



“Best Practices For Addressing Smartphones in Civil Discovery & Reasonable Attorney-Client Communication Security Measures”

Smartphones, such as iPhones and Android phones, have become ubiquitous in daily life, can be as powerful as laptop and desktop computers, and can store many gigabytes of evidence potentially relevant to civil lawsuits of all types. This class will educate students as to the important categories of evidence that can be recovered from smartphones and how these categories can be leveraged in not only a defensive manner but also an offensive manner in civil litigation. Finally, the class will provide reasonable steps one should take to protect attorney-client communications from spying.

Sponsor: **Scarab Consulting / Litigation Services**

Faculty: **Larry Lieb, LCE, FEXE Scarab Consulting, Frederick Kopec, GC, Scarab Consulting**

- SECTION I: Smartphones are Basically Big File Cabinets
 - Smartphones Contain 10 Basic Cabinet Drawers
 - Some Cabinet Drawers are Locked
 - Contents of the Locked Drawers
 - Why Sell Smartphones With Locked Drawers?
 - Some Deleted Evidence Can Be Recovered From The Unlocked Drawers
 - Practice Point
- SECTION II: Alternative Locations From Which Smartphone Evidence Can Be Recovered
 - Mobile Backups (iTunes & iCloud)
 - Examples of Evidence Stored in iTunes Backups
 - Android Backups
 - Practice Point
- SECTION III: Examples of Smartphone File Cabinet Drawer Contents
 - Photograph Drawer Details
 - Call Records Drawer
 - Text Message Drawer
- SECTION IV: Location Based Evidence
 - Photos and Facebook Message Locations
 - Map Queries
 - Location Based Evidence War Story
 - Location Based Evidence Practice Points
- SECTION V: Timelines & Chronological Photography Reports
 - Chronological Photography Reports
 - Example timeline from a Smartphone
 - An iPhone Mobile Backup War Story
- SECTION V: Moving to the Offensive, Elements of an Agreed Order
 - Specific devices and accounts to be imaged and examined

- Limiting date range and key word filters
- Privilege review process
- Key word responsive review and production process
- SECTION VI: Reasonable Attorney-Client Communication Security Measures
 - Three Easy Ways to Spy on One Another
 - Physical Access Questionnaire
 - Three Communication Privacy Preservation Measures
 - Possible Scenarios For Your Own Practice

About the Speaker

Larry Lieb has worked as a subject matter expert in the field of computer forensics and electronic discovery since 1998 and has been with Scarab Consulting since 2011. He is a Lantern Certified Examiner (LCE), Forensic Explorer Examiner (FEEXE) and has completed the Magnet Forensics Internet Evidence Finder Certified Training. He has published articles on original computer forensic research findings on Microsoft Windows 8, “Navigating the Sea of Change in eDiscovery Technology” and “When Dealing with Electronic Discovery, Don’t Be Afraid; Just Don’t Go Alone.” He has served as an expert witness in dozen of matters.