SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Herausforderungen bei der digitalen Spurensuche auf Smartphones

Autor : Andreas Habegger

Datum : 2. April 2019

Die Smartphone-Forensik ist ein relativ junges, sich sehr rasant weiter entwickelndes Interessengebiet, innerhalb der digitalen Forensik. Die Markteinführung von "Simon", dem ersten Smartphone aus dem Hause BellSouth und IBM, führte 1995 noch nicht zur Geburtsstunde der Smartphone-Forensik im heutigen Sinne. Dies sollte sich noch einige Jahre hinziehen, nämlich bis zur Markteinführung des ersten iPhones 2007.

Es war diese Technologie, welche in der Gesellschaft einen Wandel auslöste, hin zu der heutigen Digitalen Gesellschaft. Die klassische SMS oder der traditionelle Telefonanruf werden heute zunehmend verdrängt durch andere Arten des Informationsaustausches. Zwei Beispiele für die Kommunikationsformation der heutigen Zeit sind die Videotelefonie und der Austausch von Standortdaten. Mit diesen zwei neuen Möglichkeiten können wir Nachrichten mit grösserem Informationsgehalt einfacher und schneller erstellen. Aktuelle Geräte können weit mehr als nur

Nachrichten im klassischen Sinn austauschen. Da sie eine Vielzahl von Sensoren enthalten, sind sie kleine Alltagshelfer, die wir gerne bei uns haben und vielseitig einsetzen. Dies führt nun dazu, dass die Geräte eine riesige Sammlung von sensiblen Daten über ihre Besitzer enthalten.

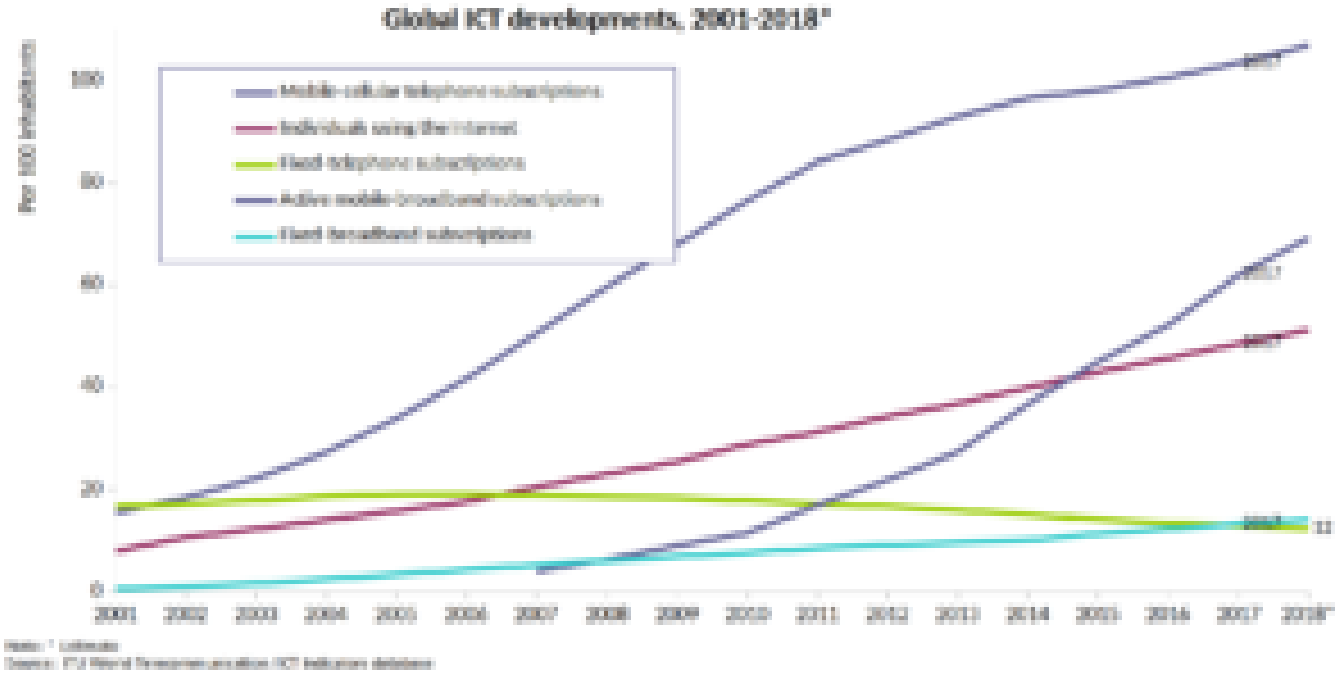

Abb. 1: Globale Entwicklung des ICT-Marktsegments

Sensible Nutzerdaten

Angesichts des Tempos, mit welchem die Entwicklung in den letzten Jahren fortgeschritten ist, ist auch die Notwendigkeit einer forensischen Untersuchung solcher Geräte gegeben. Von Interesse sind die gespeicherten, sensiblen Nutzerdaten, welche entscheidend zum Erfolg einer Untersuchung beitragen können. Somit versteht man unter diesem Teilgebiet der Digitalen-Forensik das Sicherstellen, die Wiederherstellung und Analyse von digitalen Informationen in der kriminalistischen Untersuchung. Zentral ist die Wahrung der Integrität der Daten. Damit die verborgenen Informationen extrahiert werden können, braucht es eine Vielzahl verschiedener Techniken [1]. Welche adäquate Technik im konkreten Fall anzuwenden ist, wird durch die Spezialisten entschieden. Der Entscheid basiert auf einem grossen Fundus an Erfahrungen und beeinflusst den Erfolg einer Ermittlung stark.

4 Verfahren für die Datenextraktion

Es werden mehrheitlich vier Arten zur Datengewinnung unterschieden.

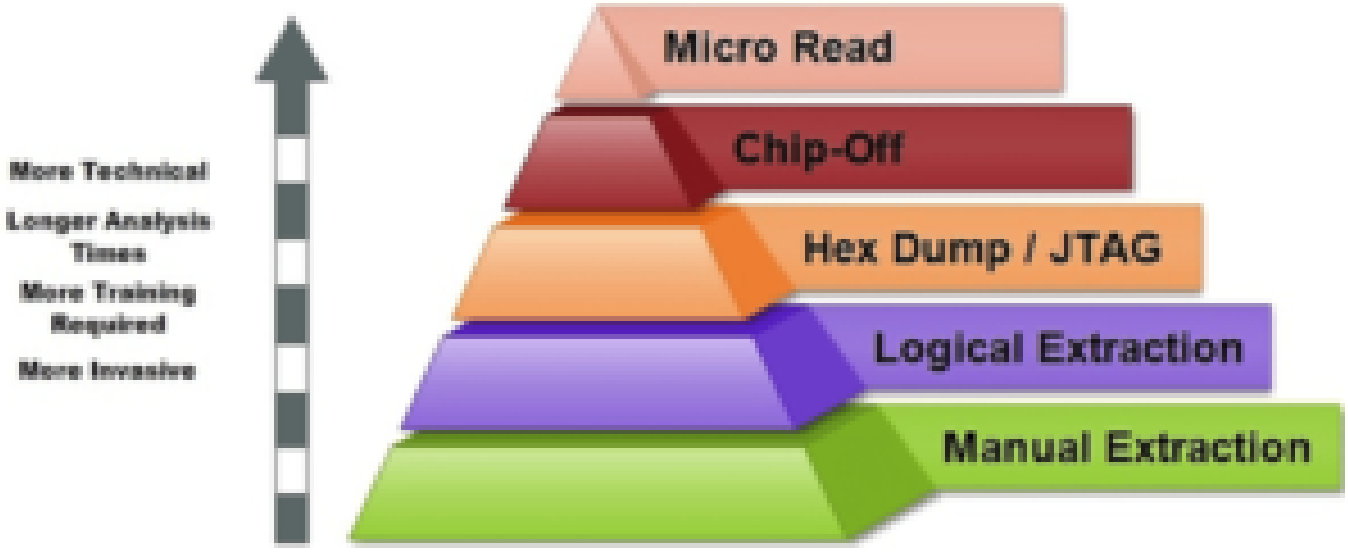

Abb. 2: Mobile Forensik, Pyramide der Verfahrensklassen, [3]

Die Letzte, die "Physische Datenextraktion", werden wir etwas vertiefter betrachten. Dabei gibt es verschiedene Kriterien, wie die Methoden verglichen werden können. In diesem Beitrag werden wir uns einer rein technischen Betrachtung zuwenden und andere Aspekte nicht einbeziehen.

Ein erstes Verfahren nutzt die Tatsache, dass heutige Geräte umfassende Cloud-Backups erzeugen. Hierbei kann der Ermittler bei vorhandenen Zugriffsdaten ein Abbild, der in der Cloud gespeicherten Information beschaffen. Diese Methode bezeichnen Fachleute als "Over-the-air Datenextraktion". Sie bietet eine relativ bescheidene Tiefe an Informationen. Ein besonderer Nachteil ist, dass gelöschte oder nicht in der Cloud gespeicherte Daten dem Ermittler vorenthalten bleiben. Um diesen Nachteil zu mindern kommt eine weitere Variante zum Einsatz, welche als «Logische Datenextraktion» bezeichnet wird. Diese Technik nutzt die offline Backupfähigkeit gängiger Geräte aus, um an Daten zu gelangen. Hierzu muss das zu untersuchende Gerät mit einer Auslesestation direkt verbunden sein. Oft sind anschliessend noch spezielle Einstellungen notwendig, wie zum Beispiel das aktivieren von Softwareschnittstellen. Um solche Softwareschnittstellen aktivieren zu können, braucht es den Zugriff auf die Geräteeinstellungen. Dies kann meist nur mit bekanntem Zugangscode oder einer Sicherheitslücke im System realisiert werden. Diese Methode ist weit verbreitet und daher sind auch viele standardisierte Prozeduren bekannt und erprobt. Dies wirkt sich äusserst positiv auf die Effizienz und Reproduzierbarkeit aus. Auf dem Markt gibt es einige Hersteller, die genau hier ansetzen und Tool-Kits anbieten. Die bekanntesten, um nur einige zu nennen, sind Cellebrite UFED [5], Micro Systemation [6] und Oxygen Forensic Suite [7]. Diese Werkzeuge haben einige Vorteile, wie zum Beispiel den mobilen Einsatz, das zeitnahe Extrahieren und automatisierte Analysieren der Daten hinzu kommt die intuitive und einfache Bedienbarkeit.

Methode abhängig vom Smartphone

Dem kritischen Leser ist sicherlich aufgefallen, dass die genannten Verfahren nicht in allen Fällen zum Erfolg führen werden. Eine besondere Knacknuss stellen gelöschte Daten oder sehr stark beschädigte Geräte dar. Denn oft sind es diese Informationsstücke, die einen zusätzlichen Hinweis enthalten, um eine entscheidende Rolle bei der Begründung der Evidenz einzunehmen. Ein Gerät, das auf Werkseinstellungen zurück gesetzt worden ist – unter Umständen willentlich, enthält sehr viele Daten die logisch gelöscht, jedoch physisch vorhanden sind. Um nun in solchen Situationen richtig zu verfahren braucht es besondere Fertigkeiten. Dies führt uns nun zur Diskussion der Verfahren welche auf der Methode der "Physischen Datenextraktion" basieren. Sie stellen hohe Anforderungen an die Methodik, die Werkzeuge und die Kompetenz der Spezialisten. Besonders weil sich die Technologie sehr schnell weiter entwickelt. Ein neues Geräte basiert mehrheitlich auf den neusten Speicher- und Mobile-Prozessorentechnologien. Eine weitere Hürde stellt die Integrationsdichte sowie die Zugänglichkeit an konkreten Informationen zum Aufbau und den Bauelementen eines Geräts dar.
Die physische Datenauslesung kann in zwei Hauptgruppen unterteilt werden. Bei den einen Verfahren handelt es sich um sogenannt destruktive Extraktionsmethoden wobei die andere Gruppe die nicht-destruktiven vereint.

Extrahieren via JTAG-Schnittstellen

Eine gängige nicht-destruktiv Methode bedient sich der JTAG Schnittstelle von Integrierten Schaltungen (IC). Der Name JTAG ist ein Akronym für Joint Test Action Group, was wiederum eine gängige Bezeichnung für den IEEE-Standard 1149 [12].1 ist. In diesem Standard wird eine Methode für das Testen und Debuggen von ICs direkt auf der Leiterplatte definiert. Das nun resultierende Extraktion-Prozedere über die JTAG Schnittstelle ist der sogenannte Boundary Scan Test nach IEEE 1149.1, welcher ein Auslesen der internen Zustände eines ICs ermöglicht. ICs, die JTAG fähig sind, besitzen daher zusätzliche Schaltungslogik, die im Normalbetrieb vollkommen abgetrennt ist und somit die Funktion des Bauteils nicht beeinflusst. Erst nach der Aktivierung der JTAG-Funktion an einem bestimmten Pin, dem TMS (Test Mode Select) Eingang, kann mit Hilfe dieser zusätzlichen Funktionalität das Hardwaresystem beeinflusst werden. Dies ermöglicht zu Test- und Analyse-Zwecken die internen Zustände der Speicherzellen auszulesen oder zu verändern.

Was ohne Schnittstellen funktioniert

Da gewisse Mobile-Geräte Hersteller bewusst auf dieses Verfahren zum Hardware Test verzichten oder diese Schnittstellen dauerhaft deaktivieren, braucht es weitere Methoden. Eine vielversprechende aber auch anspruchsvolle Methode ist das "Chip-Off". Beim "Chip-Off" handelt es sich um eine Datenextraktion, bei der das Gerät zerstört wird. Dabei werden die relevanten ICs physisch von der Geräteplatine entfernt, um diese direkt über ihre standardisierte Schnittstelle anzusprechen [8, 9]. Hierzu werden verschiedene Lese- und Schreibgeräte verwendet. In gewissen Fällen müssen sogar massgeschneiderte Verfahren

konzipiert und entwickelt werden, damit exotische Speicher IC’s auslesbar werden. Beim "Chip-Off" Verfahren ist das Ablösen des Speicher ICs der kritische Schritt. Um diesen möglichst schonend zu vollziehen, gibt es verschiedene Möglichkeiten. Eine besteht darin, die Platine gerade ausreichend stark zu erhitzen, so dass die Lötverbindung zwischen Platine und dem zu untersuchenden Bauelement aufgetrennt werden kann. Die präzise Einhaltung von Temperaturprofilen ist dabei ein zentrales Element. Wenn dies nicht gelingt, werden die Daten unter Umständen verändert oder die Speicherzelle vollständig zerstört [10, 11]. Eine thermische Zerstörung ist irreparabel und führt zum vollständigen Verlust der Daten.

Nutzen für kriminalistische Untersuchungen

Nach der physischen Extraktion liegen die Daten als Binäres-Speicherabbild vor. Ein solches Speicherabbild muss weiterverarbeitet werden, bis schlussendlich die Informationen in geeigneter Form vorliegen. Es ist dann diese Information, die in einer kriminalistischen Untersuchung zur Begründung von Evidenz verwendet wird.

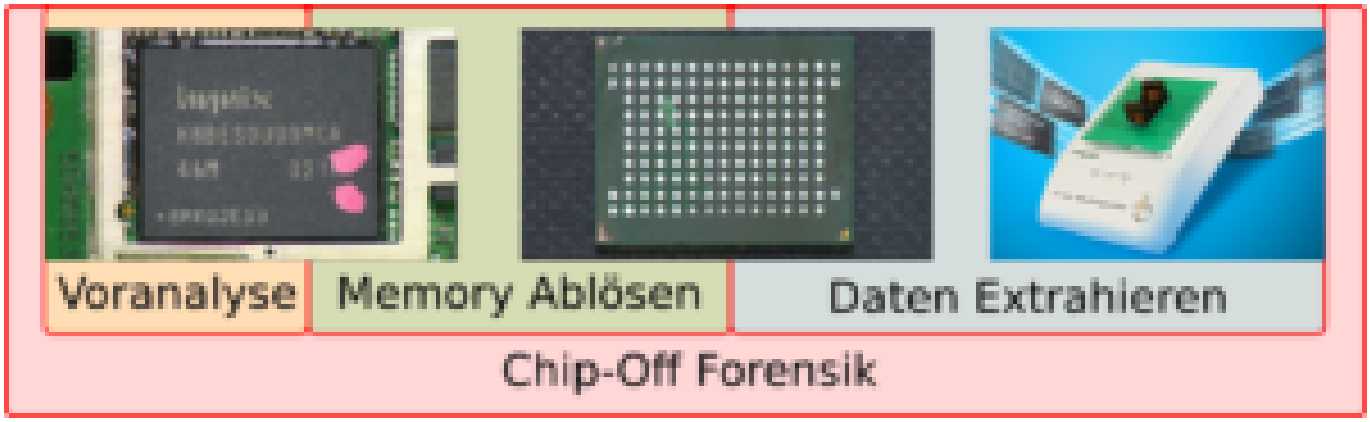

Abb. 3: Die drei Phasen eines Chip-Off-Prozesses [4]

Im jeweiligen Fall die richtige Methode zu wählen, erfordert viel Erfahrung. Besonders bei den physischen Verfahren, wo zudem eine hohe technische Fachkompetenz in Kombination mit Verfahrenskreativität gefordert ist. Für die Spezialisten ist das Besondere an diesen Herausforderungen die Null-Fehlertoleranz. Die spezifischen Daten in einer Ermittlung sind immer einzigartig und daher wertvoll.

Referenzen

1. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
2. Mobile Forensics: Investigation Process Model (DFRWS 2003)
3. Guidelines on Mobile Device Forensics

4. https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/
5. A. Habegger, Ausbau und Sicherung von Speicher-Chips, 11. Nationalen IT-Ermittler Tagung in Bern, 2015
6. https://www.cellebrite.com/de/products/ufed-ultimate-de/
7. https://www.msab.com/
8. https://www.oxygen-forensic.com/en/products/oxygen-forensic-kit
9. M. Breeuwsma, et al. Forensic Data Recovery from Flash Memory (SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 1, NO. 1, JUNE 2007)
10. Svein Y. Willassen, Norwegian University of Science and Technology, Forensic analysis of mobile phone internal memory
11. Improving the Reliability of Chip-O#Forensic Analysis of NAND Flash Memory Devices
12. SWGDE Tech Notes regarding Chip-off via Material Removal Using a Lap and Polish Process
13. https://standards.ieee.org/standard/1149_8_1-2012.html