Common Digital Forensics Terms, Acronyms, and Certifications

CAS – See Cellebrite Advanced Services.

CCE – See Certified Computer Examiner.

CCME – See Cellebrite Certified Mobile Examiner.

CCO – See Cellebrite Certified Operator.

CCPA – See Cellebrite Certified Physical Analyst.

Cellebrite – a popular mobile digital forensics company.

Cellebrite Advanced Services (CAS) – a Cellebrite service that uses a secretive method to unlock or "crack" phones that could not be unlocked by standard mobile forensics tools. It was formerly referred to as Cellebrite Advanced Investigative Services (CAIS).

Cellebrite Certified Mobile Examiner (CCME) – "Cellebrite's top forensic examiner core certification which certifies that mobile device examiners have attained a level of mastery in the discipline of mobile device forensic investigation methodology and digital forensic analysis as well as a high degree of proficiency with Cellebrite Physical Analyzer software and a high level of working and practical knowledge regarding Cellebrite's UFED technology. CCME certification indicates that an investigator is a skilled mobile device examiner."[1]

Cellebrite Certified Operator (CCO) – an intermediate-level training course, focusing on using the Cellebrite UFED Touch suite of products and the Cellebrite Physical Analyzer software. This course is often paired with the Cellebrite Certified Physical Analyst (CCPA) training with the CCO course taken first. Cellebrite Certified Operator was formerly known as Cellebrite Certified Logical Operator (CCLO) and the older name may still appear on experts' curricula vitae.

Cellebrite Certified Physical Analyst (CCPA) – an advanced level course, focusing on using the Cellebrite Physical Analyzer software to recover, analyze, verify, and validate data extracted from mobile devices. The course also covers generating reports and advanced search techniques. The CCPA course is often paired with the Cellebrite Certified Operator (CCO) course, with the CCPA course taken after the CCO course.

Cellebrite Cloud Analyzer – a software program that preserves and obtains cloud-based content in a forensically sound manner, including email accounts, social media, file storage, and mobile device cloud backups.

Cellebrite Pathfinder – a software program that uses machine learning algorithms to identify patterns and connections in large amounts of data from multiple sources. Examples include, but are not limited to, finding contact connections across multiple devices, recognizing drugs or weapons in images, and discovering location patterns. It was formerly known as Cellebrite Analytics.

Cellebrite Physical Analyzer – a software program that opens extractions of mobile devices to enable the user to search through the data, analyze it, and generate reports.

Cellebrite Premium – an in-house version of Cellebrite Advanced Services, offered only to law enforcement, intelligence agencies, and the military. It was formerly known as Cellebrite UFED Premium.

Cellebrite UFED 4PC – a software program that enables a user to perform many of the same functions as Cellebrite UFED Touch to extract data from mobile devices but directly from their computer, instead of needing a separate specialized tablet.

Cellebrite UFED Reader – similar in appearance and function to Cellebrite Physical Analyzer, Reader is a free software program used to open UFED Reader reports, reports generated from mobile device extractions. A copy of the program should be included with a copy of the report. Reader allows for easier and more comprehensive review of reports, especially by comparison to PDF or printed reports. However, unlike Physical Analyzer, Reader can only open reports, not extractions, and is missing Analyzer's more advanced features.

Cellebrite UFED Touch – a tablet-sized device made by Cellebrite that can extract data from a wide variety of mobile devices. UFED is an acronym for Universal Forensic Extraction Device. The current model is known as the UFED Touch2. *See also* Cellebrite UFED 4PC.

Certified Computer Examiner (CCE) – a vendor neutral certification issued by The International Society of Forensic Computer Examiners (ISFCE). "The CCE testing process is designed to test an applicant's proficiency in several areas pertinent to digital forensics. The applicant is required to complete an online test and forensically examine three pieces of media, submitting a report after each examination."[2]

Cloud Storage – "a third-party service provides hard drive space on the Internet for people and businesses to store data."[3]

Digital Forensics – "the collection, preservation, analysis, and presentation of electronic evidence for use in a legal matter using forensically sound and generally accepted processes, tools, and practices."[4]

EnCase – a popular digital forensic software by OpenText (formerly Guidance Software). While Encase can be used for mobile devices (like cell phones), it is most commonly used to image and analyze traditional computer hard drives (like those from a desktop or laptop computer).

EnCase Certified Examiner (EnCE) Certification – the "certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase software during complex computer examinations."[5]

EnCE – See EnCase Certified Examiner Certification.

Extraction – the process of copying data from a mobile device and the resulting files.

Faraday Bag (or Box) – a bag (or box) that prevents signals from being received or emitted by any electronic devices contained therein. It is used to store or transport electronic devices, ensuring that data and information cannot be sent from the contained device nor can any changes be made to the device remotely (e.g. the data on a cell phone in a Faraday bag or box cannot be remotely deleted). The name Faraday derives from scientist Michael Faraday.

GrayKey – a law enforcement only device made by Grayshift that uses a secretive technique to unlock or "crack" phones that cannot be unlocked by standard mobile forensics tools. Previously it only supported iPhones, but it recently added support for Android phones.

Grayshift – A mobile digital forensics company, known for its GrayKey product. Grayshift has recently partnered with Magnet Forensics.

Hash Value – sometimes referred to as a "digital fingerprint," a hash value is a numerical value used to identify a file. The hash value is the result of a file being processed through a particular mathematical function, such as MD5 or SHA1.

Image – (1) a visual representation of something. (2) "An exact bit-stream copy of all electronic data on a device, performed in a manner that ensures the information is not altered."[6]

MAC Times – modified, access, and created dates and times for a file, found in the file's metadata.

Magnet Axiom – Magnet Forensics' flagship product, used for traditional computer, mobile, and cloud digital forensics investigations.

Magnet Certified Forensic Examiner – "an accreditation that showcases an examiners' expert-level competence with Magnet Forensics products to peers, internal stakeholders and external audiences, including legal teams or clients."[7]

Magnet Forensics – a digital forensics company that originally focused on traditional computer forensics (desktops and laptops) but has branched out into mobile digital forensics and become the main competitor to Cellebrite over the last few years. In early 2019, Magnet, in a partnership with Grayshift, began offering the GrayKey product but only to its law enforcement customers.

MCFE – See Magnet Certified Forensic Examiner.

Metadata – data that describes and gives information about other data.

Oxygen Forensics – a mobile digital forensics company

Oxygen Forensic Detective – Oxygen Forensics' flagship product, which includes support for traditional computers, mobile devices, and cloud storage.

UFED – abbreviation for Universal Forensic Extraction Device. See Cellebrite UFED 4PC and Cellebrite UFED Touch.

Unallocated Space – "The area of computer media, such as a hard drive, that does not contain readily accessible data. Unallocated space is usually the result of a file being deleted. When a file is deleted, it is not actually erased but is simply no longer accessible through normal means. The space that it occupied becomes unallocated space, i.e., space on the drive that can be reused to store new information. Until portions of the unallocated space are used for new data storage, in most instances, the old data remains and can be retrieved using forensic techniques."[8]

---

[1] Cellebrite: Global Training Division, *Cellebrite Certification Policy*, GTD-CCP-Ver 1.3 [Nov. 3, 2020], available at https://www.cellebritelearningcenter.com/mod/page/view.php?id=31199 [last accessed Apr. 21, 2021].

[2] The International Society of Forensic Computer Examiners, *Certified Computer Examiner: CCE Competencies*, ISFCE.com, available at https://www.isfce.com/competencies.htm [last accessed Apr. 21, 2021].

[3] Larry Daniel & Lars Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, p. 4, Elsevier, Inc. [2012].

[4] Larry Daniel & Lars Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, p. 3, Elsevier, Inc. [2012].

[5] OpenText, *EnCase Certified Examiner (EnCE) Certification Program*, OpenText.com, available at https://www.opentext.com/products-and-solutions/services/training-and-learning-services/encase-training/examiner-certification [last accessed Apr. 21, 2021].

[6] National Institute of Standards and Technology, *Guidelines on Mobile Device Forensics, Appendix B: Glossary*, NIST Special Publication 800-101, Revision 1 [May 2014], available at https://doi.org/10.6028/NIST.SP.800-101r1 [last accessed Apr. 21, 2021].

[7] Magnet Forensics, *Magnet Certified Forensics Examiner – AXIOM – Magnet Forensics*, Training.MagnetForensics.com, available at https://training.magnetforensics.com/w/courses/25-magnet-certified-forensics-examiner-axiom [last accessed Apr. 21, 2021].

[8] The Sedona Conference, *The Sedona Conference Glossary: eDiscovery & Digital Information Management*, Fifth Edition, 21 SEDONA CONF. J. 263 [2020], available at https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary [last accessed Apr. 21, 2021].