

Obnova dát zo zariadenia poškodeného vodou

Radovan Šašala

<https://bcstudent.fpvucm.sk/~sasalaradovan/dfa/prezentacia.pdf>

Motivácia

Cieľom vyšetrovania je obnoviť kľúčové údaje z elektronického zariadenia (napr. smartfón, tablet, notebook), ktoré bolo poškodené vodou. Zariadenie môže obsahovať dôležité informácie, ako sú správy, fotografie, videá alebo GPS údaje, ktoré môžu byť rozhodujúce pri vyšetrovaní trestného činu alebo inej právnej záležitosti. Obnova týchto dát je nevyhnutná pre získanie dôkazov a podporu právnych procesov.

Ciele vyšetrovania

1. Zistiť rozsah poškodenia a možnosti obnovy dát:

- Preskúmať mieru poškodenia zariadenia v dôsledku kontaktu s vodou.
- Vyhodnotiť, ktoré dátové segmenty sú stále obnoviteľné.

2. Obnoviť dáta zo zariadenia:

- Získať zmazané alebo poškodené súbory pomocou špecializovaných forenzných softvérov.

3. Podporiť vyšetrovanie a právne procesy:

- Poskytnúť jasné a nespochybniteľné dôkazy získané z obnovených dát.
- Pripraviť forenznú správu, ktorá môže slúžiť ako dôkaz v súdnom konaní.

Zdroje

https://dfrws.org/wp-content/uploads/2019/11/2019_USA_paper-forensic_analysis_of_water_damaged_mobile_devices.pdf

Vodou poškodené mobilné zariadenia sa často dostávajú do forenzných laboratórií, či už v dôsledku nehody alebo zámerného ničenia dôkazov. Tradičná metóda obnovy dát pomocou čipovej extrakcie (chip-off) je pri šifrovaných zariadeniach neúčinná bez odomykacieho kódu. Účinným riešením je preto obnovenie funkčnosti zariadenia, čo umožní prístup k dátam po zadaní dešifrovacieho kódu. Hoci transplantácia pamäťových čipov na inú dosku môže pomôcť, ide o časovo náročnú metódu. Článok opisuje elektrochemické poškodenia spôsobené vodou a účinné opravné postupy, ktoré môžu zariadenie uviesť späť do prevádzkyschopného stavu a umožniť úspešnú obnovu dát.

<https://dfrws.org/presentation/behind-the-scenes-of-memory-extraction/>

Extrakcia pamäte je prvým krokom pri forenznej analýze systému. Existuje celý rad nástrojov - bezplatných aj komerčných, softvérových aj hardvérových - ktoré tomuto procesu pomáhajú, ale čo sa vlastne deje na najnižších úrovniach? Začneme hlbokým technickým ponorom do toho,

ako hardvérové zariadenie pristupuje k pamäti, a potom prejdeme niekoľkými praktickými laboratóriami, v ktorých budeme extrahovať pamäť z cieľa, identifikovať mechanizmy na opravu cieľa a nakoniec vykonať úpravy pamäte cieľa. Ak nám to čas dovoľí, použijeme na prístup k pamäti na vývojovej doske x86 protokoly PCIe aj JTAG. Na záver budeme diskutovať o súčasných ťažkostiach pri extrakcii pamäte, ako aj o niektorých súčasných a budúcich obchádzkach rôznych ochranných mechanizmov.

Kto?

- Páchateľ: Neznámy bankový lupič
- Vyšetrovatelia: Forenzní analytici, polícia
- Svedkovia: Pracovníci banky, zákazníci, prípadne iní ľudia v okolí

Čo?

- Banková lúpež, počas ktorej páchateľ zahodil mobilný telefón
- Mobilný telefón bol nájdený vo vode
- Cieľom je získať údaje z telefónu, ktoré by mohli pomôcť identifikovať páchateľa

Kde?

- Miesto lúpeže: Banka
- Miesto nájdenia telefónu: Vodný útvar (rieka Trnávka)

Ako?

- Páchateľ pri úteku zahodil telefón
- Telefón bol neskôr nájdený vyšetrovateľmi vo rieke
- Forenzná analýza bude zahŕňať sušenie, dekódovanie dát a snahu o obnovu údajov

Kedy?

- 4.3.2025 o +/- 16:00 podľa svedkov
- Čas, kedy bol telefón nájdený vo vode bol 16:45
- Čas, ktorý prešiel, kým bol telefón vo vode (+/-45min)

Prečo?

- Cieľom je identifikovať páchateľa a získať dôkazy, ktoré ho spoja s lúpežou
- Telefón môže obsahovať dôležité informácie, ako napr. kontakty, správy, fotografie, GPS údaje či posledné hovory

Hypotéza č. 1: Mobilný telefón patrí páchatelovi bankovej lúpeže a obsahuje dôkazy

- Telefón, ktorý bol nájdený vo vode, patrí priamo lupičovi.
- Obsahuje relevantné údaje, ako napríklad správy, hovory alebo GPS záznamy, ktoré môžu potvrdiť jeho účasť na lúpeži.
- Kamerané záznamy môžu preukázať, že páchatel mal tento telefón pri sebe pred alebo počas lúpeže.

Hypotéza č. 2: Telefón nepatrí lupičovi, ale bol náhodne nájdený na mieste činu

- Telefón mohol patriť nevinnému človeku, ktorý ho stratil pred lúpežou alebo krátko po nej.
- Lupič ho mohol nájsť, omylom stratiť alebo zahodiť do vody, aby zničil dôkazy.
- Forenzná analýza nemusí poskytnúť priamy dôkaz o jeho prepojení s trestným činom.

Hypotéza č. 3: Telefón bol úmyselne hodený do vody na zničenie dôkazov

- Páchatel si uvedomil, že telefón môže obsahovať usvedčujúce dôkazy, a preto ho hodil do vody, aby znemožnil prístup k dátam.
- Napriek poškodeniu vodou môžu forenzní odborníci obnoviť niektoré údaje, ktoré pomôžu identifikovať páchatela.
- Kamerané záznamy môžu zachytiť moment, keď telefón skončil vo vode, čo pomôže rekonštruovať priebeh udalostí.

4,457 súborov, 1.9GB dát , zdroj dataset: <http://roussev.net/t5/t5.html>

Typ analyzovanej stopy:

V rámci forenzej analýzy zariadenia boli skúmané rôzne typy digitálnych stôp, ktoré môžu obsahovať relevantné informácie súvisiace s prípadom. Medzi analyzované súbory patria:

- **Textové dokumenty:**
 - **TXT, DOC, PDF, PPT, XLS** – potenciálne obsahujú textovú komunikáciu, finančné záznamy, prezentácie alebo tabuľky s dôležitými údajmi.
- **Obrázkové a multimediálne súbory:**
 - **JPG, GIF** – vizuálne dôkazy, ako sú snímky dokumentov, fotografie miest činu alebo iné grafické súbory, ktoré môžu obsahovať skryté informácie.
- **Webové a elektronické dokumenty:**
 - **HTML** – zachytené webové stránky, uložené emaily alebo iné digitálne informácie relevantné pre vyšetrovanie.

Tieto súbory boli podrobené analýze s cieľom obnoviť prípadne zmazané dáta, identifikovať ich pôvod a zistiť, či obsahujú dôkazy súvisiace s trestnou činnosťou.

Dáta uložené na mobilnom zariadení boli presunuté na USB zariadenie. Bolo tak urobené z dôvodu lepšej manipulácie so zariadením a aby nedošlo k ďalšiemu poškodeniu zariadenia.

Forenzná analýza USB zariadenia v kontexte bezpečnostného incidentu

Zariadenie: USB kľúč

Značka: Kingston

Model: Exodia White 32GB

Sériové číslo: 55EA573DF1731793C0360&0

Kapacita úložiska: 32 GB

Rozhranie: USB 3.2 Gen 1

Konektor: USB-A

Rýchlosť čítania: 100 MB/s

Rýchlosť zápisu: 30 MB/s

Materiál: Plast

Vyhotovenie: Platové prevedenie s krytkou na konektor

Rozmery: 60 mm (dĺžka) x 20,1 mm (šírka) x 9.8 mm (výška)

Hmotnosť: 8 g

Farba: Biela

Bezpečnostné opatrenia pri manipulácii s USB:

1. Fyzická ochrana

- USB kľúč bol uložený do antistatického obalu a bezpečnostného puzdra.
- Chránený pred teplotnými výkyvmi, vlhkosťou a elektromagnetickými poľami.

2. Digitálna ochrana

- USB kľúč nebol pripájaný k bežnému počítaču, aby sa predišlo zmene dát.
- Použitý write-blocker na ochranu pred zápisom a zabezpečenie integrity dát.
- Čo najskôr vytvorený forenzný obraz pomocou FTK Imager.

3. Dokumentácia a skladovanie

- Evidovaný dátum, čas a miesto nálezu, ako aj všetky manipulácie s USB kľúčom.
- Uchovávaný v zabezpečenom trezore a analyzovaný v izolovanom prostredí, aby sa predišlo neoprávnenému prístupu.

Bezpečnostné opatrenie pri manipulácii s mobilným telefónom:

1. Fyzická ochrana

- Telefón bol po nájdení ihneď vložený do vodotesného a antistatického obalu, aby sa zabránilo ďalšiemu poškodeniu.
- Zariadenie bolo osušené a stabilizované v kontrolovanom prostredí s regulovanou vlhkosťou a teplotou.
- Počas manipulácie boli použité rukavice a ochranné pomôcky, aby sa predišlo kontaminácii dôkazového materiálu.

2. Digitálna ochrana

- Telefón nebol zapnutý v bežnom prostredí – zapnutie a analýza prebehli výhradne v forenznom laboratóriu.
- Použité boli metódy na zabezpečenie integrity dát – vrátane výpočtu hash hodnôt (MD5, SHA1) a vytvorenia kópií na zabezpečené úložisko.

3. Dokumentácia a skladovanie

- Boli zaznamenané všetky údaje o náleze telefónu – dátum, čas, miesto (rieka), meno osoby, ktorá ho našla, a spôsob zaistenia.
- Telefón bol evidovaný v Chain of Custody protokole a označený jedinečným identifikačným číslom.

ČO

- Zariadenie bolo uložené do uzamykateľného trezoru v laboratóriu a manipulovalo sa s ním výhradne v kontrolovanom prostredí pod dohľadom forenzného špecialistu.



Bitové kópie:

Po úspešnej extrakcii dát z mobilného telefónu boli vytvorené dve identické forenzné kópie dát. Jedna z týchto kópií bola uložená na **forenzne zaistený USB kľúč**, ktorý slúži ako referenčná verzia na analytické účely. Druhá kópia bola uložená na **zabezpečený server v laboratóriu**, kde je chránená proti neoprávnenému prístupu a slúži ako záložná verzia. Pri tvorbe oboch kópií boli vypočítané hash hodnoty (MD5 a SHA1), ktoré potvrdzujú ich integritu a nemennosť počas celej manipulácie.

Použité nástroje:

- **FTK Imager** – softvér určený na vytvorenie forenzných obrazov USB zariadení a zabezpečenie ich integrity.
- **Autopsy** – forenzný nástroj na podrobnú analýzu obsahu USB diskov, vrátane obnovy zmazaných súborov.
- **HxD Hex Editor** – nástroj na nízkoúrovňovú analýzu dát a pamäte v hexadecimálnom formáte, vhodný na identifikáciu skrytých alebo manipulovaných informácií.

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 123

Unique description: 071

Examiner: Radovan Šašala

Notes: USB kľúč Kingston, biely, 32GB

Information for D:\usb-biele-32gb-kingston\usb-kluc-32gb-kingston:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3 768

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 60 538 881

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: 0000000005

Drive Interface Type: USB

Removable drive: True

Source data size: 29560 MB

Sector count: 60538881

[Computed Hashes]

MD5 checksum: c0880ecd35dd5a09a7b7fba4195b922a

SHA1 checksum: 84c41c600939fed7e93495bc9841db1d36eea7c7

Image Information:

Acquisition started: Mon Mar 3 17:45:12 2025

Acquisition finished: Mon Mar 3 17:46:10 2025

Segment list:

D:\usb-biele-32gb-kingston\usb-kluc-32gb-kingston.001

COMPUTED HASH : c0880ecd35dd5a09a7b7fba4195b922a

COMPUTED HASH : 84c41c600939fed7e93495bc9841db1d36eea7c7

Image Verification Results:

Verification started: Mon Mar 3 17:48:10 2025

Verification finished: Mon Mar 3 17:49:36 2025

MD5 checksum: c0880ecd35dd5a09a7b7fba4195b922a : verified

SHA1 checksum: 84c41c600939fed7e93495bc9841db1d36eea7c7 : verified

Dôkazový nález v forenznom obraze zariadenia:

Pri analýze forenzného obrazu získaného zo zariadenia bol v hexadecimálnom zobrazení identifikovaný reťazec obsahujúci slovo "BANKA". Tento nález naznačuje možnú súvislosť zariadenia s trestnou činnosťou súvisiacou s bankou.

Detailná analýza:

- Hexadecimálny výpis obsahuje adresár „loads\V.U“ a následný reťazec „BANKA“, čo môže naznačovať uložené alebo spracované informácie súvisiace s bankovou činnosťou.
- Výskyt slova "BANKA" v dátach môže znamenať, že zariadenie obsahovalo dokumenty, transakčné údaje alebo iné citlivé informácie relevantné k prípadu.
- Na ďalšiu analýzu budú využité nástroje Autopsy a HxD Hex Editor, ktoré umožnia hlbšie skúmanie a rekonštrukciu možných zmazaných súborov obsahujúcich kľúčové dôkazy.

Tento nález posilňuje hypotézu, že zariadenie mohlo byť použité na plánovanie alebo realizáciu trestného činu súvisiaceho s bankou. Na základe získaných dôkazov sa odporúča vykonať ďalšiu forenznú analýzu obsahu pamäte a vyhľadať ďalšie relevantné informácie.

```
15b0feb60 | 6C 00 6F 00 61 00 64 00-73 00 5C 00 56 00 55 00 | 1·o·a·d·s·\·V·U·
15b0feb70 | 01 03 42 00 20 00 42 00-41 00 4E 00 4B 00 41 00 | ·B· ·B·A·N·K·A·
```

Chain of Custody (USB)

Číslo	1	Typ Súborov	.mem	Obnovený súbor	Nie	Veľkosť	17271808kB
Popis prípadu		Obsah mobilného zariadenia (na USB)					
Názov súboru		memdump.mem					
Miesto získanie digitálnej stopy		Presunuté dáta z hlavného zariadenia					
Poznámky		Po získaní dát sa presunuli na USB kľúč					
Digitálny otlačok (hash)	MD5	c0880ecd35dd5a09a7b7fba4195b922a					
	SHA1	84c41c600939fed7e93495bc9841db1d36eea7c7					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Mon Mar 3 17:45:10 2025		Začiatok kontroly					
Mon Mar 3 17:46:36 2025		Koniec kontroly					

Chain of Custody (Mobil)

Číslo	1	Typ Súborov	.mem	Obnovený súbor	Nie	Veľkosť	17271808kB
Popis prípadu		Samsung Galaxy A52					
Názov súboru		samsungS21_memdump.mem					
Miesto získanie digitálnej stopy		Zariadenie bolo nájdené v rieke					
Poznámky		Po získaní dát sa presunuli na USB kľúč					
Digitálny otlačok (hash)	MD5	c0880ecd35dd5a09a7b7fba4195b922a					
	SHA1	84c41c600939fed7e93495bc9841db1d36eea7c7					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Mon Mar 3 17:55:46 2025		Začiatok kontroly					
Mon Mar 3 18:02:51 2025		Koniec kontroly					

Analýza zaujímavých údajov:

From: miro.novak@protonmail.com
To: r.kovac82@tutanota.com
Subject: Dokumenty pre =?utf-8?q?=C5=A1tvrtkov=C3=A9?= stretnutie
Date: Sat, 01 Mar 2025 19:47:00 +0100
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0

Ahoj Robo,

v pr=C3=ADlohe nen=C3=A1jde=C5=A1 =C5=BEiadne "ofici=C3=A1lne" papiere, ale v=ie=C5=A1, =C4=8Do t=C3=BDm mysl=C3=ADm. Utorok e=C5=A1te skontroluj pr=C3=ADs=tupov=C3=BD bod vzadu =E2=80=93 =C3=BAďajne tam niekto menil z=C3=A1mky. Nech=ceme =C5=BEiadne prekvapenia.

Mimochodom, info z vn=C3=BAtra: od 03:15 do 03:45 nebe=C5=BEia z=C3=A1znamy. =M=C3=A1me presne 30 min=C3=BAť.

Daj vedie=C5=A5, =C4=8Di m=C3=A1=C5=A1 tie n=C3=A1stroje.

M.|

Táto mailová komunikácia zreteľne poukazuje na plánovanie tajnej akcie v čase, keď bezpečnostné záznamy nie sú aktívne. Použité formulácie ako „žiadne oficiálne papiere“, „prístupový bod“ a „nebežia záznamy“ naznačujú pokus o utajenie činnosti a koordináciu prístupu do chráneného priestoru.

WhatsApp Chat - Miro & Robo

[2025-03-01 21:14] Miro: Kamera v hale bude vypnutá od 03:15 do 03:45
[2025-03-01 21:16] Robo: Paráda. Doniesol som masky a náradie
[2025-03-02 00:06] Miro: Nezapadni, rukavice – žiadne odtlačky
[2025-03-03 19:23] Robo: Dobre

Preverovanie hypotézy č. 1 sa predpokladá, že mobilný telefón nájdený vo vode patrí priamo páchatelovi bankovej lúpeže a obsahuje dôkazy, ktoré môžu potvrdiť jeho účasť na trestnej činnosti. Zariadenie bolo objavené krátko po lúpeži v blízkosti miesta činu, čo vyvoláva podozrenie, že sa ho páchatel pokúsil zbaviť s cieľom zničiť digitálne stopy. Forenzná analýza zariadenia odhalila viacero relevantných údajov, ktoré naznačujú jeho zapojenie do plánovania a realizácie lúpeže.

V pamäti telefónu sa nachádzajú správy zaslané a prijaté prostredníctvom komunikačnej aplikácie WhatsApp, ktoré obsahujú detailné informácie o čase vypnutia kamerového systému, kóde k trezoru a logistike lúpeže. Ďalej boli identifikované poznámky obsahujúce presný časový harmonogram, heslá a pokyny, ktoré korešpondujú s priebehom udalostí.

Tieto zistenia spolu vytvárajú ucelený obraz o tom, že telefón nebol len náhodným nálezom, ale ide o kľúčový dôkaz, ktorý potvrdzuje vlastníctvo zariadenia páchatelom a jeho priamu účasť na plánovaní a realizácii bankovej lúpeže.

Preverovanie hypotézy č. 3 sa predpokladá, že mobilný telefón bol po spáchaní bankovej lúpeže úmyselne zničený s cieľom znemožniť prístup k dôkazom. Krátko po čine niekoľkí svedkovia uviedli, že videli osobu v tmavom oblečení, ako cielene hádže predmet – nápadne pripomínajúci mobilný telefón – do rieky. Následne túto osobu pozorovali, ako rýchlo opúšťa miesto. Táto situácia jasne naznačuje úmyselné konanie s cieľom zbaviť sa potenciálneho dôkazového materiálu.

Telefón bol neskôr nájdený a zaistený policajnou jednotkou. Napriek kontaktu s vodou sa forenznému tímu podarilo získať dáta zariadenia. Pri analýze bolo zistené, že pred vhodením do rieky nebol vykonaný pokus o vymazanie dát ani factory reset. Všetky dáta vrátane komunikačných aplikácií, poznámok a lokalizačných údajov boli prítomné a neporušené. Telefón však neobsahoval SIM kartu, čo poukazuje na snahu páchatela minimalizovať možnosť jeho identifikácie prostredníctvom mobilného operátora.

Tieto zistenia potvrdzujú, že telefón bol úmyselne zničený hodením do rieky s cieľom zamedziť prístup k obsahu, no vďaka rýchlemu zásahu forenzného tímu sa podarilo získať relevantné dáta, ktoré majú vysokú dôkaznú hodnotu.

Hypotéza č. 1 – mobilný telefón patrí páchatelovi bankovej lúpeže a obsahuje dôkazy – bola **potvrdená**. Zariadenie obsahovalo konkrétne informácie o čase lúpeže, kóde k trezoru a plánovanom postupe, ktoré boli zachytené v aplikácii na poznámky. Navyše sa v telefóne nachádzala komunikácia cez WhatsApp, kde sa spomínalo vypnutie kamerového systému a príprava na akciu, čo jednoznačne potvrdzuje zapojenie vlastníka zariadenia do plánovania a vykonania činu.

Hypotéza č. 2, ktorá predpokladala, že telefón nepatrí páchatelovi a bol na mieste činu náhodne, bola **nepotvrdená**. Všetky získané dáta vrátane poznámok a správ jednoznačne smerujú k tomu, že zariadenie aktívne slúžilo pri príprave a realizácii lúpeže. Nenachádzajú sa žiadne indície, ktoré by naznačovali, že by telefón patril nezainteresovanej osobe.

Hypotéza č. 3, ktorá predpokladala, že telefón bol úmyselne zničený s cieľom odstrániť dôkazy – **Potvrdená**. Zariadenie bolo hodené do rieky krátko po lúpeži, pričom svedkovia uviedli, že osoba v tmavom oblečení sa ho vedomo zbavila. Aj keď telefón nebol pred vhodením premazaný, jeho fyzická likvidácia nasvedčuje tomu, že páchatel si uvedomoval jeho dôkaznú hodnotu a snažil sa zabrániť jeho analýze.

Záver:

Na základe vykonanej digitálnej forenznej analýzy mobilného telefónu nájdeného v rieke možno s vysokou mierou istoty potvrdiť, že zariadenie patrilo priamo páchatelovi bankovej lúpeže. Telefón obsahoval usvedčujúce dáta vo forme poznámok, komunikačných správ, ktoré jasne dokumentujú plánovanie aj realizáciu trestného činu.

Z troch stanovených hypotéz bola potvrdená hypotéza č. 1 – telefón patril páchatelovi a obsahoval dôkazy, a tiež hypotéza č. 3 – telefón bol úmyselne zničený vhadením do rieky v snahe zabrániť prístupu k týmto dátam. Hypotéza č. 2, ktorá predpokladala náhodný nález telefónu bez súvisu s činom, bola na základe analýzy obsahu jednoznačne vyvrátená.

Po zaistenej extrakcii boli vytvorené dve forenzne kópie dát – jedna bola uložená na zabezpečený USB kľúč a druhá na interný server v laboratóriu. Obe verzie boli overené pomocou hash funkcií, čo zabezpečilo integritu digitálnych dôkazov počas celého procesu.

Vyšetrenie preukázalo, že dôsledná digitálna analýza dokáže aj napriek pokusu o likvidáciu dôkazov odhaliť kľúčové informácie a prispieť k objasneniu trestnej činnosti. Forenzne postupy boli realizované s dôrazom na bezpečnosť, transparentnosť a zachovanie dôkaznej hodnoty.