iPhone Forensics

An Update on Capabilities

September 26th, 2019

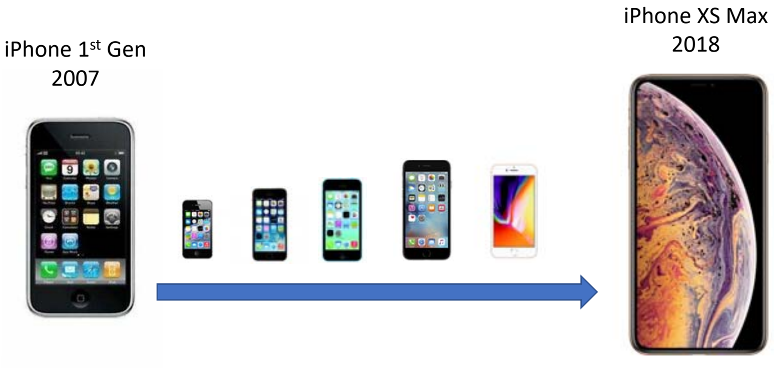
Mike Maschke CEO
Sensei Enterprises, Inc.

DC Bar

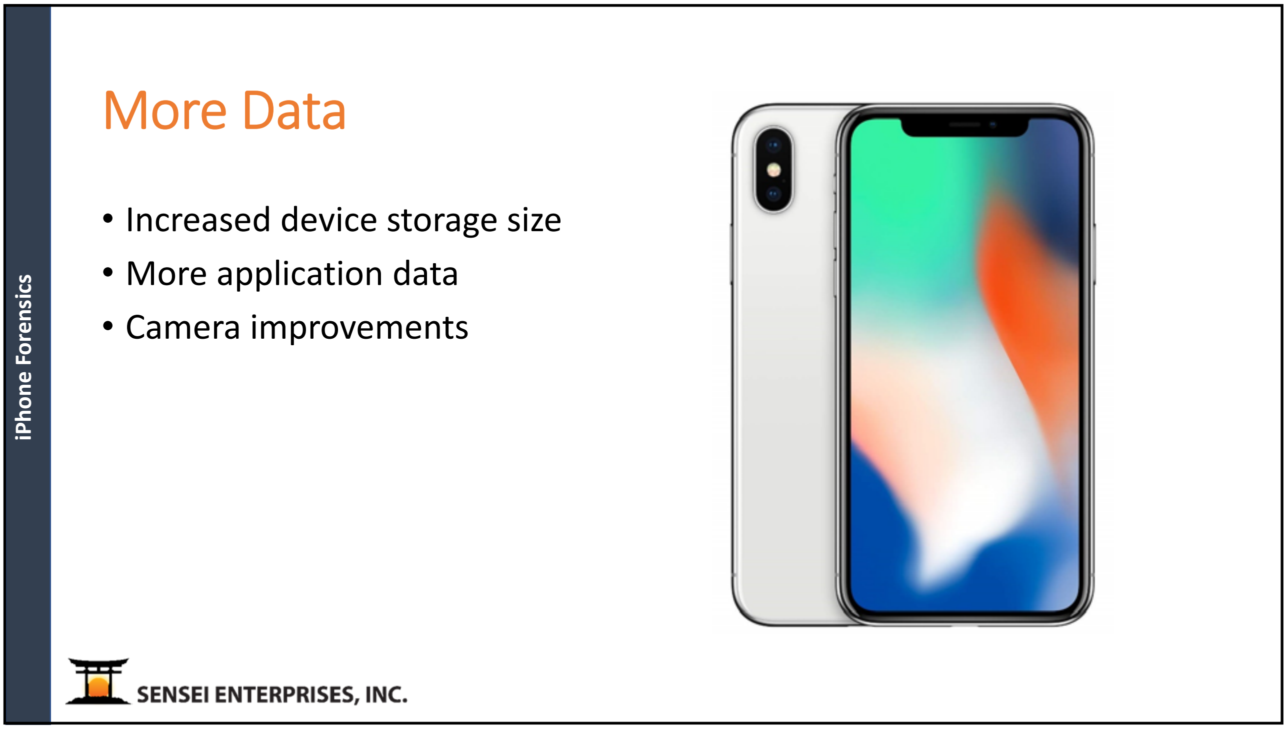
iPhone Forensics

iPhone Basics

- Introduced June of 2007 from Apple
- To date, more than 20 models released



SENSEI ENTERPRISES, INC.

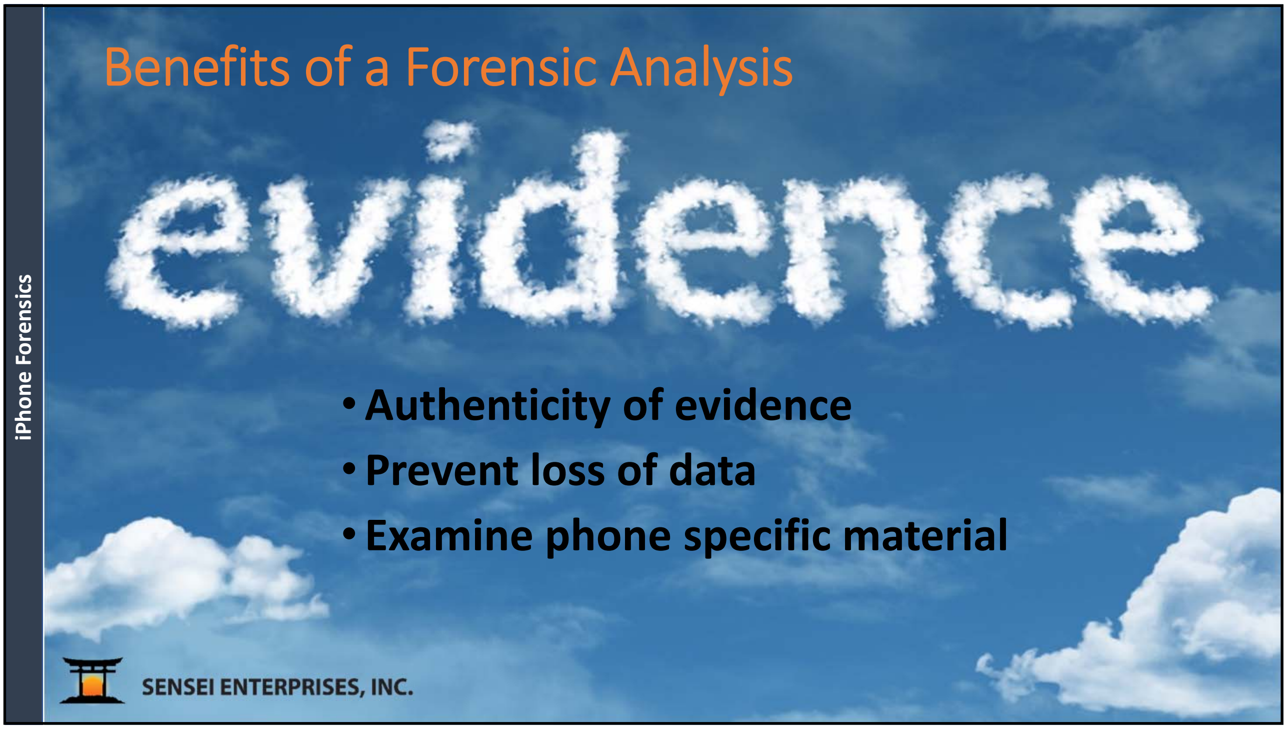


iPhone Forensics

More Data

- Increased device storage size
- More application data
- Camera improvements

SENSEI ENTERPRISES, INC.

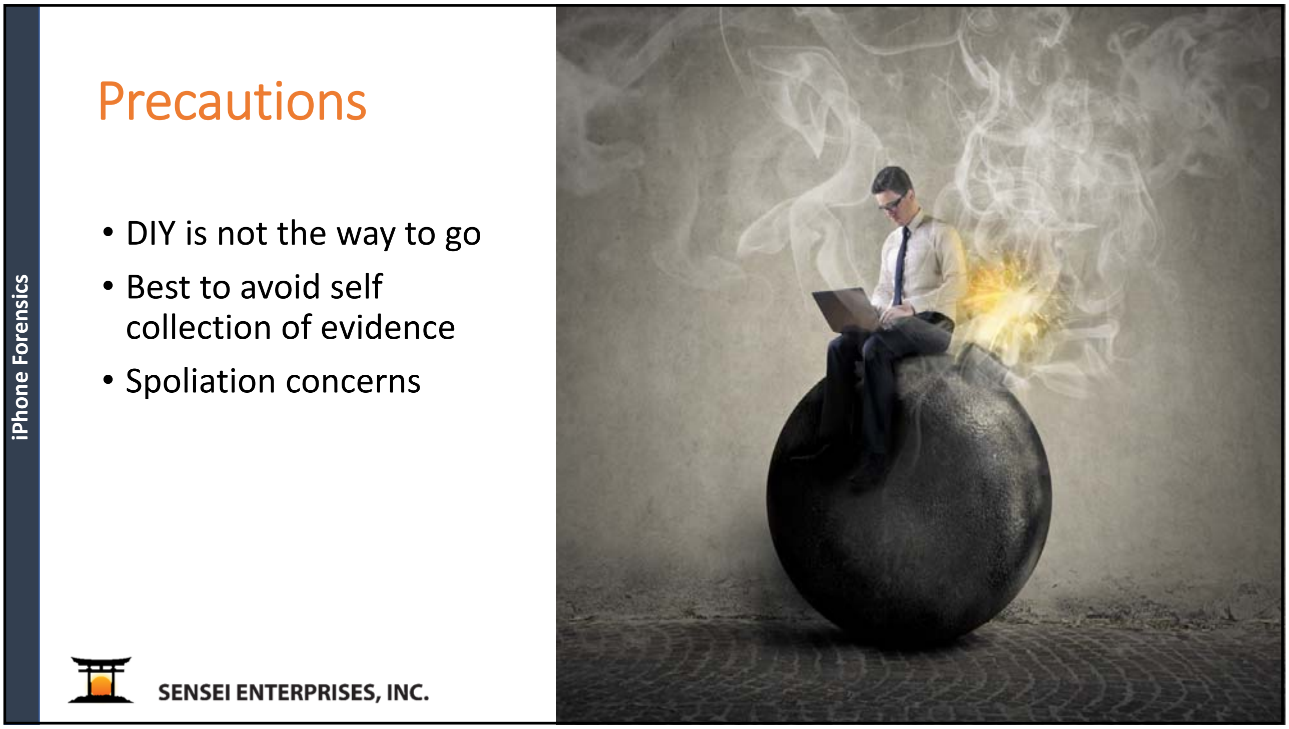


iPhone Forensics

Benefits of a Forensic Analysis

- **Authenticity of evidence**
- **Prevent loss of data**
- **Examine phone specific material**

SENSEI ENTERPRISES, INC.



iPhone Forensics

Precautions

- DIY is not the way to go
- Best to avoid self collection of evidence
- Spoliation concerns

SENSEI ENTERPRISES, INC.

iPhone Forensics

Steps in a iPhone Analysis

Consultation

Preservation

Analysis

Findings

SENSEI ENTERPRISES, INC.

iPhone Forensics

Pre-Analysis

- Follow best practices before analysis
- Information is constantly being sent and received
- Best to turn off device, or place in airplane mode to preserve the integrity of evidence
- Ensures data does not change

SENSEI ENTERPRISES, INC.

iPhone Forensics

Proper Handling

- Documentation
- Photographs
- Protection against Remote Wiping
  - Ex: Airplane Mode, Faraday Technology
- Data Preservation
  - Ex: Creation of a forensic image

SENSEI ENTERPRISES, INC.

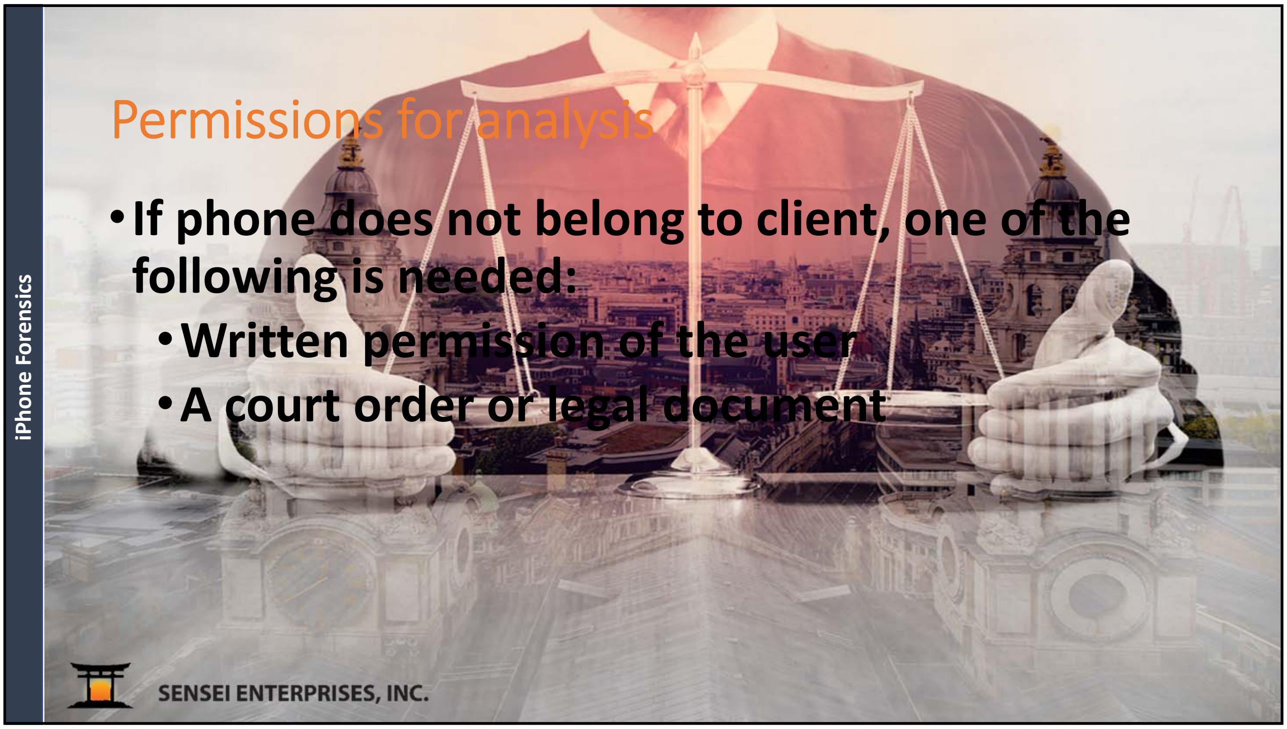
iPhone Forensics

Retaining an Expert

What to look for:

- Experience with mobile forensics
- Utilizing industry standard software
- Mobile device certifications

SENSEI ENTERPRISES, INC.



iPhone Forensics

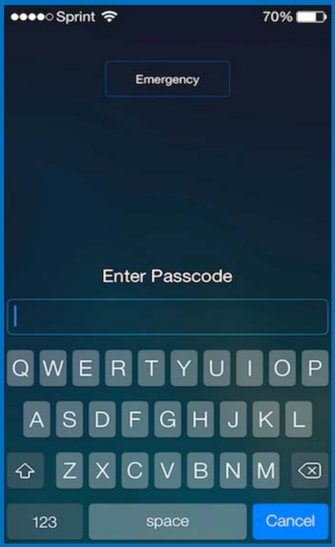
Permissions for analysis

- If phone does not belong to client, one of the following is needed:
  - Written permission of the user
  - A court order or legal document

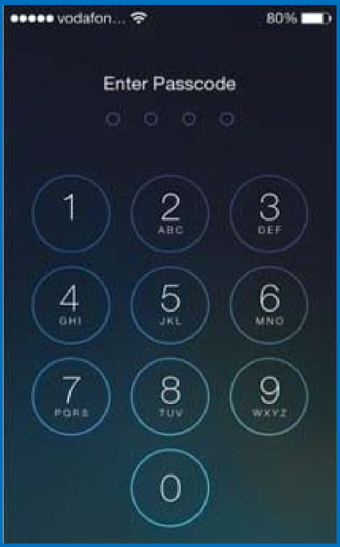
SENSEI ENTERPRISES, INC.

- An encrypted device prevents analysis
- Password for iPhone must be known in order to perform an examination

Passwords



Alphanumeric



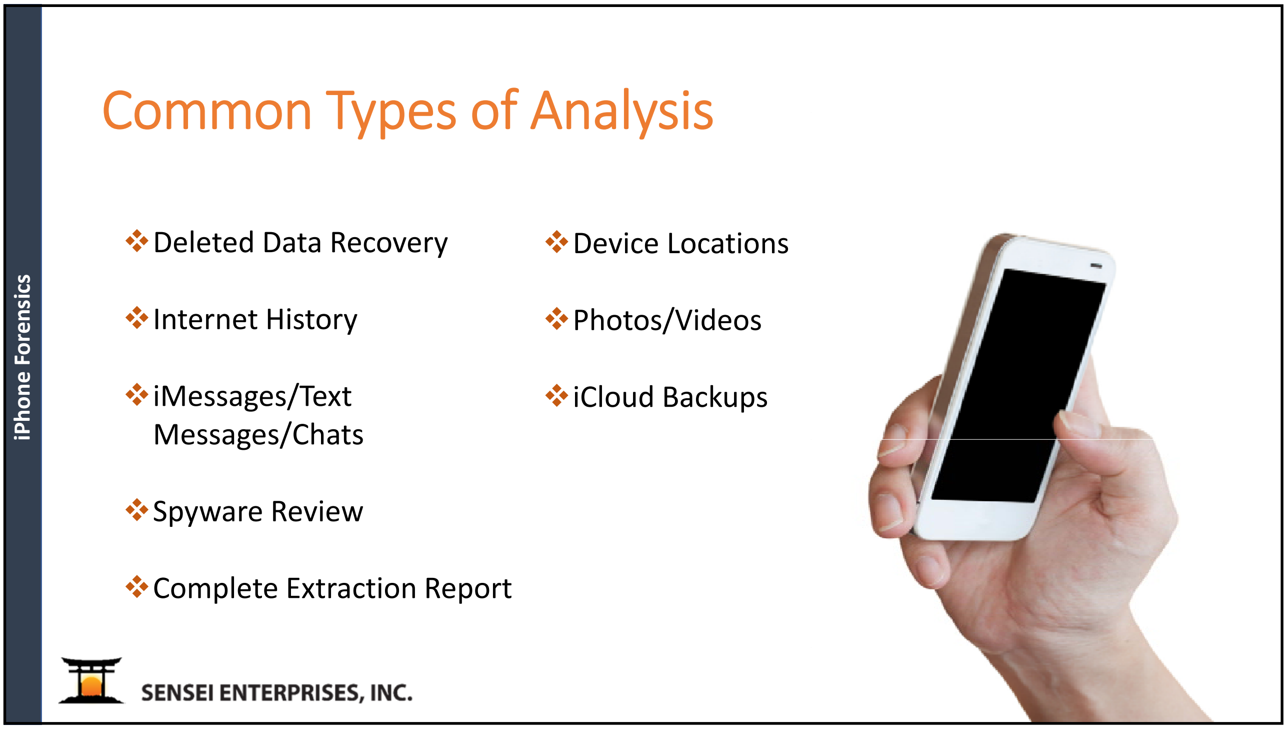
Passcode

iPhone Forensics

Unlocking Features

Face ID
Touch ID

SENSEI ENTERPRISES, INC.



iPhone Forensics

Common Types of Analysis

- ❖ Deleted Data Recovery
- ❖ Internet History
- ❖ iMessages/Text Messages/Chats
- ❖ Spyware Review
- ❖ Complete Extraction Report
- ❖ Device Locations
- ❖ Photos/Videos
- ❖ iCloud Backups

SENSEI ENTERPRISES, INC.

iPhone Forensics

Deleted Data Recovery

- Regularly recovered data:
  - Communications (text messages, iMessages, instant messages, call logs, voicemails)
  - Internet History (websites visited, search terms, bookmarks)
  - Deleted images and videos
    - Not likely retained when deleted, possibly contained in backups

iPhone Forensics

Factors that affect recoverability

- Length of time that has passed since deletion
- Amount of new device activity

Overwritten data is unrecoverable

Welcome to the DMV License line! You're currently 16th in line, and your estimated wait is 54 minutes. We'll text when you reach the front of the line.

Your estimated wait is now 15 min. Please head to the Murdock Office. Need more time? Reply with "M".

You have reached the front of the License line! Please proceed to Window 7. Thanks for waiting!

iPhone Forensics

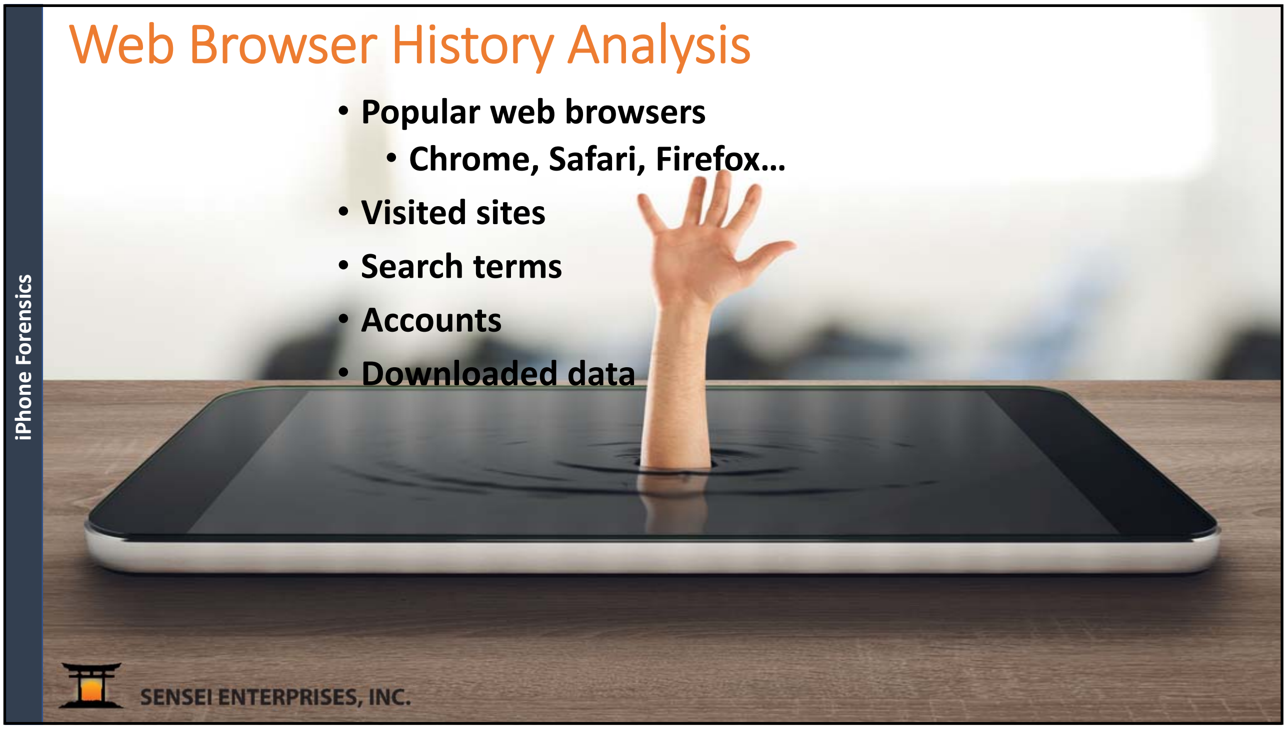
iCloud Backups

iCloud

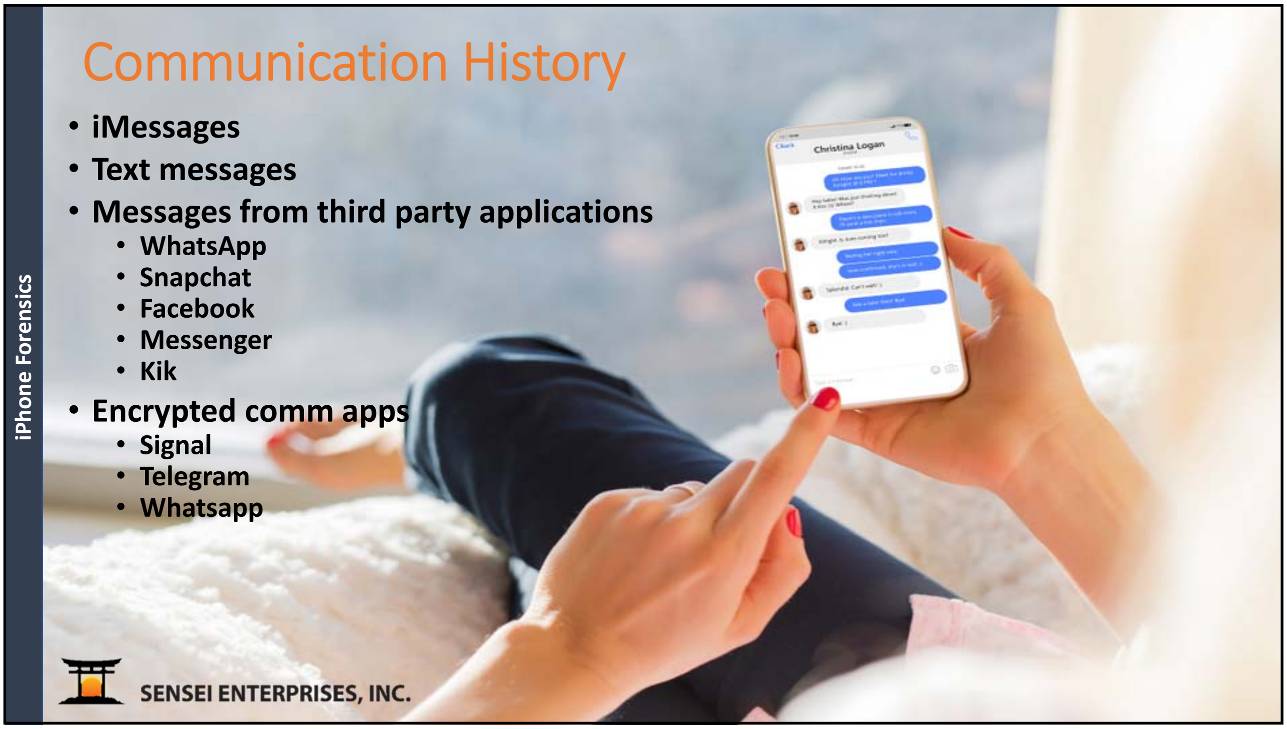
- Service tasked with backing up information stored on Apple devices
- If enabled, may contain information that has since been deleted from the iPhone
- To verify if backups are present, use Apple ID credentials
- Cannot get if two-factor authentication is enabled, which is now by default

iPhone Forensics

Web Browser History Analysis



- Popular web browsers
  - Chrome, Safari, Firefox…
- Visited sites
- Search terms
- Accounts
- Downloaded data



iPhone Forensics

Communication History

- iMessages
- Text messages
- Messages from third party applications
  - WhatsApp
  - Snapchat
  - Facebook
  - Messenger
  - Kik
- Encrypted comm apps
  - Signal
  - Telegram
  - Whatsapp

SENSEI ENTERPRISES, INC.