https://www.envistaforensics.com/services/digital-forensics/

Example Discovery Items Pertaining to Mobile Device, Computers, and Cloud Service Forensics

Extracted or Collected Forensic Data Files believed to have been collected with FTK Imager, Tableau Imager, Linux Live Boot Disk, Cellebrite, XRY, GrayKey, or similar forensic extraction software to include but not limited to:

a. UFED Files, .BIN (Binary Files), .TAR, .ZIP, .E01, .AD1, .raw, .dd, or other archival or forensic image files
b. Evidence Log of all digital Evidence with full chain of custody for each item;
c. Complete Search Warrants, Affidavits for Search Warrants, Signed Consent to Search Forms, or documentation of exigent circumstances that were utilized to access, search and download these devices or data;
d. All data as originally produced by Cellebrite UFED (Universal Forensic Extraction Device) or other forensic analysis software to include the original folder structure and all files;
e. All exported reports in native format (i.e. PDF, Excel, HTML, UFDR, etc.);
f. Any passwords (security or encryption), PIN, pattern locks collected during the law enforcement investigation to unlock said devices;
g. Any Cellebrite Project files (.pas files);
h. Any Cellebrite Multiple Dumps (UFDX files);
i. All GrayKey files to include: Extraction Report (typically .pdf), Keychain.PLIST, Mem.zip, Passwords.txt, AFU.zip, or BFU.zip;
j. Any data in its originally produced state, produced by a third party in response to a request for Cloud data by Law Enforcement;
k. Any digital forensic exam reports such as but not limited to Encase, Axiom, FTK, IEF, BlackLight or XRY reports;
l. Any photographs taken of the device(s) at time of seizure and examination;
m. Any notes written by police regarding their handling, examination, or analysis of the digital evidence;
n. National Center For Missing and Exploited Children (NCMEC) cyber tip reports;
o. Internet Crimes Against Children (ICAC) cyber tip and/or referral reports;
p. Complete police investigative reports to include all supplementals, narratives, written or electronically held notes generated by investigators pertaining to the case against the defendant leading to the request for all search warrants and criminal charges.
q. Law Enforcement Peer To Peer/P2P/Bit Torrent Investigative Software files such as, but not limited to: ShareazaLE Summary Report for IP: “0.0.0.0”, Datawritten.xml, Details.txt, Downloadstatus.xml, Netstat.txt, Summary.txt, Torrentinfo.txt, SummaryLog.txt, DetailedLog.txt, IdentityLogging.txt, IdentitySignatures.xml

Please contact Digital Forensic Examiner Jake Green with any questions or new case inquiries.

jake.green@envistaforensics.com
(984) 269-2709