



## MAC OS X Development – Case Study

Author	Naresh Babu.D
Reviewer	P. Vasudeva Kiran
Date	March 01 2010

## Document History

Version	Date	Author	Reviewed By	Changes done
1.0	01-03-2010	Naresh Babu	P. Vasudeva Kiran	Initial Version

## Table of Contents

1. Introduction .....	4
2. Client .....	5
3. Requirement .....	<b>Error! Bookmark not defined.</b>
4. Solution Provided.....	7

## 1. Introduction

MAC OS X is a modern operating system that combines a stable core with advanced technologies to help you deliver world-class products. The technologies in MAC OS X help you do everything from manage your data to display high-resolution graphics and multimedia content, all while delivering the consistency and ease of use that are hallmarks of the Macintosh experience.

## 2. Client

Computer forensics and eDiscovery have not only become more challenging in the last few years, they have become practically unmanageable for volume and cost. Many tools seem to ignore the issues facing computer forensic examiners and investigators by shepherding them into a one size fits all approach. One company has been watching and listening to the clamor of complaints ... Perlustro.

SUMURI is Cellebrite's oldest and longest running officially authorized training provider. SUMURI's Training is designed for front-line law enforcement, intelligence, military and corporate investigators who want to gain a practical, hands-on understanding of cellular technology in addition to obtaining an official certification as a Certified Cellebrite UFED Mobile Device Examiner

With tools designed to not only handle the obstacles that exist today but also to handle those of tomorrow, Perlustro has solutions that overcome the limitations that exist in other forensic tools to allow your examiners and agency to be more productive and efficient with today's ever-increasing case loads.

### 3. Requirement

Computer forensic and E-Discovery software for examining Macintosh computers and devices is limited at best. The purpose of computer forensics and E-Discovery is to extract, preserve and report on data contained on a computer which may be of evidentiary value. One common problem with Macintosh forensics is that those tasked with performing an analysis of a Macintosh computer or Apple device usually do not have the knowledge base or skills to successfully conduct an examination.

The primary purpose of this project is to develop a forensic application to assist computer forensic examiners or E-Discovery professionals in extracting items of evidentiary value and place that information into a well organized report via a simplistic user interface. This application should conform to current E-Discovery standards for producing reports if this option is selected (E-Discovery Mode).

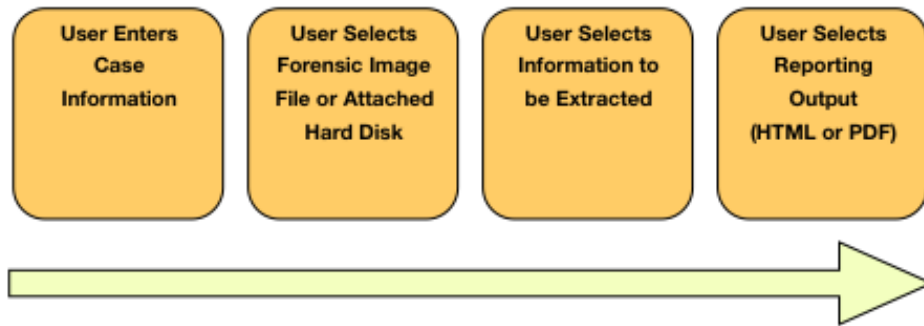
Items of value to an investigator are:

- System Information/Log Files
- Emails
- Contacts
- Calendar/Event data
- Document Files
- Internet History
- Chat/VOIP Communications and Data
- Media Files
- iPhone Backup Files
- Peer 2 Peer data
- Bit-torrent data
- Trash Files

## 4. Solution Provided

Each section represents a step in the examination process. Each new run of the application is referred as “CASE”. Some steps are mandatory and other are optional. Each section user has to select options and provide necessary information for the examination. The selection information will be saved as the user can retrieve the selection or save as template.

User enters the appropriate case information and select’s the forensic image or drive from which data has to be extracted. User select’s the various options under each sections regarding type of data that is to be extracted.



[Various sections involved in the process are described below](#)

### CASE INFORMATION

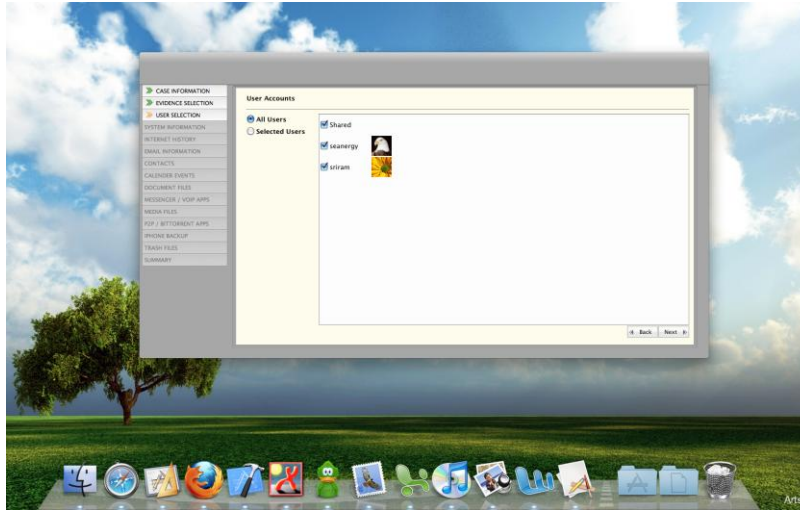
The User would enter the Case Details, Examiner Details and Investigator’s Details.

### EVIDENCE SELECTION

The user would attach the hard drive that is to be examined. The user can attach Hard drive with physical write blocker, also can attach hard drive with Disk Arbitration Turned off. The user can attach a Forensic Image file. The user is provided with an option to disable or enable Disk Arbitration

## USER SELECTION

This section provides the user accounts that they would like to examine. Once the user selects the user account then the examine process starts where user can select items of interest.

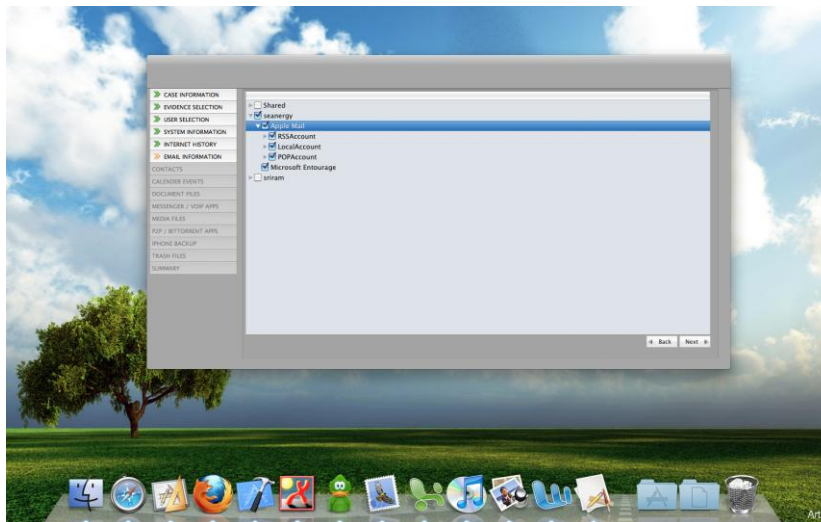


## SYSTEM INFORMATION

The user would extract information, which relates to the system. This section provides user with available Log files from which user can extract the data

## EMAIL INVESTIGATION

This Section allows the user to extract information, which relates to the email (Apple Mail Client and Entourage)



### CONTACTS

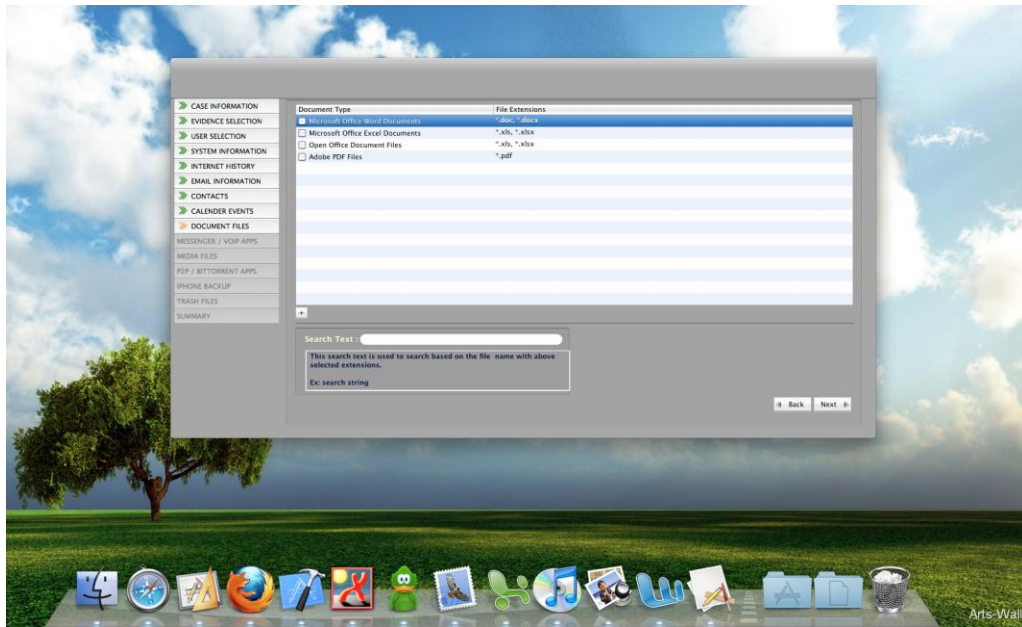
This section allows the user to extract information, which relates to Contacts (Apple Address Book and Entourage)

### CALENDAR EVENTS

This section allows the user to extract information, which relates to Calendar Events (Apple iCal and Entourage)

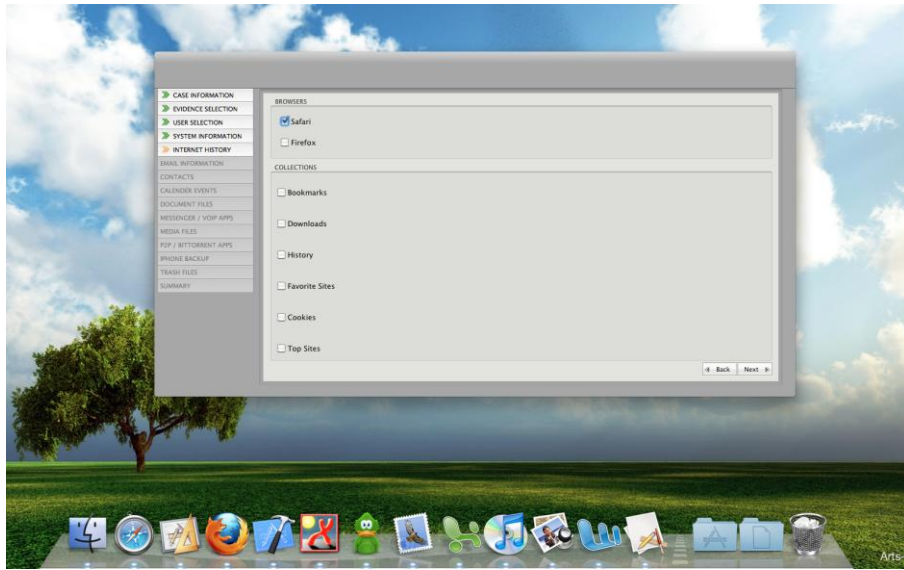
### DOCUMENT FILES

This section allows the user to extract information, which relates to Documents.



### INTERNET HISTORY

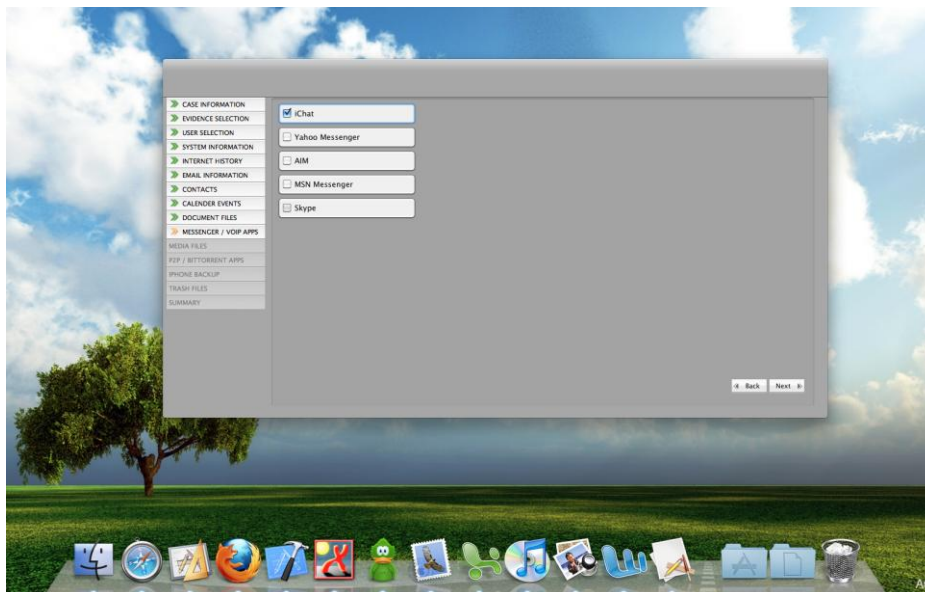
This section allows the user to extract information, which relates to Internet History (Safari and Firefox).



### INSTANT MESSENGER/ VOIP Applications

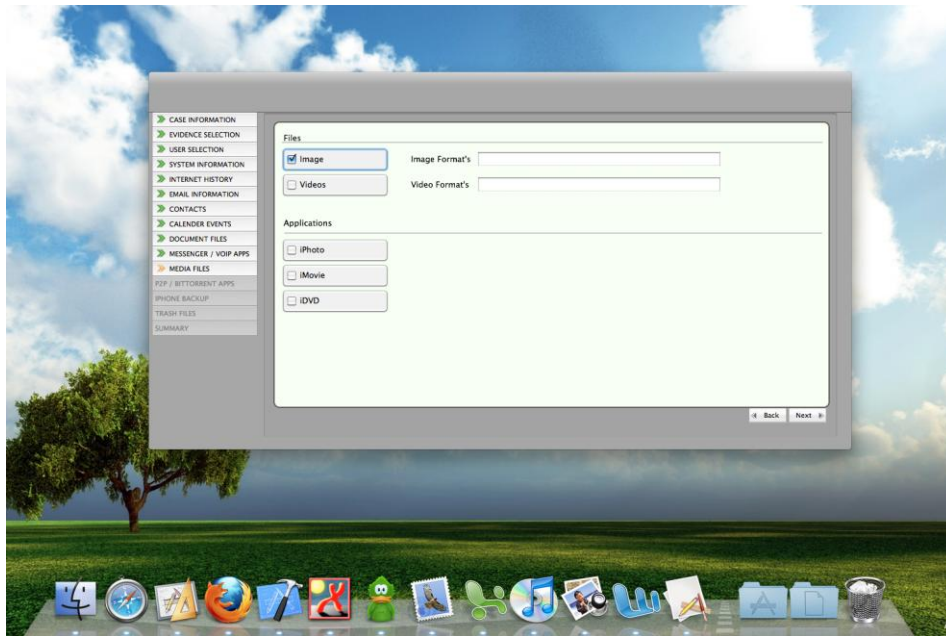
This section allows the user to extract information, which relates to Instant Messenger and VOIP Applications

(IChat, Yahoo Messenger, AIM, MSN Messenger, Skype).



**MEDIA FILES**

This section allows the user to export files and/or information, which relates to media files and applications (images, videos, iPhoto, iMovie, iDVD).



**PEER 2 PEER/BITTORRENT Applications**

This section allows the user to extract information, which relates to P2P and Bit Torrent applications (Limewire, Vuze).

**IPHONE/IPOD TOUCH BACKUP FILES**

This section allows the user to extract information contained in the iPhone backup files.

**TRASH FILES**

This section allows the user to list and extract information about files found in the hidden Trash directory.