Fall Kremers/Froon

Das Verschwinden von Bild 509 und andere Auffälligkeiten auf der vorgefundenen Digitalkamera

Inhaltsverzeichnis

Einleitung

Dieses Dokument beleuchtet die Untersuchung der im Fall Kremers/Froon vorgefundenen Digitalkamera Canon Powershot SX270 HS durch den NFI und weitere Personen und versucht, dem Leser technische Details hierzu näher zu bringen.

Die folgenden Erklärungen bezogen auf den Fall basieren hauptsächllich auf den vorliegenden Auszügen aus der ursprünglichen forensischen Untersuchung durch den NFI. Der vollständige NFI-Bericht ist dem Autor nicht bekannt.

Die Schlussfolgerung über die Einwirkung eines PC und somit einer Fremdperson, die der NFI-Bericht auf Grund der fehlenden Bilddatei 509 zieht, haben zu zahlreichen falschen Vorstellungen und Mythen über die Thematik geführt, die bei Darstellungen dieses Falls immer weiter im Internet verbreitet werden. Daher wird hier auch der Versuch unternommen, einer weiteren Verbreitung dieser Mythen vorzubeugen.

Neben der Untersuchung durch den NFI wurden nachträglich durch Privatpersonen weitere Tests mit entsprechend gleicher oder baugleicher Kamera durchgeführt, um das Verschwinden von Bild 509 zu klären. Hier sind vor allen Dingen die Reiseblogger Imperfectplan (IP) zu nennen, die bereits ein ähnliches Dokument veröffentlicht haben:

`https://imperfectplan.com/2021/04/06/kris-kremers-lisanne-froon-missing-photo-509-testing-canon-powershot-sx270-hs/`

-

Dateisystem

Die Bilddateien lagen im vorliegenden Fall auf einer **SD-Karte** mit einer Speicherkapazität von **16GB** vor.

Neben den eigentlichen Dateien sind auf einem Datenträger grundsätzlich noch zusätzliche Metainformationen gespeichert, die dazu dienen sollen, abgespeicherte Dateien schnell wiederzufinden. Diese bezeichnet man als **Dateisystem**. Im vorliegenden Fall wurde auf dem Datenträger das Dateisystem **FAT32** vorgefunden, was bei einem solchen Datenträger erwartbar ist.

Das Grundprinzip des Dateisystems ist relativ einfach erklärt. Die auf dem Datenträger abgespeicherten Dateien werden wie in einem Buch in einem Inhaltsverzeichnis alle aufgelistet, welches separat von den Dateien abgespeichert wird. Die Dateieinträge in diesem Verzeichnis verweisen dann auf den konkreten Speicherort der eigentlichen Datei. Tatsächlich können die ganzen Dateien sogar in mehrere Verzeichnisse aufgeteilt werden, die dann in einer baumartigen Struktur miteinander verbunden sind. Dieses Prinzip sollte jedem geübten Windows-Benutzer in Form von Ordnern und Unterordnern bekannt vorkommen. Daher werden im Folgenden die Begriffe Ordner und Unterordner verwendet. Die Ordnerstruktur beginnt mit dem Stammordner (engl.: root) in dem neben Dateieinträgen auch Einträge über Unterordner enthalten sein können, die dann wieder selbst Einträge über Unterordner haben können. Auf dem vorliegenden Datenträger waren die Bilddateien z.B. in 3 verschiedene Ordner für die Monate Januar, März und April aufgeteilt.

Ein Dateieintrag in einem Ordner enthält unter anderem die folgenden Informationen:

- Dateiname und Dateiendung
- Dateigröße
- Zeitstempel Dateianlage
- Zeitstempel Dateiänderung
- Verweis auf den Speicherort der Datei

Die Zeitstempel sind hier nicht zu verwechseln mit den im Fall angesprochenen digitalen Zeitstempeln in den Bilddateien selbst.

Sektoren, Kluster und Speicheraufteilung

Grundsätzlich wird ein Datenträger logisch in gleichgroße Speicherblöcke aufgeteilt. Bereits auf Ebene der Hardware passiert das. Hier wird der Datenträger vollständig in 512Byte große Blöcke aufgeteilt, die man als **Sektoren** bezeichnet. Das Dateisystem selbst unterteilt den von ihm verwalteten Bereich auf dem Datenträger ebenfalls in gleichgroße Speicherblöcke. Da die Aufteilung in Sektoren hier für das Dateisystem meist zu fein ist, werden aus Sicht des Dateisystems in der Regel mehrere Sektoren zu einem größeren Block zusammengefasst, den man als **Kluster** oder auch Zuordnungseinheit bezeichnet. Auf dem Datenträger lag eine Klustergröße von 32KB (64 Sektoren) vor.

Man kann sich hier den Speicher in zwei Bereiche aufgeteilt vorstellen:

1. Dateisystem-Metadatenbereich
2. Datenbereich

Auf die Informationen in den Dateisystem-Metadaten wird nicht näher eingegangen.
Die Aufteilung in Kluster beginnt hier im Datenbereich, der sowohl die ganzen Ordner als auch die Dateien selbst enthält.

Die folgende Tabelle zeigt exemplarisch einen Auszug eines in Kluster aufgeteilten Datenbereichs mit Ordnern und Dateien:

#300	**#301**	**#302**	**#303**	**#304**	**#305**	**#306**
Ordner	*Datei1*	*Datei2*	*Unterordner*	*Datei3*	*Datei4*	*Datei5*
---			---			
Datei1->301			Datei3->304			
Datei2->302			Datei4->305			
Unterordner->303			Datei5->306			

Kluster 300 enthält einen Ordner, der auf die Dateien Datei1 und Datei2 verweist, welche sich in den Klustern 301 und 302 befinden. Außerdem enthält er einen Verweis auf einen Unterordner in Kluster 303. Dort finden sich die Einträger der Dateien Datei3, Datei4 und Datei5, welche in den Klustern 304, 305 und 306 abgespeichert sind.

Normalerweise belegen Dateien je nach Größe natürlich gleich mehrere Kluster. Hierbei verweist der Dateieintrag im Ordner zunächst nur auf den Startkluster. Die restlichen Kluster, in denen die Datei abgespeichert wurde, kann man über die sogenannte Zuordnungstabelle ermitteln, die selbst im Dateisystem-Metadatenbereich abgespeichert ist und auf deren Funktionsweise hier nicht näher eingegangen wird. Es sei nur erwähnt, dass die Kluster einer Datei nicht zwangsläufig alle aufeinander folgen müssen. Theoretisch erlaubt die Funktionsweise dieser Zuordnungstabelle, dass alle Kluster der Datei willkürlich verstreut im Datenbereich liegen können. Man spricht hier von einer Fragmentierung der Datei. Allerdings versucht man in der Praxis starke Fragmentierungen bei der Abspeicherung von Dateien zu vermeiden. Meist sind fragmentierte Dateien nur in wenige Fragmente aufgeteilt.

An dieser Stelle sei auch kurz erwähnt, dass die hier beschriebene Funktionsweise des Dateisystems unabhängig davon ist, auf welcher Art von Datenträger es vorliegt. Es funktioniert auf der SD-Karte so, wie auf einer Festplatte.

Schlupfspeicher

Wenn die Größe einer Datei nicht zufällig ein Vielfaches der Klustergröße ist, dann wird der letzte Kluster natürlich auch nicht vollständig von der Datei beschrieben. Der übrig gebliebene Speicherplatz wird als **Schlupfspeicher** bezeichnet. Hier könnte man noch Reste der Daten finden, welche vorher in diesem Kluster gespeichert waren. Da ein Kluster im Dateisystem zu einem Zeitpunkt logisch immer nur einer Datei zugeordnet sein kann, können auch keine weiteren Daten anderer Dateien zusätzlich in den Kluster geschrieben werden. Der Schlupfspeicher ist daher im Grunde genommen verschwendeter Speicherplatz. Im Bericht von IP wird dies als „Betriebssystem-Metadaten" bezeichnet.

Löschen von Daten

Grundsätzlich muss man zwischen verschiedenen Arten des Löschens unterscheiden:

1. Normales Löschen
Hierbei wird der erste Buchstabe des Dateinamens im Ordnereintrag mit einem speziellen Wert überschrieben, der diesen Eintrag und somit die Datei als gelöscht markiert. Die Datei selbst ist direkt danach noch vollständig vorhanden und bleibt es so lange, bis die Datei durch die Anlage neuer Dateien teilweise oder vollständig überschrieben wird, da die Kluster, in denen die Datei abgespeichert ist, danach als frei markiert sind und jederzeit neu beschrieben werden können. Hierbei spielt es auch keine Rolle, ob die Löschung von einem PC oder der Kamera erfolgte. Beides führt zunächst zum selben Ergebnis. Wann die Datei wieder überschrieben wird, ist hier jedoch abhängig von dem System, welches den Datenträger geöffnet hat (Kamerafirmware, Windows etc.), da das Dateisystem selbst nicht vorschreibt, in welchen freien Klustern neue Dateien abzuspeichern sind.

2. Sicheres Löschen
Am PC besteht noch zusätzlich die Möglichkeit einer Löschung durch spezielle Programme, welche die Datei bei der Löschung direkt auch vollständig überschreiben. Somit ist die Datei direkt nach der Löschung nicht wiederherstellbar. Bei älteren Festplatten besteht eventuelle die Möglichkeit, auch überschriebene Daten wiederherzustellen, bei dieser Art von Datenträger ist das aber nicht möglich. Solche Löschprogramme sind als Freeware erhältlich und können auch von Laien ohne große Probleme bedient werden.

3. Schnellformatierung
Hierbei werden vereinfacht ausgedrückt alle Ordner und Dateien auf dem Datenträger normal gelöscht. Die Dateien sind direkt danach bis zur Anlage neuer Daten auch noch vollständig vorhanden.

4. Low-Level-Formatierung
Hierbei wird im Gegensatz zur Schnellformatierung der komplette Datenbereich initalisiert (mit 0 überschrieben). Dabei werden alle Daten überschrieben und sind nicht mehr wiederherstellbar.

Auf der Kamera stehen hier nur die Varianten 1, 3 und 4 zur Verfügung, wobei die beiden Formatierungsvarianten in diesem Fall bezogen auf die Löschung eines einzelnen Bildes zunächst keine große Rolle spielen.

Löschung von Bild 509

Für die Namen der Dateien verwendet die Kamera eine fortlaufende Nummerierung, die sich in der vorgefundenen Einstellung auch über Ordnergrenzen hinweg zieht. Die Namen haben hier die Form IMG_XXXX.JPG, wobei XXXX die fortlaufende Nummer darstellt.

Bei der Sichtung des Datenträgers durch den NFI fiel auf, dass im April-Ordner die Bilddatei mit der fortlaufenden Nummer 509 fehlt. Nicht zuletzt, weil das Bild genau zwischen der letzten Tagaufnahme und der ersten Nachtaufnahme fehlt, wirkte dies laut NFI-Bericht verdächtig. Daraufhin wurde eine Wiederherstellung des Bildes mittels Datenrettungsprogramm erfolglos versucht. Nach Angabe des NFI konnten hier grundsätzlich keine Reste dieser Bilddatei gefunden werden, was zu dem Schluss führte, dass dieses von einem PC gelöscht wurde.

Grundsätzlich steht hier zunächst die Frage im Raum, ob dieses Bild auf dem Datenträger überhaupt existierte, letztlich verweist nur noch eine Nummernlücke in den Dateinamen auf dessen Existenz. Das Bild könnte z.B. zwar aufgenommen, aber durch einen Fehler in der Kamera erst gar nicht auf die SD-Karte geschrieben worden sein. Allerdings gibt der Kamerahersteller die Wahrscheinlichkeit für einen Fehler dieser Art als sehr gering an. Auch bei Tests konnte ein solcher Fehler, der zu dem vorgefundenen Ergebnis führt, noch nicht nachgestellt werden.

Im Fall seiner Existenz muss man sich als nächstes fragen, wo im Datenbereich Bild 509 ursprünglich abgespeichert war. Nach durchgeführten Tests verfolgt die Kamera hier grundsätzlich eine relativ einfache Ablagestrategie der Dateien. Wenn sonst keine durch die Löschung von vorherigen Dateien entstandenen Freispeicherlücken vorhanden sind, legt sie die Bilddateien lückenlos hintereinander ab, ansonsten nutzt sie normalerweise diese Freispeicherlücken, allerdings nur unter gewissen Bedingungen. Bei der Abspeicherung der Datei in Speicherlücken wird die Datei eventuell auch auf mehre Lücken aufgeteilt (fragmentiert). Daher ist davon auszugehen, dass sich Bild 509 entweder direkt hinter Bild 508 oder in einer durch die Löschung mindestens eines vorherigen Bildes entstandenen Freispeicherlücke abgespeichert war.

Die Abspeicherung in einer Speicherlücke ist hier allerdings nach den Tests und auf Grund der starken Vermutung, dass es zu diesem Zeitpunkt solche Freispeicherlücken noch nicht gab, als unwahrscheinlich anzusehen. Daher wird hier davon ausgegangen, dass Bild 509 genauso lückenlos hinter Bild 508 abgespeichert war, wie alle anderen Aprilbilder ebenfalls lückenlos hintereinander abgespeichert aufgefunden wurden.

Löschung von Bild 509 durch die Kamera

Bei einer Löschung des Bildes 509 kann man zunächst zwei grundsätzliche Szenarien unterscheiden, eine Löschung vor oder nach Aufnahme der Nachtaufnahmen oder zumindest der ersten Nachtaufnahme. Eine reine Löschung durch die Kamera (normales Löschen), ohne weitere Einwirkungen durch einen PC, kann man hier im zweiten Fall (nach den Nachtaufnahmen) ausschließen, da in diesem Fall im Datenbereich zwischen Bild 508 und Bild 510 trotzdem auf jeden Fall eine Lücke übrig geblieben wäre, die nicht vorhanden war und die man auch mit der Kamera alleine nicht wegbekommt. Das Bild müsste also nach Aufnahme von Bild 508 und vor Aufnahme von Bild 510 gelöscht und nachträglich von Bild 510 überschrieben worden sein, da direkt hinter Bild 508 eben Bild 510 ohne Lücke vorgefunden wurde.

An dieser Stelle wird der im vorherigen Kapitel erwähnte Schlupfspeicher von zentraler Bedeutung, da man hierbei im Schlupfspeicher von Bild 510 Reste von Bild 509 erwarten würde, sofern Bild 509 nicht kleiner war als Bild 510. Zwar erwähnt der NFI-Bericht den Schlupfspeicher hier nicht direkt, aber es ist davon auszugehen, dass mit dem Nichtauffinden von Resten auch der Schlupfspeicher gemeint ist, zumal eine manuelle Sichtung des Schlupfspeichers mit den eingesetzten Programmen nicht mehr als ein paar Mausklicks an Aufwand bedeuten.
Im Grunde genommen müsste man also tatsächlich davon ausgehen, dass Bild 509 kleiner gewesen sein muss als Bild 510 und somit eventuell sogar eine komplette Dunkelaufnahme war, da Bild 510 bereits wahrscheinlich das kleinste Bild auf dem Datenträger darstellt. Die Bilddaten liegen in den Dateien hier in komprimierter Form vor, wobei die Größe der komprimierten Daten stärker variieren kann. Die Nachtaufnahmen lassen sich z.B. wesentlich besser komprimieren als die Tagaufnahmen, weswegen diese grundsätzlich kleiner sind und Bild 510 ist hier sogar das Kleinste der Nachtaufnahmen.

Man kann sich aus Sicht des Falls die Frage stellen, warum der Benutzer eine einzelne Nachtaufnahme, auf der man wahrscheinlich nichts gesehen hat, löscht und die anderen Nachtaufnahmen noch vorhanden sind. Da hier aber alle Informationen nebst Ordnereintrag mit Zeitstempeln nicht vorhanden sind (auch die als gelöscht markierten Dateieinträge im Ordner können von neuen Einträgen überschrieben werden), haben wir keinerlei Informationen darüber, wann genau das Bild aufgenommen wurde. Es könnte z.B. auch in einer anderen Nacht aufgenommen worden sein und gar nicht zur Serie der Nachtbilder gehören. Wir kennen schlichtweg die Umstände nicht, um hier zuverlässig auszusagen, wie wahrscheinlich etwas ist oder nicht.

Fazit: Es muss hier auf jeden Fall die Löschung mit Einfluss durch einen PC in Erwägung gezogen werden, so eindeutig, wie es der NFI-Bericht hier suggeriert, ist die Sachlage jedoch nicht.

Löschung von Bild 509 mit Einfluss durch einen PC

Bei einer normalen Löschung durch einen PC ergäben sich zunächst die selben Fragen wie bei einer normalen Löschung durch die Kamera. Auch hier wären Reste von Bild 509 im Schlupfspeicher von Bild 510 erwartbar, sofern wir von einer Löschung vor den Nachtaufnahmen sprechen. An dieser Stelle wäre tatsächlich der Einsatz eines Löschprogramms denkbar, dass die Datei mit 0 überschrieben hat, was den angenommenen leeren Schlupfspeicher von Bild 510 erklären würde. Die Nachtaufnahmen bzw. Bild 510 wurde dann eben nachträglich nochmals darüber geschrieben.

Auch die Löschung nach den Nachtaufnahmen mit entstandener Lücke wäre hier durch den Einfluss eines PC möglich. Allerdings wäre diese Manipulation schwieriger in der Umsetzung, als ein Löschprogramm herunterzuladen und auszuführen. Ein Laie könnte dies eventuell mit entsprechendem Willen, Zeit und Recherche im Internet auch noch hinbekommen, es würde aber eher auf eine Person mit technischem Hintergrundwissen deuten. Übrigens: Die Lücke bleibt hier auch übrig, wenn ein normales Löschprogramm die Datei überschreibt. Diese überschreiben einfach nur die Daten und kümmern sich normalerweise nicht darum, irgendwelche Freispeicherlücken, die dabei entstanden sind, wegzubekommen.

Grundsätzlich ist hier eine gezielte Löschung des Bildes durch Einfluss eines PC natürlich problemlos möglich, allerdings wirkt auch dies etwas unplausibel, da sich hierbei die Frage stellt, warum überhaupt die Lücke in der Nummerierung der Dateinamen noch vorhanden ist. Tatsächlich ist dies der auffälligste und gleichzeitig einzig übrig gebliebene Hinweis auf das Bild,

der sich aber noch mit am einfachsten wegbekommen lässt.

Sogar ein Laie würde das durch einfaches Umbenennen wahrscheinlich hinbekommen. Bei einem Experten und auch einer Person mit technischem Hintergrundwissen sollte man unter normalen Umständen davon ausgehen, dass wir heute nichts mehr von der Existenz dieses Bildes wüssten. Natürlich gibt es auch hier Gründe, die man immer aufführen kann, um diese Merkwürdigkeit zu erklären, so, wie sich immer Gründe finden lassen, warum ein Benutzer eine einzelne Dunkelaufnahme löscht.

Natürlich gäbe es hier noch viele andere Möglichkeiten, sobald der Einfluss eines PC hinzukommt. So wäre das Verschwinden des Bildes eventuell auch als Nebeneffekt einer noch umfangreicheren Datenmanipulation, bei der auch die anderen Bilder beteiligt waren, möglich.

Fazit: Auch die gezielte Löschung mit Einfluss eines PC wirft Fragen auf. Daher ist die Sachlage hier m.E. nicht so eindeutig, wie viele glauben. Eine Reduzierung der Fragestellung auf statistische Wahrscheinlichkeit halte ich so oder so für sehr fragwürdig, da wir hier in beiden Fällen von menschlichen Aktionen sprechen, bei denen uns die Umstände völlig unbekannt sind.

Weitere Auffälligkeiten

Neben dem fehlenden Bild 509 wurden noch 2 weitere Auffälligkeiten durch den NFI festgestellt.

Zum einen fanden sich in den Ordnern Dateieinträge mit der Endung .TMP, welche von der Kamera selbst nicht erzeugt werden. Es stellte sich heraus, dass diese höchstwahrscheinlich durch ein Bildanzeigeprogramm (wahrscheinlich sogar die interne Bild-/Fotoanzeige von Windows) durch Öffnung von Bildern auf dem Datenträger und Drehung der Ansicht erzeugt wurden. Auf Grund eines gefundenen Zeitstempels fällt diese Aktion in den Zeitraum, in dem die Behörden in Panama den Datenträger vorliegen hatten, so dass sich dieses eindeutige Indiz für den Einfluss eines PC den Behörden in Panama zuordnen lässt.

Weiterhin wurden auf dem Datenträger mehrere Bilder wiederhergestellt, bei denen es sich jedoch um Miniaturansichten (Tumbnails) bestehender Bilder handelte. Da diese „Vorschaubilder" in den existierenden Bilddateien selbst mit abgespeichert sind und eigentlich nicht wiederhergestellt werden müssen, ist hier davon auszugehen, dass diese nochmals separat im Freispeicher abgespeichert waren, was ebenfalls auf den Einfluss eines Bildanzeigeprogramms hindeutet, welches die ganzen Tumbnails aus den Dateien eines Ordners extrahiert und alle in einer separaten temporären Datei abgespeichert hat. Daher ist es wahrscheinlich, dass auch dies durch die Behörden in Panama verursacht wurde. Leider gibt in diesem Fall aber kein Zeitstempel klare Auskunft darüber.

Zumindest ist hier die Einwirkung durch einen PC in Form der Behörden in Panama relativ eindeutig nachgewiesen. Ob hierdurch auch Bild 509 verschwunden ist, lässt sich jedoch nicht sagen, zumindest gibt es hierfür keine Anzeichen. Während sich die Verursachung der TMP-Dateien und Tumbnails ohne Probleme als Unkenntnis eines normalen Anwenders erklären lässt, wären für eine Erklärung des Verschwindens von Bild 509 noch andere Benutzeraktionen notwendig gewesen, die sich nicht so einfach als Versehen erklären lassen. Bei einem absichtlichen Löschen ergibt sich jedoch wieder die Frage, warum man nicht das offensichtlichste Anzeichen (Lücke in der Nummerierung) auch gleich mit „beseitigt" hat, was ohne Probleme möglich gewesen wäre.