Zajišťování dat z počítačů od firmy Apple

Dominik Novák

Anotace:
Zatímco v minulosti byly počítače Apple v českém prostředí zastoupeny jen zcela minimálně a problematiku jejich forenzní analýzy nebylo v podstatě nutno systémově řešit, jejich podíl v posledních letech výrazným způsobem roste a s tím i potřeba postupů a nástrojů pro zajištění a analýzu dat z těchto zařízení. Úvodní článek nové série pojednává o základních způsobech zajištění dat z počítačů s operačním systémem macOS.

Annotation:
Whereas a market share of Apple computers was insignificant in Czechia only few years ago and therefore there was no need of systematical forensic approach to these devices, their growing numbers in the last years bring forward a need of processes and tools helping to acquire and analyze data from these devices. This first article, out of more planned, explains some basic approaches to forensic data acquisition from macOS computers.

Klíčová slova:
forenzní analýza apple, zajištění dat, soudní znalec, blacklight, recon

Key words:
digital forensics, mac forensics, data acquisition, forensic expert, blacklight, recon

Úvod

Stále zvyšující se počet zařízení Apple navyšuje i počet případů, kdy je potřeba data z nich zkoumat. Firma Apple velmi dbá na bezpečnost a ochranu dat svých zákazníků, a tak se zajišťování a zkoumaní dat z těchto zařízení stává stále složitější. Ukázkový příklad jejich už starší novinky je čip T2, který seskupuje některé řadiče, které se nacházely v počítači na různých místech. Stojí tak nad celým systémem a tím umožňuje lepší zabezpečení – slouží jako základ pro šifrování celého úložiště a zabezpečeného spouštění. I přesto už dnes existují možnosti, jak tento typ zařízení zajistit. My se v tomto článku pokusíme podívat na úplné základy zajišťování dat z počítačů od firmy Apple.

Počítač s vyměnitelným diskem

Po příchodu k vypnutému a zaheslovanému počítači, můžeme postupovat klasickým způsobem. Při štěstí se dnes ještě můžeme dostat ke starším MacBookům, které jsou vybaveny vyměnitelným diskem. Starší modely Unibody MacBooku Pro (2008-2012) většinou obsahují klasický SATA 2,5“ disk, ze kterého je možné pak udělat kopii pomocí blokátoru nebo duplikátoru. Pozdější MacBooky Pro s retina displejem (2012-2015) mají místo klasických disků flash paměť, která se jeví jako SSD s rozhraním M.2, ale z výroby tomu tak není. Je nutné použít redukci právě na M.2, aby se disk dal bez problému připojit.

Počítač s integrovaným diskem

Poslední modely všech Macbooků (2015 - dodnes) mají paměťový čip připájený na desce, proto jej není možné jednoduše demontovat a zajistit data běžným způsobem. Ostatní modely stolních počítačů Apple z dnešní doby (iMac, Mac mini) jsou na tom obdobně. Výjimkou je Mac Pro, kde lze fyzicky disky vyjmout. Nejjednodušší způsob, jak z vypnutého počítače data zajistit je přes tzv. Target mode, který z počítače udělá externí disk a data tak lze stáhnout. Do Target modu počítač dostaneme zapínacím tlačítkem a stisknutím klávesy T. Problém nastává, když zařízení v Target modu připojíte k počítači, který neumí číst souborový systém Applu. Starší souborový systém HFS+, v macOS nazývaný Mac OS Extended, využíval Apple do konce roku 2017. S tím většina SW a HW dnes nemá problém, proto můžeme takový disk zajistit i pomocí freeware nástroje FTK Imager, nebo přes forenzní duplikátor. Velkou překážkou při zajišťování může být nový souborový systém Apple File System (APFS), se kterým si většina nástrojů dodnes neumí poradit. Nejjednodušším příkladem, jak počítač s APFS zajistit v Target modu, je s využitím počítače běžícím na macOS. Ten totiž zařízení bez problému rozpozná, v případě využití šifrování FileVault 2 (předchozí generace šifrovala jen domovskou složku) je možné zadat heslo a tak disk okamžitě procházet. Vytvoření image ve formátu .dd je možné přes jednoduchý příkaz v Terminálu. Image lze vytvořit i bez zadání hesla.

Pro vytvoření obrazu disku ve formátu .dd je potřeba nejdříve ověřit, který disk hledáme. K tomu napomůže příkaz:

```
$ diskutil list
```

V případě, že jsme disk připojili dešifrovaný, nebo jsme zadali heslo, je třeba disk softwarově vysunout. V opačném případě tento příkaz můžeme ignorovat.

```
$ diskutil unmountDisk /dev/diskX
```

(X pouze vyměníme za číslo vybraného disku)

Teď už pouze s příkazem dd vytvoříme image požadovaného disku. V příkazu zadáme za if= zdrojový disk a za of= cestu, kam chceme image uložit.

Číslo za bs= značí velikost bloku (není nutné mít v příkazu vůbec).

```
$ sudo dd if=/dev/diskX of=/Volumes/image.dd bs=1m
```

Pokud chceme kontrolovat průběh vytváření image, klávesovou zkratkou Ctrl + Shift + T zjistíme aktuální stav.

Použití speciálních nástrojů

Jednou z dalších možností, jak vytvořit image z počítačů Apple, je využití speciálních nástrojů. Nejběžnějším je řešení MacQuisition od firmy BlackBagTech, další možností je RECON Imager od SUMURI. Oba produkty fungují obdobným způsobem, dokáží pracovat s APFS, FileVault 2, Fusion Drive a zvládnou zajistit data RAM i bez zadání hesla. Dokonce se po čerstvých updatech zvládnou vypořádat i s čipem T2. To v praxi znamená, že lze zajistit zařízení bez problémů přes Target mode z jiného zařízení Apple, v opačném případě je nutné znát administrátorské údaje a vypnout Secure Boot.

U daných řešení je možné zajistit data tak, aby šla zpracovat v jakémkoli forenzním nástroji – na logické úrovni. Souborový systém APFS už částečně zvládá i EnCase nebo Magnet AXIOM. Nejlepší je samozřejmě pracovat se softwarem od firmy, která řešení nabízí. V případě MacQuisitionu je jím Blacklight a výsledky z RECON Imageru spolehlivě zpracujeme v RECON Labu.

Protože zařízení běžící na macOS fungují jinak, než ty na Windows, zajištěná data se zkoumají jiným způsobem, i když výsledky mohou být obdobné. Jednou z důležitých položek na seznamu, která je obdobná souboru Windows.edb jsou tzv. Apple Extended Attributes. Díky těmto atributům je celý obsah počítače naindexovaný a lze z nich získat zajímavá data.

Další specialitou jsou disky Fusion Drive, které spojují více fyzických disků a jsou zobrazovány jako jeden. Původní myšlenka tohoto systému byla využít menší disk SSD na operace vyžadující rychlý přístup a větší disk HDD na objemná a méně často potřebná data. Tyto disky byly původně instalované z výroby jako jeden disk, nicméně Fusion Drive může být použitý i na více fyzických discích najednou. Problém pak nastává v momentě, kdy zajistíme 2 disky a každý zvlášť necháme zpracovat. Podobně jako u RAIDu z disků nebudeme schopni zpracovat žádná data. Samozřejmě je možné disky později spojit na zařízení macOS a vytvořit z nich novou image, ale lepší možnost je tomu předejít užitím zmíněných nástrojů.

Obdobou Volume Shadow Copies ze zařízení Windows jsou Local Time Machine Snapshots. Ty využívá aplikace Time Machine v případě, že se zálohy provádí přímo na zařízení, ne na jiný cílový disk. Jejich analýza může odhalit různé starší verze souborů, nebo některé již smazané soubory.

Hojně využívanou funkcí na macOS je BootCamp. Ten umožňuje uživatelům rozdělit interní disk a nainstalovat operační systém jiných výrobců, zejména Windows. Z této části disku jsou oba nástroje schopny vytvořit image, se kterou lze následně pracovat jako s jakýmkoli jiným obrazem daného systému.

Použití zmíněných nástrojů je jednoduché a intuitivní. Pomocí kláves Alt/Option a tlačítka zapnutí se počítač zapne ve Startup Manageru. Tam nalezneme možnost volby startovacího disku. Mimo Macintosh HD nalezneme v případě RECON Imageru další tři spustitelné ikony, z těch je pak nutné vybrat tu správnou v závislosti na modelu počítače. V cestě může zabránit již zmíněný Secure Boot a nebo Firmware Password, který však Apple Certified Technician může odstranit. Po nabootování se zobrazí okno macOS Utilities, kde je nutné vybrat aplikaci RECON Imager a zvolit Continue.

Následně se zobrazí okno aplikace. V horní části je několik ikon, které otevírají okna daných funkcí. Seznam všech připojených zařízení a interních disků se nalézá hned pod tou první, s názvem Disk Manager. Mimo běžné informace (model, velikost, typ, souborový systém) zobrazuje Disk Manager i informace o spuštěném šifrování (FileVault), nebo discích ve Fusion Drive. Před zajišťováním zašifrovaného disku je možnost jej hned dešifrovat pomocí hesla nebo recovery klíče.

Disk Imager zajistí, jak již název napovídá, vytvoření image disku. RECON Imager umí zajišťovat v běžných formátech – DD, E01, Ex01, nebo DMG. Logicky data zajistí do složky, archivu, nebo zmíněného DMG formátu, ten je ovšem nadále spustitelný jen na zařízeních Apple. Před spuštěním lze samozřejmě vybrat cíl, zadat název, vlastníka, nebo sériové číslo zařízení. Je možné také vybrat datumově jen některé zálohy (Time Machine Snapshots).

Samozřejmostí je i verifikace image, u fyzických formátu lze spočítat kontrolní sumy MD5 a SHA-1. U logických lze udělat to samé, je ale nutné počítat s prodloužením doby zpracování, protože se kontrolní sumy budou počítat i na vstupních souborech. Výhodou následného procesování v aplikaci RECON Lab je, že zvládá zpracovat i Apple Extended Metadata, která jsou specialitou souborového systému APFS a v jistých případech mohou ukládat podstatná data o souborech, ale o tom až někdy příště. Pokud se u konkurence do doby vydání článku nic nezměnilo, bylo SUMURI jediné s tímto řešením na trhu.

MacQuisition má širší možnosti nastavování pro zajištění. V menu má 3 důležité ikony, první jsou informace o případu (Case Details), další je ikona Data Collection, která dává možnost nastavení typů dat, která chceme zajistit. Nastavit lze různé uživatelské složky, typy souborů, nebo systémová data.

V některém z dalších článků si určitě rozebereme, k čemu různé soubory slouží a co z nich lze získat.

Vytvoření image v MacQuisitionu je podobně jednoduché, jako v RECON Labu. Stačí vybrat disk, formát, kontrolní sumy a cílovou destinaci, to vše se skrývá v poslední důležité ikoně Image Device. Image lze zapsat i na disk ve formátu NTFS, což není standartní vlastnost počítačů běžících na macOS. Nespornou výhodou MacQuisitonu je možnost zajišťování dat na běžícím počítači. Na to SUMURI myslelo dalším softwarem – RECON Triage.

K zajišťování dat na běžícím počítači samozřejmě nejsou třeba výše zmiňovaná řešení. Bez hlubších znalostí systému a příkazů v Terminálu nám ale značně ulehčí život. Můžeme si ale ukázat alespoň pár základních příkazů, které nám pomůžou při zajišťování.

Následující příkaz vypíše seznam uživatelů a uloží jej to souboru formátu txt. Název souboru si můžete samozřejmě vybrat, stejně jako cestu.

```
dscl . list /Users | grep -v '_' > users.txt
```

Informace o počítači a další informace jako nainstalované aplikace vypíšou tyto příkazy.

```
system_profiler -detailLevel full SPHardwareDataType > hwdatatype.txt

system_profiler -detailLevel full SPApplicationsDataType > apps.txt

system_profiler -detailLevel full SPSerialATADataType > hdd.txt

system_profiler -detailLevel full SPNVMeDataType > hdd2.txt

system_profiler -detailLevel full SPUSBDataType > usb.txt

system_profiler -detailLevel full SPInstallHistoryDataType > apps.txt
```

Kontrolní součet SHA-1 zkopírovaných, nebo jinak potřebných souborů zajistíme následujícím příkazem. Tečka značí aktuální místo (složku), ve které se nacházíme. Lze nahradit jakoukoli cestou.

```
find . -exec shasum {} \; > sum.txt
```

Závěr

Zajišťování dat na zařízeních Apple není nikterak složité, stačí znát drobné základy a pár odlišností, které se daného systému týkají. Problém může být s čipem T2 nebo šifrováním FileVault, na druhou stranu to není nic nového, s čím bychom se na počítačích s Windows ještě nesetkali. Rozhodně se vyplatí k zajišťování využívat řešení od BlackBagTechu nebo Sumuri, to může zjednodušit celý proces, navíc v kombinaci s jejich nástroji pro následnou analýzu. Jejich nástroje dosud na trhu nemají konkurenci.

Dominik Novák *je nezávislým expertem v oblasti digitální forenzní analýzy mobilních zařízení a eDiscovery. Dlouhodobě se specializuje na zařízení s operačními systémy iOS a macOS.*

PRVNÍ END-TO-END ŘEŠENÍ PRO ZAJIŠTĚNÍ DAT A ANALÝZU APFS

+

BLACKLIGHT® MACQUISITION™

BlackLight 2019 R1 je univerzálním forenzním nástrojem pro analýzu dat z počítačů s OS Windows, macOS i Linux.

Školení pro BlackLight a MacQuisition v češtině!

MOBILYZE

Rozšiřte své možnosti při zajišťování dat z telefonů s iOS a Android s Mobilyze 2019

BlackBag® TECHNOLOGIES

Distribuci, prodej a školení v ČR a SR zajišťuje:

FIREWIRE REVOLUTION CZ
by forensee
5. května 2
140 00 Praha 4

www.firewire-revolution.cz
info@firewire-revolution.cz

+420 315 55 88 70

FWR FIREWIRE REVOLUTION

forensee digital forensics