MAGAZYN
INFORMATYKI ŚLEDCZEJ

mediarecovery
Wyższy poziom bezpieczeństwa

www.mediarecovery.pl

2018

W tym wydaniu

Wszystkie Magazyny możesz bezpłatnie pobrać na:

http://magazyn.mediarecovery.pl

Techno Mode

– najszybsza droga dostępu do materiału dowodowego z uszkodzonych SSD.

Roman Morozov

Pojawiające się ostatnio statystyki pokazują, że dyski półprzewodnikowe mają znaczny udział w rynku pamięci masowych. Zakłada się, że popularność dysków SSD wzrośnie, co spowoduje, iż pojawi się więcej mało znanych producentów - w rezultacie na rynek z łatwością trafią znaczne ilości produktów o niskiej jakości.

Specjaliści muszą być na to przygotowani i zawsze szukać skutecznych sposobów rozwiązywania problemów, pojawiających się w ich codziennej pracy.

Prawie wszystkie współczesne dyski SSD wyposażone są w sprzętowe szyfrowanie danych. Dlatego metoda Chip-off staje się bezużyteczna, jeśli chodzi o dostęp do dowodów cyfrowych na uszkodzonym urządzeniu. W takim przypadku tryb Techno jest jedynym możliwym sposobem przywrócenia logicznego dostępu do danych na SSD.

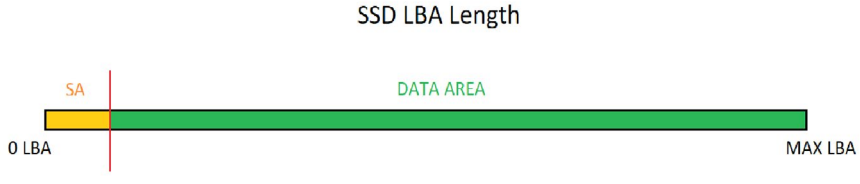
W artykule wyjaśnimy przyczynę awarii dysków SSD bez wyczerpania liczby dostępnych cykli przepisywania i przedstawimy metodę dostępu do danych na urządzeniach, które przestały działać. Aby lepiej zrozumieć, cały proces, zacznijmy od przeglądu wewnętrznej struktury SSD. Obecnie SSD są produkowane w oparciu o mikroczipy NAND Flash. Podobnie jak w przypadku wszelkich zaawansowanych urządzeń elektronicznych, chipy te podlegają „starzeniu" technologicznemu. Wynika to przede wszystkim z komórek pamięci, podstawy chipów NAND Flash, zużywających się i nie mogących utrzymać ładunku elektrycznego.

Tryb Techno jest jedynym możliwym sposobem przywrócenia logicznego dostępu do danych na SSD.

Warstwa specjalnej izolacji oddziela komórki chipa. Przy każdym procesie zapisu komórka pamięci pobiera prąd 12V, który przebija izolację i w niej pozostaje. Im cieńsza jest ta warstwa izolacji - tym mniej cykli przepisywania dany chip może wytrzymać.

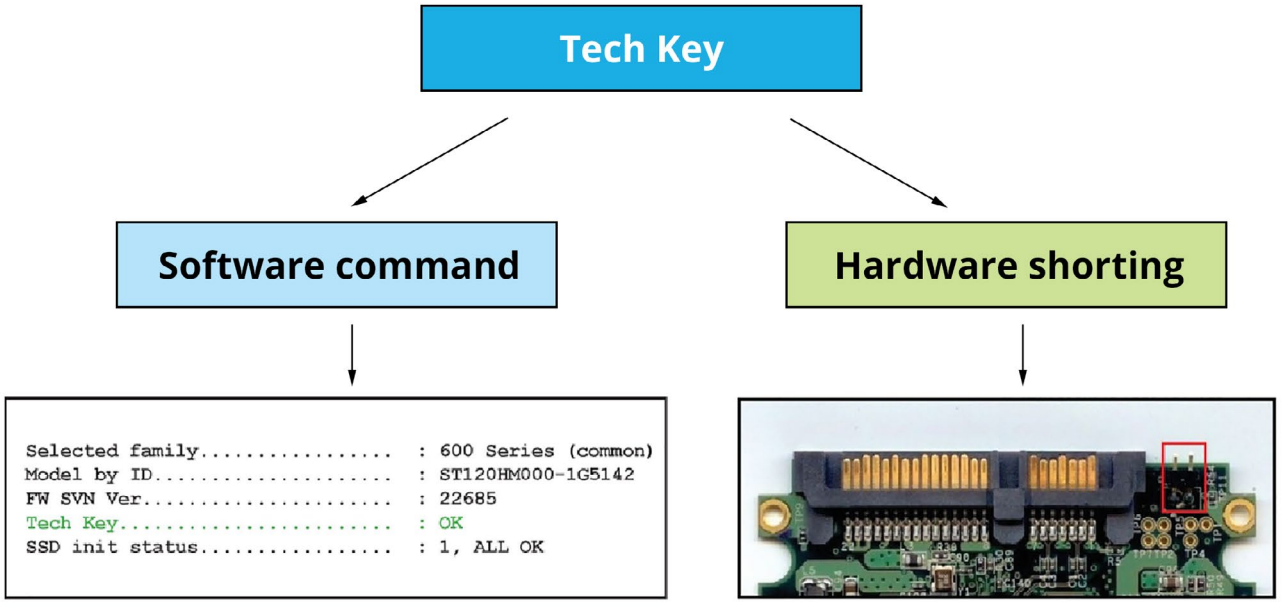
Nowoczesne chipy są produkowane przy minimalnych procesach techno - 19nm, 15nm, 14nm. W związku z tym ich cykl życia nie będzie długi. Ponadto większość niedrogich dysków SSD jest produkowanych przy użyciu taniego typu pamięci TLC (Triple Level Cell). Ten typ pamięci przechowuje 3 bity informacji w każdej komórce, zwiększając w ten sposób ilość przestrzeni dyskowej. Jednak oparte na TLC urządzenia NAND Flash są bardzo niewiarygodne i znacznie bardziej podatne na awarie. W każdym razie od 30 do 90 cykli przepisywania wystarczy, aby dotrzeć do krytycznej liczby uszkodzonych komórek. Dla porównania SLC to od 30 000 do 100 000 cykli, a MLC od 1 000 do 5 000 cykli.

Mimo tego nowo zakupione dyski nie powinny działać nieprawidłowo. Wystarczy pomyśleć o czasie potrzebnym do całkowitego przepisania całej przestrzeni dysku 128-512 GB.



Rys. 1 Obszar serwisowy i obszar danych w SSD

SSD mają specjalną przestrzeń zwaną Service Area (SA). Obszar ten jest poświęcony komponentom usług, modułom, tabelom specjalnym, częściom mikrokodu, informacjom o oprogramowaniu itd. Zmiany dokonane w rejestrze



Rys. 2 Dostęp do trybu Techno - za pomocą polecenia programowego i zwarcia sprzętowego

obszaru danych użytkownika (DA) w tak zwanych tabelach tłumaczeń, znajdują się wewnątrz SA. SA to stała (i bardzo mała) część całej dostępnej przestrzeni dyskowej, dlatego zapisywanie i przepisywanie informacji o usługach może szybko wyczerpać liczbę możliwych do wykonania cykli. Nawet 20 lub 30 cykli może wystarczyć do „zapchania" SA uszkodzonymi komórkami i całkowitego zerwania translatora. Zazwyczaj w takich przypadkach dyski SSD wykazują następujące symptomy: do 2 Mb dostępnej wolnej przestrzeni, stały stan BSY (busy-zajęty), błąd ABR przy adresowaniu DA lub całkowita niemożność zarejestrowania dysku w menedżerze urządzeń. Jest jednak sposób pomocny w uzyskaniu dostępu do danych nawet w pozornie uszkodzonym dysku (powyższe oznaczenia to status rejestrów i błędów w programie PC-3000).

Wszystkie dyski SSD są dostarczane z wbudowanym trybem Techno. Służy on do debugowania urządzeń. Producenci używają go do badania niesprawnych napędów w celu zidentyfikowania uszkodzonej części mikrokodu i rozwiązania problemu w przyszłych wersjach oprogramowania.

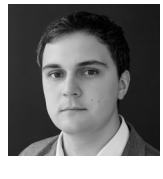
Inżynierowie ACE Lab poszli o krok dalej. Lata badań pozwoliły stworzyć metodę użycia trybu Techno w celu rzeczywistego przywrócenia dostępu do danych na uszkodzonych dyskach SSD. Osiąga się to poprzez użycie określonych narzędzi, które wymuszają na uszkodzonych urządzeniach przejście do trybu Techno. Ponieważ najczęstszą przyczyną awarii SSD jest zepsuty translator, użycie trybu Techno daje możliwość zbudowania nowego. Nowy translator jest ładowany do pamięci RAM urządzenia, zadanie jest tworzone w specjalnym oprogramowaniu, a użytkownik uzyskuje pełny dostęp do struktury plików na dysku SSD. Narzędzia SSD PC-3000 mogą pomóc w:

- **Uzyskaniu dostępu do obszaru usług.**
- **Stworzeniu translatora pozwalającego na dostęp do dowodów cyfrowych.**
- **Zebranie informacji o liczbie układów pamięci i części logicznych.**
- **Zapisie obrazów chipów bez lutowania NAND.**
- **Tymczasowym wyłączeniu polecenia TRIM.**
- **Wykryciu hasła, a nawet jego odczycie lub usunięciu.**
- **Przeglądaniu uszkodzeń i wad układów pamięci za pomocą dedykowanego Menadżera.**
- **Użyciu poleceń niskopoziomowego formatu (Low-Level Format), czy przywróceniu oryginalnych ustawień Repair Functions.**

Aktualnie PC-3000 SSD obsługuje szeroką gamę dysków Solid State wielu producentów: ADATA, AMD, Corsair, Crucial, OCZ, Intel, Kingston, Micron, Patriot, Plextor, Lite-On, PNY, Samsung, SanDisk, Seagate, Silicon Power, Smartbuy, GoodRAM, G.Skill, RunCore i innych.

Wiele z produkowanych SSD posiada standardowy tryb Techno, dlatego opisana metoda może być stosowana do różnych urządzeń. Zdarza się jednak, że SSD mają własne wersje trybu Techno. Nawet dwa podobne modele, na przykład Plextor, Sandisk, Micron lub Crucial mogą mieć różne pary „Firmware-Controller". ACE Lab prowadzi ciągłe badania w celu ulepszenia metody, oprogramowania i narzędzi, aby można było zastosować je dla każdej znanej marki i producenta.

Ponadto, tryb Techno można wykorzystać do odzyskania plików z uszkodzonego SSD, które mogłyby zostać usunięte w przeciągu kilku godzin. Inną ważną zaletą korzystania z trybu Techno jest możliwość zarówno obejścia, jak i wykrycia haseł, które wcześniej zostały ustawione na SSD. Ta opcja jest bardzo korzystna, w sytuacji gdy podejrzany używa tego samego hasła na komputerze, telefonie komórkowym, koncie e-mail lub innych dyskach.



Roman Morozov, NAND Data Recovery Tutor, ACE Lab.

ACELab®

PROFESSIONAL SYSTEMS
FOR RECOVERING DIGITAL EVIDENCE
FROM DAMAGED STORAGE DEVICES

PC-3000

THE MOST POWERFUL HARDWARE-SOFTWARE SOLUTIONS:

- To recover digital evidence from HDD, RAID, SSD, Flash drives and Mobile devices
- To restore the operability of drives and access the data on them
- To bypass the drive password protection

... and much more!

e-mail: sales@acelab.eu.com
www.acelab.eu.com

IoT

Michał Tatar

Internet rzeczy (IoT) ma ogromne możliwości, a także poważne problemy z bezpieczeństwem i prywatnością.

Chociaż od dawna przeprowadza się badania dowodów cyfrowych wszelakich urządzeń elektronicznych, badania kryminalistyczne w zakresie IoT są stosunkowo nowe i nie zostały jeszcze dokładnie zgłębione. Kiedy Kevin Ashton w 1999 roku zaproponował termin IoT (ang. Internet of Things), czyli koncepcję, wedle której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem np. sieci komputerowej, zapewne nie spodziewał się, że progres technologiczny nastąpi tak szybko i przyniesie za sobą tyle problemów, zwłaszcza tych związanych z poczuciem bezpieczeństwa. Czy w związku z tym, dzisiejsi forensicowi specjaliści mają jakieś możliwości, aby badać nośniki cyfrowe pochodzące z wszelakiej maści urządzeń skategoryzowanych jako IoT? Spróbujmy się temu przyjrzeć.

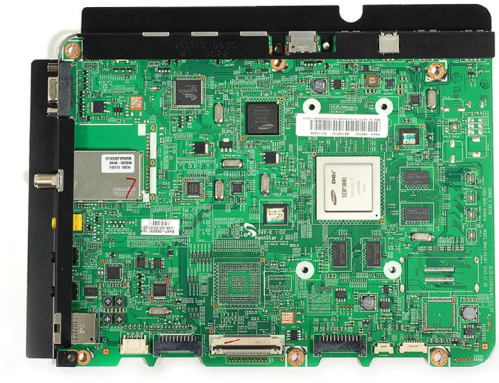
Device Name	Image Name	Partition Map	Mount Path
/dev/mmcblk0p0	onboot.bin	BOOTLOADER0	NONE
/dev/mmcblk0p1	u-boot.bin	BOOTLOADER1	NONE
/dev/mmcblk0p2	secos.bin	SECOS0	NONE
/dev/mmcblk0p3	secos.bin	SECOS1	NONE
/dev/mmcblk0p4	ex_partition	NONE	NONE
/dev/mmcblk0p5	seret.bin	SECOS0	NONE
/dev/mmcblk0p6	seret.bin	SECOS1	NONE
/dev/mmcblk0p7	uImage	KERNEL0	NONE
/dev/mmcblk0p8	rootfs.img	RFS0	NONE
/dev/mmcblk0p9	uImage	KERNEL1	NONE
/dev/mmcblk0p10	rootfs.img	RFS1	NONE
/dev/mmcblk0p11	sign0.bin	SECUREMAC0	NONE
/dev/mmcblk0p12	sign1.bin	SECUREMAC1	NONE
/dev/mmcblk0p13	VD-HEADER	NONE	NONE
/dev/mmcblk0p14	NONE	NONE	mtd_drmregion_a
/dev/mmcblk0p15	NONE	NONE	mtd_drmregion_b
/dev/mmcblk0p16	NONE	NONE	mtd_rwarea
/dev/mmcblk0p17	exe.img	EXE0	mtd_exe
/dev/mmcblk0p18	exe.img	EXE1	mtd_exe
/dev/mmcblk0p19	rocommon.img	CONTENT0	mtd_rocommon
/dev/mmcblk0p20	rocommon.img	CONTENT1	mtd_rocommon
/dev/mmcblk0p21	emanual.img	NONE	mtd_emanual
/dev/mmcblk0p22	NONE	NONE	mtd_contents
/dev/mmcblk0p23	NONE	NONE	mtd_swu
/dev/mmcblk0p24	rwcommon.img	NONE	mtd_rwcommon

Rys. 2 Partycjonowanie systemu

Podstawowym celem Internetu Rzeczy jest stworzenie inteligentnych przestrzeni tj. inteligentnych miast, transportu, produktów, budynków, systemów energetycznych, systemów zdrowia czy innych związanych z życiem codziennym. W każdej z przestrzeni znajdują się przedmioty, które do niej należą. Samochody (zwłaszcza te określane jako bezzałogowe), drony (którymi steruje cyfrowe AI), oświetlenie miejskie, inteligentne domy, czujniki zbierające informacje o stanie zdrowia, telewizory, lodówki czy nawet kosze na śmieci w formie określanej jako 'smart'... Wszystkie te i inne przedmioty już istnieją i lada moment zaczynie się ich ekspansja. Bo dlaczego lodówka nie miałaby sama zamówić produktów, których zaczyna w niej brakować? Dlaczego kosz na śmieci nie mógłby sam informować domowników, że jego pojemność jest bliska wyczerpania? A telewizory, które same dobierają odpowiednie transmisje dla osoby, która właśnie je ogląda? Świat jest dzisiaj cyfrowy i z dnia na dzień nasze życie też siłą rzeczy staje się coraz bardziej cyfrowe. Z naszego punktu widzenia, czyli specjalistów informatyki śledczej, wszystko to określane jako smart, bezzałogowe, czy sterowane sztuczną inteligencją musi być postrzegane nie tylko w sposób użytkowy, ale przede wszystkim jako cyfrowe dane. Dane, które prędzej czy później mogą pojawić się jako dowody elektroniczne. Tych 'zer i jedynek' będzie przybywać, a my musimy sobie z tym poradzić. Bo skoro - na przykład - było włamanie do inteligentnego domu, to zapewne czujniki zarejestrowały odpowiednie informacje. Dlaczego nie mielibyśmy się w takim razie nimi posłużyć i pomóc rozwiązać taką sprawę?

Na chwilę obecną, dane z urządzeń IoT gromadzone są głównie w pamięciach typu flash (najczęściej są to kości eMMC), dołączanych kart pamięci lub zasobach sieciowych (jeśli urządzenie nie posiada własnego magazynu pamięci). Najprostszą sprawą jest taka, w której urządzenie IoT korzysta z karty pamięci. Wówczas odczyt takiej karty i analiza odczytanych danych rozwiązuje problem. W przypadku pamięci eMMC sprawa jest nieco bardziej skomplikowana. Na szczęście ten rodzaj pamięci flash ma możliwość odczytu ISP i potrzebuje pięciu podłączonych linii sygnałowych: Vss, Vdd, Clock, Command & Data0. Odpowiednie połączenie do układu daje nam możliwość pozyskania całej zawartości kości pamięci. Spróbujmy zatem prześledzić taki proces na przykładzie zabezpieczenia pamięci telewizora typu smart.

Zdjęcie na rys. 1 przedstawia płytę



Rys. 1 Płyta główna TV

główną takiego telewizora. Można zauważyć podobieństwa do płyt głównych umieszczanych w smartfonach. Odnajdujemy na płycie procesor, kość pamięci i dodatkowe układy sterujące

```
<manufacturerURL>
http://www.samsung.com/sec
</manufacturerURL>
<modelDescription>
SamsungTVDMR
</modelDescription>
<modelName>
UE40F7000
</modelName>
<modelNumber>
AllShare1.0
</modelNumber>
<modelURL>http://www.samsung.com/sec
</modelURL>
<serialNumber>REMOVED by Authors</serialNumber>
<UDN>REMOVED by Authors</UDN>
<sec:deviceID>REMOVED by Authors</sec:deviceID>
```

Rys. 3 Zawartość XML

forensics na przykładzie analizy SmartTV

odpowiednimi funkcjami. Dla nas najważniejsza jest oczywiście kość pamięci. Takową najczęściej musimy z płyty głównej wyciągnąć (metodą Chip-Off) i nawiązać z nią połączenie. Wynikiem poprawnego połączenia będzie pełny dump pamięci do pliku binarnego (.BIN). Następnie zaczyna się proces analizy takiej pamięci.

Systemy plików na pamięciach eMMC zostały opracowane dla systemów wbudowanych korzystających z pamięci flash. Ten typ pamięci flash wykorzystuje dane wejściowe/wyjściowe oparte na blokach, co wymaga precyzyjnego mapowania, zmiany układu i usuwania pamięci. Jest również kompatybilny z systemami operacyjnymi opartymi na systemie Linux. Zwykle systemy plików na układach eMMC są spersonalizowane przez producenta telewizora. W przypadku telewizorów smart jednym z systemów plików jest Squash FS. To oparty na systemie Linux system plików tylko do odczytu, opracowany z myślą o systemach wbudowanych. Podstawowym atrybutem Squash FS jest to, że kompresuje katalogi, pliki i węzły indeksu. Partycjonowanie tego systemu wygląda jak na rysunku nr 2.

Inteligentne telewizory zwykle przechowują większość danych w plikach XML. Informacje takie jak adres URL producenta, opis modelu, nazwa, numer, URL modelu, numer seryjny itp. Ta informacja staje się bardzo ważna podczas badania urządzenia i potwierdzania informacji o samym urządzeniu.

Telewizory smart na ogół mają zaimplementowaną łączność sieciową, która umożliwia użytkownikom dostęp do Internetu i pobieranie aplikacji. Biorąc pod uwagę nasz punkt widzenia, czyli forensicowca, zdobywanie informacji o sieci jest bardzo cenne. Znajdziemy tam takie dane jak: nazwa urządzenia w sieci, numery portów, adresy IP, czy też sparowane urządzenia wraz z adresem MAC.

Zainstalowane aplikacje również są cennym źródłem danych. Wszelkie aplikacje społecznościowe, typu Facebook czy Twitter, zapisują dane w formie plików cache, które następnie możemy poddać szczegółowej analizie. Aktywność preinstalowanej przeglądarki internetowej gromadzona jest w formie pliku bazy danych SQLite. Poddając analizie bazę danych otrzymujemy dostęp do wszystkich odwiedzonych witryn internetowych.

Jak widać na powyższym, analiza danych pochodzących z urządzeń IoT jest możliwa. Wymaga jednak precyzyjnego podejścia do tematu – umiejętnego odczytu zawartości pamięci takich urządzeń oraz wnikliwej (często manualnej) analizie odczytanych danych.

Kwestia informatyki śledczej w stosunku do Internetu Rzeczy na pewno przyniesie sporo wyzwań i zapewne zmieni w jakiś sposób podejście do tematu materiału dowodowego. IoT to zjawisko, które przynosi (bądź przyniesie) wszystkim sporo dobrego w codziennym życiu, ale także wzbudza co raz częściej pewnego rodzaju niepokój, płynący z postępu technologicznego i zmieniającego się w związku z tym naszego świata.

"widgetname":"Facebook","vendor":"Samsung",
"install_date":"Wed, 19 May2010 15:57:57+0900",
"account_id":null,"login_token":null,"external_cp_app":true,
"sso_id":"test@hotmail.com",
"is_logged_in":false,"is_installed":true,"is_activated":true
,"is_init_state":true,"is_latest_verion":true,
"installed_version":"1.18128","widget_type":null,"
name":"Twitter","widgetname":"Twitter",
"vendor":"Samsung","install_date":"Sat, 13 Mar 2010 11:31:03
+0900",

Rys. 4 Zawartość plików CACHE

Table: FullBrowserHistory — New Record

	URL	Title	Count	VisitDay
1	http://www.bing.com/	Bing	1	1970-01-01
2	http://nl.msn.com/?pc=SMTV	MSN NL: Hotmail, Outlook, Skype, het	89	1970-01-01
3	http://nieuws.nl.msn.com/afbeeldingen/heb-je-	Roemeense bedelaar heeft drie luxe a	1	1970-01-01
4	http://www.telegraaf.nl/	Nieuws | Altijd op de hoogte van het l	3	1970-01-01
5	http://tmgonlinemedia.nl/consent/consent/?ret	Nieuws | Altijd op de hoogte van het l	1	1970-01-01
6	http://www.telegraaf.nl/prive/22152971/__Ma	Man sterft na winnen prijs in show Elle	1	1970-01-01
7	http://www.dumpert.nl/	dumpert.nl	3	1970-01-01
8	http://www.dumpert.nl/mediabase/6577295/e	dumpert.nl - KOMT DIE GOLF!!!	1	1970-01-01
9	http://www.dumpert.nl/mediabase/6577257/7f	dumpert.nl - Helikoptercrew redt kraa	1	1970-01-01

Rys. 5 Dane SQLite

Michał Tatar jest specjalistą w zakresie analizy urządzeń mobilnych (Mobile Forensics) w Laboratorium Informatyki Śledczej Mediarecovery. Zajmuje się również implementacją rozwiązań mobilnych zarówno w sektorze prywatnym jak i publicznym (m.in. Mobile Device Management). Trener w ramach Akademii Informatyki Śledczej.

Car&Drone forensics w praktyce

Czy samochód osobowy lub dron może być dowodem elektronicznym? Okazuje się, że tak! Często bardzo szczegółowym i wartościowym.

Aleksander Juraszek

Rys. 1 Volkswagen electronic brain, 1968

Kiedy w 1968 roku marka Volkswagen wprowadziła pierwszy na świecie komputer zarządzający elektronicznym wtryskiem paliwa, prawdopodobnie nikt nie przypuszczał ile dodatkowych funkcji znajdzie się w module ECU (ang. Electronic Controll Unit) po ponad 50 latach rozwoju idei zarządzania funkcjami pojazdu. Dziś samochody mają być przede wszystkim bezpieczne, komfortowe i niezawodne. Aby sprostać tym założeniom w każdym pojeździe montuje się wiele systemów odpowiedzialnych za prawidłową pracę pojazdu oraz diagnostykę. Oczywiście wraz z rozwojem technologii funkcji przybywa, a ECU stają się coraz bardziej wydajnymi komputerami, które rejestrują znacznie więcej niż nam się wydaje. W przeciętnym aucie sprzed 10 lat można było odnaleźć do 10 modułów ECU. W chwili obecnej jest ich średnio 70. Każdy nowoczesny samochód to imponująco zaprojektowany system elektroniczny. Często z niezależnymi sieciami dystrybucji danych, przez które przepływa nawet do 25 gigabajtów na godzinę.

Samochody są naszą codziennością. Statystyki są imponujące. W pierwszym kwartale 2017 roku sprzedano w Europie ponad 4 200 000 pojazdów osobowych – w samej Polsce ok 120 000 sztuk. Każdego roku spędzamy w aucie ok 700 godzin, pokonując średnio 15 000 kilometrów. Biorąc te liczby pod uwagę, wyobraźmy sobie ile informacji jest przetwarzanych w każdym

Rys. 2 Platforma iVe firmy Berla

Rys. 3 Przechwycony dron przemytników

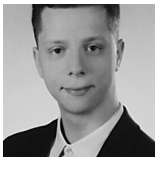
z tych aut, jaką mogą one mieć wartość i w końcu jak można się do nich dostać.

Ciekawym rozwiązaniem typowo forensicowym jest platforma iVe firmy Berla. Za pomocą tego wyspecjalizowanego zestawu narzędzi oraz oprogramowania, jesteśmy w stanie pobrać dane z ponad 5 200 typów pojazdów. iVe daje szeroki wachlarz możliwości podczas prowadzenia czynności informatyki śledczej samochodu. Za pomocą aplikacji i odpowiedniego adaptera wykonamy logiczne i fizyczne zabezpieczenie danych oraz odzyskamy skasowane pliki i logi pojazdu. Podczas analizy system zdekoduje treści i samodzielnie przypisze je do poszczególnych kategorii. Oprócz informacji o połączeniach telefonicznych, wiadomościach sms, zdjęciach, znajdziemy również w raporcie historię tras nawigacji, a także listę połączonych urządzeń przez interfejs bluetooth, usb lub nawet WiFi. Lista pobranej zawartości z poszczególnych modułów auta jest zaskakująco długa. Po zabezpieczeniu wszystkich danych możemy wygenerować czytelny raport.

A gdybyśmy na warsztat analizy danych wzięli drona? Te niewielkich rozmiarów, bezzałogowe statki powietrzne, stają się coraz bardziej popularne na świecie. W tym momencie warto podać kilka interesujących faktów: w pierwszych trzech kwartałach 2017 roku wyprodukowano ok 2 milionów dronów. Średnia sprzedaż firmy DJI to 20 000 quadrocopterów miesięcznie. Drony wykorzystuje się do robienia zdjęć, nagrywania filmów, koncerny usługowe stawiają na transport za ich pośrednictwem, a agenci nieruchomości używają do celów marketingowych. Z kolei przestępcy przemycają narkotyki przez granice państw lub dostarczają broń do zakładów karnych. Spektrum zastosowań jest szerokie.

Analizowany przez nas DJI Phantom 3 to chyba najpopularniejszy, cywilny, statek bezzałogowy na świecie. Może unosić się w powietrzu do 25 minut z prędkością nie przekraczającą 16 metrów na sekundę. Wiemy, że ma wbudowane pozycjonowanie GPS i gniazdo karty pamięci micro SD, na której zapisywane są zdjęcia i filmy z kamery. Do wszystkich nagrań dopisywane są metadane takie jak data, godzina, pozycja geograficzna, ciśnienie atmosferyczne, oraz ustawienia kamery. Uwaga! Na płycie głównej drona znajduje się jeszcze jeden slot karty micro SD, na której zapisywane są wszystkie logi lotów, dane dotyczące pojemności baterii, a także prędkości silników. Analizę urządzenia można wykonać na wiele sposobów, począwszy od odczytania wartości pliku FLY.DAT i wyszukaniu odpowiednich parametrów w tekście. Można też wykorzystać gotowe rozwiązanie jakie oferuje pakiet firmy MSAB – XRY, który wspiera wszystkie statki powietrzne firmy DJI. Za jego pomocą bez problemu dokonamy logicznego zabezpieczenia wszystkich danych, a następnie automatycznie wygenerujemy raport z analizy drona. Szwedzki producent oprogramowania XRY zapowiada, że już wkrótce będą wspierane kolejne platformy pojazdów typu UAV, a w tym między innymi Parrot.

Podsumowując, informatyka śledcza to dziedzina, która rozwija się równie szybko, jak technologie, które nas otaczają. Coraz więcej elementów otaczającego nas świata rejestruje coraz więcej danych, które mają nam ułatwić życie, to z kolei daje nieograniczony potencjał analizy zabezpieczonych zasobów. Dane dotyczące czasu, lokalizacji czy też odpowiednich zdarzeń na pewno przydadzą się w prowadzeniu kolejnych spraw.



Aleksander Juraszek jest specjalistą informatyki śledczej w laboratorium Mediarecovery, gdzie zajmuje się analizą danych. Wielokrotnie brał udział w zabezpieczaniu danych podczas operacji przeprowadzanych przez służby odpowiedzialne za zachowanie bezpieczeństwa i porządku publicznego.

Rys. 4 Płyta główna i metadane z nagrania kamery drona

Logiczna ekstrakcja danych z urządzeń iOS:

zapobieganie szyfrowaniu kopii zapasowych

Oleg Afonin

Akwizycja logiczna jest najczęstszym sposobem wyodrębniania informacji z najnowszych urządzeń iPhone i iPad. W przeciwieństwie do innych metod zabezpieczania danych, które mogą być trudne pod względem prawnym i technicznym, ekstrakcja logiczna jest najbardziej zgodnym z najlepszymi praktykami informatyki śledczej sposobem pozyskania danych użytkownika bez wprowadzania niepożądanych modyfikacji urządzenia lub uzyskiwania dostępu do zewnętrznych usług w chmurze. Jednak ta metoda nie jest pozbawiona wyzwań, z których jednym z najważniejszych jest hasło kopii zapasowej.

Czym jest logiczna ekstrakcja danych?

W systemie iOS termin „akwizycji logicznej" jest używany do zdefiniowania metody wyodrębniania, powodującej, że urządzenie tworzy lokalną kopię zapasową („kopia zapasowa iTunes", chociaż sam iTunes nie jest wymagany do jej utworzenia). Lokalne kopie zapasowe urządzeń iOS zawierają prawie wszystko to, co znajduje się w pamięci urządzenia. Obejmują one dane większości aplikacji systemowych i tych stworzonych przez firmy zewnętrzne (z wyjątkiem tych, których twórcy wyraźnie wyłączają kopie zapasowe), ustawienia systemu, niektóre – ograniczone - dane o lokalizacji, dane dzienników połączeń, wiadomości tekstowe i głosowe, kalendarze, pliki z aparatu (zdjęcia oraz wideo), a także wszystkie zapisane hasła.

Akwizycja logiczna jest najczęstszym sposobem wyodrębniania informacji z najnowszych urządzeń iPhone i iPad.

Hasło kopii zapasowej i konsekwencje dla analizy danych

iOS umożliwia szyfrowanie lokalnych kopii zapasowych za pomocą hasła utworzonego przez użytkownika. Może ustawić on swoje hasło lokalnej kopii zapasowej w iTunes podczas tworzenia jej po raz pierwszy. Po ustawieniu hasło zapisuje się w urządzeniu (iPhone lub iPad). Jeśli hasło jest włączone, żadne niezaszyfrowane dane nigdy nie opuszczają urządzenia; iTunes lub Elcomsoft iOS Forensic Toolkit po prostu przechwytują zaszyfrowany strumień danych i zapisują go jako grupę plików, aby wykonać kopię zapasową.

Hasło kopii zapasowej rodzi istotne konse-

	Bez hasła	Backup chroniony hasłem
Kontakty, połączenia, zdjęcia, dane aplikacji	Dostępne	Dostępne (zaszyfrowane hasłem)
Hasła Wi-Fi, formularze logowania, hasła użytkowników, tokeny uwierzytelniania	Szyfrowane za pomocą klucza "securityd"; niedostępne	Dostępne (zaszyfrowane hasłem)

Rys. 1 Tabela

kwencje dla analizy danych, wykraczające daleko poza ochronę kopii zapasowych. Użycie hasła wpływa na sposób ochrony różnych części kopii zapasowej. Bez hasła główna część kopii zapasowej nie zostanie zaszyfrowana; jednak iOS użyje bardzo bezpiecznego klucza specyficznego dla sprzętu do zaszyfrowania keychain, który przechowuje hasła użytkownika, tokeny i poświadczenia uwierzytelniające. W efekcie zawartość keychain z niechronionych kopii zapasowych nie może zostać odszyfrowana. Przywrócić ją można tylko na dokładnie tym samym urządzeniu, z którego wcześniej została uzyskana.

Rys. 2

Jeśli kopia zapasowa jest chroniona hasłem, keychain jest szyfrowany przy użyciu tego samego hasła, co reszta kopii zapasowej. Z tego powodu ustawienie tymczasowego, znanego hasła jest bezwzględnie konieczne podczas wykonywania ekstrakcji logicznej.

iOS 10 i wersje starsze

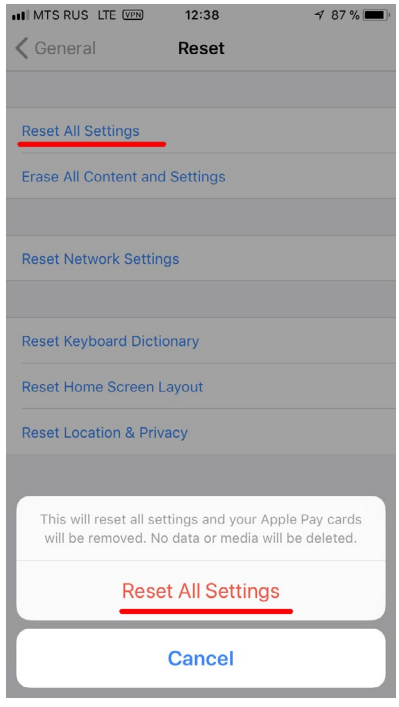
Podczas wyodrębniania danych z urządzenia z systemem iOS w wersji od 8 do 10 należy pamiętać, że hasła kopii zapasowej nie można zmienić ani usunąć bez uprzedniego wprowadzenia poprzedniego hasła. Jeśli oryginalne hasło do kopii zapasowej było nieznane, jedynym sposobem na odszyfrowanie kopii zapasowej byłoby odzyskanie oryginalnego hasła przez przeprowadzenie ataku brute-force lub słownikowego za pomocą narzędzia Elcomsoft Phone Breaker. Należy postępować zgodnie z instrukcjami poniżej, aby odzyskać oryginalne hasło tekstowe. Ponieważ iOS 11 dodaje możliwość resetowania haseł kopii zapasowych, można zaktualizować urządzenie iPhone lub iPad, którego kopia zapasowa jest chroniona nieznanym hasłem do iOS 11. Jeśli urządzenie jest chronione hasłem, bezwzględnie będzie ono potrzebne, aby wykonać aktualizację i reset hasła kopii zapasowej.

iOS 11: Resetowanie hasła kopii zapasowej

Podczas wyodrębniania danych z urządzenia iPhone lub iPad z systemem iOS 11 można łatwo zresetować hasło kopii zapasowej, wykonując „Reset ustawień sieci" z poziomu „Ustawień" urządzenia.

Uwaga: jeśli urządzenie ma hasło, musisz je wprowadzić podczas próby resetowania ustawień sieci.

Aby zresetować hasło kopii zapasowej w systemie iOS 11, wykonaj następujące kroki:



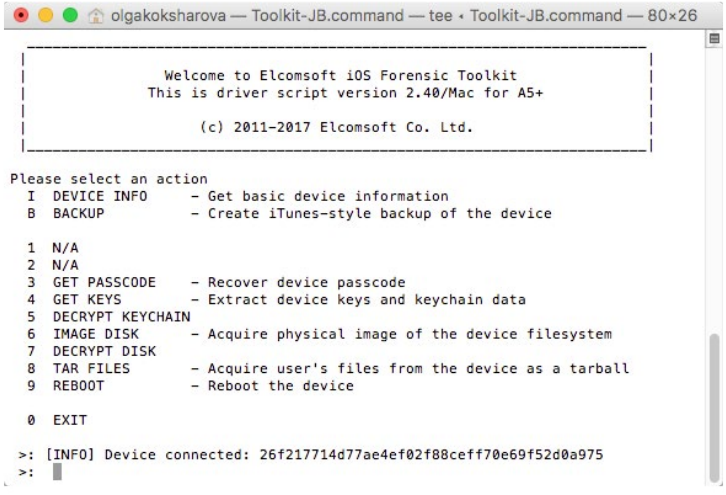
Rys. 3

1. **Odblokuj urządzenie za pomocą Touch ID, Face ID lub kodu dostępu**
2. **Przejdź do Ustawienia - Ogólne, następnie przewiń do opcji Reset. (Rys. 2)**
3. **Wybierz Resetuj wszystkie ustawienia**
4. **Wprowadź hasło urządzenia (będzie wymagane, jeśli hasło jest włączone)**

Polecenie „Resetuj wszystkie ustawienia" kasuje następujące ustawienia:

- **ustawienia jasności**
- **czy wyświetlać procent baterii**
- **hasła Wi-Fi (ale nie inne hasła lub tokeny zapisane w keychain)**
- **apple.wifi.plist**
- **hasło kopii zapasowej iTunes**

Co zrobić, jeśli nie znasz hasła i nie możesz zresetować hasła kopii zapasowej? W takim przypadku powrócimy do pierwszego etapu: mimo to wykonamy lokalną kopię zapasową i za pomocą Elcomsoft Phone Breaker spróbujemy złamać hasło.



Rys. 4

Kopia logiczna krok po kroku

Zalecamy następujące podejście do logicznego zabezpieczania urządzeń z systemem iOS.

Warunki wstępne:

1. Urządzenie iPhone lub iPad
2. Elcomsoft iOS Forensic Toolkit 2.40 lub nowszy
3. iOS 10 i starsze: urządzenie jest odblokowane za pomocą Touch ID, hasła lub zapisu blokady
4. iOS 11: hasło musi być powiązane z komputerem. Alternatywnie można użyć rekordu blokowania wyodrębnionego z komputera użytkownika.

Sprawdź, czy kopia zapasowa jest chroniona hasłem:

1. Podłącz urządzenie iPhone lub iPad do komputera.
2. Odblokuj urządzenie iPhone lub iPad i potwierdź monit „Zaufaj temu komputerowi”

Uwaga: w systemie iOS 11 wymagane będzie wprowadzenie hasła urządzenia. Jeśli nie znasz hasła, użyj rekordu blokady (jeśli jest dostępny)

1. Uruchom Elcomsoft iOS Forensic Toolkit 2.40 lub nowszy i użyj opcji „I(nfo)”, aby sprawdzić, czy kopia zapasowa ma hasło.
2. Zresetuj nieznane hasło zapasowe (tylko iOS 11). Na urządzeniu z systemem iOS otwórz Ustawienia - Ogólne - Resetuj, a następnie dotknij i potwierdź Resetuj wszystkie ustawienia.

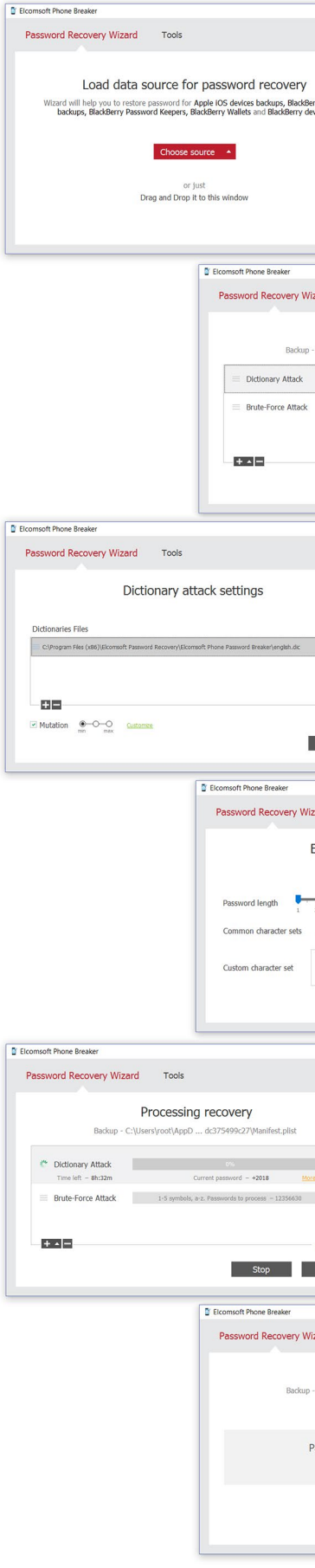
Uwaga: iOS 11 będzie wymagać wprowadzenia hasła dostępu do urządzenia (jeśli jest włączone).

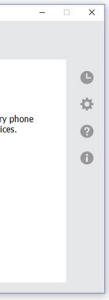
Utwórz lokalną kopię zapasową:

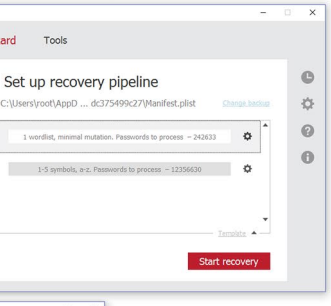
1. Podłącz urządzenie z systemem iOS do komputera. Zostaniesz poproszony o ustanowienie zaufanego połączenia z komputerem. Potwierdź monity na komputerze i urządzeniu iPhone lub iPad.
2. (tylko iOS 11) Zostanie wyświetlony monit o wprowadzenie kodu urządzenia na urządzeniu iPhone lub iPad. Podaj hasło, aby zakończyć parowanie.
3. Po nawiązaniu relacji parowania uruchom Elcomsoft iOS Forensic Toolkit 2.40 lub nowszy.
4. Naciśnij “B” (Backup), aby utworzyć nową kopię zapasową (Rys.4)

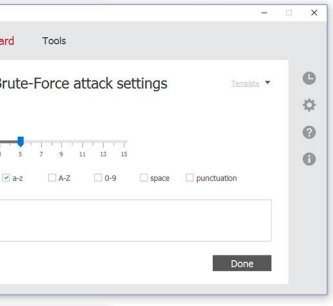
Uwaga: w narzędziu iOS Forensic Toolkit ustawiono tymczasowe hasło „123”; to pozwoli ci odszyfrować itemy z keychain. Możesz użyć istniejącego pliku blokady (rekordu parowania), aby utworzyć kopię zapasową.

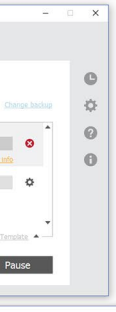
W tym momencie powinieneś mieć lokalną kopię zapasową. Jeśli kopia zapasowa jest chroniona hasłem, którego nie znasz, musisz odzyskać to hasło, aby odszyfrować kopię zapasową.

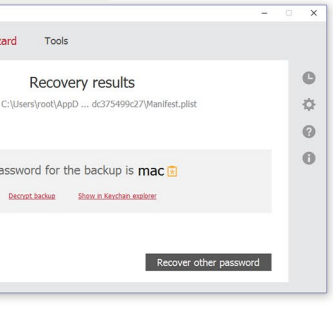












Łamanie haseł w kopii zapasowej iOS

iOS używa bezpiecznego szyfrowania, aby chronić kopie zapasowe, jeśli użytkownik włączył hasło kopii zapasowej. Jeśli go nie znasz, jedynym sposobem na jej złamanie jest wykonanie ataku brute-force lub słownikowego. W zależności od wersji systemu iOS i sprzętu używanego do atakowania hasła, możesz spodziewać się następujących prędkości odzyskiwania:

- **iOS 4 do 9 (i 10.1): około 150 000 haseł na sekundę na GPU (NVIDIA GeForce 1080)**
- **iOS 10.0: około 6 000 000 haseł na sekundę z procesorem Intel i5 ze względu na wykryty błąd**
- **iOS 10.2 i nowsze (w tym iOS 11): około 5 haseł na minutę (procesor); ~ 100 haseł na sekundę na GPU (GeForce 1080)**

Uwaga: aby osiągnąć najszybszy poziom odzyskiwania, zalecamy użycie wielu akceleratorów GPU, takich jak kilka kart NVIDIA GTX 1080.

1. **Otwórz stronę Kreator odzyskiwania hasła.**
2. **Określ plik kopii zapasowej, wybierając go za pomocą polecenia „Wybierz źródło" lub przeciągając i upuszczając plik Manifest.plist w oknie Kreator odzyskiwania hasła.**

Domyślnie iTunes przechowuje kopie zapasowe iOS w następujących lokalizacjach:

Windows XP:

\Documents and Settings\(nazwa użytkownika)\Dane aplikacji\Apple Computer\MobileSync\Backup

Windows 7, 8 i 10:

\Users\nazwa_użytkownika\AppData\Roaming\Apple Computer\MobileSync\Backup

System operacyjny Mac:

~/Library/Application Support/MobileSync/Backup/

Po określeniu pliku kopii zapasowej, musisz zdefiniować ataki, które zostaną użyte do złamania hasła. Kliknij „+", aby dodać ataki do strumienia. Domyślnie ataki słownikowy i brute-force są dodawane automatycznie. Możesz opcjonalnie je skonfigurować, klikając ikonę koła zębatego po prawej stronie każdej metody. Kliknij „Rozpocznij odzyskiwanie". Elcomsoft Phone Breaker zacznie atakować hasło. Zostanie wyświetlony szacowany czas oraz aktualnie przetwarzane słowo. Możesz kliknąć „Więcej informacji" obok nazwy ataku, aby zobaczyć dodatkowe informacje, takie jak liczba prób uzyskania hasła i średnia prędkość ataku.

Jeśli atak się powiedzie, odkryte hasło zostanie wyświetlone w oknie wyników odzyskiwania.

Po odzyskaniu hasła można go użyć do odszyfrowania kopii zapasowej. Ponadto możesz przeglądać informacje przechowywane w keychain za pomocą wbudowanego narzędzia Keychain Explorer Tool.

Podsumowanie

Dokładnie przejrzeliśmy ochronę kopii zapasowych systemu iOS używanych w trakcie akwizycji logicznej. Dowiedzieliśmy się o różnicach pomiędzy danymi zabezpieczonymi hasłem i tymi niechronionymi w kopiach zapasowych oraz ich konsekwencjami dla analizy śledczej. Dowiedzieliśmy się, jak resetować hasła do kopii zapasowych na urządzeniach iPhone i iPad z systemem iOS 11 oraz jak atakować istniejące hasła kopii zapasowych.

Oleg Afonin, jest researcherem i ekspertem informatyki śledczej w Elcomsoft. Jest współautorem książki "Mobile Forensics – Advanced Investigative Strategies" oraz prelegentem wielu konferencji i sympozjów.

Analiza powiązań

- Opowieść ze świata dowodów cyfrowych

Peter Warnke

W informatyce śledczej prezentacja wyników analizy – przenalizowanych artefaktów systemu operacyjnego, które mogą udowodnić, że podejrzany wiedział o dokumentach lub plikach znajdujących się na badanym urządzeniu - jest jednym z kluczowych elementów realizowanej sprawy. Najważniejszym jej elementem jest pokazanie „opowieści dowodowej" - jak dany plik znalazł się na komputerze podejrzanego – przez kogo został wysłany i jakie były jego kolejne losy.

Analiza powiązań między danymi nie jest nową koncepcją w informatyce śledczej. Jednakże, często skupia się na tradycyjnej analizie wymiany informacji, a nie na artefaktach, które zostały utworzone. Tytułowa analiza pozwala odkryć więcej, niż tylko ścieżkę powiązań między dwoma osobami podejrzanymi w sprawie. Dzięki niej powiązane zostają dane plików i systemu operacyjnego, które pomagają śledczemu zwizualizować „relacje" między elementami zebranego materiału dowodowego z różnych źródeł (komputery, urządzenia mobilne oraz przestrzeń w chmurze).

Śledząc przenoszenie / przemieszanie plików między systemami i urządzeniami, śledczy jest w stanie zbudować historię dotyczącą pochodzenia dowodu, wliczając w to gdzie aktualnie się on znajduje, jakim sposobem był udostępniony i komu.

Ręczne budowanie powiązań jest czasochłonne i wymaga dużego nakładu zasobów, dlatego tak istotne jest zastosowanie automatyzacji, na którą pozwala oprogramowanie Magnet AXIOM. Dzięki temu rozwiązaniu śledczy może wykorzystać zdefiniowaną wcześniej zasadę automatyzacji, w każdej z prowadzonych spraw. Przewagą AXIOM jest zdolność do wyciągania danych z chmury, informacji ze smartfonów i komputerów do jednego pliku sprawy. Dzięki temu, „funkcja Connections" pozwala śledczym podążać za kluczowymi dowodami i powiązać je z urządzeniami, podejrzanymi osobami i innymi składowymi sprawy.

Jak działa automatyczna analiza powiązań pomiędzy artefaktami?

Powyższa funkcjonalność jest istotnym elementem analizy spraw dotyczących przestępstw z wykorzystywaniem dzieci, terroryzmu i kradzieży własności intelektualnej oraz w przypadkach kiedy podejrzany zaprzecza, że wie cokolwiek na temat ujawnionych danych.

Zasadniczy proces zaczyna się od uporządkowanych danych pozyskanych z urządzeń mobilnych, komputerów, pamięci przenośnych i chmury zawierających informacje o tym kiedy, w jaki sposób i jak często pliki były przenoszone i przez kogo. Te informacje pozwalają określić kiedy pliki zostały utworzone i zmodyfikowane. Śledczy może zbadać czym dany plik jest, jaka jest historia jego pobierania, kim był pierwotny autor i kolejni modyfikujący, w jaki jeszcze sposób plik był przeglądany oraz poznać inne zdarzenia z jego „cyfrowego życia".

Od tego momentu istnieje możliwość dodania kontekstu, nie tylko związanego z metadanymi plików, ale również z przetwarzaną zawartością. Grupowanie danych po takich samych właściwościach np. nazwa, ścieżka do-

stępu pozwala określić istotne powiązania z innymi artefaktami. Powiazania mogą być także utworzone poprzez kategorie artefaktów, takie jak załączniki wymieniane między aplikacjami.

Pozyskane w ten sposób informacje o pliku zyskują na znaczeniu kiedy powiążemy je z elementami systemu operacyjnego, które pomagają zidentyfikować gdzie plik był przechowywany, czy był otwarty i czy utworzono do niego skrót. Te dodatkowe informacje są istotne, kiedy podejrzany twierdzi, że ktoś inny mający dostęp do komputera pobrał nielegalne treści.

W takim przypadku, filtr czasu zastosowany w odniesieniu do daty eksploracji, zawartej w kluczach rejestru (shellbags) plików, pozwala zobaczyć inne artefakty utworzone w tym samym czasie np. dane logowania czy aktywności w Internecie. Widząc inne ściągane lub otwierane pliki, dane o komunikacji czy nawet dane logowania do innych kont, śledczy może zbudować linię czasu aktywności użytkownika która potwierdza lub zaprzecza linii obrony podejrzanego.

Biorąc pod uwagę wszystkie omówione rzeczy, możemy wyciągnąć wniosek, iż artefakty posiadają informacje, których nie widać gołym okiem, a które mogą być kluczowym elementem sprawy. Stosując analizę powiązań wszystkich artefaktów w danym systemie lub urządzeniu, informatycy śledczy mogą zaoszczędzić sporo czasu i wysiłku w szybkim znalezieniu wzajemnych „relacji" – tak aby uzyskane informacje stworzyły historię, ukazały zamiary i przypisały dowód właściwemu podejrzanemu.

Peter Warnke jest Central Europe Account Executive w Magnet Forensics, posiada duże doświadczenie w zakresie informatyki śledczej, mobile forensics, integracji systemów, bezpieczeństwa i infrastruktury sieciowej.

Zabezpieczanie dysków SSD

Udział dysków SSD w światowym rynku sprzętu komputerowego zwiększa się z roku na rok. Jak szacują ośrodki badawcze już niedługo ilość SSD będących w użyciu przeskoczy ilość HDD. Zmiana technologiczna dostrzegalna jest też w informatyce śledczej.

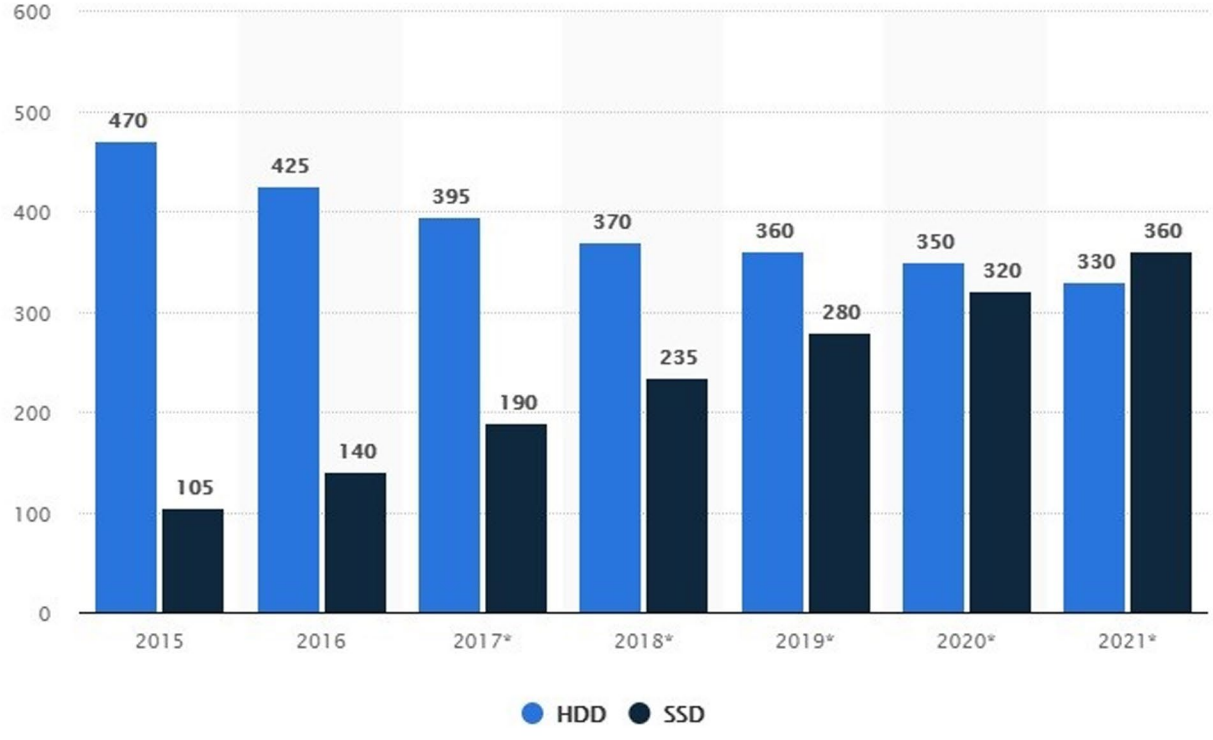
Największy wpływ na wzrost popularności SSD ma z pewnością ich coraz niższa cena. Zakup takiego nośnika to najprostszy sposób na poprawę wydajności komputera.

Więcej dysków SSD w domach i firmach przekłada się na coraz częstsze napotykanie ich w praktyce specjalisty informatyki śledczej. Trzeba zauważyć, iż różnice w sposobie zapisu danych na dyskach SSD przekładają się na niespotykane w przypadku HDD problemy.

Jedną z podstaw i najlepszych praktyk informatyki śledczej jest wyliczanie sumy kontrolnej i wykonywanie kopii binarnych badanych nośników. Wykonuje się je by mieć pewność, że dane zapisane na nośniku w 100% pokrywają się z tymi, które znajdowały się na nim w momencie zabezpieczenia.

Wpływa to doskonale na przejrzystość całego procesu informatyki śledczej i daje pewność, że każda sugestia o manipulację danymi będzie oddalona przez Sąd. Zastosowanie profesjonalnego sprzętu zwiększa wielokrotnie zarówno pewność informatyka śledczego, jak i szybkość jego pracy.

Co jednak w sytuacji kiedy te same kopie mają różne sumy kontrolne? Co jeśli suma kontrolna oryginału różni się od kopii? Takie sytuacje mają miejsce w przy-



Wykres pochodzi z zasobów: Statista.com (HDDs and SSDs: global shipments 2015-2021)

padku SSD. Zdarzać się to może bardzo często. Po prostu niektóre SSD wyposażone są w wewnętrzne mechanizmy relokacji danych, które mogą wpłynąć na finalną sumę kontrolną zabezpieczanego nośnika. Co ciekawe rodzaj zastosowanego blokera nie ma znaczenia.

Jak rozwiązać problem? Bardzo prosto:

1. **Świadomość**
   Informatyk śledczy musi wiedzieć, że takie zjawisko może wystąpić i znać jego technologiczne podłoże.
2. **Rozszerzona dokumentacja**
   Z uwagi na to warto nieco rozszerzyć standardową dokumentację o informacje na temat zabezpieczanego nośnika.
3. **Suma kontrolna dla każdego pliku**
   W odróżnieniu od HDD gdzie wyliczamy ją dla całego dysku, w przypadku SSD dodatkowo powinna zostać wyliczona dla każdego z zapisanych plików. Nie powinno to za bardzo przedłużyć tej fazy całego procesu. Różnica w wyliczeniu sumy kontrolnej dla całego dysku HDD jest podobna, w porównaniu z wyliczaniem jej dla każdego z plików zapisanych na SSD tej samej pojemności.

Żeby jednak nie było, że dyski SSD to tylko dodatkowe kłopoty. Z naszych wewnętrznych badań wynika, że zastosowanie SSD w laboratorium informatyki śledczej pozwala nawet trzykrotnie skrócić czas potrzebny na wykonanie analizy!

Redakcja

Przestępstwa związane z kryptowalutami

Bitcoin, ethereum, litecoin, dash, monero, ripple, zcash... Kryptowaluty oparte na technologii blockchain z impetem wkroczyły na salony. BTC powstały zaledwie w 2009 r., jednak szybko zyskały globalną popularność, lansowane jako uczciwa, przejrzysta, oparta na mocy obliczeniowej, matematyce, kryptografii i sieci rozproszonej alternatywa dla systemu bankowego.

Alternatywne systemy kryptowalut stale rozwijają się obok tradycyjnego systemu opartego na pieniądzu, stanowiącym ekwiwalent złota. Przedstawiciele świata finansjery, tacy jak Warren Buffett, Nouriel Roubini, czy też Augustin Carstens, krytykują i ostrzegają, uważając kryptowaluty za niebezpieczną bańkę finansową, jednak te, pozostając poza regulacją prawną, każdego dnia zyskują rzesze nowych zwolenników, niezrażonych skokami notowań. Właśnie, skoro te cyberwaluty nie zostały objęte regulacją prawną, to czy można je np. ukraść? Jakie zagrożenia czyhają na właścicieli kryptowalut i jakiej ewentualnej reakcji państwa można się spodziewać, gdyby te zagrożenia się ziściły?

Skoncentrujmy się na najpopularniejszej obecnie kryptowalucie, a więc bitcoinach i polskim porządku prawnym. Własność BTC sprowadza się w zasadzie do posiadania prywatnego klucza, który znany tylko osobie właściciela pozwala na nabywanie i rozporządzanie bitcoinami. Z tego też względu podstawowe znaczenie ma zabezpieczenie tego poufnego klucza przed jego ujawnieniem. Zagrożenie polega bowiem na tym, że inna osoba niż właściciel BTC pozna ten prywatny klucz i wbrew woli/wiedzy właściciela dokona transferu bitcoinów do innego portfela. Czy w takiej sytuacji właściciel pozbawiony swoich bitcoinów może liczyć na pomoc organów ścigania? Intuicyjnie wydaje się, że zubożały zwolennik kryptowalut powinien złożyć zawiadomienie o popełnieniu przestępstwa kradzieży. Czy słusznie?

Zgodnie z art. 278 § 1 kodeksu karnego kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Przepis ten znajdzie zastosowanie również w przypadku uzyskania cudzego programu komputerowego (§ 2), jak i kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego (§ 5). Rzeczy ruchome to zgodnie z prawem cywilnym, do którego należy się odwołać, przedmioty materialne. Na gruncie prawa karnego pojęcie to zostało nieco doprecyzowane. Zgodnie bowiem z art. 115 § 9 kodeksu karnego rzeczą ruchomą lub przedmiotem jest także polski albo obcy pieniądz lub inny środek płatniczy, środek pieniężny zapisany na rachunku oraz dokument uprawniający do otrzymania sumy pieniężnej albo za-

wierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach, albo stwierdzenie uczestnictwa w spółce. Celowo użyłem słowa „doprecyzowano", a nie „rozszerzono", bowiem wymienione w przywołanym przepisie pieniądze, środki płatnicze, dokumenty itd. to również rzeczy, przedmioty materialne.

Bitcoin z całą pewnością rzeczą nie jest, nie ma bowiem postaci materialnej, co z resztą postrzegane jest przez zwolenników kryptowalut za ich zaletę. Nie za bardzo można taką kryptowalutę zakwalifikować jako program komputerowy, ani środek płatniczy. Jakkolwiek bowiem bitcoiny służą obecnie również do płacenia, nawet za bardzo powszechne dobra, takie jak jedzenie, książki, czy bilety lotnicze, to jednak w rozumieniu prawa dewizowego krajowymi środkami płatniczymi są waluta polska oraz papiery wartościowe i inne dokumenty, pełniące funkcję środka płatniczego, wystawione w walucie polskiej. Tych przesłanek BTC nie spełnia.

Co jednak ciekawe, bitcoiny identyfikuje się w ramach Polskiej Klasyfikacji Wyrobów i Usług oraz Polskiej Klasyfikacji Działalności. Obrót i wytwarzanie BTC uznaje się bowiem za „Pozostałe pośrednictwo pieniężne" (PKD 64.19.Z) i „Pozostałe pośrednictwo pieniężne, gdzie indziej niesklasyfikowane" (PKWiU 64.19.30.0). Jak wiemy ta cyfrowa waluta jest również identyfikowana przez fiskus i generowany przez nią dochód podlega opodatkowaniu. Również na gruncie prawa europejskiego bitcoiny uważa się raczej za pełniący funkcję środka płatniczego – warto przywołać wyrok Trybunału Sprawiedliwości z dnia 22 października 2015 r. w sprawie C-264/14, w którym uznano, że transakcja wymiany walut tradycyjnych na wirtualną walutę bitcoin stanowi transakcję zwolnioną z podatku VAT.

Bitcoin z całą pewnością rzeczą nie jest, nie ma bowiem postaci materialnej, co z resztą postrzegane jest przez zwolenników kryptowalut za ich zaletę.

Niemniej jednak mam poważne wątpliwości, czy na gruncie polskiego kodeksu karnego „kradzież" bitcoinów zostanie przez organy ścigania zakwalifikowana jako kradzież w rozumieniu art. 278 k.k. Najpewniej Policja odmówi przyjęcia zawiadomienia albo umorzy postępowanie z uwagi na brak spełnienia znamion czynu zabronionego przez zachowanie sprawcy. Jednak czyn omawiany wyżej może zostać uznany za inny rodzaj przestępstwa. Mianowicie, bezprawne pozyskanie dostępu do portfela posiadacza BTC, jego adresu i klucza prywatnego, wiązać się będzie z przełamaniem lub ominięciem zabezpieczeń, zatem najpewniej oznaczać będzie realizację znamion czynu zabronionego z art. 267 § 1 kodeksu karnego regulującego przestępstwo tzw. hackingu. Co jednak ciekawe, karalne w tym przypadku będzie samo uzyskanie dostępu do portfela, jeśli nastąpiło po przełamaniu lub ominięciu zabezpieczeń, a nie sam fakt „kradzieży" BTC.

Bezprawne pozyskanie dostępu do portfela posiadacza BTC, wiązać się będzie z przełamaniem zabezpieczeń, zatem najpewniej oznaczać będzie realizację znamion czynu zabronionego z art. 267 § 1 kodeksu karnego regulującego przestępstwo tzw. hackingu.

Tak postawionej sprawy organy ścigania nie powinny zignorować, ale co dalej? Specyfika funkcjonowania BTC i całej technologii blockchain sprawia, że identyfikacja miejsca docelowego, gdzie przetransferowano bitcoiny wbrew woli ich pierwotnego właściciela nie powinno nastarczać trudności. Sprawny informatyk śledczy będzie w stanie ustalić te informacje. Tutaj jednak można uderzyć w ścianę, bowiem problemem będzie identyfikacja sprawcy, którym tylko prawdopodobnie jest posiadacz „zasilonego" portfela, co jednak gorsze, sieć nie zna granic, jurysdykcja polskich organów ścigania granice jednak zna i powinna się ich trzymać. Współpraca międzynarodowa w ściganiu cyberprzestępców pozostawia natomiast wiele do życzenia.

Powyższe skłania do uznania, że właściciele bitcoinów nie są na gruncie polskich regulacji prawnych objęci ochroną analogiczną do posiadaczy tradycyjnych pieniędzy, natomiast organy ścigania mimo szczerych chęci, mogą natrafić na przeszkody nie do przeskoczenia uniemożliwiające skuteczne ustalenie sprawcy i doprowadzenie go przed oblicze sprawiedliwości.

Jarosław Góra jest adwokatem, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.

MAGAZYN INFORMATYKI ŚLEDCZEJ

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza

Skład, łamanie, grafika:
Mariusz Ruski

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl
www.mediarecovery.pl

mediarecovery Wyższy poziom bezpieczeństwa