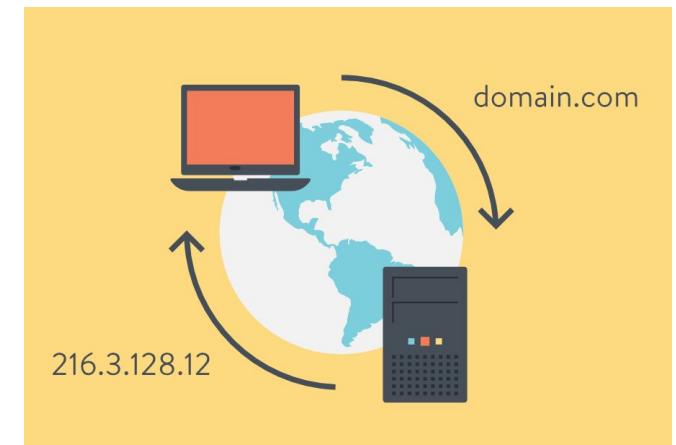
Gateway

- Address of a **router** that connects you to the rest of the Internet
- Connects first to your Internet Provider
- Part of your local network



DNS (Domain Name Service)

- Translates names to IP numbers
- Example: **santarosa.edu** translates to **198.189.195.52**
- Your Internet Provider supplies DNS server IP address number(s)



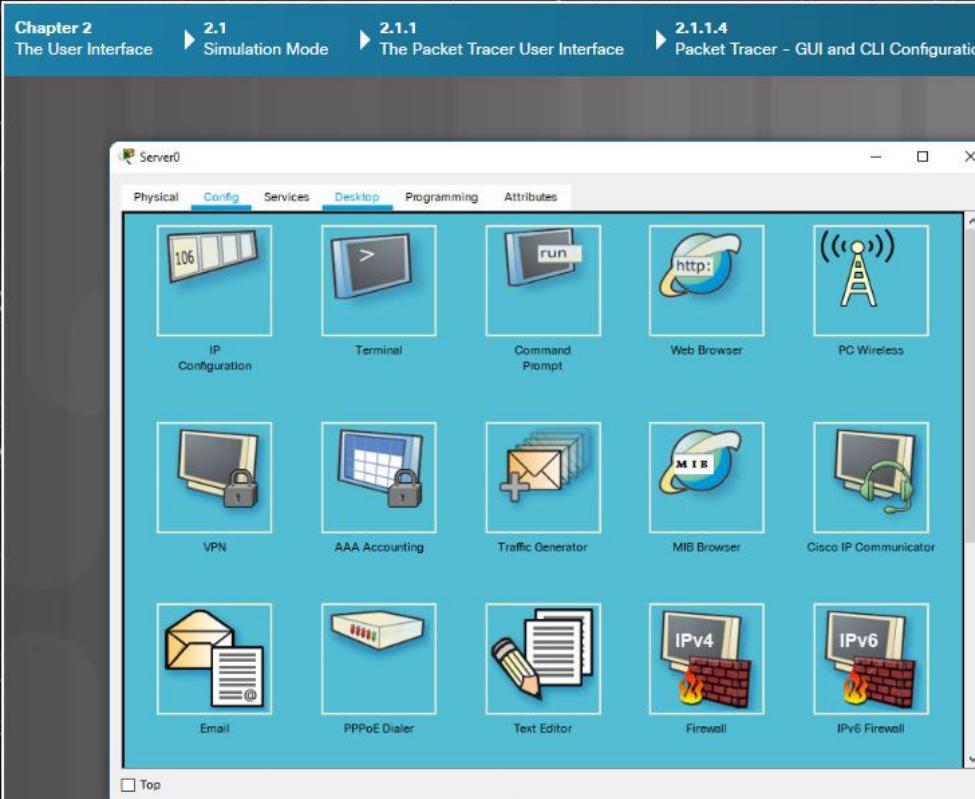
DHCP (Dynamic Host Configuration Protocol)

- Automatically gives a temporary address number, subnet mask, etc.
- Used in most connections from Internet providers
- A network **router** in your home or office may provide separate DHCP to your computer



2.1.1.4 Packet Tracer - GUI and CLI Configuration

2.1.1.4 "Configure End Devices" activity



The screenshot shows the 'Config' tab of the 'Server0' window in Packet Tracer. The tab bar at the top includes 'Physical', 'Config', 'Services', 'Desktop', 'Programming', and 'Attributes'. The 'Config' tab is selected, indicated by a blue background. Below the tabs, there are five rows of icons representing various configuration options:

- Row 1: IP Configuration, Terminal, Command Prompt, Web Browser, PC Wireless.
- Row 2: VPN, AAA Accounting, Traffic Generator, MIB Browser, Cisco IP Communicator.
- Row 3: Email, PPPoE Dialer, Text Editor, Firewall, IPv6 Firewall.

A vertical scroll bar is visible on the right side of the window. The main title bar of the application is 'Chapter 2: The User Interface > 2.1: Simulation Mode > 2.1.1: The Packet Tracer User Interface > 2.1.1.4: Packet Tracer - GUI and CLI Configuration'. The status bar at the bottom shows 'Figures' and navigation icons.

Packet Tracer - GUI and CLI Configuration

For intermediate devices such as routers and switches, there are two methods of configuration available. Devices can be configured or investigated via a Config tab (a GUI interface) or a command line interface (CLI) (Figure 1). The Config tab does not exist in most physical equipment. This tab is a learning tab in Packet Tracer. If you don't know how to use the command line interface, this tab provides a way to "fill in the blank" to do basic configurations. It will show the equivalent CLI commands that would do the same thing if using the Command Line Interface. The CLI interface requires knowledge of device configuration.

For some of the end devices, such as PCs and laptops, Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a Web browser, and much more (Figure 2).

If you are configuring a server, the server has all of the functions of the Host with the addition of one more tab, the services tab (Figure 3). This tab allows a server to be configured as a web server, a DHCP server, a DNS server, or various other servers visible in the graphic.

Packet Tracer - Configure End devices Instructions

1 2 3 Figures

2.1.1.5 Packet Tracer – Creating a Simple Network

2.1.1.5 "Creating a Simple Network Using Packet Tracer" activity

The screenshot shows the Cisco Packet Tracer interface. At the top, a navigation bar displays: Chapter 2 The User Interface > 2.1 Simulation Mode > 2.1.1 The Packet Tracer User Interface > 2.1.1.5 Packet Tracer - Creating a Simple Network Using Packet Tracer. The main area features a network diagram with various devices like switches, routers, and hosts connected to the Internet. A configuration window titled "Packet Tracer - Configuring a Zone-Based Firewall (ZPF)" is open, showing an "Addressing Table" with two entries:

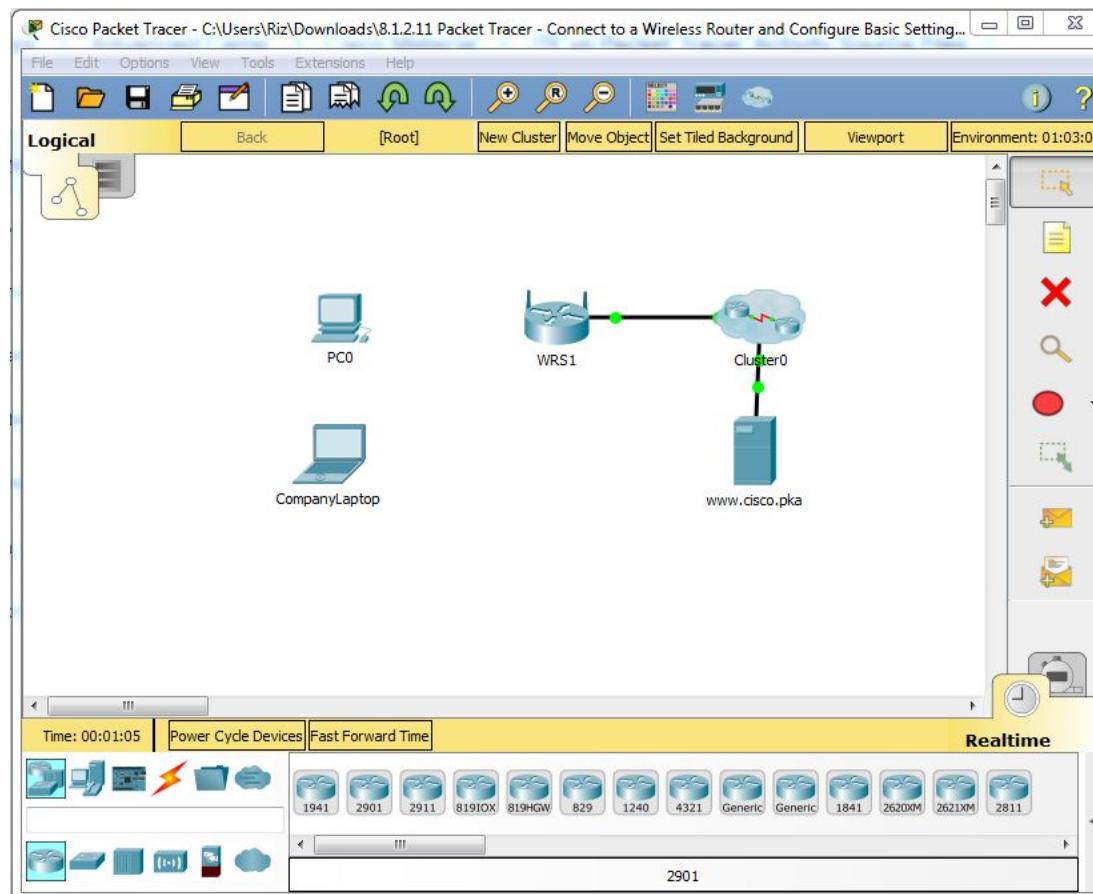
Device	Interface	IP Address	Subnet Mask	Def Gw
B1	Ethernet 0/1	192.168.1.1	255.255.255.0	N/A
B2	Ethernet 0/0	19.1.1.1	255.255.255.0	N/A

Below the main window, there's a workspace showing a detailed network setup in a house-like environment, and a background image of a globe with a network of connections. At the bottom right are standard navigation icons.

Activity: Configure Basic Wireless Settings

Packet Tracer - 8.1.2.11

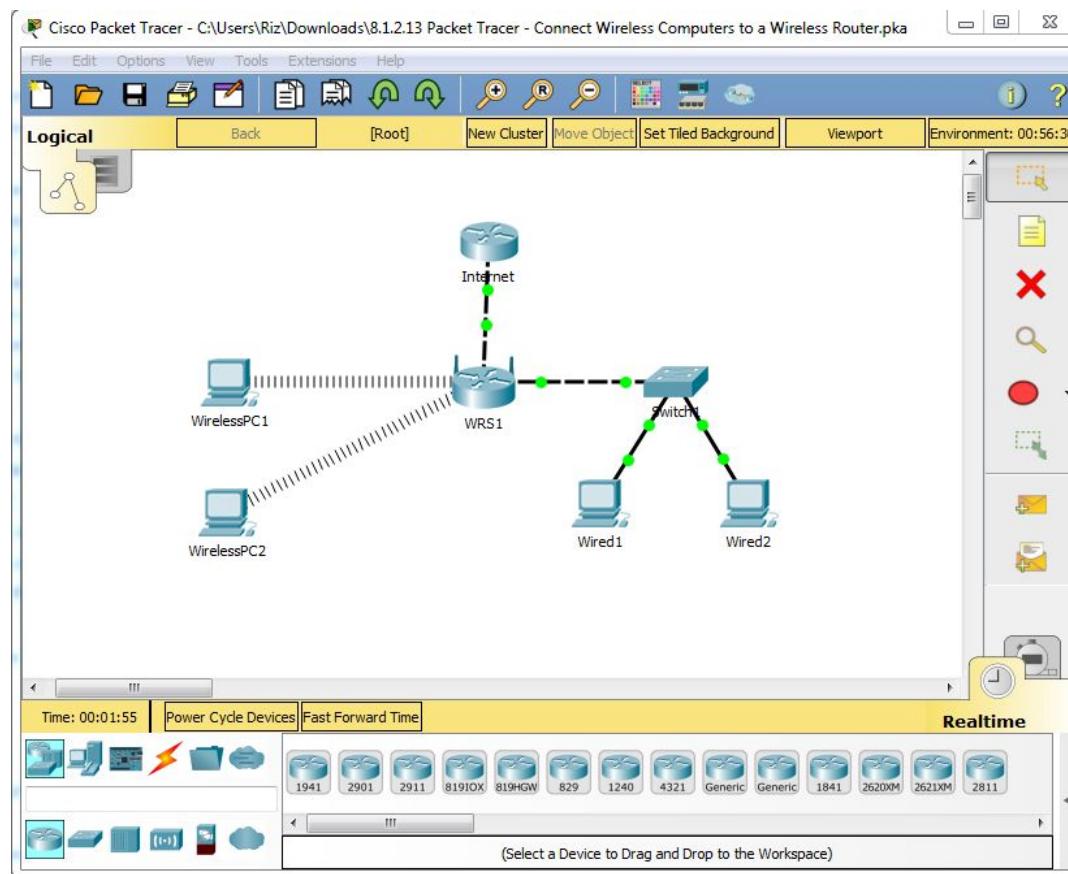
Configure Basic Home Wireless Router Settings



Activity: Connect Wireless Computers to a Router

Packet Tracer - 8.1.2.13

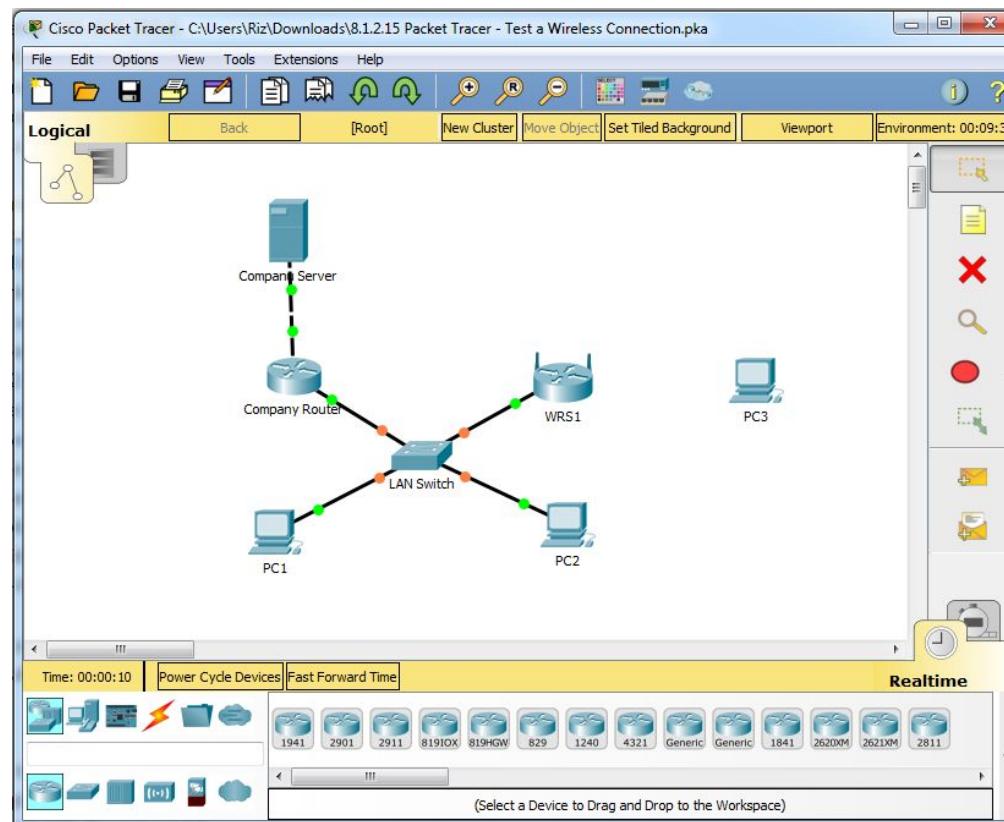
More Advanced Home Wireless Router Configuration



Activity: Troubleshoot a Wireless Connection

Packet Tracer - 8.1.2.15

Troubleshoot Wireless Connectivity



Intro Cybercamp

Digital Forensics &
Networking

