MICHAEL SAYEGH

Junior Consultant, Forensics

iDiscovery Solutions, Inc.
3000 K Street NW, Suite 425
Washington, DC 20007

+1.313.516.3749

msayegh@idsinc.com

Profile on LinkedIn

@iDiscoveryInc

Mr. Sayegh came to digital forensics through one of the most rigorous academic paths in the field, and he brought that foundation directly into practice.

At iDS, he works across the full evidentiary lifecycle, supporting forensic evidence acquisition, mobile device imaging, legal hold preservation, and forensic lab operations. He conducts digital evidence acquisition and forensic imaging across macOS, iOS, and Android environments using FTK Imager, Cellebrite UFED, Cellebrite Physical Analyzer, Cellebrite Digital Collector, and Magnet AXIOM. His work spans active litigation and investigative matters, with a consistent focus on forensic defensibility: chain of custody documentation, hash verification, and evidence integrity at every stage. He has also developed PowerShell automation to streamline forensic lab audit workflows, and his work extends into malware analysis and behavioral examination using REMnux, PEStudio, Procmon, and related tools.

Mr. Sayegh holds a Master of Science in Digital Forensics and a Bachelor of Applied Science in Cybersecurity from George Mason University, where he graduated with Dean's List and Presidential Scholar honors. He completed additional academic study in Digital Warfare and Digital Forensics Ethics at the University of Oxford.

EDUCATION

- George Mason University, M.S. Digital Forensics | B.A.S. Cybersecurity; Dean's List, Presidential Scholar
- University of Oxford, Academic Study Abroad Program, Digital Warfare and Digital Forensics Ethics

EXPERIENCE

- iDiscovery Solutions; Digital Forensics Intern; March 2026 to present

PROFESSIONAL EXPERIENCE

- Mr. Sayegh conducted digital evidence acquisition and forensic imaging across macOS, iOS, and Android devices using FTK Imager, Cellebrite UFED, Cellebrite Physical Analyzer, Cellebrite Digital Collector, and Magnet AXIOM.
- Full evidence intake, device inventory validation, chain of custody documentation, and hash verification were performed across litigation and investigative matters to ensure forensic defensibility.
- Advanced logical and full file system acquisitions of iOS devices were completed in support of active litigation and investigative engagements.
- Legal hold preservation workflows were supported by securing client devices and maintaining evidentiary integrity throughout the evidence lifecycle.
- Client return media was encrypted using BitLocker to ensure secure transfer and delivery of sensitive client data.
- Secure media sanitization and drive wiping were conducted using Logicube Falcon for forensic reuse and client return workflows.
- Forensic lab audits were conducted by reconciling physical evidence inventory against documented holdings, developing PowerShell scripts to automate storage drive file listing collection, and maintaining synchronized evidence records in Agility Blue to improve evidence accountability and audit efficiency.
- Collaborated with senior leadership to evaluate and develop tiered forensic workstation replacement strategies aligned to budget and investigative workloads.
- Maintained forensic lab operational readiness by ensuring workstations and mobile forensic kits were updated with current software versions and prepared with required cables, storage media, and collection tools for analyst deployment to on-site evidence collections.
- Developed forensic examination reports documenting evidentiary findings, technical

methodology, and conclusions in a format consistent with expert witness standards and legal proceedings.

- Static and dynamic malware analysis was conducted using REMnux, Detect It Easy, PEStudio, Procmon, Regshot, and ProcDOT to identify persistence mechanisms, dropped artifacts, system modifications, and malware execution behaviors.
- Behavioral analysis was performed in sandboxed virtual machine environments to document process execution flow, registry changes, file system modifications, and network communication indicators.

TECHNICAL SKILLS

- Malware Analysis and Reverse Engineering: REMnux, Detect It Easy (DIE), PEStudio, Process Monitor (Procmon), Regshot, ProcDOT
- Security Operations and Monitoring: Splunk Enterprise Security, Wireshark, Snort, NetWitness Investigator, Nessus, Metasploit, Nmap
- Scripting and Automation: Python, PowerShell, Bash, Go
- OSINT: VirusTotal, Shodan, PhishTank, WHOIS, Wayback Machine, PACER
- Additional Tools: Nuix, Volatility, Autopsy, EnCase, SQLite