Intro Cybercamp

BACCC
BAY AREA
COMMUNITY COLLEGE CONSORTIUM

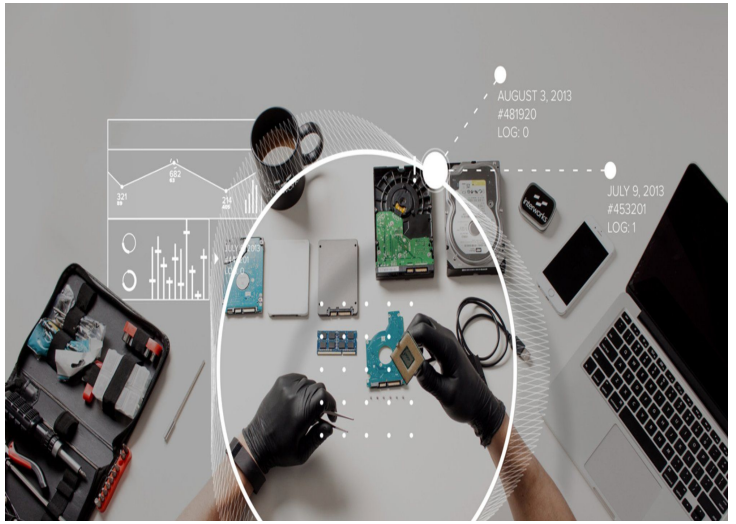
SUMMER CAMP


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



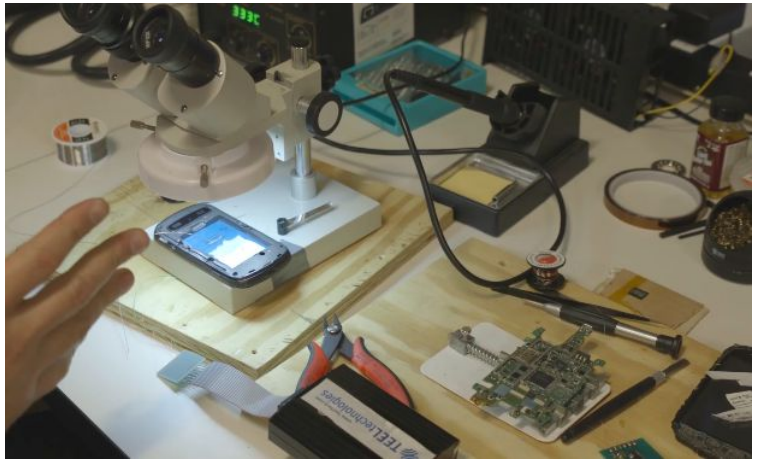
The experts who do digital forensics are often called "analysts" or "investigators".

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.

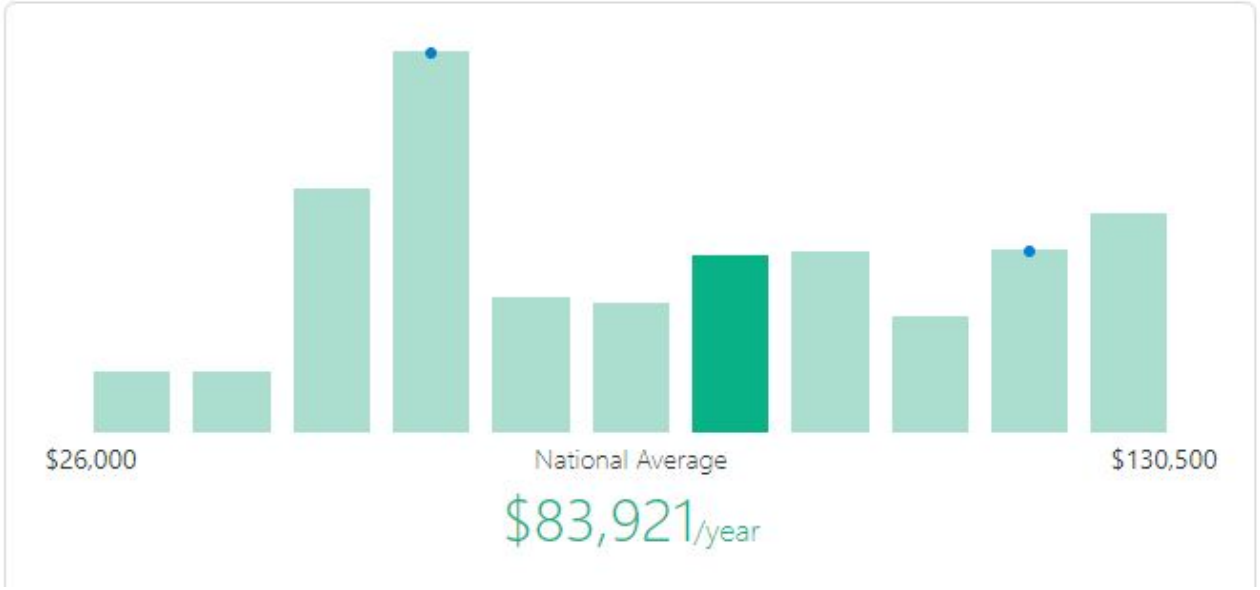
Careers in Digital Forensics

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?

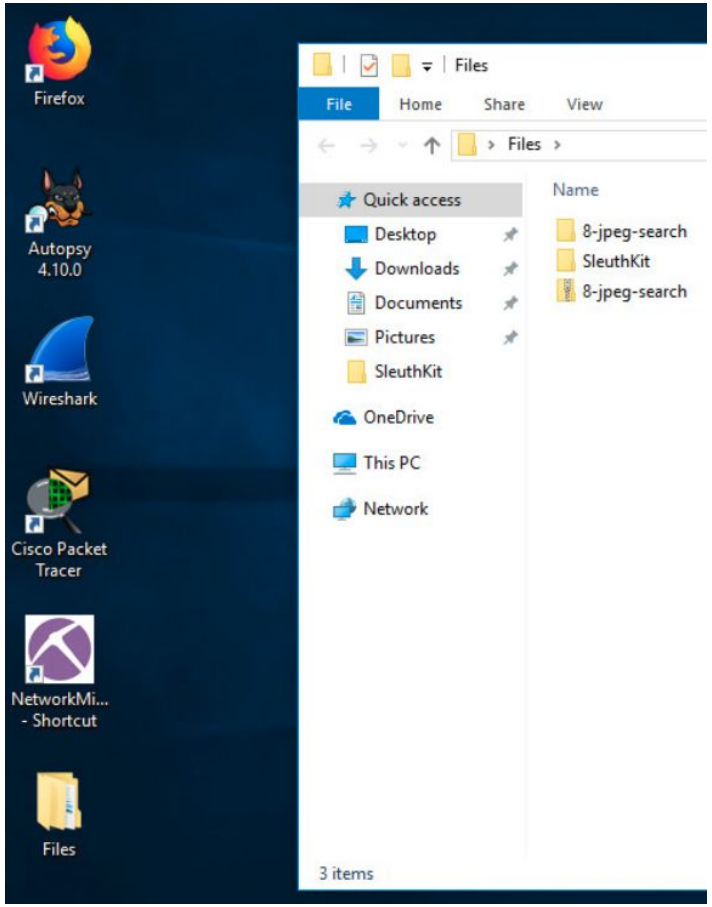
- A Digital forensics tool
- Used by law enforcement, military, and corporate examiners to investigate what happened on a computer.

What is Autopsy?

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

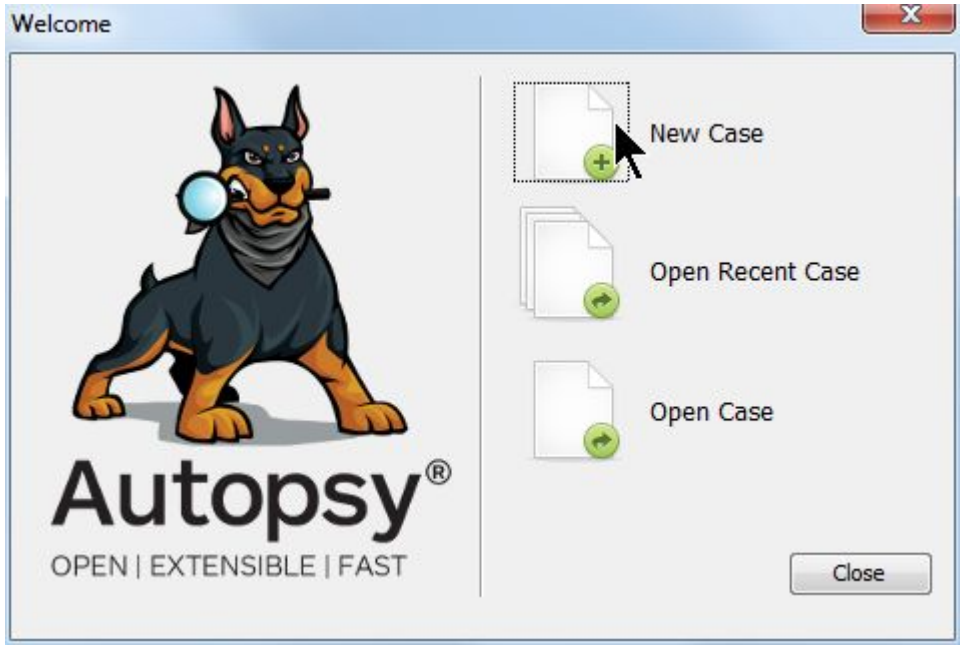
Image Files to Use in Autopsy

Files are located on the Desktop



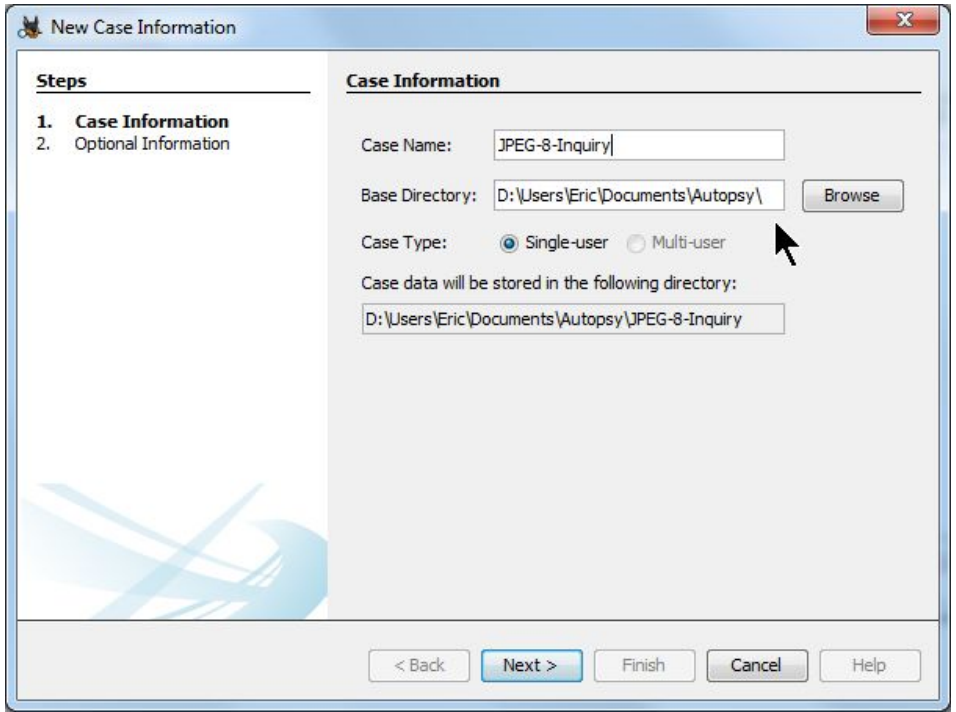
Create a Case

- Launch Autopsy
- Click **New Case**



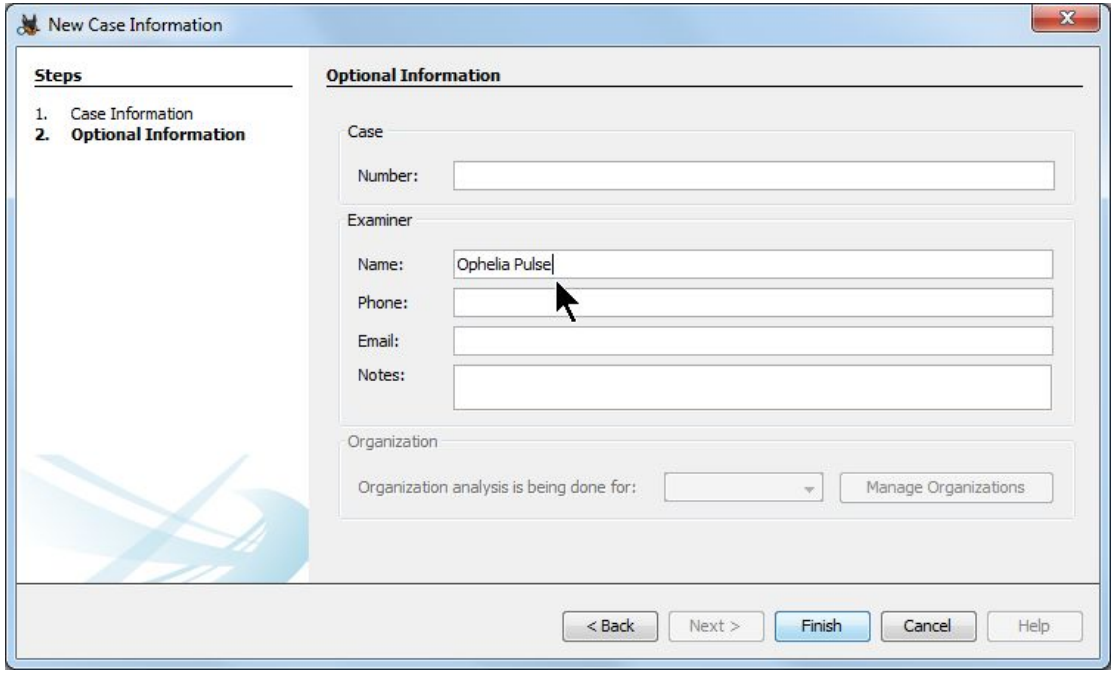
Enter Case Name & Base Directory Folder

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



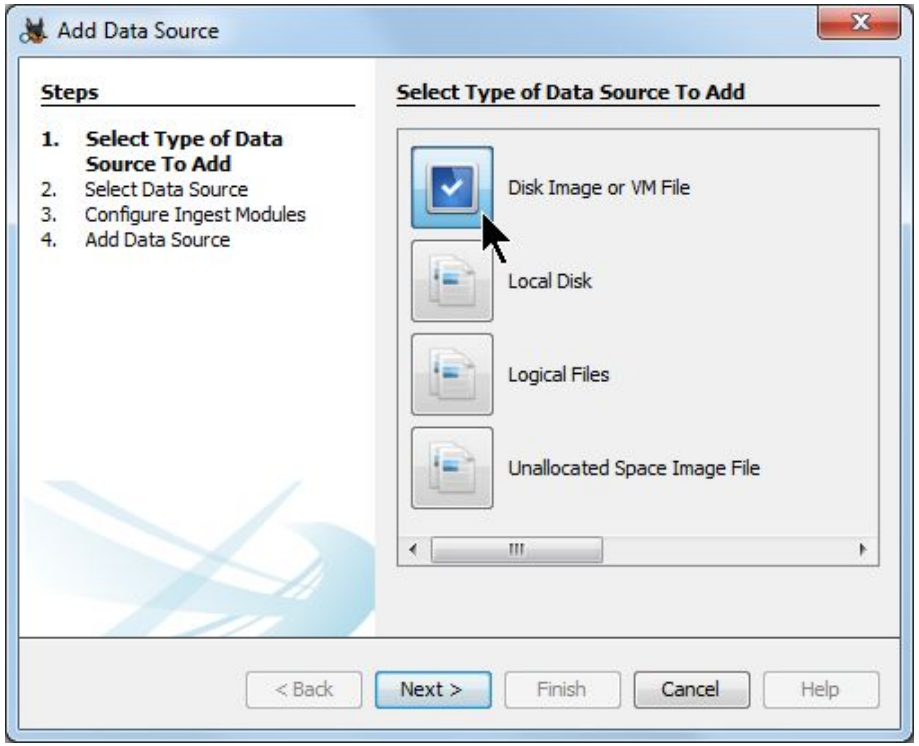
Enter your name

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



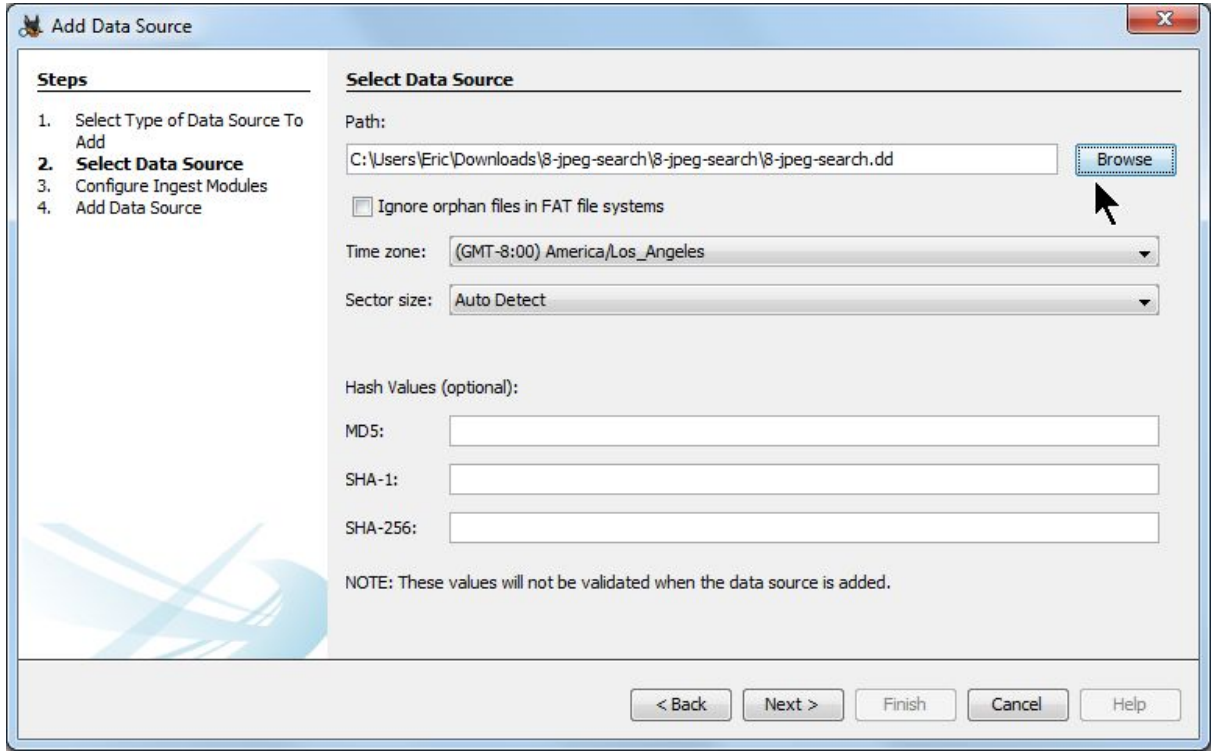
Add a Data Source

- 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**



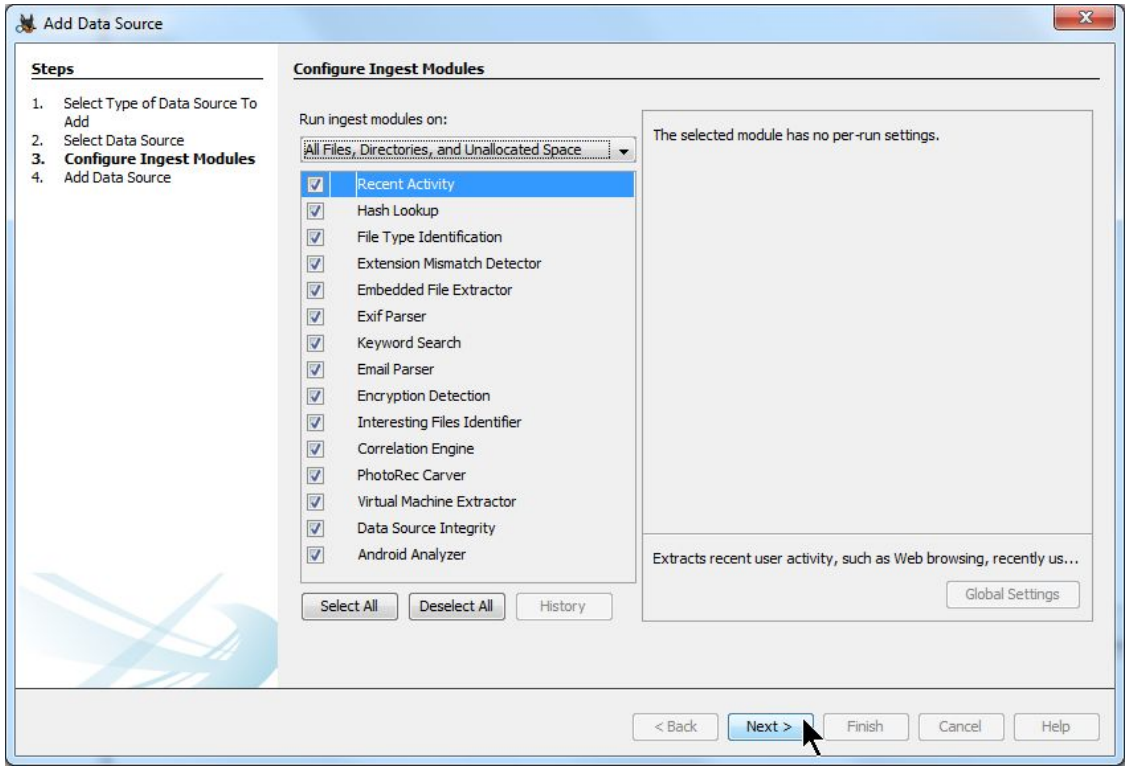
Select the Drive Image

- 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**



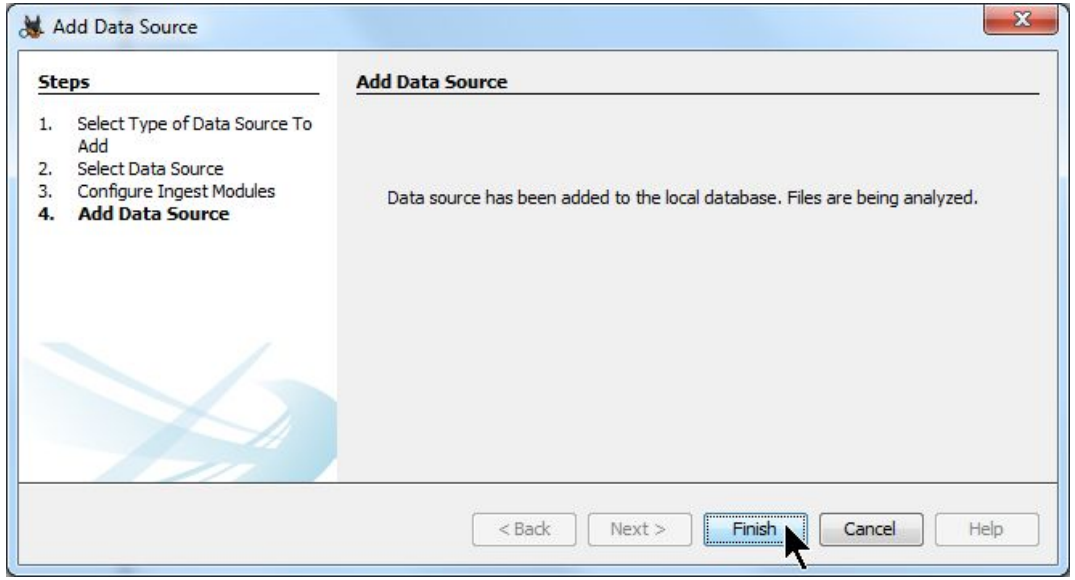
Select Ingest Modules

- 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.



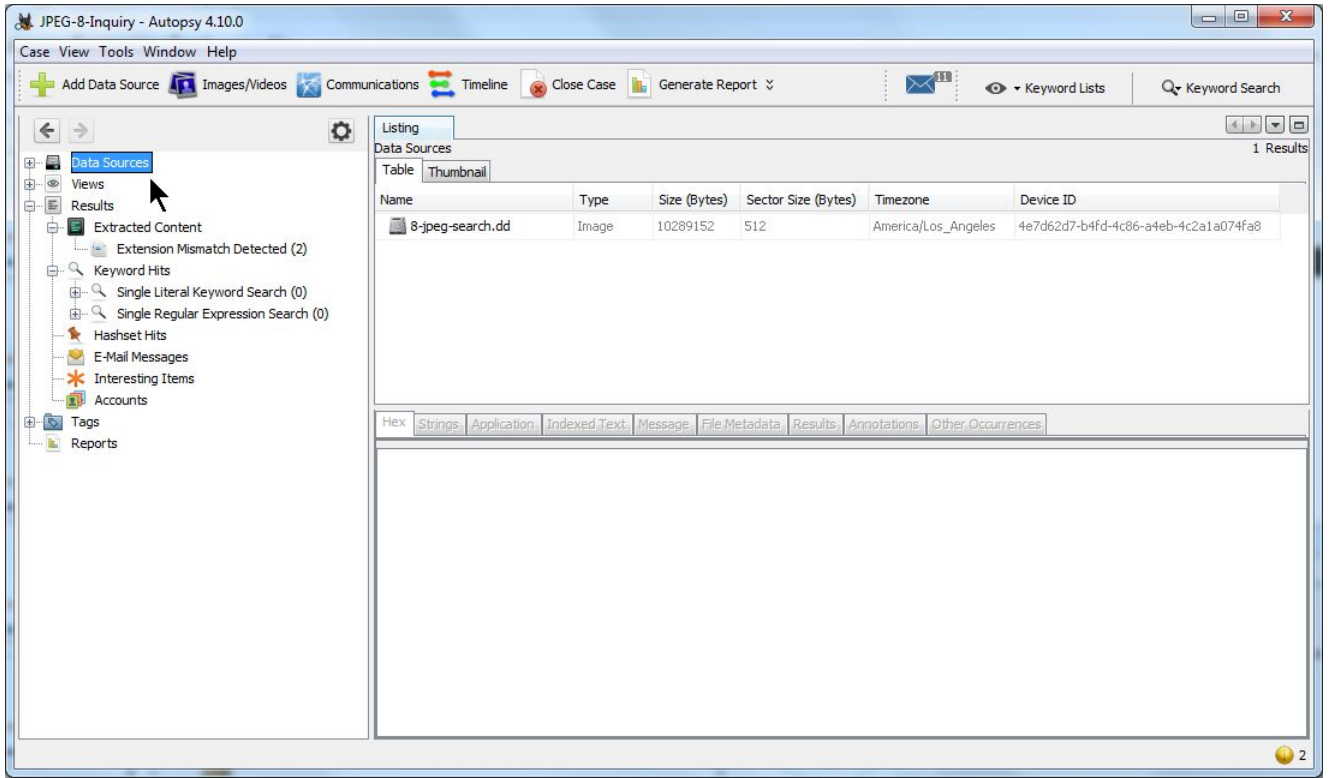
Finish Data Source

- Click **Finish**



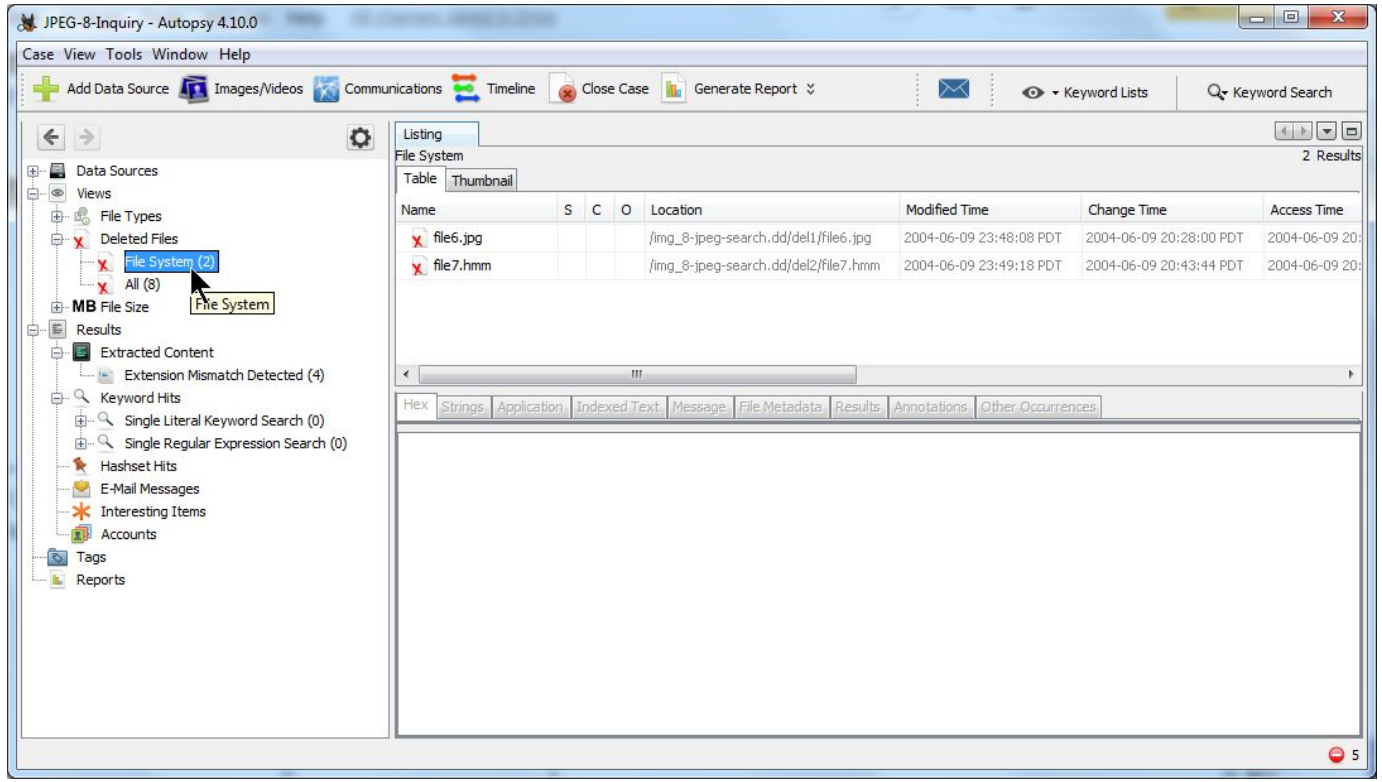
Autopsy Workspace

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



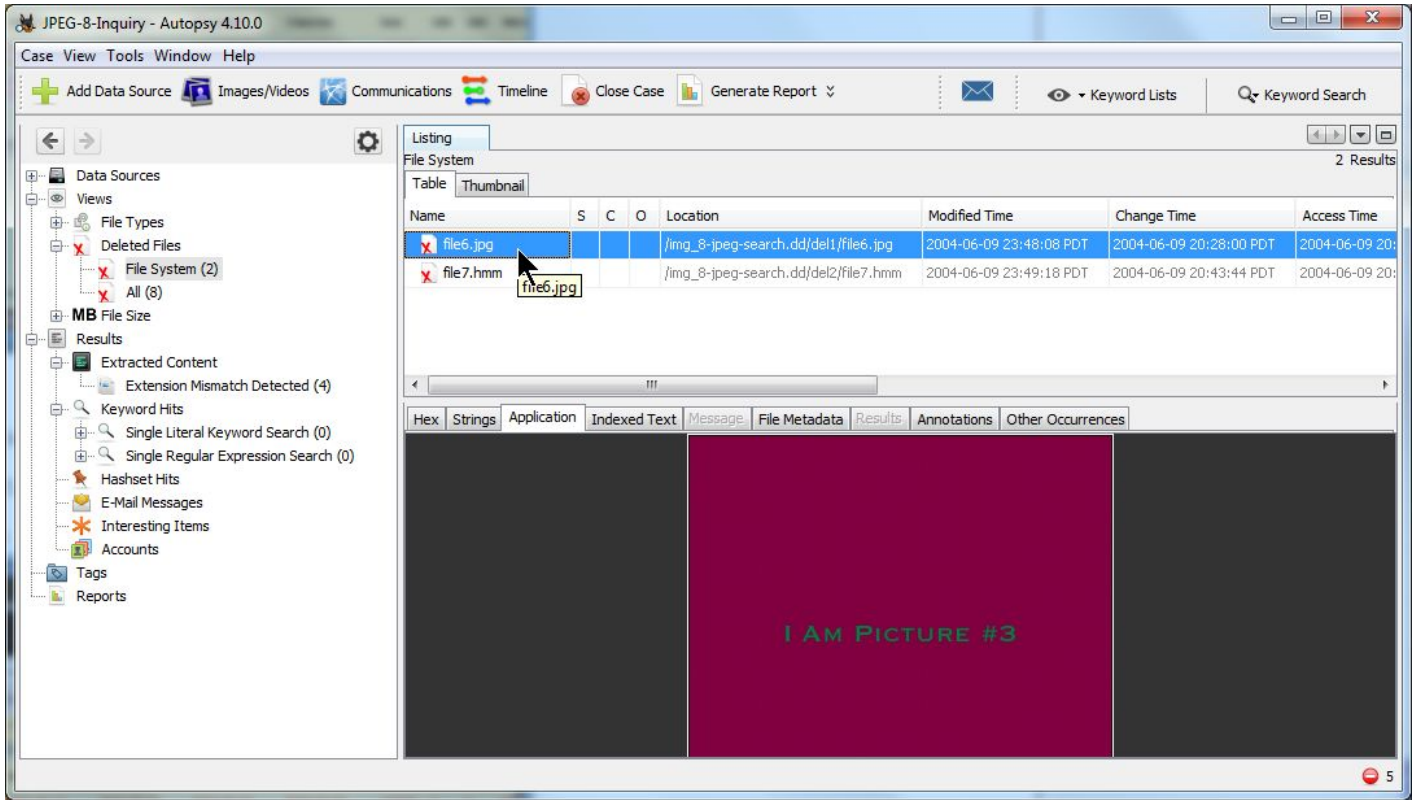
Show Deleted Files

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



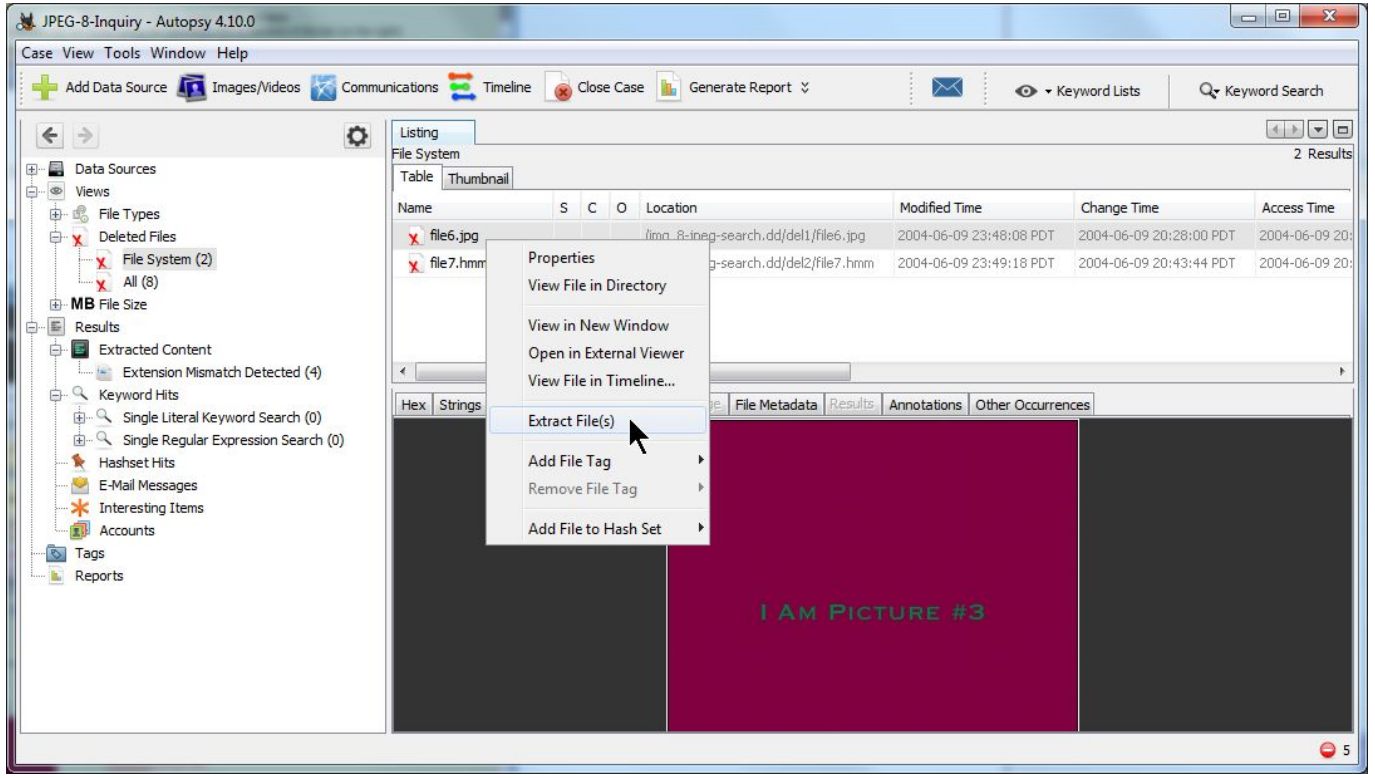
Preview Deleted File

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



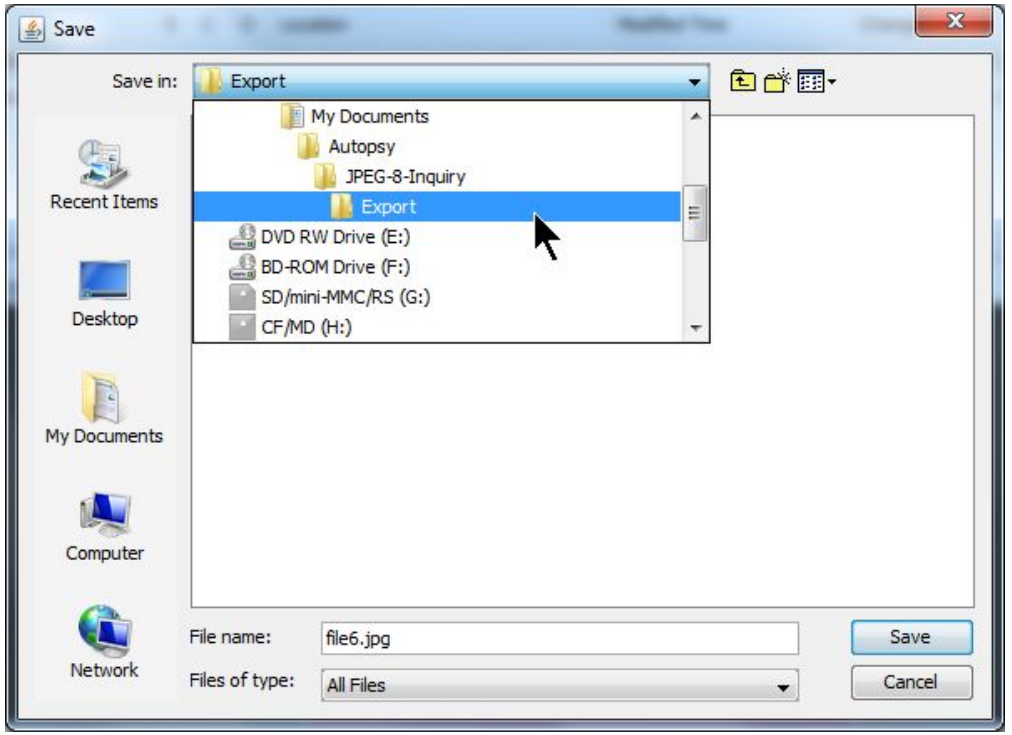
Extract (Export) a File

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



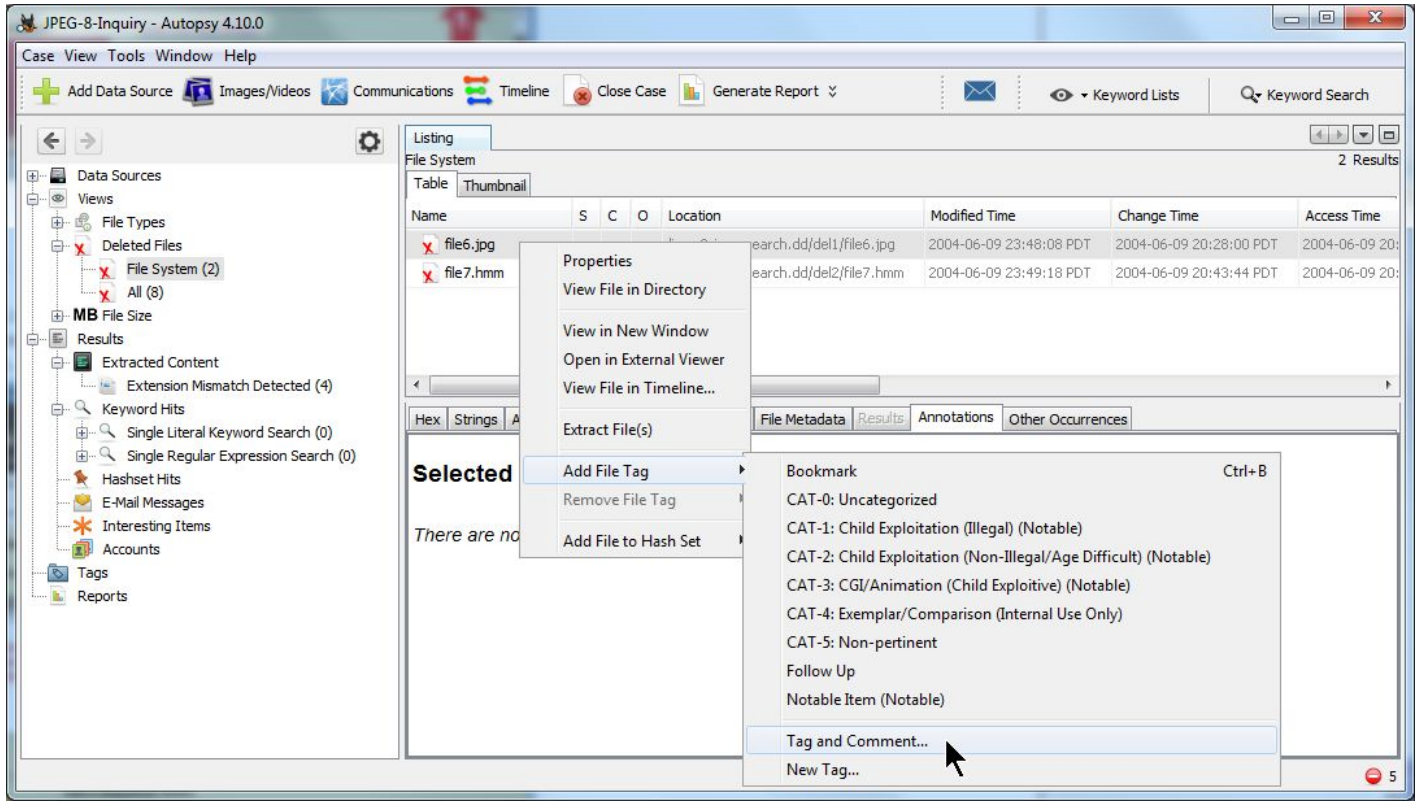
Save the Exported File

- 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.



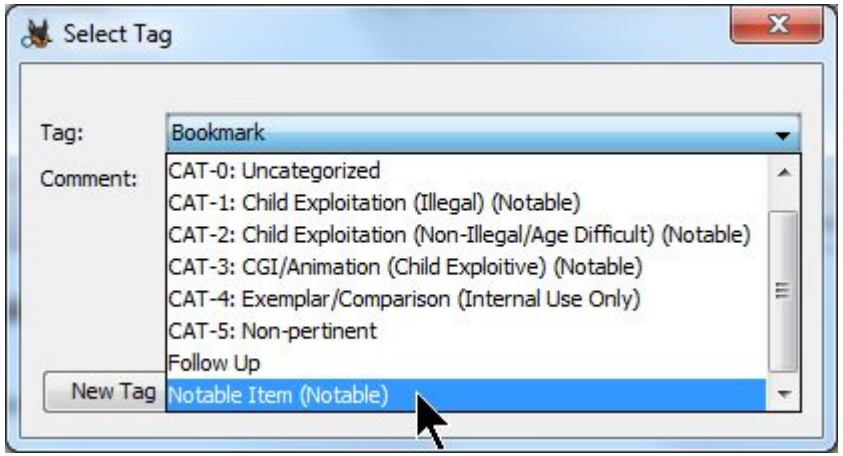
Add a Note

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



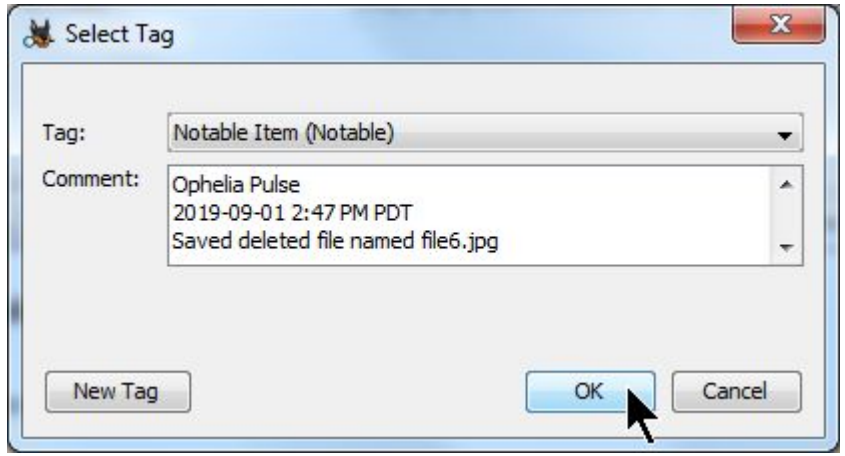
Tag Category

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



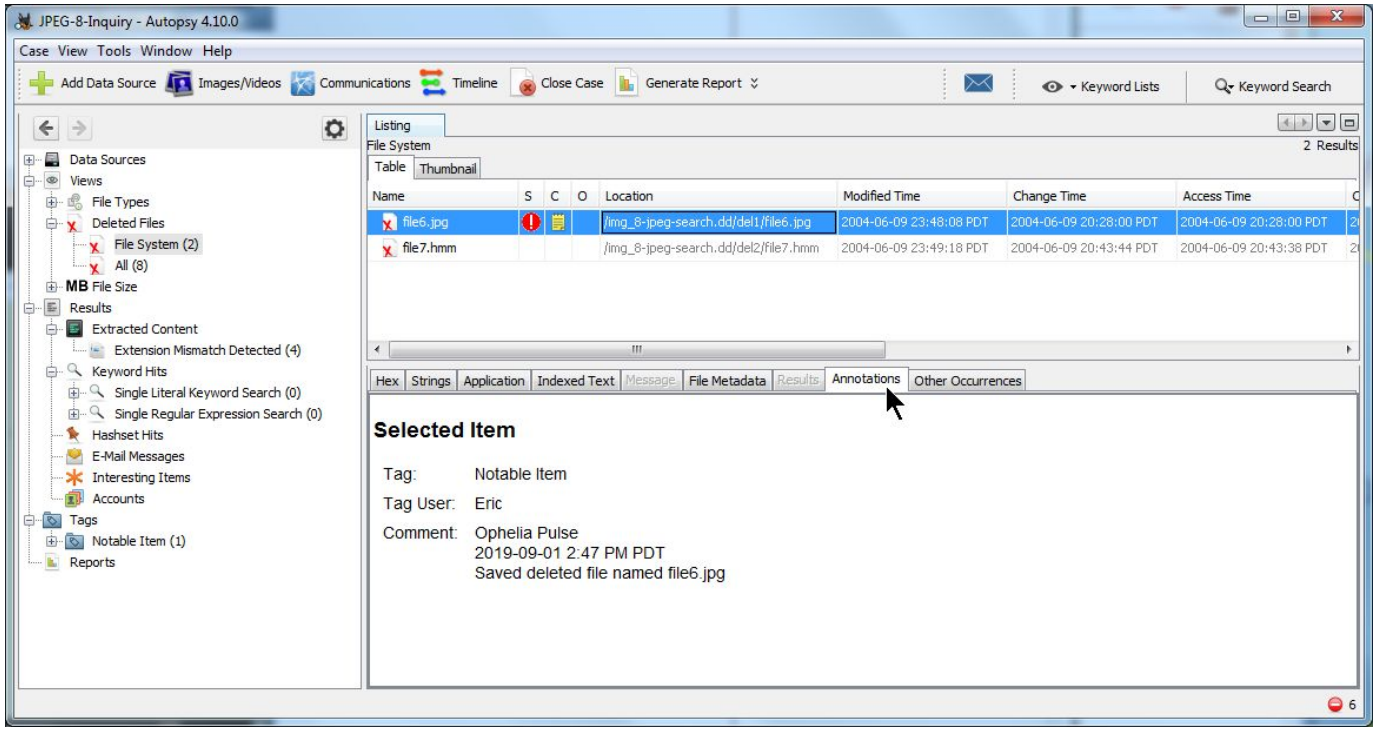
Write a Comment

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



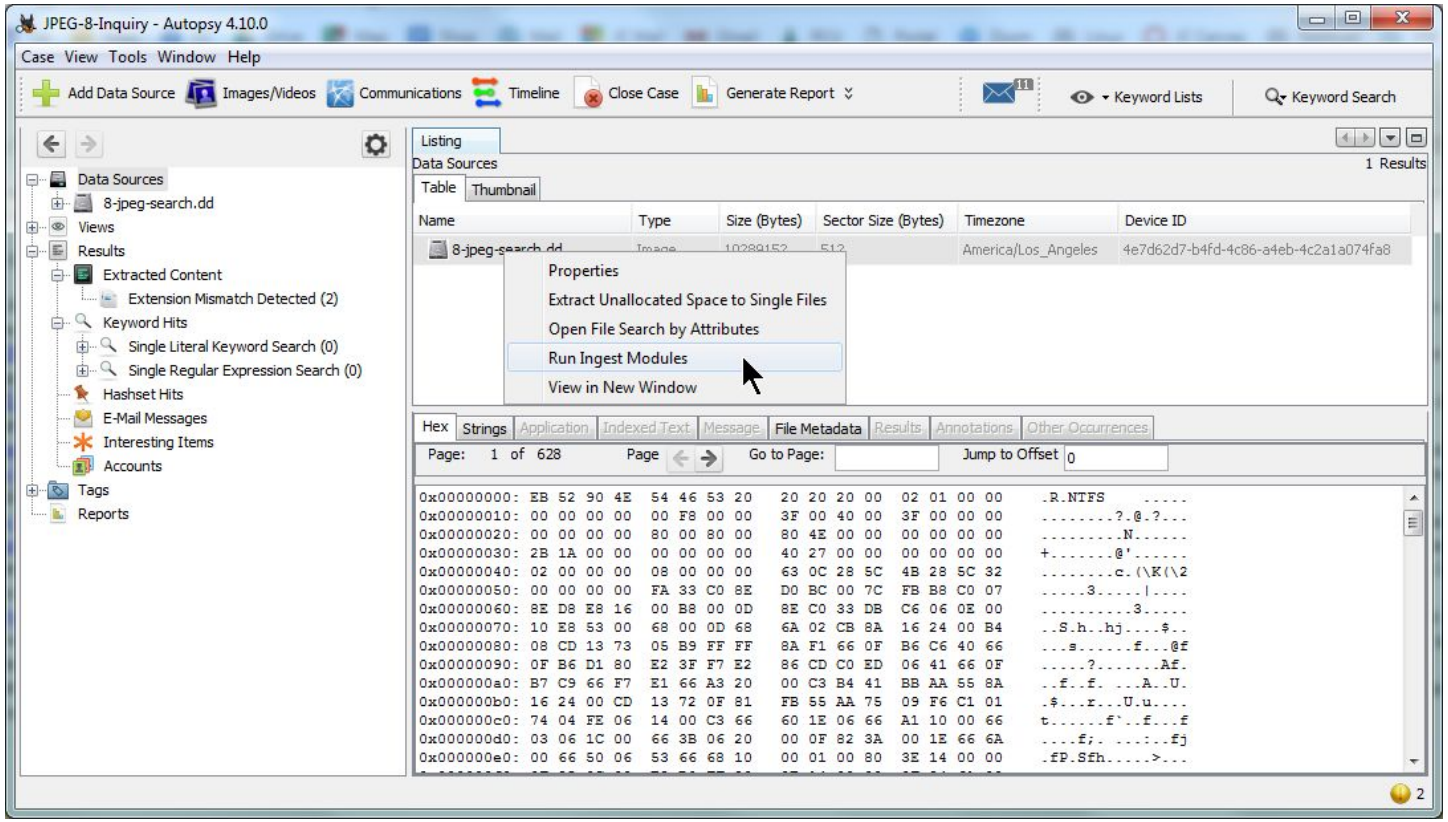
View Tag Information

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



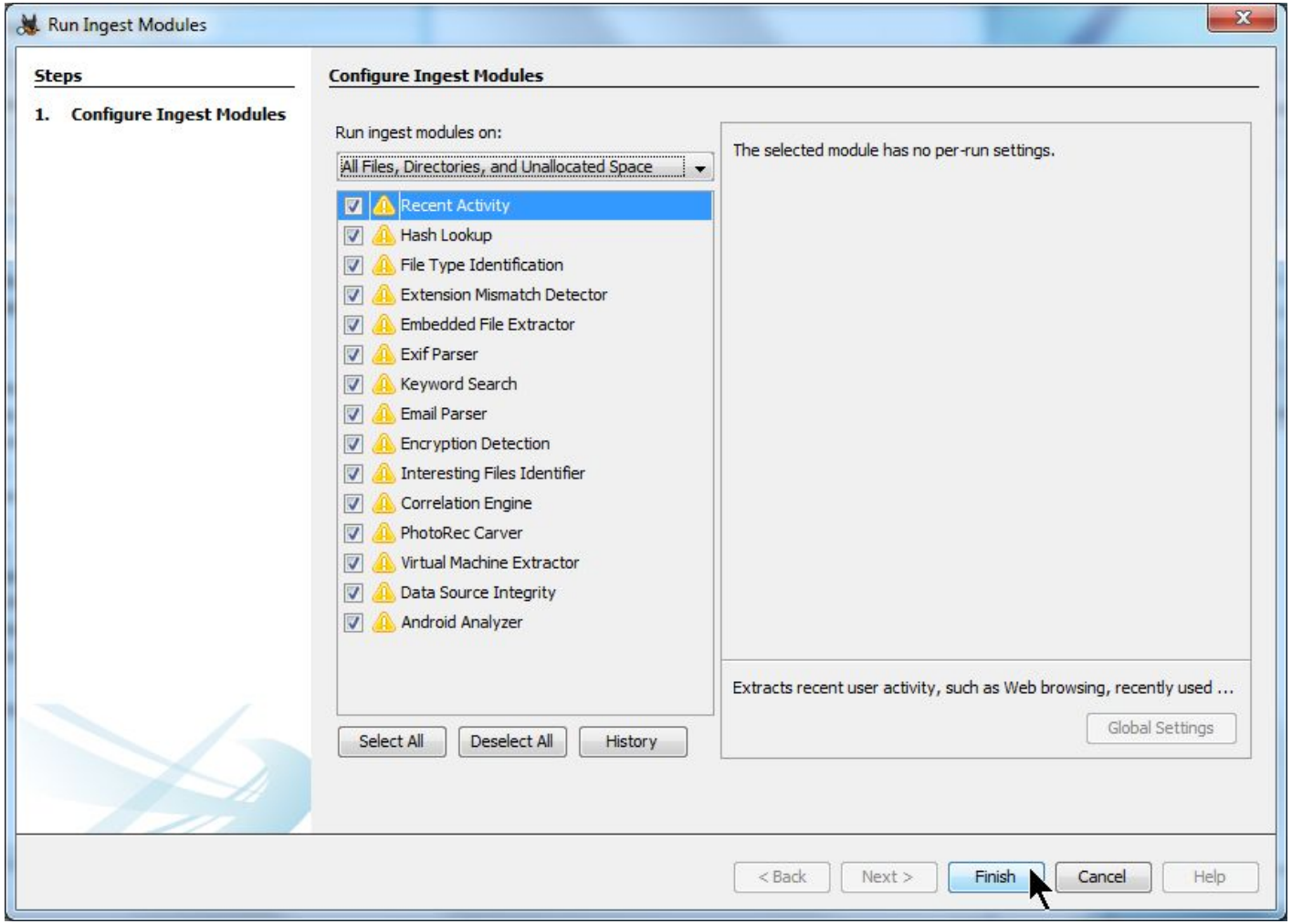
Checking Drive Image Integrity: Run Ingest Modules Again

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



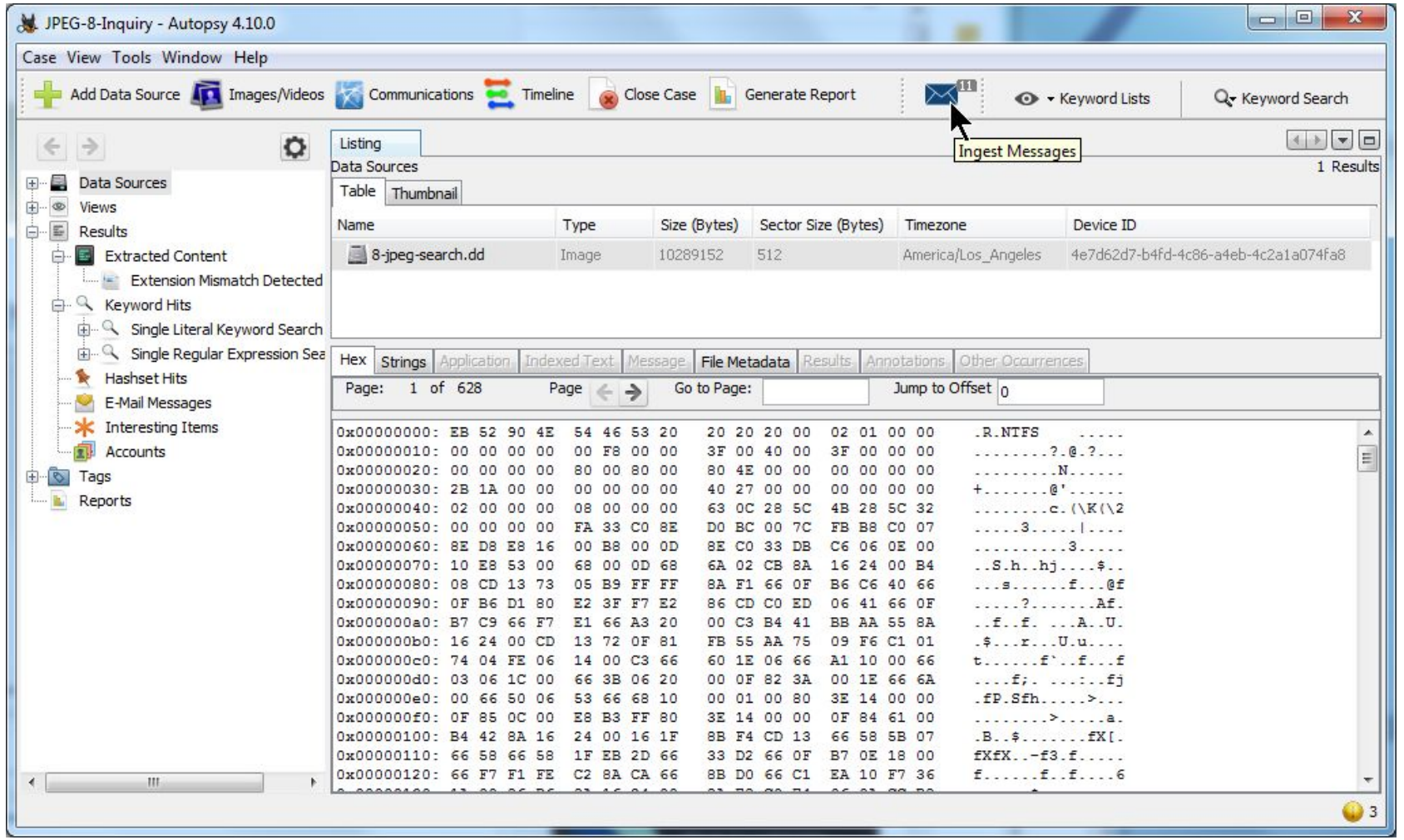
Run Ingest Modules

- Click **Finish** to run all Ingest Modules



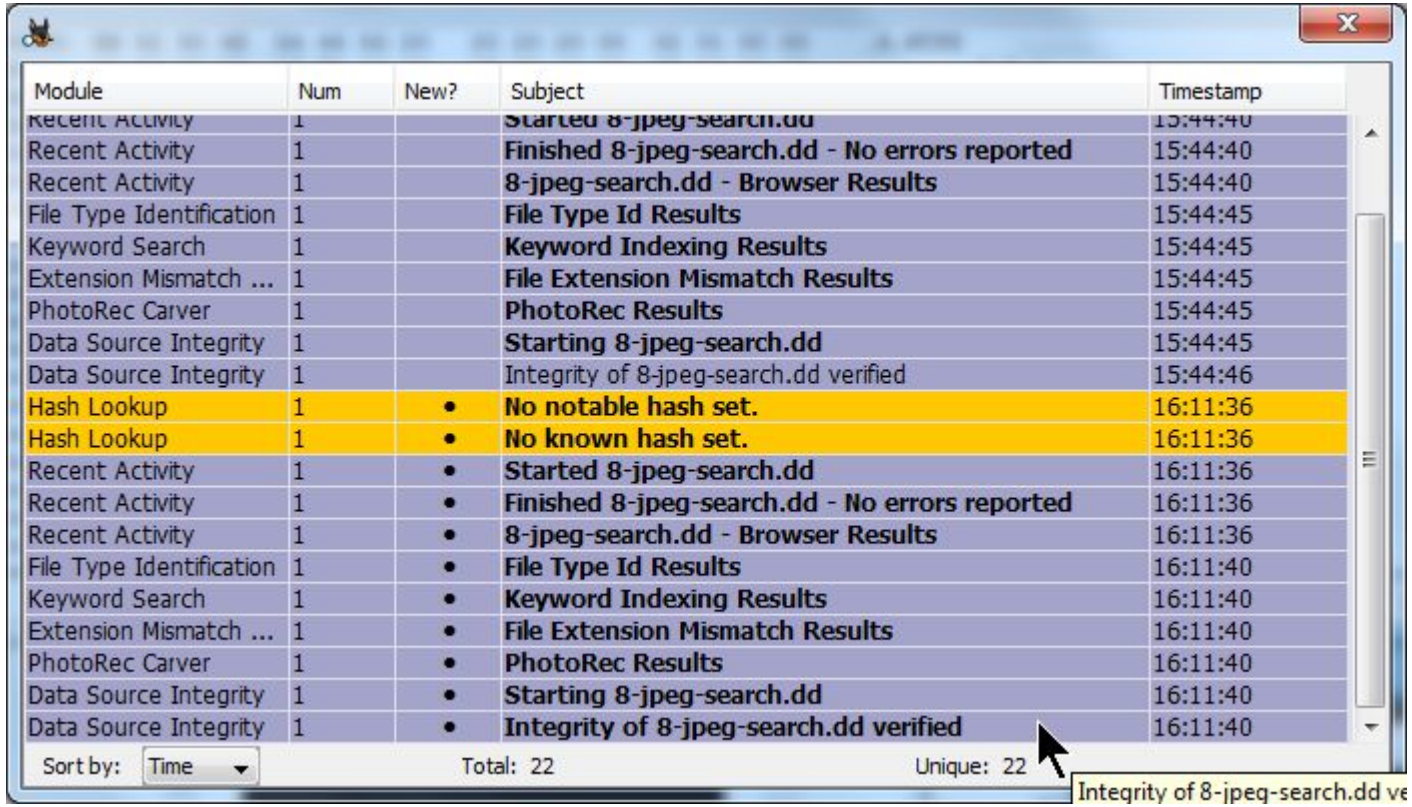
Open Ingest Messages

- Click the blue envelope to open Ingest Messages



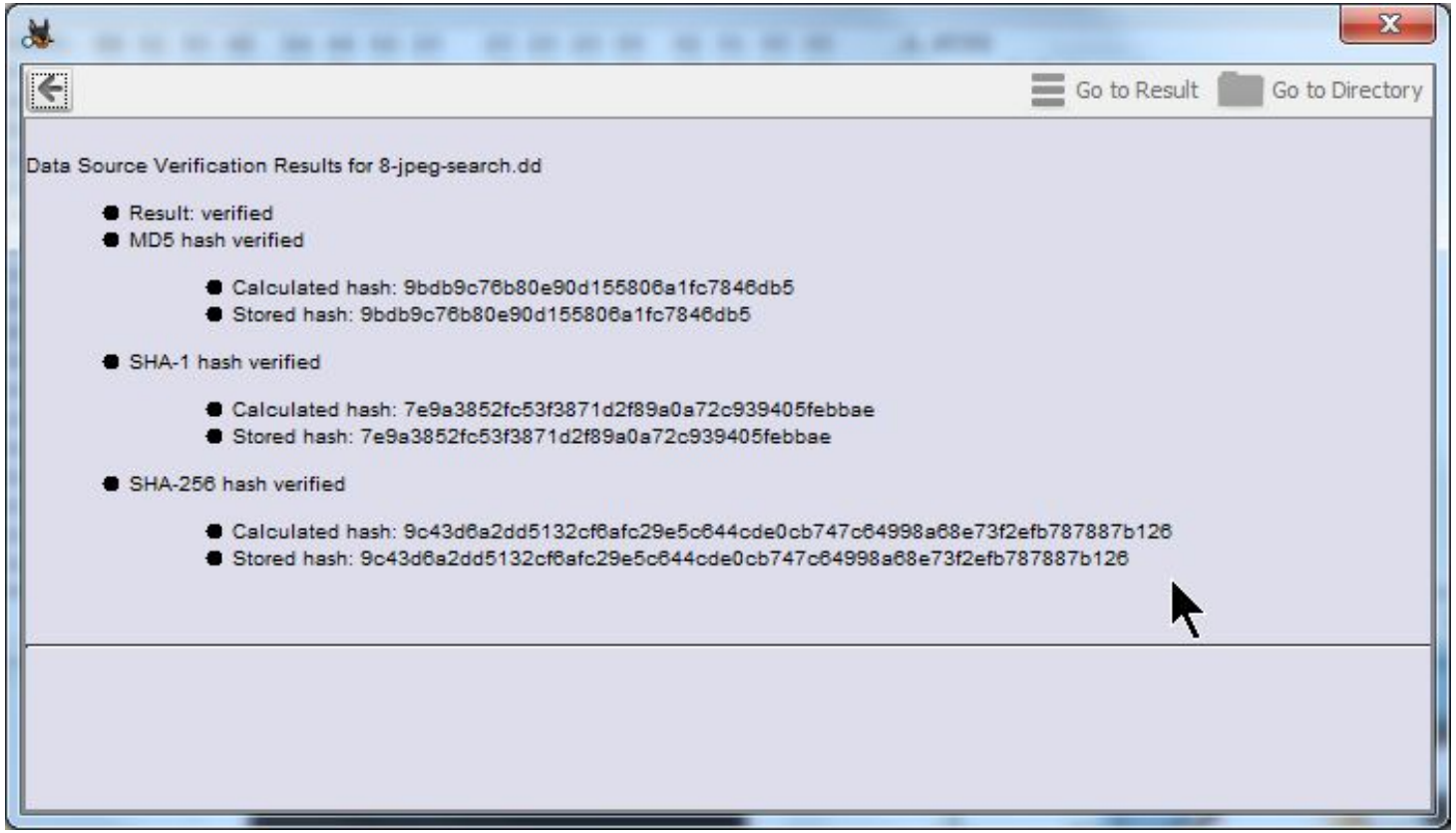
Open Image Integrity Message

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

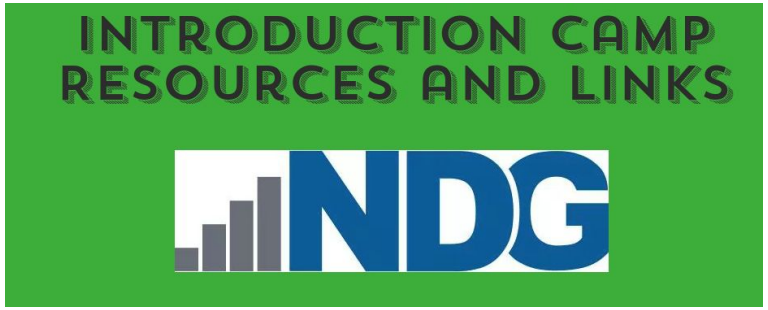


Open Image Integrity Message

- 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

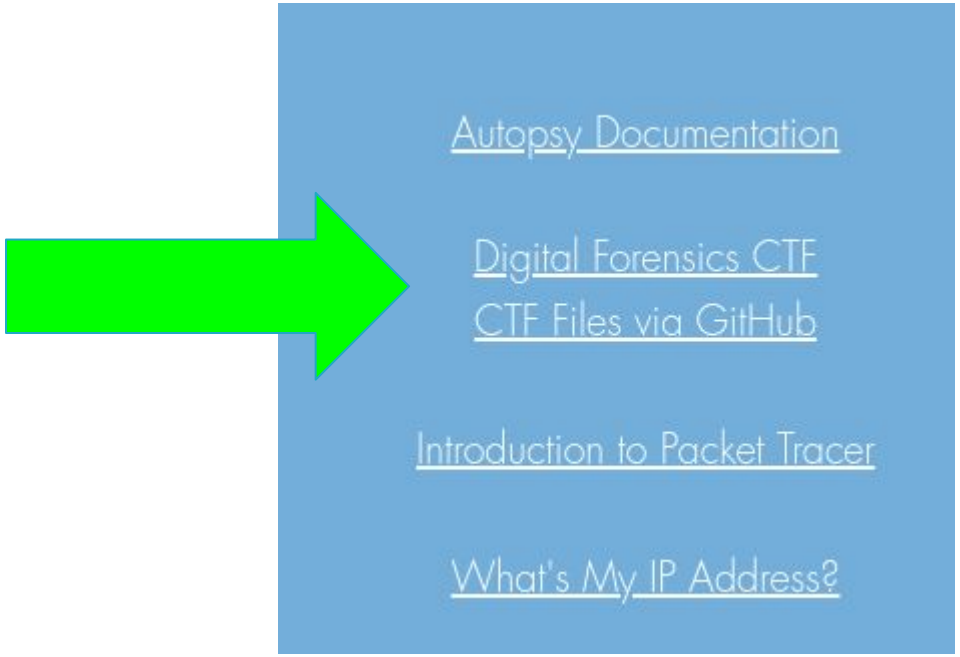


1. Log in to Netlab baycyber.net/intro
2. Click on the large “NDG” logo to access Netlab
3. Create a **Team Reservation** for **Cyber_Camp_2019_Forensic Access**

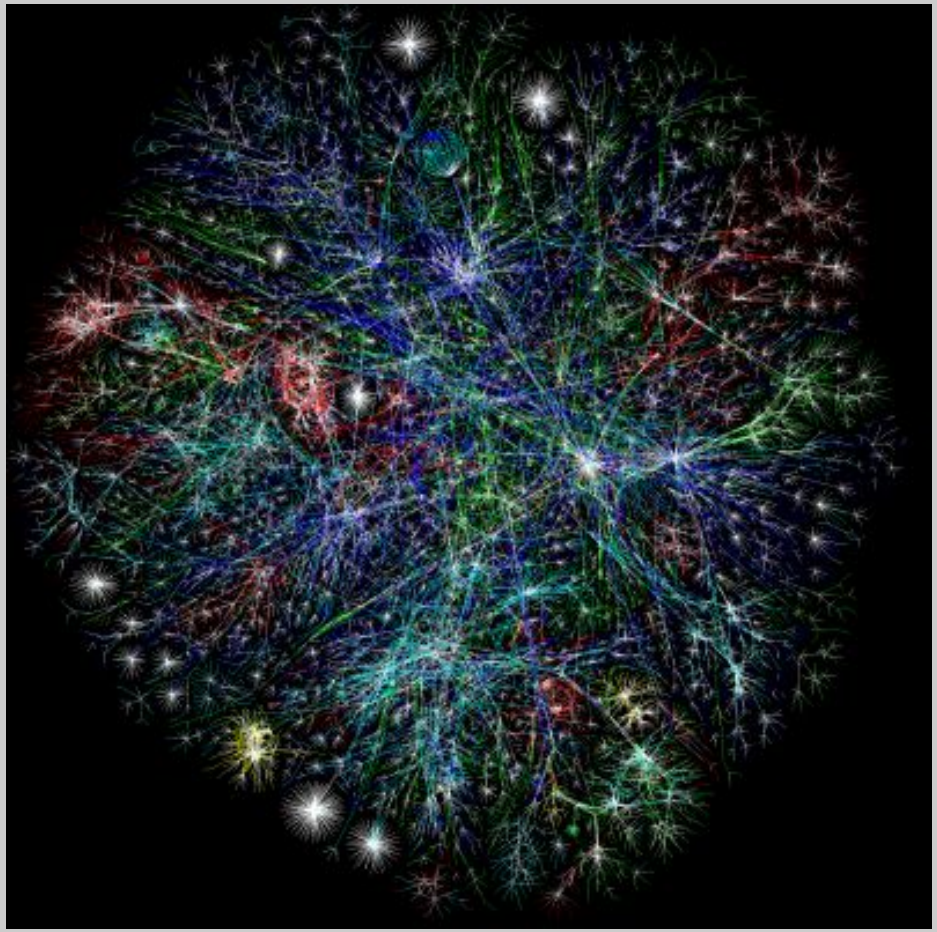
   (same Netlab as tomorrow’s Wireshark exercise)
4. Use the Autopsy reference guide

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

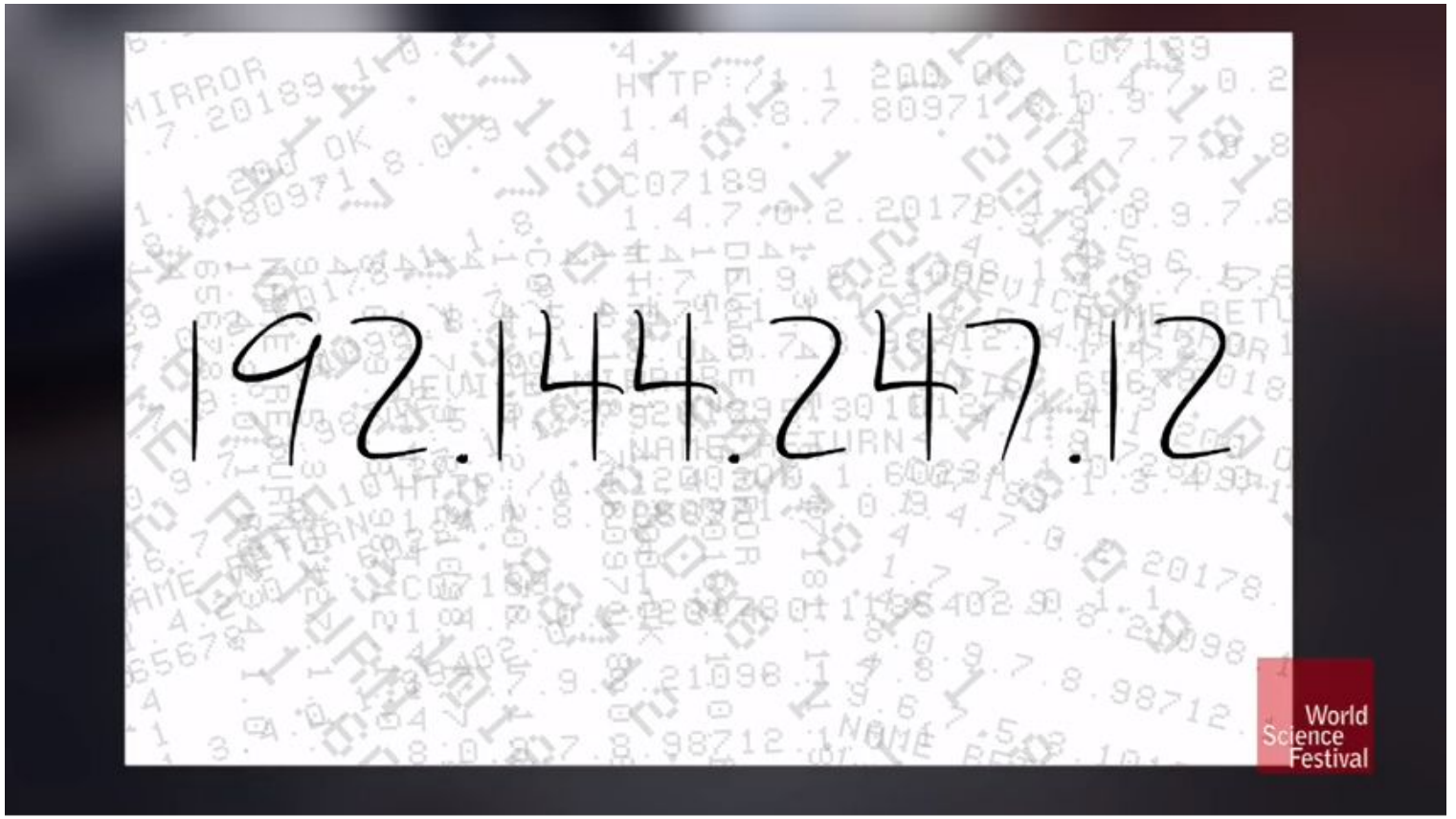


Networking & The Internet



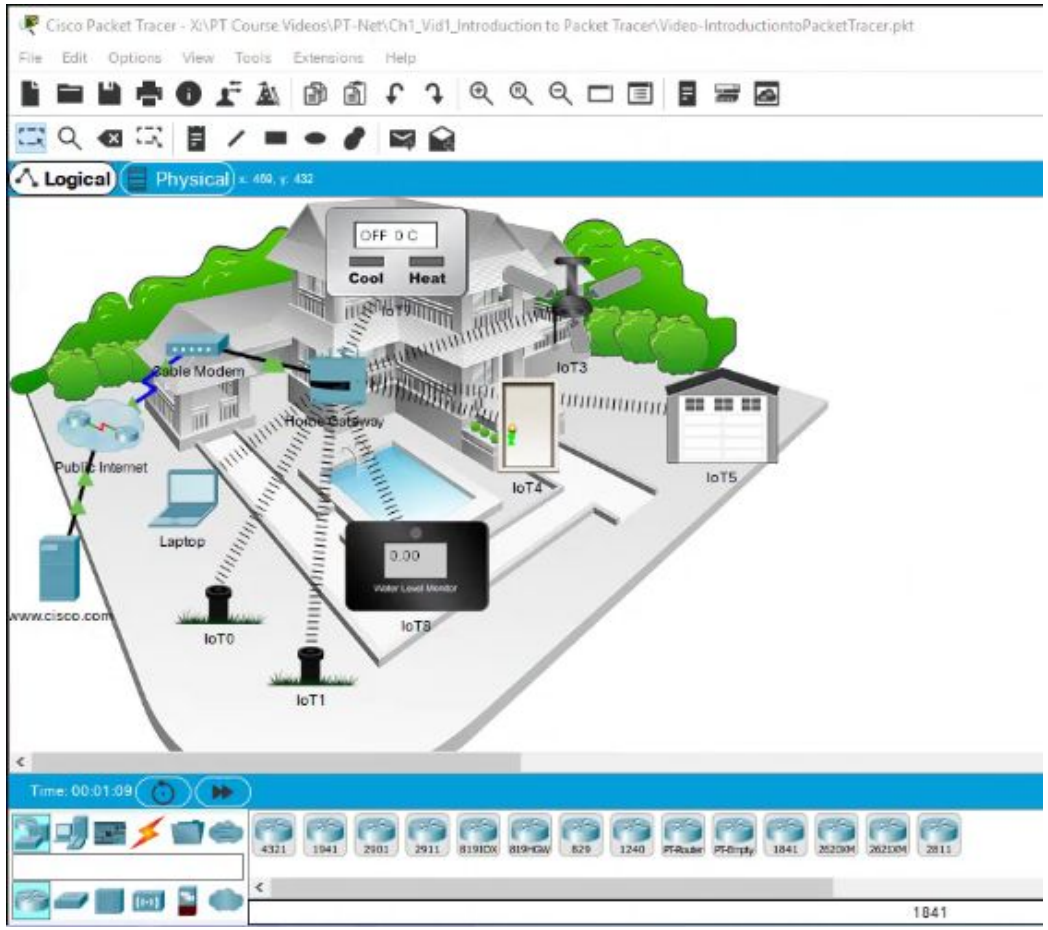
How Does the Internet Work?

Video: Internet Overview



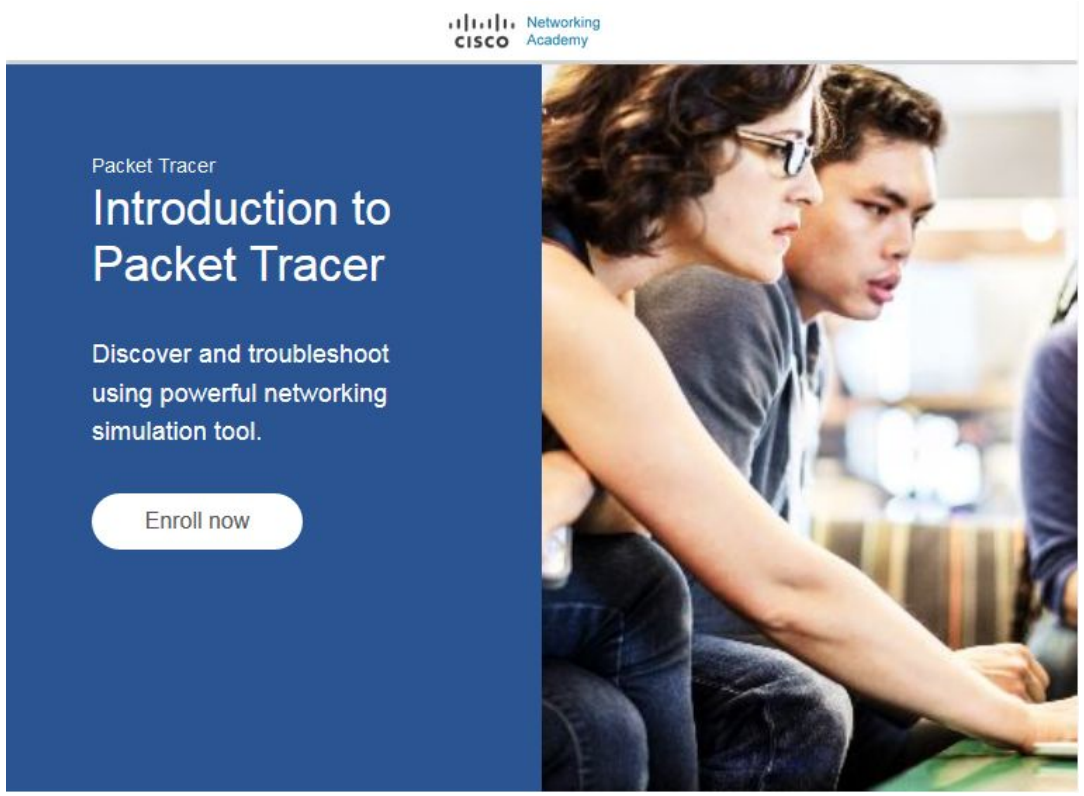
What is Packet Tracer?

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

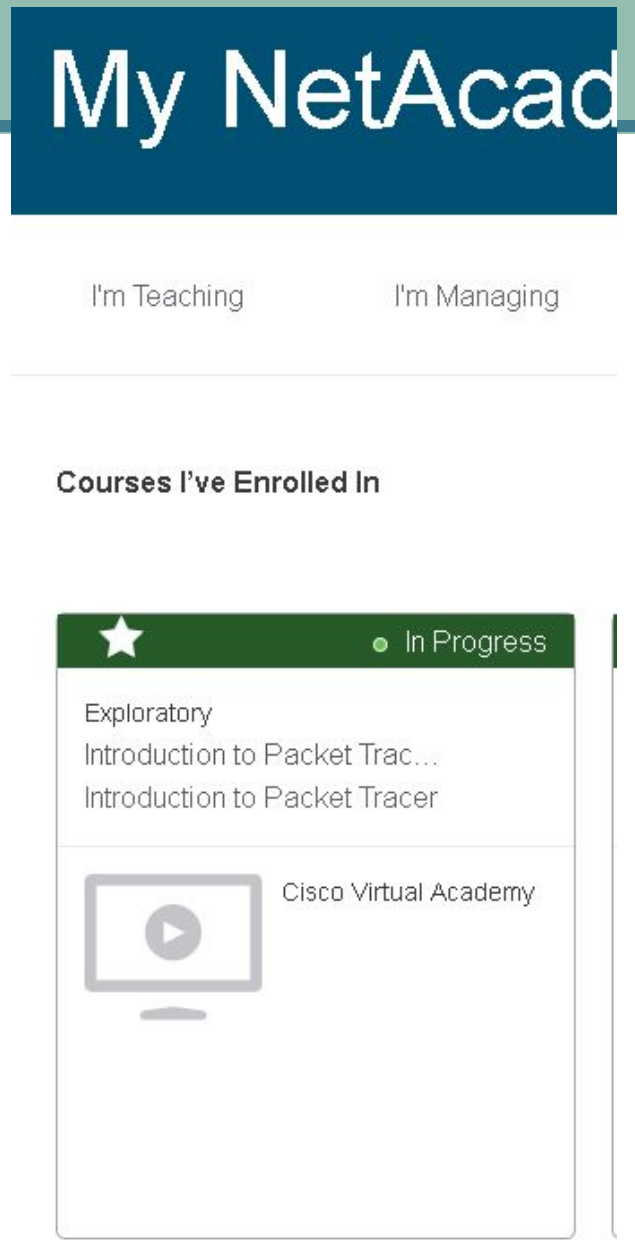


Packet Tracer Online Course

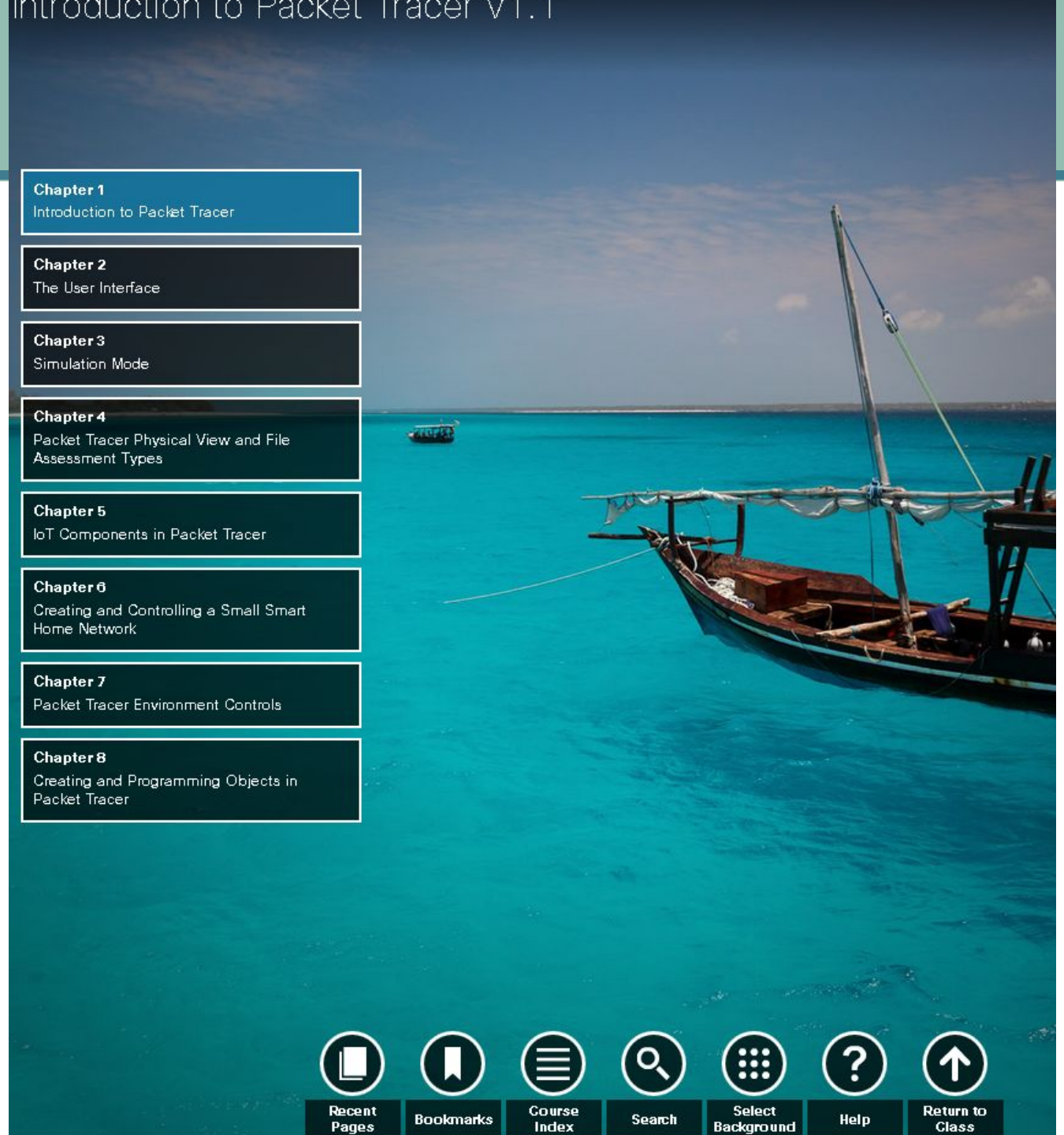
Enroll or sign in here:



Networking using Packet Tracer




My NetAcad
Account
Dashboard
Courses
Calendar
Inbox
Home
Modules
Discussions
Grades
Assignments
Quizzes
Introduction to Packet Tracer 0419 g
If this is your first time in the course, click here for more information.
Introduction to Packet Tracer
Launch Course
Student Resources



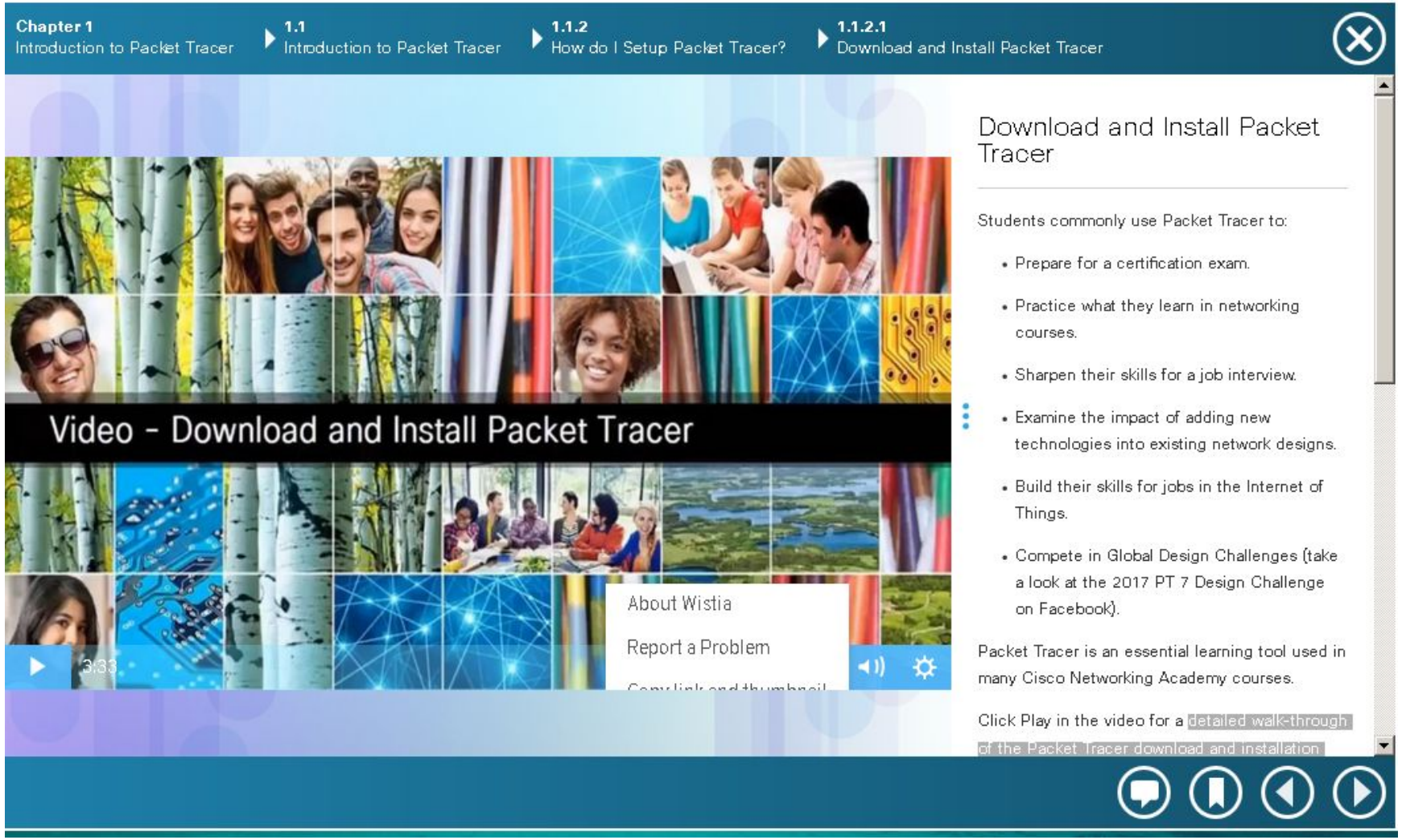
Chapter 1

Overview of Packet Tracer

Video to Overview

Download and Install Packet Tracer

How to install Packet Tracer for home use

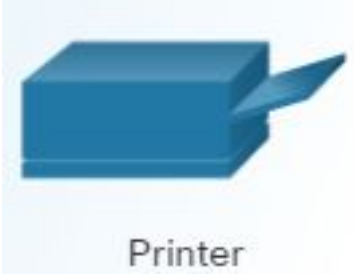


Host Devices

Host: Any Kind of computer that uses the network. Also called "**End Devices**"

"**Client**" and "**Server**" are jobs that a host can have.

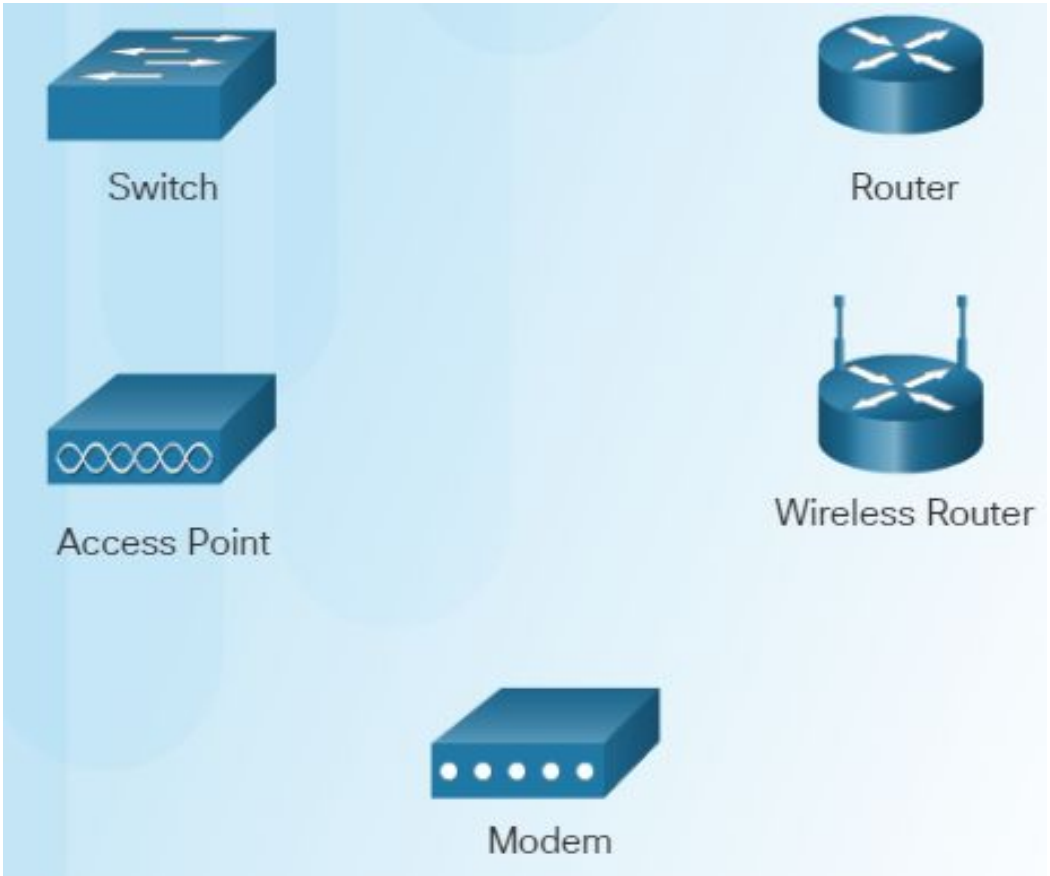
- **Clients** are devices that ask for content.
- **Servers** are devices that provide content



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 (**mo**dulates & **dem**odulates) outside cable or DSL.
- **Router** – Connects Internet with inside network.
- **Switch** – A set Ethernet ports to make a wired **LAN** (**L**ocal **A**rea **N**etwork).
- **Wifi: wireless access point (WAP)** as part of the LAN

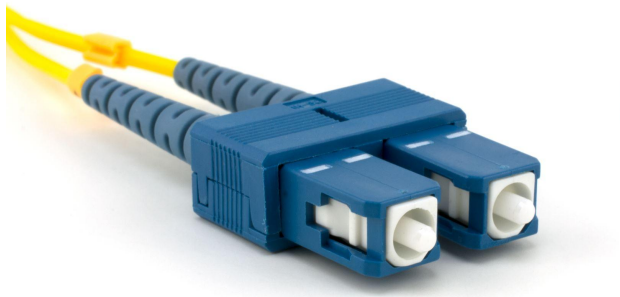
Network Media

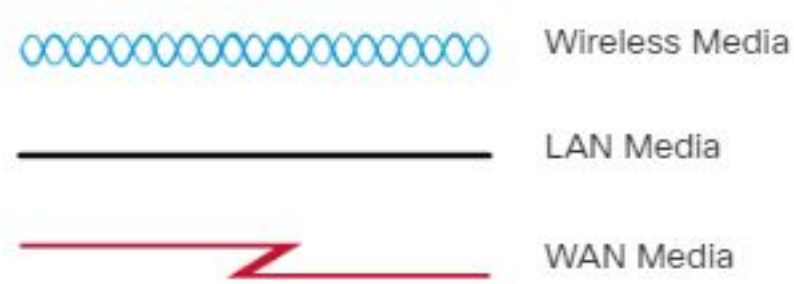
Network Media: Provides the channel over which the message travels from source to destination. The actual path that data, as electrical signals, travels between devices.

Example: Wireless, Optical, Copper

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

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



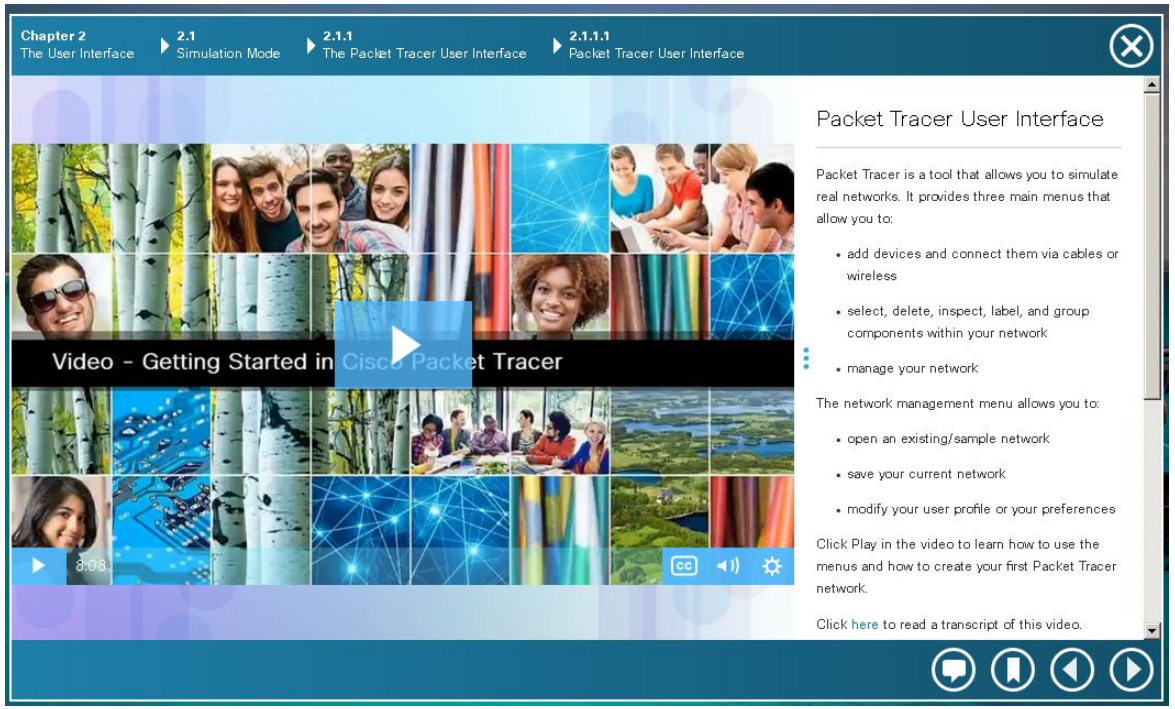


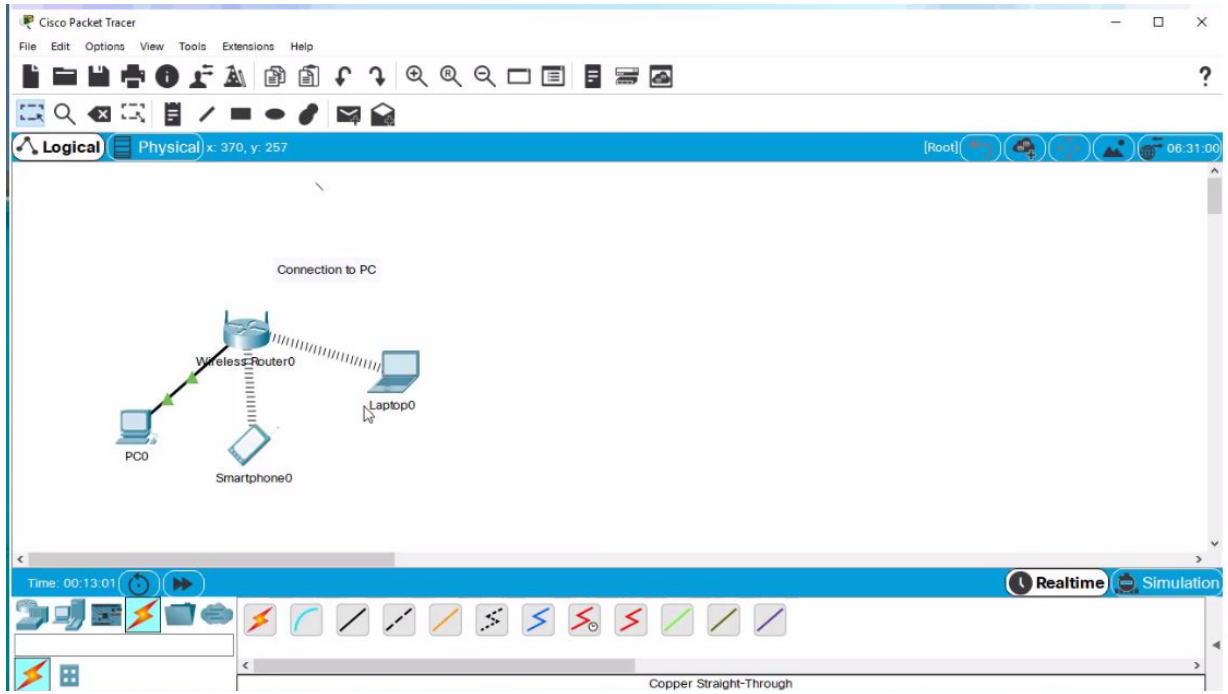
Introduction to Packet Tracer v1.1

Networking Academy

Packet Tracer User Interface

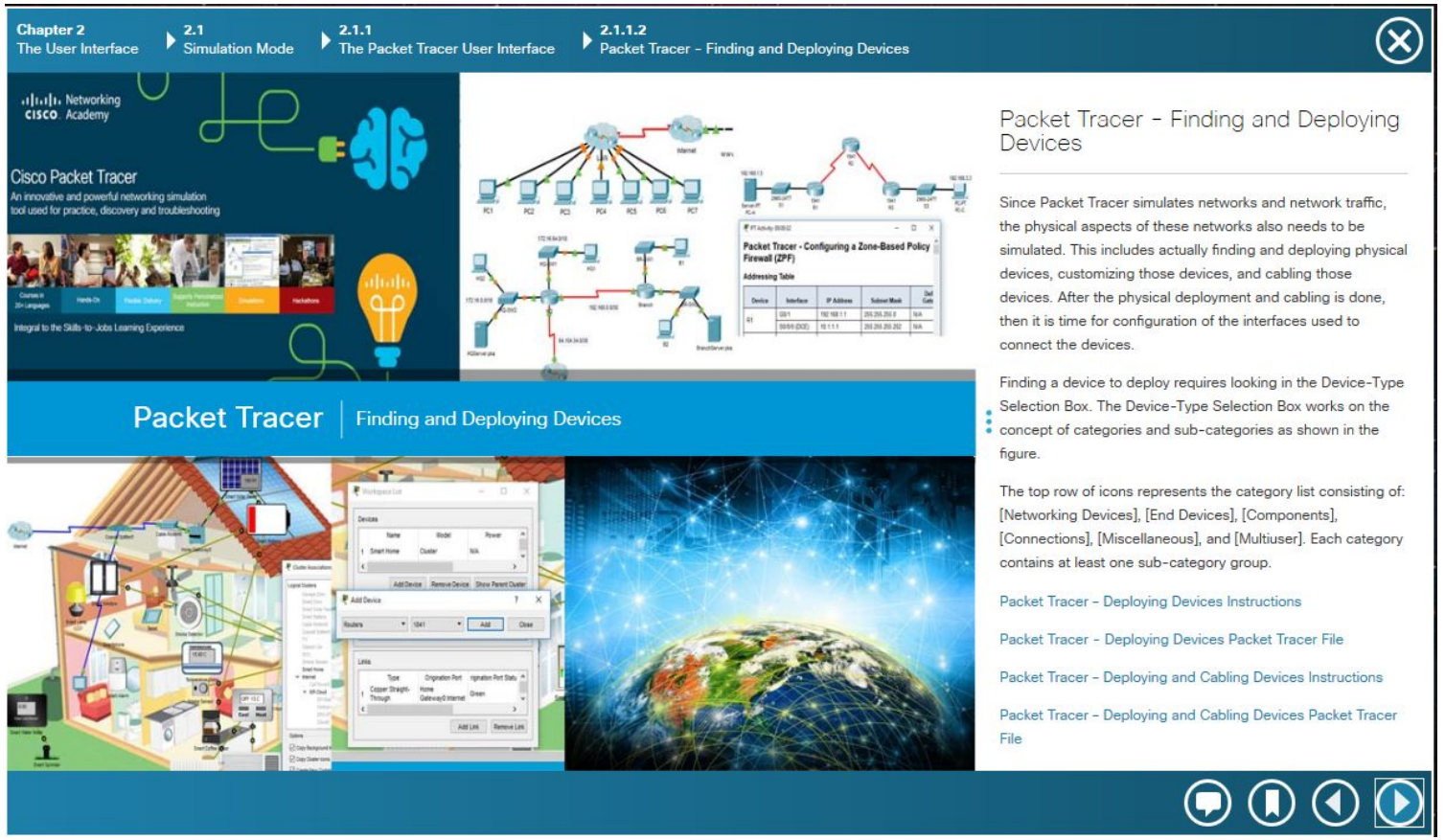
2.1.1.1 Video: Getting Started in Packet Tracer View and follow along with the video in page 2.1.1.1





Packet Tracer - Finding and Deploying Devices

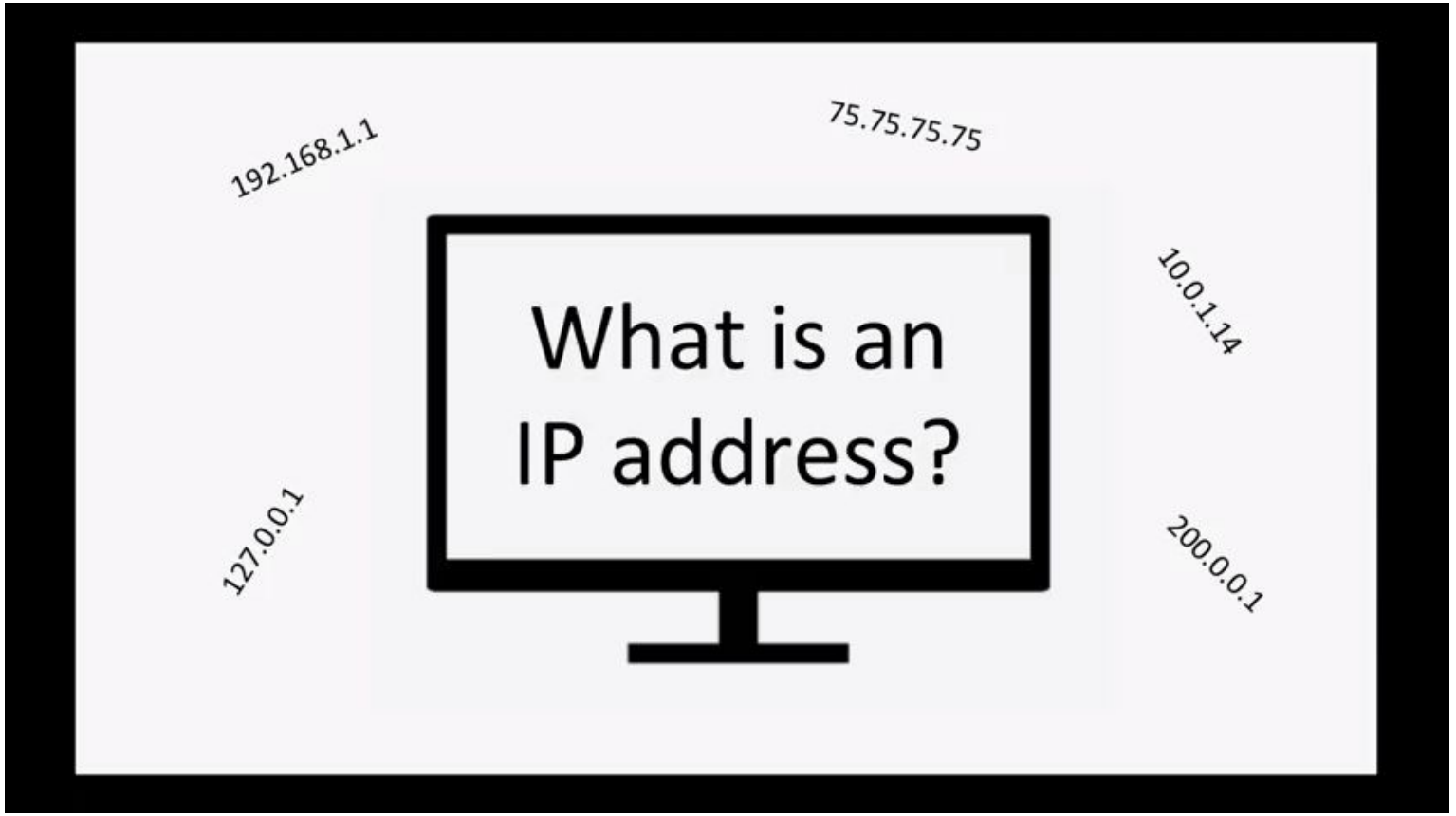
Do both 2.1.1.2 exercises: **Deploying Devices** & **Deploying and Cabling Devices**



The 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 address 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

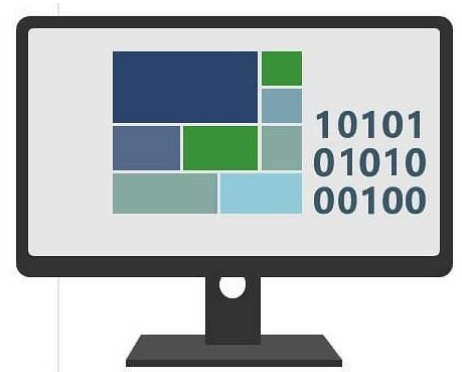
- Address number of a computer (or device) on the Internet or local network
- Shown as 4 numbers (max 255), separated by periods
- For example: **192.168.1.12**
- But really, it's 32 binary digits (bits), like this: **11000000.10101000.00000001.00001100**

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

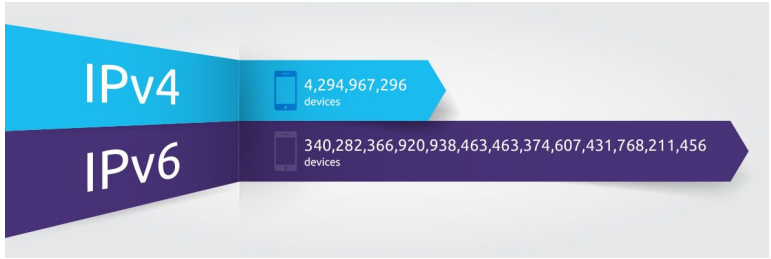
IPv6 (IP version 6) Address

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

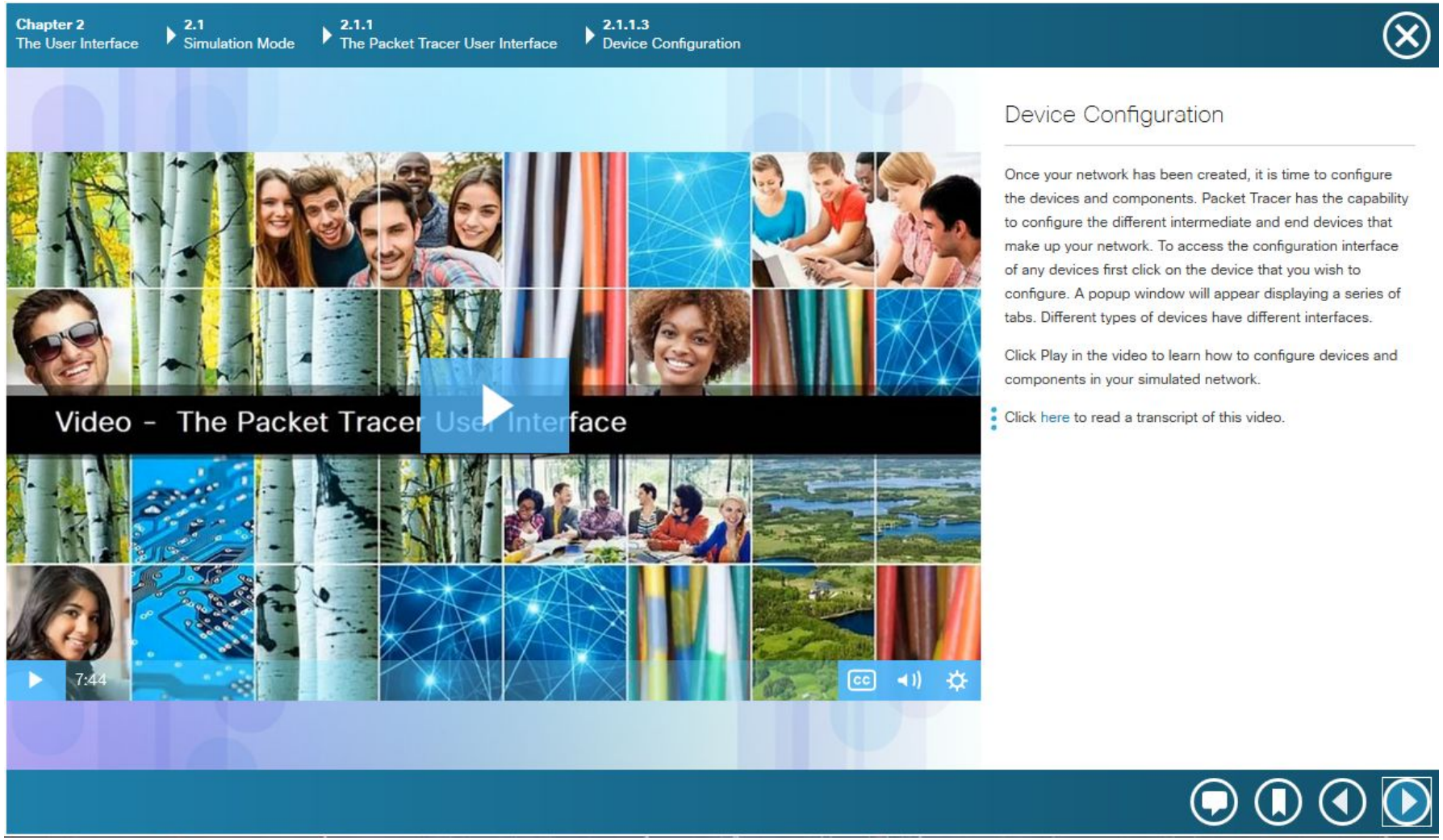
128 bit IPv6 Address Format:

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

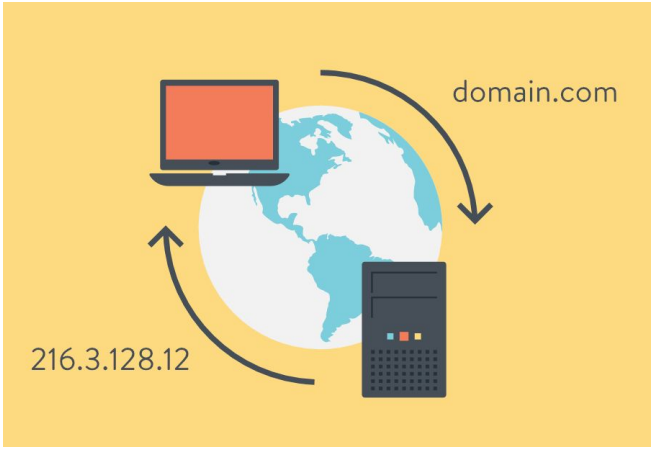


Gateway

- 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)

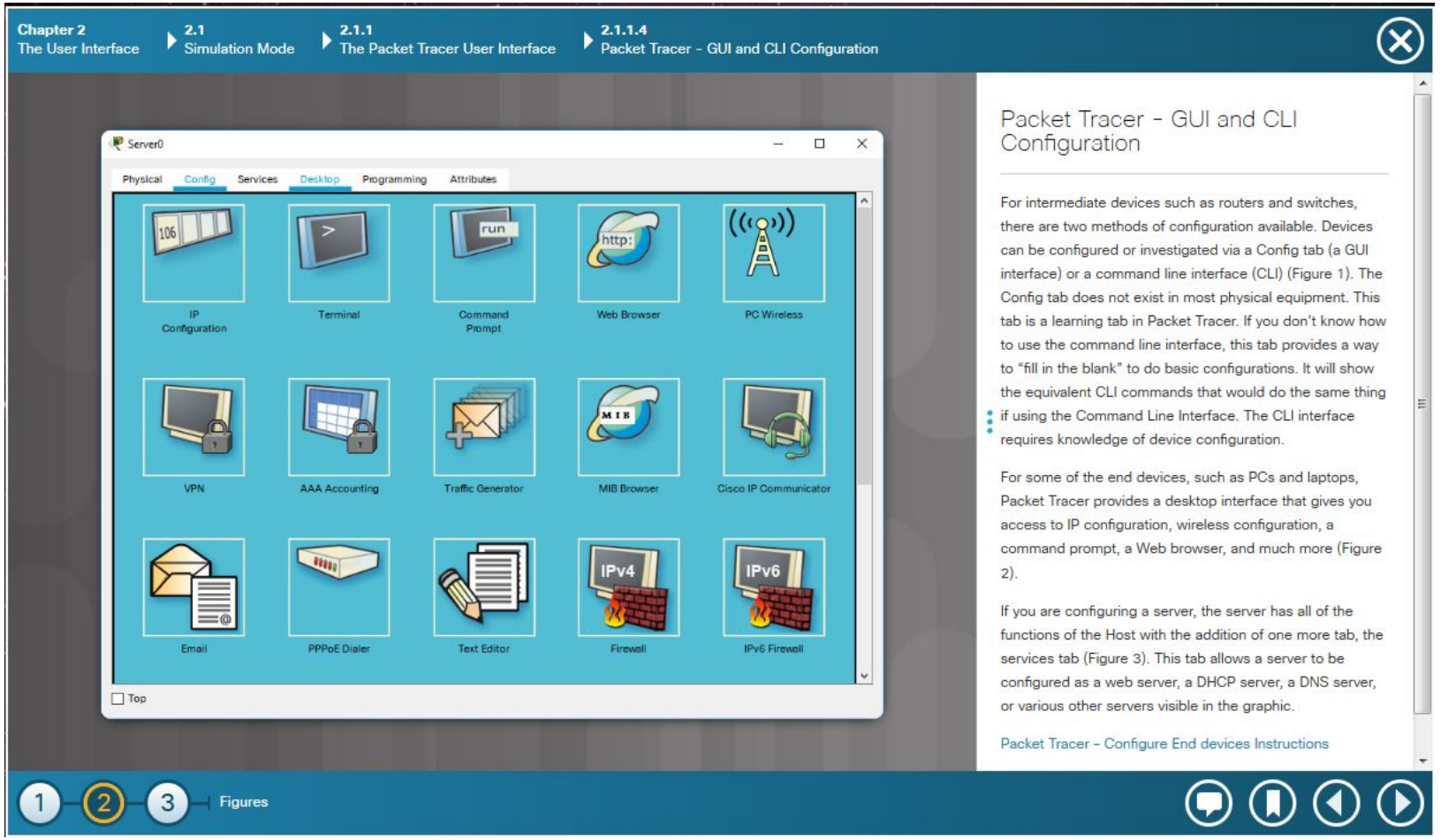
- Automatically gives a temporary address number, subnet mask, etc.

- Used in most connections from Internet providers

- A network ***router*** in your home or office may provide separate DHCP to your computer

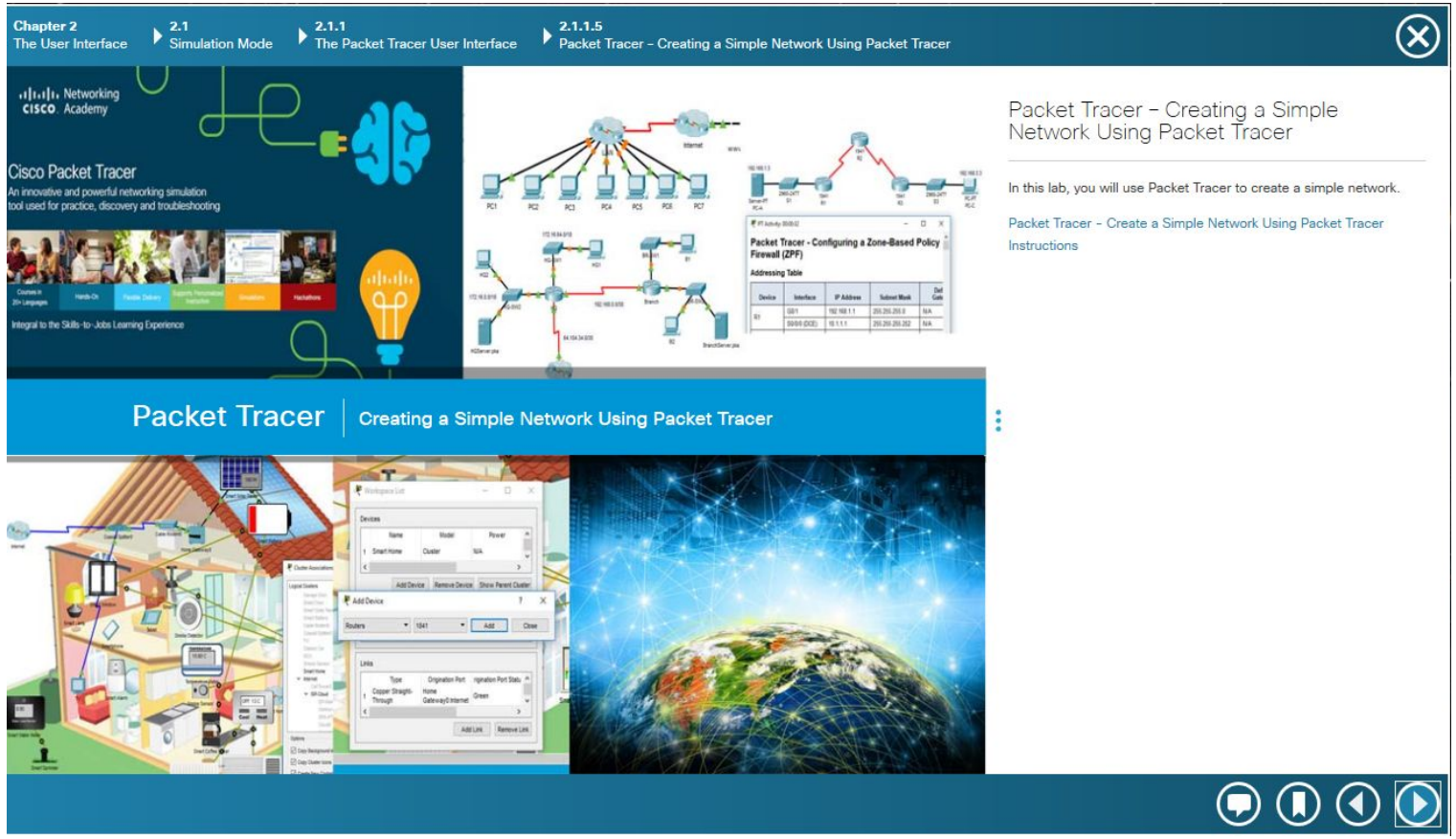
2.1.1.4 Packet Tracer - GUI and CLI Configuration

2.1.1.4 "Configure End Devices" activity



2.1.1.5 Packet Tracer – Creating a Simple Network

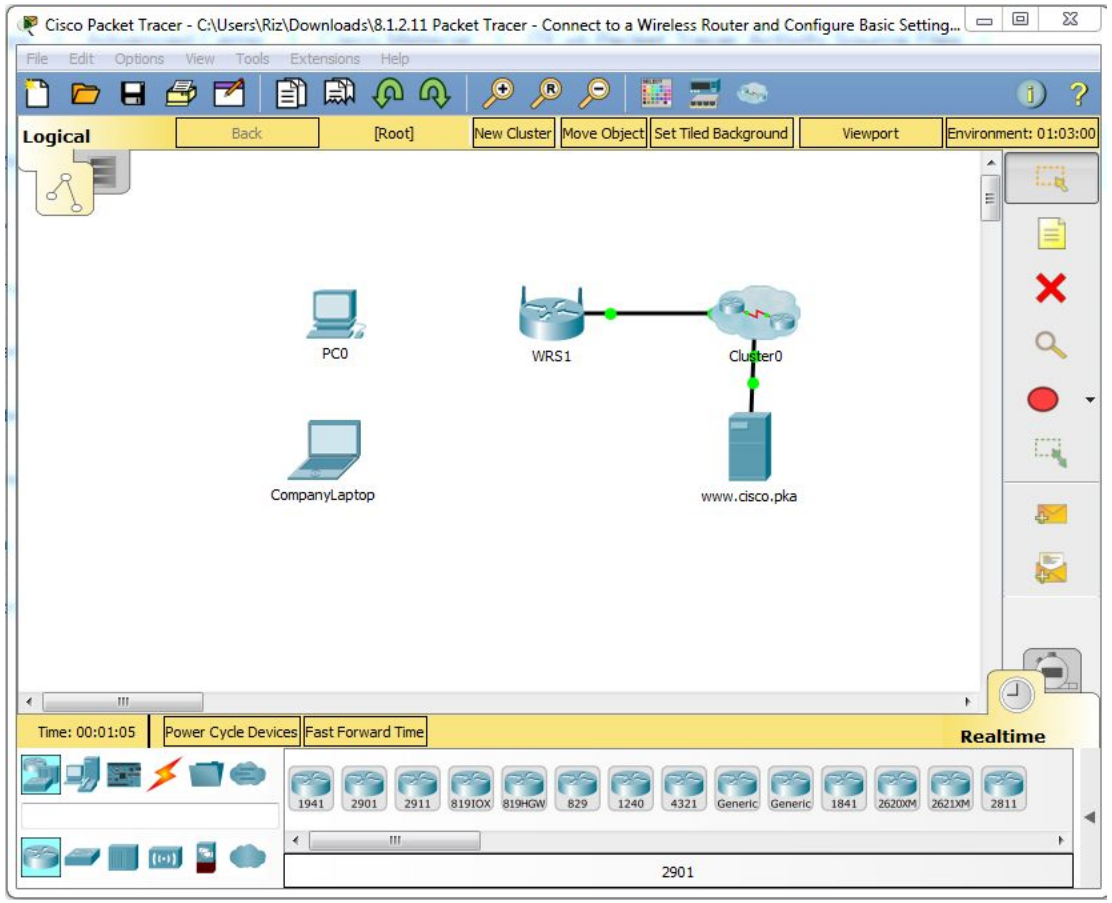
2.1.1.5 "Creating a Simple Network Using Packet Tracer" activity



Activity: Configure Basic Wireless Settings

Packet Tracer - 8.1.2.11

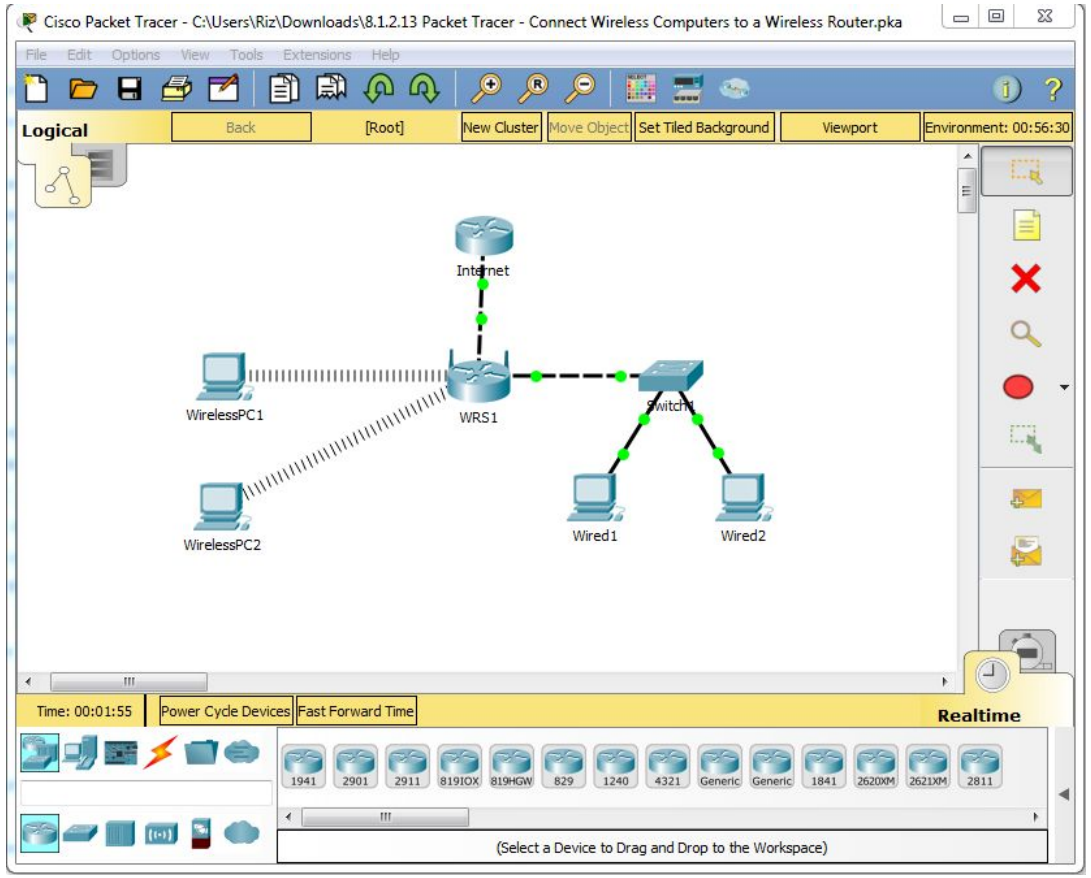
Configure Basic Home Wireless Router Settings



Activity: Connect Wireless Computers to a Router

Packet Tracer - 8.1.2.13

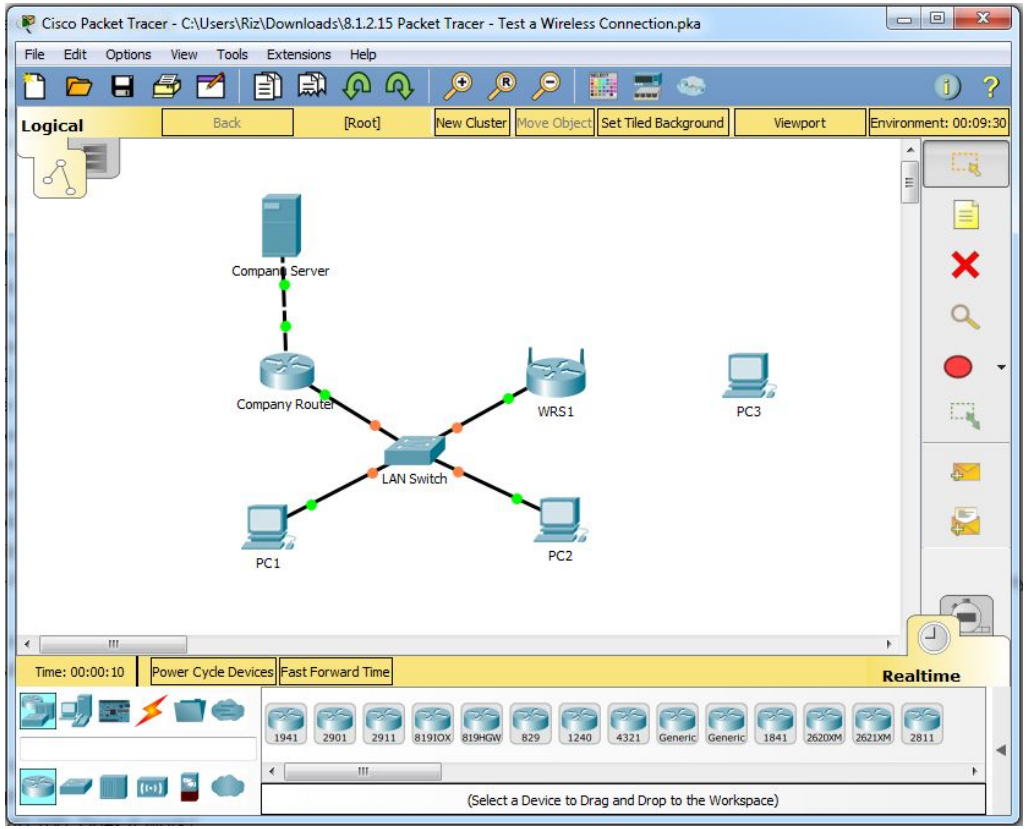
More Advanced Home Wireless Router Configuration



Activity: Troubleshoot a Wireless Connection

Packet Tracer - 8.1.2.15

Troubleshoot Wireless Connectivity



Intro Cybercamp

Digital Forensics & Networking

BACCC
BAY AREA
COMMUNITY COLLEGE CONSORTIUM