Anlage 2

REPORTER OHNE GRENZEN

Technische Einschätzungen zu verschlüsselungsbrechender Mobilforensik-Software

Viktor Schlüter, Janik Besendorf

Inhalt

1 Technische Einschätzungen zu Cellebrite

Im Folgenden sollen diese Fragen erörtert werden:

- Sind Analyseergebnisse von Forensiksoftware wie Cellebrite manipulationssicher?
- Ist es wahrscheinlich, dass eine Manipulation mit den üblichen Auswertungsmethoden von Strafverfolgungsbehörden entdeckt werden würde?
- Könnte eine Manipulation in einer späteren, unabhängigen Untersuchung aufgeklärt werden?
- Inwiefern beeinträchtigt die Auswertung eines Mobiltelefons mit Forensiksoftware den Besitzer oder die Besitzerin?

1.1 Sind Analyseergebnisse von Forensiksoftware wie Cellebrite manipulationssicher?

Um diese Frage zu beantworten, muss zunächst betrachtet werden wie eine Forensiksoftware (wir bspw. Cellebrite oder Magnet Forensics) funktioniert. Die Forensik-Software liest Daten über ein Datenkabel von Smartphones aus. Gegebenenfalls werden vorher Sicherheitslücken ausgenutzt um Verschlüsselung oder Authentisierung zu umgehen. Deshalb muss das Mobiltelefon im Besitz der Strafverfolgungsbehörde sein.

Nachdem das Mobiltelefon an das Auswertungssystem angeschlossen wird, muss von dem*der Beamt*in ausgewählt werden, um welches Model und um welche Software-Version es sich bei dem Mobiltelefon handelt. Die Auswertungssoftware verfügt über Informationen, für welche Modelle und Versionen Angriffswerkzeuge (Exploits) vorhanden sind.

Moderne Geräte sind heutzutage meist mit einem verschlüsselten Datenspeicher ausgestattet. Damit ist es bei allen aktuellen Geräten nicht mehr möglich, auf die Daten zuzugreifen, ohne die Sicherheitsmechanismen des Gerätes zu überwinden. Für das Überwinden bietet die Analysesoftware nun verschiedene Angriffswerkzeuge an.

Bei modernen Smartphones wird der Datenspeicher beim Anschalten entschlüsselt. Dies passiert mit der Eingabe des Sperrcodes durch die nutzende Person: Somit wird verhindert, dass Fremde auf die Daten zugreifen können, die nicht den Sperrcode kennen. Deshalb gibt es zwei verschiedene Orte, an denen die Forensiksoftware ansetzen kann, um die Verschlüsselung des Smartphones zu überwinden:

1. Ein Ansatz ist die Zeitsperre nach der Eingabe von einer gewissen Anzahl falscher Sperrcodes zu umgehen. Anschließend kann der Sperrcode ermittelt werden, indem alle möglichen Sperr-Codes automatisiert ausprobiert werden (Brute-Force Angriff).
2. Andere Angriffe interagieren über die USB- oder Lightning-Schnittstelle mit dem Smartphone und nutzen dort eine Sicherheitslücke aus.

Ziel des Angriffs ist es, sogenannte Root-Rechte zu erlangen. Diese sind vergleichbar mit einem Administrator-Konto auf einem Computer. Denn erst mit diesem Berechtigungslevel hat man Zugriff auf alle Daten auf dem Smartphone-Speicher.

Um diese Root-Rechte zu erlangen, muss zuerst der Schutz vor dem unbefugten Ausführen von Programmcode umgangen werden. Falls der Prozess, in dem nun Code ausgeführt wird, nicht mit Root-Rechten ausgeführt wird, muss in einem zweiten Schritt eine weitere Komponente des Betriebssystems erfolgreich angegriffen werden, um erweiterte Rechte zu erlangen. Diese Sicherheitsmechanismen sind wichtig für die Nutzer*innen des Smartphones und sollen vor unbefugtem Zugriff auf die Daten auf dem Smartphone schützen.

Wenn nun die Root-Rechte erlangt wurden, dann wird üblicherweise ein Dateisystem-Abbild des Smartphones erstellt, auf englisch als “full file system image” bezeichnet und von Cellebrite oft als FFS (“EXTRACTION_FFS.zip”) abgekürzt.

Mit dem Erlangen von Root-Rechten verlieren alle Sicherheitsmechanismen ihre Wirksamkeit, die den Datenspeicher des Smartphones vor Veränderung und Manipulation schützen: Prozesse mit Root-Berechtigung können alle Dateien auf dem System lesen und verändern. Weil diese Root-Berechtigungen zwingend nötig sind, um ein Dateisystem-Abbild des Smartphones zu erstellen, wäre Forensiksoftware - technisch gesehen - auch in der Lage Dateien auf dem Smartphone zu erstellen. Natürlich kann die Manipulation auch stattfinden, indem die Forensiksoftware lediglich bei der Ausgabe des Dateisystem-Abbilds Details verändert, dies wäre aber deutlich leichter festzustellen. In einer zweiten, unabhängigen Analyse könnten die Inhalte der Dateien der zwei Dateisystem-Abbilder verglichen werden und die Manipulation des ersten klar festgestellt werden. Um die Frage nach der Manipulationssicherheit zu beantworten, betrachtet dieser Text ausschließlich solche Manipulationsansätze, welche möglichst schwierig nachvollziehbar sind.

Mit Root-Rechten wäre die Forensiksoftware ebenfalls in der Lage, die Veränderung von Dateien zu verschleiern, indem sie den Zeitstempel der letzten Veränderung der Datei manipuliert, damit nicht ersichtlich wird, dass die Datei von der Forensiksoftware verändert wurde. Bei Dateien, die auch ohne Root-Rechte verändert werden können, können Nutzer*innen auch selber die Zeitstempel verändern. Hier gibt es allerdings die Möglichkeit, dass das vermeintliche Ereignis auf dem Smartphone auch Spuren in Dateien hinterlässt, die nur mit Root-Rechten einseh- und veränderbar sind. In diesem Fall könnte die Zeitstempelmanipulation von Nutzer*innen leicht erkannt werden, die Manipulation von Zeistempeln mit Root-Rechten ist aber erkennbar, vorausgesetzt dass sie ausreichend gut vorgenommen wird.

Es gäbe hierbei theoretisch zwei Wege, auf die eine Manipulation stattfinden könnte:

1. Ein*e Beamt*in könnte die Forensiksoftware verwenden um Inhalte auf dem Smartphone zu verändern. Ob und welche Forensiksoftware-Produkte dazu in der Lage sind, ist dem Autor dieses Textes nicht abschließend bekannt, allerdings sind die Produkte technisch

dazu in der Lage: Für das vollständige Auslesen des Dateisystem-Abbilds sind die gleichen Root-Berechtigungen notwendig wie für das beliebige Verändern des Dateisystems. Nachdem das Smartphone verändert wurde, würde der*die Beamt*in in einem zweiten Schritt eine Forensiksoftware verwenden, um ein Dateisystemabbild zu erstellen.

2. Der Hersteller der Forensiksoftware könnte in der Software Funktionen einbauen, die bei bestimmten Smartphones die ausgegebenen Daten verändern. Hierbei würde die Software Root-Rechte erlangen, die Dateien auf dem Gerät verändern und abschließend ein Dateisystemabbild erstellen. Das scheint unwahrscheinlich, aber es kann aber nicht vollständig ausgeschlossen werden, da der Programmcode von Cellebrite nicht einsehbar ist (auch “Closed Source” oder proprietäre Software genannt).

In beiden Fällen würde die Forensiksoftware ein reguläres Dateisystemabbild ausgeben und darstellen. Diese würden allerdings den Datenstand nach der Manipulation und nicht den ursprünglichen Zustand des Gerätes widerspiegeln.

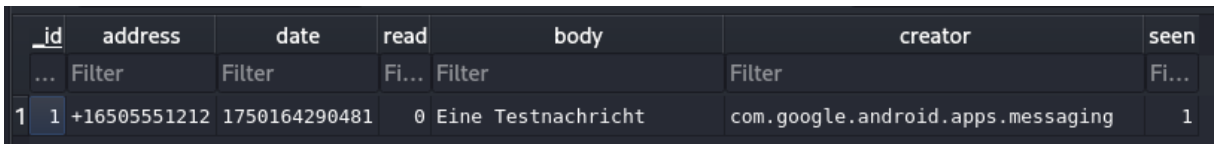
1.2 Ist es wahrscheinlich, dass eine Manipulation mit den üblichen Auswertungsmethoden von Strafverfolgungsbehörden entdeckt werden würde?

Die genaue Arbeitsweise von Ermittlungsbehörden ist nicht öffentlich bekannt, deshalb lässt sich diese Frage nicht mit abschließender Sicherheit beantwortet.
Allerdings gibt es anerkannte Kurse für die forensische Analyse von Smartphones, die von vielen Mitarbeitenden von Strafverfolgungsbehörden besucht werden. Ein Beispiel hierfür ist der Kurs zu mobiler Forensik des SANS-Insituts. Daher können auf Basis dieser Kurse Annahmen über die Arbeitsweise getroffen werden, auf dessen Grundlage die folgenden Überlegungen angestellt werden.

Die folgende Betrachtung bezieht sich in ihren Beispielen auf Android-Mobiltelefone, ist für iOS Geräte aber ebenso gültig.

Eine Manipulation auf einem Smartphone festzustellen ist nicht trivial: Die Daten sind meist in sog. SQLite Datenbanken gespeichert und nicht kryptographisch signiert. Damit ist es nicht leicht festzustellen, ob ein Eintrag vom Gerät selbst vorgenommen wurde oder später verändert wurde.

In der folgenden Abbildung ist angezeigt, wie eine Beispiel-SMS in der Android-SMS Datenbank abgespeichert wird. Die Datenbank befindet sich am Pfad */data/com.android.providers.telephony/databases/mmssms.db* (zur besseren Übersichtlichkeit wurden einige Spalten ausgeblendet) Es gibt keine Spalte, in der eine kryptografische Signatur dieses Datenbankeintrags enthalten ist, die Nachricht kann mit Root-Zugriff ohne weiteres geändert werden ohne dass die Veränderung feststellbar ist. Jedes Programm, welches mit Root-Rechten auf das Android-Smartphone zugreifen kann, könnte die Veränderung also durchführen, technisch gesehen also auch eine Forensiksoftware.



	_id	address	date	read	body	creator	seen
	...	Filter	Filter	Fi...	Filter	Filter	Fi...
1	1	+16505551212	1750164290481	0	Eine Testnachricht	com.google.android.apps.messaging	1

Figure 1: Eine Beispiel-SMS in der Datenbank mmssms.db

Um eine Manipulation zu bemerken, müsste von den analysierenden Strafverfolgungsbeamt*innen also eine Analysetechnik angewendet werden, die geeignet ist, eine solche Manipulation aufzudecken. Welche Möglichkeiten es dafür gibt wird im Folgenden betrachtet.

Wenn durch eine Manipulation keine kryptografische Signatur ungültig wird, kann nur durch Analyse weiterer Daten eine Manipulation festgestellt werden: Metadaten und Inhaltsdaten, wobei auch Zusammenhänge zwischen unterschiedlichen Dateien betrachtet werden können.

Manipulationserkennung durch Analyse der Metadaten Die relevanten Metadaten sind im Fall des Android Dateisystems die Zeitstempel von Dateien und Ordnern. Falls also zu Manipulationszwecken eine Datei verändert wird, könnte durch die Analyse identifiziert werden, dass sich eine Unstimmigkeit in der Relation der Zeitstempel des Dateisystems ergibt. Das könnte zum Beispiel bemerkt werden, falls bekannt ist, dass zwei Dateien von Android immer gleichzeitig geändert werden. Wenn am Zeitstempel der letzten Änderung ersichtlich wird, dass nur eine Datei zu einem gewissen Zeitpunkt geändert wurde, aber eine andere nicht, kann damit die Manipulation erkannt werden. Ein anderes Beispiel wäre, wenn eine Log-Datei einen Eintrag enthält der später datiert ist als der “zuletzt modifiziert”-Zeitstempel der Datei selbst. Weil das Hinzufügen des Log-Eintrags auch die Datei geändert haben muss, läge auch hier eine Manipulation nahe.

Allerdings kann diese Erkennung leicht verhindert werden: Da für die angenommenen Manipulationsszenarien ohnehin Schreibberechtigungen für das ganze Dateisystem vorhanden sind, kann ebenfalls der Zeitstempel der Dateien so angepasst werden, dass die Manipulation nicht in den Metadaten erkennbar ist. Somit könnte eine wenig aufwändige Manipulation erkannt werden, eine hochentwickelte Manipulation könnte aber nicht erkannt werden.

Manipulationserkennung durch Analyse der Inhaltsdaten Auch durch die Analyse der Inhaltsdaten von Dateien auf dem Android-Smartphone kann versucht werden, eine Manipulation zu erkennen. Ähnlich wie bei der Analyse der Metadaten würde hierbei untersucht, ob es in den Inhalten der forensisch relevanten Dateien Unstimmigkeiten gibt. Beispielsweise könnte erkannt werden, ob ein Foto auf dem Smartphone platziert wurde und nicht mit dem Smartphone selbst aufgenommen wurde.

Hierbei würde eine Analyse der Datei */data/com.google.android.apps.photos/databases/gphotos-1.db* helfen die Manipulation aufzudecken. In ihr sind, wie in der folgenden Abbildung dargestellt, die Zeitstempel aller mit dem Smartphone aufgenommenen Fotos enthalten:

utc_timestamp	duration	filename	filepath
Filter	Filter	Filter	Filter
1716905897000	113451	Lyle-Lyle-Crocodile_HD_Stereo.mp4	/storage/emulated/0/Movies/Lyle-Lyle-…
1716905895000	*NULL*	SceneDetection-Food.jpg	/storage/emulated/0/Pictures/SceneDetection-Food.jpg
1716905895000	*NULL*	SceneDetection-Pet.jpg	/storage/emulated/0/Pictures/SceneDetection-Pet.jpg
1716905895000	*NULL*	21-9_WallOfFlowers.jpg	/storage/emulated/0/Pictures/21-9_WallOfFlowers.jpg
1716905894000	*NULL*	NightShot.jpg	/storage/emulated/0/Pictures/NightShot.jpg
1750259395000	*NULL*	20250618_170953.JPG	/storage/emulated/0/DCIM/CAMERA/20250618_170953.JPG
1750259391000	*NULL*	20250618_170949.JPG	/storage/emulated/0/DCIM/CAMERA/20250618_170949.JPG

Figure 2: Auszug der “gphotos-1.db”-Datenbank von einem Android-Gerät

Falls nun im Ordner */sdcard/DCIM* Fotos enthalten sind, die nicht in der gphotos-1.db gelistet sind, so kann geschlussfolgert werden, dass diese nicht auf dem Smartphone selber aufgenommen wurden.

Allerdings könnte auch diese Analysetechnik durch eine aufwändige Manipulation unmöglich gemacht werden: Wenn alle notwendigen Dateien verändert werden, so dass die Beziehung deren Inhalte untereinander nicht von einer tatsächlichen Eintragung des Android-Systems zu unterscheiden wären.

Natürlich lassen sich auch diese beiden Ansätze kombinieren. So stellt etwa ein Paper aus dem Jahr 2015 Ansätze vor, in denen Einträge aus Datenbanken mit bekannten, gleichzeitig auftretenden Dateisystemänderungen korreliert werden. Wenn nicht beide Ereignisse vorhanden sind, so wird die Manipulation erkannt.

Die Erfolgsaussichten zum Erkennen einer Manipulation hängen also davon ab, welcher Akteur das bessere Wissen über gutartiges und authentisches Verhalten von Android-Systemen hat: Die Person, die die Manipulation durchführt, oder die Person, die bei den Strafverfolgungsbehörden den Datensatz auf eine Manipulation untersucht. Es ist also durchaus wahrscheinlich, dass eine hochentwickelte Manipulation sehr schwer oder überhaupt nicht erkannt werden kann.

1.3 Könnte eine Manipulation in einer späteren, unabhängigen Untersuchung aufgeklärt werden?

Hierbei gibt es verschiedene Szenarien zu unterscheiden, wie die Manipulation durchgeführt wird:

1. Durch aus der Ferne installierte Schadsoftware wird auf dem Smartphone die Manipulation vorgenommen. Später analysiert eine Strafverfolgungsbehörde das Smartphone und erfasst die Daten inklusive der Änderungen, die im Rahmen der Manipulation durch die Schadsoftware vorgenommen wurden. Dieser Fall wurde in den vorherigen Fragen nicht behandelt, weil es sich hier nicht um eine Manipulation *durch* die Forensiksoftware handelt, aber trotzdem die Nachvollziehbarkeit eines zurückliegenden Angriffs durch die Verwendung von Forensiksoftware eingeschränkt wird.
2. Mit den Angriffswerkzeugen einer Forensiksoftware wird die Verschlüsselung des Smartphones gebrochen und die Manipulation vorgenommen. Später verwendet eine Strafverfolgungsbehörde ein weiteres mal eine Forensiksoftware um ein Dateisystem-Abbild des Smartphones zu erstellen. Hier werden alle Daten inklusive der Änderungen erfasst, die im Rahmen der Manipulation vorgenommen wurden.
3. Eine Forensiksoftware wird vom Hersteller so programmiert, dass es in bestimmten Fällen, beispielsweise bei Smartphones die eine bestimmte Mobilfunknummer benutzen, die Daten auf dem Smartphone erst verändert und dann die Analyseergebnisse auf Basis der veränderten Daten ausgibt.

   Für alle drei Fälle gilt: Sollte im Nachhinein eine unabhängige Stelle das Smartphone ein weiteres mal analysieren und die Daten kopieren, so erhält auch sie den Datensatz inklusive der Veränderungen durch die Manipulation. Die unabhängige Stelle hat dabei keine Möglichkeit, sicher nachzuvollziehen, dass die Daten auf dem Smartphone verändert wurden. Sie kann lediglich die Analysemethoden anwenden, die im Rahmen der letzten Frage vorgestellt wurden. Da diese aber durch eine technische anspruchsvolle Manipulation schwierig bis unmöglich gemacht werden gilt: Die spätere Untersuchung einer unabhängigen Stelle kann nicht sicher feststellen, ob eine Manipulation der Daten auf dem Smartphone stattgefunden hat. Ausschließlich Manipulationen, die nicht vollständig durchdacht sind, können erkannt werden.

1.4 Inwiefern beeinträchtigt die Auswertung eines Mobiltelefons mit Forensiksoftware den Besitzer oder die Besitzerin?

Da bei der Auswertung eines Mobiltelefons durch eine Forensiksoftware die Sicherheitsmechanismen des Geräts gebrochen werden, kann eine Verschleierung vorheriger Angriffe stattfinden: Falls vor oder nach der Auswertung des Mobiltelefons durch Strafverfolgungsbehörden eines der folgenden Szenarien eingetreten ist, so können diese schlechter oder nicht mehr nachvollzogen werden.

1. Das Mobiltelefons wurde durch andere Behörden, beispielsweise bei der Einreise in ein anderes Land mit Forensiksoftware analysiert.

2. Das Mobiltelefon wurde durch Spähsoftware angegriffen, wie etwa Pegasus von der NSO Group

Die Verschleierung der Spuren der früheren Angriffe auf das Mobiltelefon kommt dabei so zustande, dass solche Angriffe oft Spuren hinterlassen, die teilweise aber nicht mehr zeitlich zugeordnet werden können. Eine vergleichbare Analogie wäre das Aufbrechen eines Türschlosses: Es ist einfach festzustellen, ob eine Tür mit Gewalt geöffnet wurde, aber deutlich schwerer, festzustellen, ob die Tür zuerst von einer Partei und danach von einer zweiten Partei mit Gewalt geöffnet wurde. Sehr ähnlich können auch auf Mobiltelefone unterschiedliche Angriffe Spuren hinterlassen, die aber nicht eindeutig dem einen oder anderen Angriff zugeordnet werden können. Dadurch erschwert die Anwendung von Forensiksoftware die Analyse bereits geschehener Angriffe auf das Gerät. Technisch betrachtet sind sowohl das Brechen der Sicherheitsmechanismen durch eine Forensiksoftware als auch die Infizierung eines Geräts durch Spähsoftware als Angriffe zu qualifizieren, welche forensisch nur schwer zu unterscheiden sind.