Autopsy and iPhone Forensics

Cybersecurity

Digital Forensics Day 2

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Class Objectives

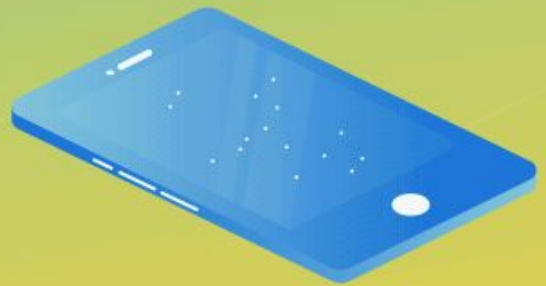
By the end of class, you will be able to:

- Identify the methods used in smartphone forensics investigations.
- Navigate the database and file structure of an iPhone's flash drive.
- Locate identifiable evidence on an iPhone in order to establish ownership.
- Use Autopsy to access and tag evidence in an iPhone image.
- Extract image content for offline reviewing in other applications.

(apple.com)

In the previous class, we covered the basic principles of digital forensic methodologies and used Autopsy to preserve and document evidence.

Today, we will hone in on mobile forensics and continue the National Gallery investigation, using Autopsy to access and tag evidence from an iPhone image.



(Source)

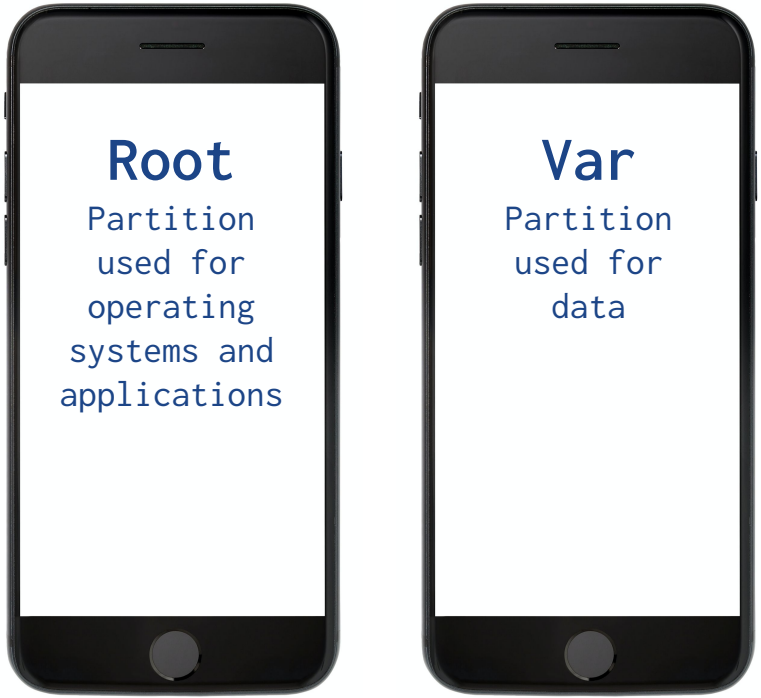
Where’s the Data?
File Systems and Data Storage

Where's the Data? File Systems and Data Storage

It's important to know where data is stored, how to access it, and how to recover it.

Instead of external storage, iPhones use **flash memory**.

Flash memory contains two disk partitions:



REMEMBER

Data is first imaged using a **bit-level copy**.

iPhone texts, GPS coordinates, and cell tower locations can all be recovered.

Important Directories, Databases, and Files

The following directories are worth investigating for evidence:

`/mobile`

`/Applications`

`/Library`

`/root`

`/Logs`

`/logs`

iPhone users store data in SQL databases and other files.

Important Directories, Databases, and Files

SQL (Structured Query Language) is a programming language used to review, create, and update database files.

= **S** tructured **Q** uery **L** anguage

Important Directories, Databases, and Files

NAME	CONTENTS
`AddressBook.sqlitedb`	Contact info, personal data like name, email address, etc.
`AddressBookImages.sqlitedb`	Images associated with saved contacts.
`Calendar.sqlitedb`	Calendar details and events information.
`CallHistory.db`	Call logs including phone numbers and timestamps.
`sms.db`	Text and multimedia messages along with timestamps.
`voicemail.db`	Voicemail messages.
`Safari/Bookmarks`	Saved URL addresses.
`Envelope Index`	Email addresses on phone.
`consolidated.db`	GPS tracking data.
`locationd`	Google coordinates of locations.

Important Directories, Databases, and Files

iPhone also has data stored in Property Lists (`plists`).

`plists` store configuration information, call history, and cache information.

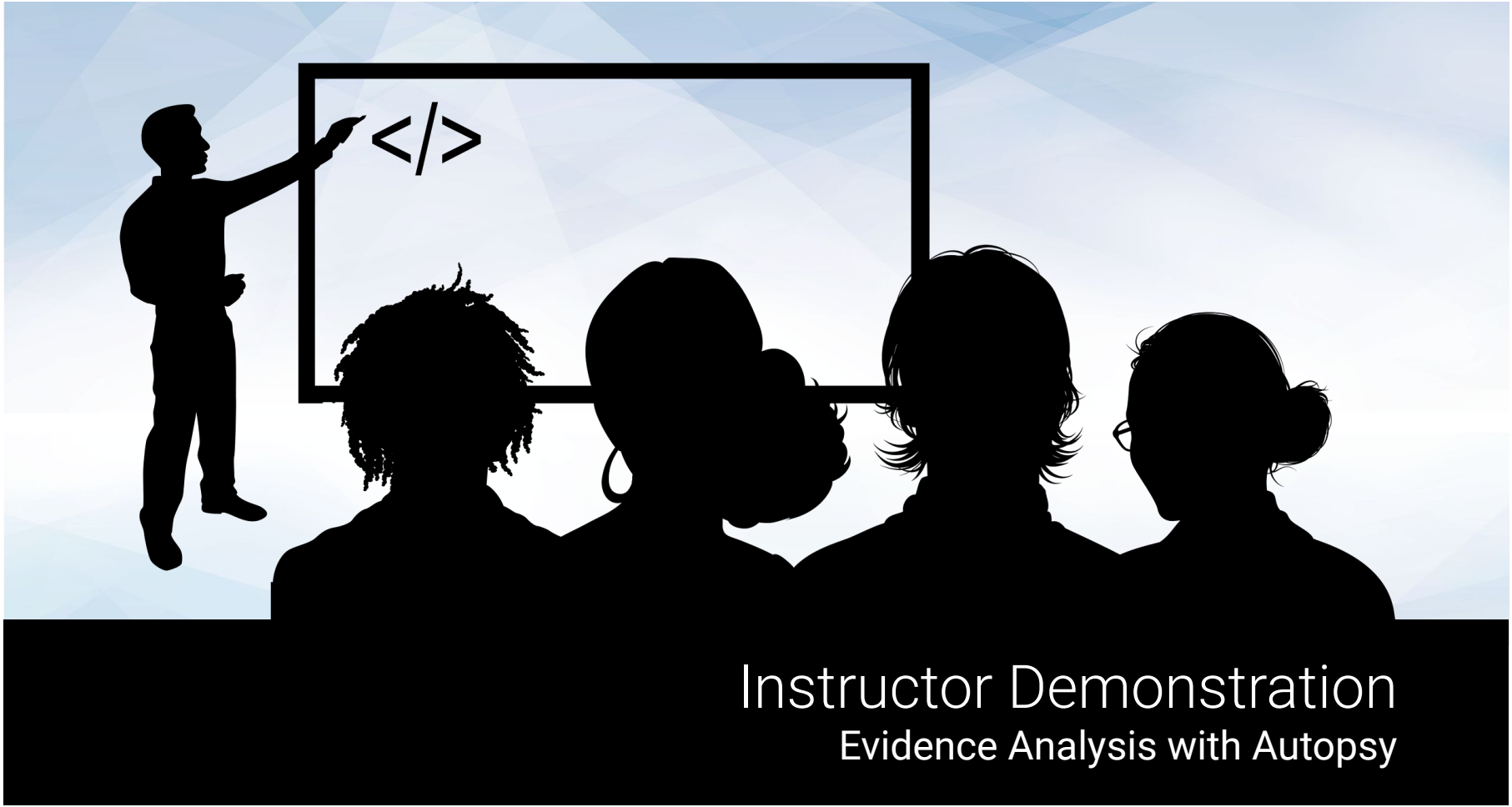
`Maps/History.plist` tracks location searches.

`Map/Bookmarks.plist` contains bookmarks.

`Safari/History` contains internet browsing history.

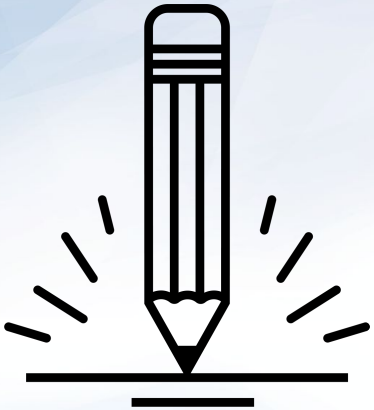
Demo Introduction

In this demonstration, we will go through various ways to obtain evidence.



Instructor Demonstration

Evidence Analysis with Autopsy



Activity: Mobile Evidence Analysis

In this activity, you will analyze evidence and document the details of Tracy's iPhone.

Suggested Time:
50 Minutes

Time’s Up! Let’s Review.

Break

Tagging Evidence

Tagging Evidence

We can use Autopsy to tag evidence.

Evidence tagging is the process of bookmarking evidence to keep critical details organized and easily accessible.

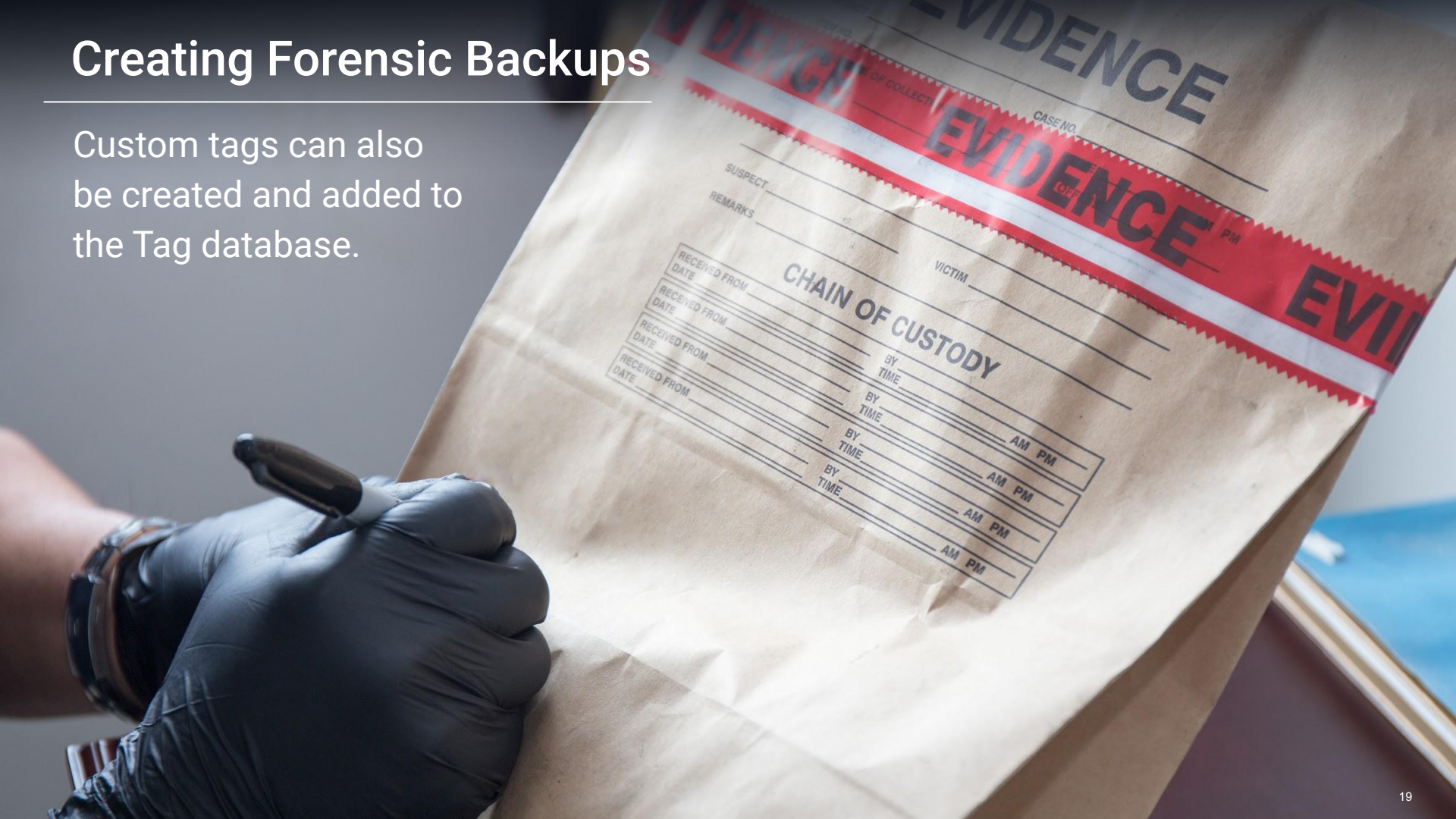
Autopsy includes an evidence-tagging feature that allows investigators to easily locate evidence contained in the program.

Pre-defined tags include:

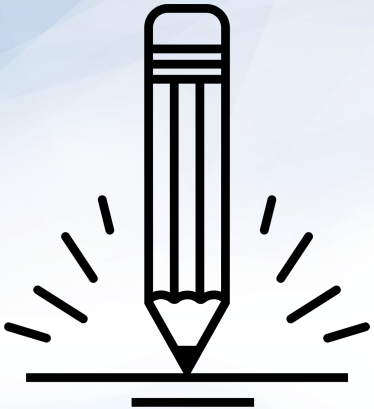
- Follow Up
- Notable Item
- Child Exploitation
- Uncategorized
- Non-Pertinent

Creating Forensic Backups

Custom tags can also be created and added to the Tag database.



In the following guided tour, we'll tag and bookmark the SMS database, which contains sent and received iPhone messages.



Activity: Tagging Evidence

In this activity, you will tag the major databases and files in the iPhone image file.

Suggested Time:
15 Minutes

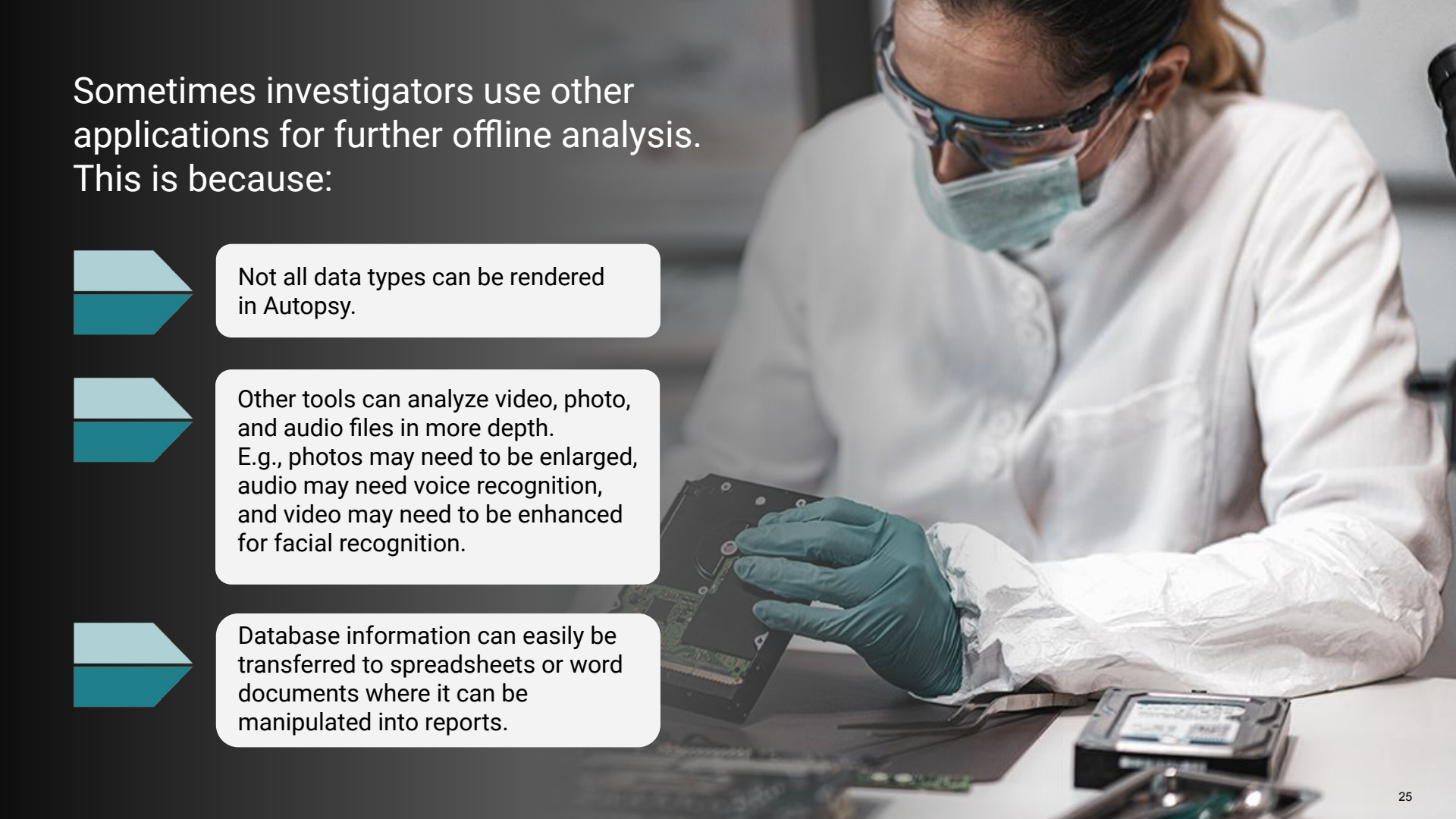
Time’s Up! Let’s Review.

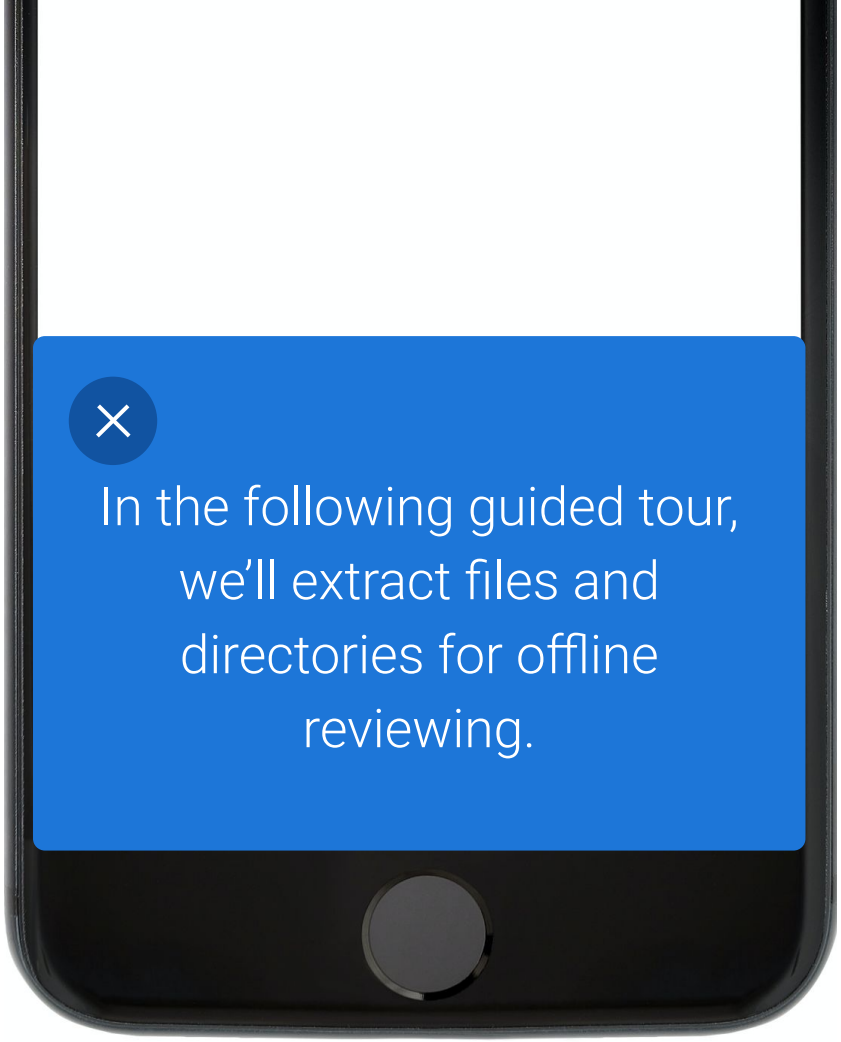
Extracting Data for Offline Analysis

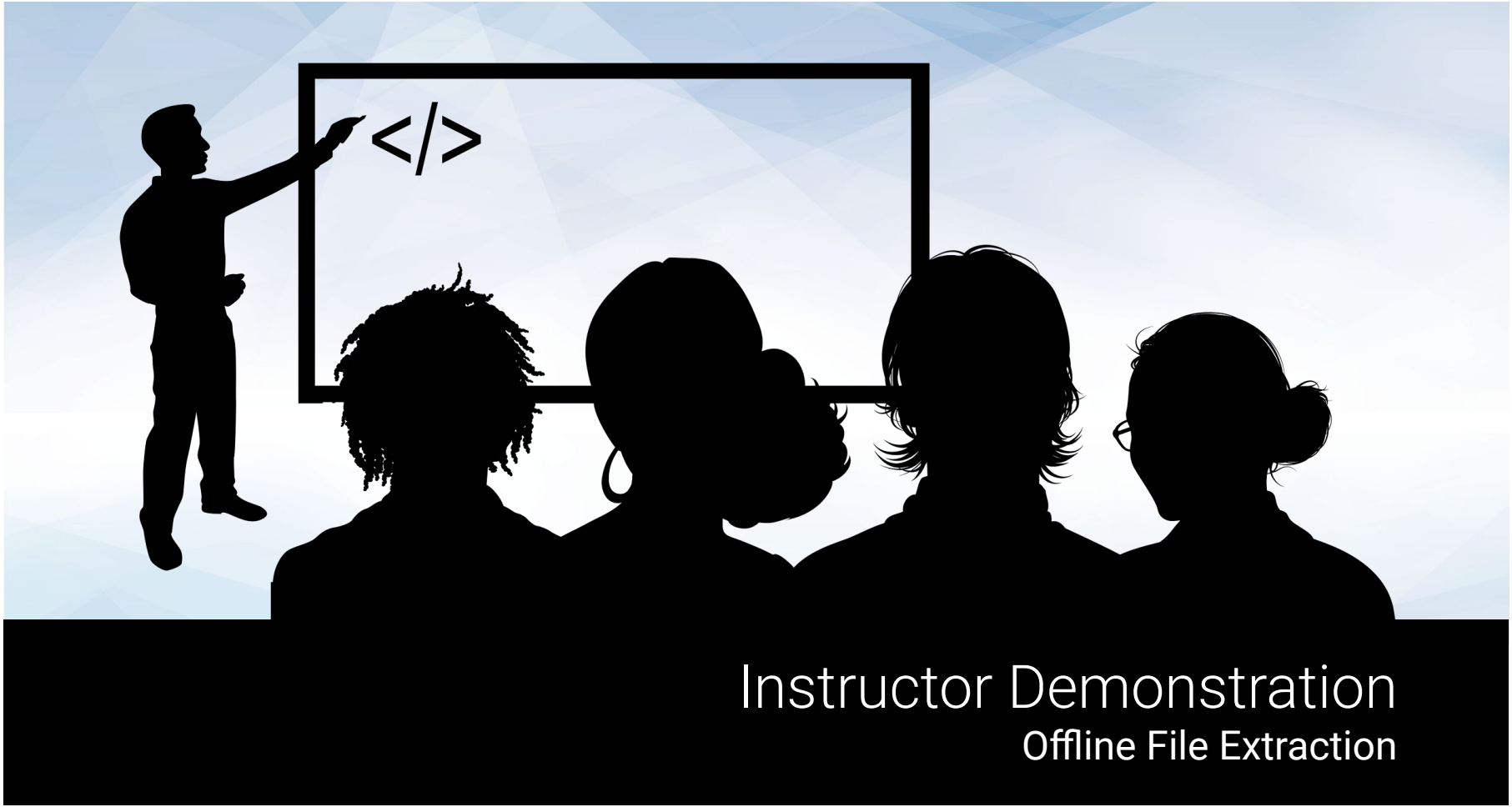
Offline reviewing refers to the process of reviewing files outside of the main program, in this case, Autopsy.

Sometimes investigators use other applications for further offline analysis. This is because:

- Not all data types can be rendered in Autopsy.
- Other tools can analyze video, photo, and audio files in more depth. E.g., photos may need to be enlarged, audio may need voice recognition, and video may need to be enhanced for facial recognition.
- Database information can easily be transferred to spreadsheets or word documents where it can be manipulated into reports.

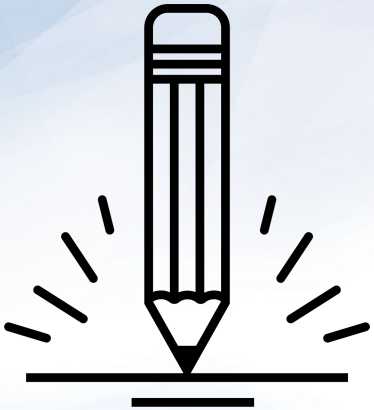



In the following guided tour, we'll extract files and directories for offline reviewing.



Instructor Demonstration

Offline File Extraction



Activity: Extracting Data for Offline Analysis

In this activity, you will export files for offline examination.

Suggested Time:
20 Minutes

Time’s Up! Let’s Review.

Wrap-Up

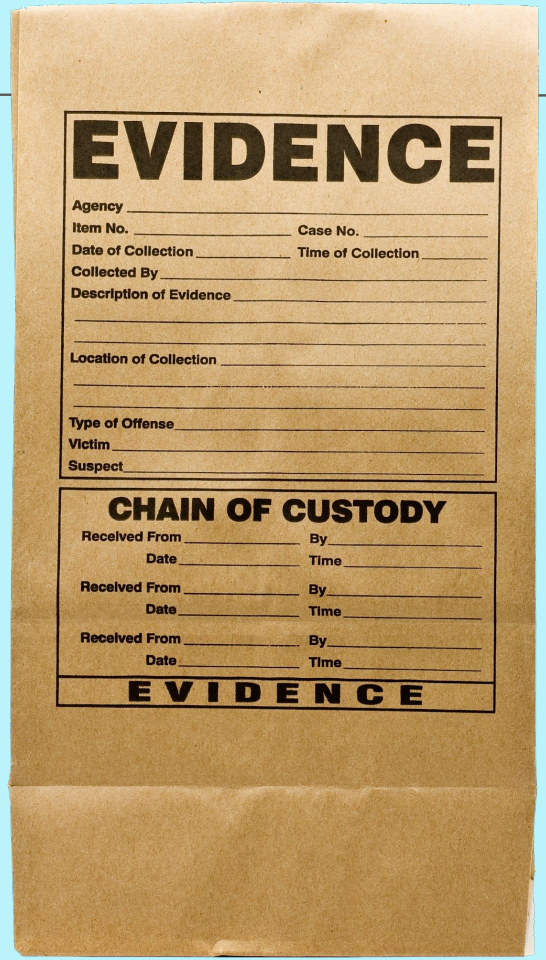
As a forensic investigator, you will work with a team as part of a large collaborative effort.

It's critical to understand how to use tools such as Autopsy and how to export data, allowing other team members to perform offline analysis of evidence.

Wrap-Up

Tagging helps categorize and label evidence that has already been screened.

This eliminates double work and helps other investigative team members continue your work if you become unavailable.



Next class, we will continue our investigation by analyzing email messages, SMS messages, and web history in order to tie Tracy to the case.

Questions?

The End