

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED

DIGITÁLNA FORENZNA ANALÝZA

Neoprávnená finančná transakcia

[Prezentácia](#)

Obsah

1. Popis prípadu	3
2. Motivácia	4
3. 5WH Analýza	5
4. Hypotézy	6
5. Identifikácia zariadenia	7
6. Zaisťovanie a zber dát	8
7. Uchovanie dôkazov	9
8. Analýza	11
8.1 Analýza SMS správ	13
8.2 Analýza prehliadača	14
9. Záver	16

Zoznam obrázkov

Obrázok 1 Prehľad dát v zariadení.....	11
Obrázok 2 Štruktúra súborového systému Samsung.....	12
Obrázok 3 SMS databáza	13
Obrázok 4 Podozrivá sms.....	14
Obrázok 5 Zobrazenie tabuľky httpbookmarks z databázy browser.db v nástroji Autopsy	14
Obrázok 6 Podozrivá url stránka	15

Popis prípadu

Dňa 14.3.2026 sa majiteľ bankového účtu dostavil do pobočky banky s požiadavkou na prešetrenie podozrivej finančnej transakcie a žiadosťou o náhradu vzniknutej škody. Podľa výpisu z účtu bola dňa 13.1.2026 realizovaná online transakcia smerujúca na neznámy účet, pričom klient uviedol, že v danom čase nevykonával žiadnu finančnú operáciu ani sa neprihlasoval do svojho internetového bankovníctva.

Klient zároveň deklaroval, že neklikol na žiadny podozrivý odkaz ani nezažadoval svoje prihlasovacie údaje na neznámych webových stránkach a že na prístup k bankovým službám využíva výhradne mobilné zariadenie. Na základe týchto skutočností bolo zo strany banky potrebné preveriť, či mohlo dôjsť k zneužitiu prihlasovacích údajov, napríklad prostredníctvom phishingového útoku, alebo či transakcia mohla byť vykonaná samotným klientom, alebo pochybením banky, kedy by musela klienta odškodniť.

Za účelom objasnenia incidentu bolo pristúpené k digitálno-forenznej analýze mobilného zariadenia klienta. Zariadenie bolo zaistené a následne analyzované pomocou forenzného nástroja Autopsy, pričom cieľom analýzy bolo identifikovať digitálne stopy súvisiace s prijatými správami, navštívenými webovými stránkami a potenciálnym únikom prihlasovacích údajov. Keďže klient nepoužíva osobný počítač ani iné zariadenia, analýza bola zameraná výhradne na mobilné zariadenie.

Počas analýzy boli skúmané najmä databázy SMS správ, história internetového prehliadača, databázy aplikácií sociálnych sietí a komunikačných aplikácií, ako aj systémové logy zariadenia. Na základe získaných poznatkov bolo cieľom rekonštruovať priebeh incidentu, identifikovať potenciálne zdroje kompromitácie a posúdiť, či klient mohol byť vystavený phishingovému útoku vedúcemu k neoprávnenému prístupu k jeho bankovému účtu.

1. Motivácia

V rámci štúdia digitálnej forenznej analýzy bol vytvorený fiktívny prípad a fiktívne dôkazy.

Použitý dataset:

https://s3.amazonaws.com/cftt.cfreds.nist.gov/cfreds/mobile/CHIPOFF/HTC+Desire+S/HTC_Desire_S.img

Cieľom vyšetovania je zodpovedať nasledujúce otázky:

1. Aké aktivity používateľa na mobilnom zariadení možno zrekonštruovať v čase pred realizáciou podozrivej finančnej transakcie a čo z nich vyplýva?
2. Existujú dôkazy o prijatí podozrivej správy alebo interakcii používateľa s potenciálne phishingovým obsahom?
3. Je možné preukázať, že používateľ bol presmerovaný na podvodnú webovú stránku alebo iným spôsobom komunikoval s neznámou externou stranou?
4. Došlo k možnému úniku prihlasovacích údajov používateľa, a ak áno, akým spôsobom mohli byť tieto údaje získané?

2. 5WH Analýza

Who? – Kto je podozrivý?

Neznámy útočník, ktorý získal prihlasovacie údaje do internetového bankovníctva a následne ich použil na vykonanie neoprávnenej finančnej transakcie.

What? – Čo sa stalo?

Došlo k neoprávnenému prístupu do internetového bankovníctva majiteľa účtu a následnému odčerpaniu finančných prostriedkov na neznámy účet bez vedomia a súhlasu majiteľa účtu.

When? - Kedy sa to stalo?

Incident bol zaznamenaný 14. januára 2026, keď majiteľ účtu zistil neoprávnenú transakciu vo svojom bankovom výpise. Samotná transakcia bola realizovaná 13. januára 2026. Na základe analýzy možno predpokladať, že ku kompromitácii prihlasovacích údajov došlo v období krátko pred realizáciou transakcie, pravdepodobne v rozmedzí niekoľkých hodín až dní pred 13. januárom 2026.

Where? – Kde sa to stalo?

K incidentu došlo v prostredí internetového bankovníctva majiteľa účtu.

Why? – Prečo sa to stalo?

Hlavným motívom útoku bola finančná motivácia. Cieľom útočníka bolo získať prihlasovacie údaje do internetového bankovníctva obete a následne ich zneužiť na neoprávnené finančné transakcie a odčerpanie finančných prostriedkov z účtu.

How? – Ako sa to mohlo stať?

Mohlo dôjsť k phishingovému útoku prostredníctvom SMS správy (smishing), alebo mohol používateľ zadať prihlasovacie údaje na podvodnej webovej stránke.

3. Hypotézy

Hypotéza 1: K neoprávnenej transakcii došlo bez vedomia používateľa v dôsledku phishingového útoku.

Overenie: Preskúmame databázu SMS správ s cieľom identifikovať podozrivé správy obsahujúce odkazy. Následne analyzujeme históriu prehliadača a cache, aby sme zistili, či došlo k otvoreniu podozrivej webovej stránky.

Výsledok: Ak nebudú identifikované podozrivé SMS správy a náznaky interakcie s webovým obsahom, hypotéza bude zamietnutá.

Hypotéza 2: K kompromitácii účtu došlo prostredníctvom škodlivého softvéru v zariadení.

Overenie: Preskúmame prítomnosť podozrivých aplikácií, spustiteľných súborov a systémových artefaktov v zariadení. Analyzujeme zoznam aplikácií a systémové logy.

Výsledok: Ak nebudú identifikované žiadne známky prítomnosti škodlivého softvéru, hypotéza bude zamietnutá.

Hypotéza 3: K úniku prihlasovacích údajov došlo prostredníctvom inej aplikácie alebo služby (napr. sociálne siete).

Overenie: Preskúmame databázy aplikácií (napr. Facebook, Gmail) a ich aktivitu, aby sme zistili, či nedošlo k podozrivej komunikácii alebo úniku údajov.

Výsledok: Ak sa nepreukáže žiadna podozrivá aktivita v týchto aplikáciách, hypotéza bude zamietnutá.

4. Identifikácia zariadenia

Mobilné zariadenie používateľa

- **Model: Samsung Galaxy S26 Ultra 5G**
 - **Operačný systém: Android 16 (Samsung One UI)**
 - **Typ úložiska: Interná flash pamäť (UFS)**
 - **Interná pamäť: 512 GB**
 - **RAM: 12 GB**
- **Parametre zariadenia:**
 - **Displej: 6,9" Dynamic AMOLED 2X**
 - **Rozlíšenie displeja: 3120 × 1440 px**
 - **Obnovovacia frekvencia: 120 Hz**
 - **Procesor: Qualcomm Snapdragon 8 Elite Gen 5**
 - **Počet jadier CPU: 8**
 - **Maximálna frekvencia procesora: 4,74 GHz**
 - **SIM: nano SIM + eSIM (Dual SIM)**
 - **Konektivita: 5G, Wi-Fi, Bluetooth, GPS, NFC**
 - **USB port: USB-C**
 - **Batéria: 5000 mAh**
 - **Odolnosť: IP68**

5. Zaist'ovanie a zber dát

Zber digitálnych dôkazov bol vykonaný s cieľom zachovať integritu dát a zabrániť ich poškodeniu alebo zmene. Postup zberu bol vykonaný podľa základných princípov digitálnej forenzej analýzy.

Postup zberu:

1. Mobilné zariadenie používateľa – Samsung Galaxy S26 Ultra

Mobilné zariadenie bolo zaistené ako potenciálny zdroj digitálnych dôkazov súvisiacich s neoprávnenou finančnou transakciou.

Po zaistení zariadenia bol vytvorený forenzný obraz úložiska zariadenia.

Evidenčné číslo: 01

Obraz zariadenia bol vytvorený pomocou forenzného nástroja FTK Imager.

Výsledný obraz bol uložený vo formáte E01 (EnCase Evidence File Format).

Následne bol tento obraz importovaný do forenzného nástroja Autopsy, kde prebiehala ďalšia analýza dát uložených v zariadení.

Poznámky k integrite dát:

- Pri vytváraní forenzného obrazu boli automaticky generované kontrolné súčty (hash hodnoty).
- Použité hash algoritmy: MD5 a SHA-1.
- Tieto hodnoty slúžia na overenie, že obraz zariadenia nebol počas analýzy zmenený.
- Forenzný obraz bol uložený do databázy prípadu v nástroji Autopsy, kde bol použitý na ďalšiu digitálnu analýzu.

6. Uchovanie dôkazov

Pri práci s digitálnymi dôkazmi boli použité základné forenzné postupy, ktorých cieľom je zachovať integritu dát a zabezpečiť ich použiteľnosť pri ďalšom vyšetrovaní.

Postupy pri uchovávaní:

- Zabezpečenie dôkazov prebehlo bez zmeny pôvodných dát – analýza bola vykonaná na forenznom obraze mobilného zariadenia, nie priamo na originálnom zariadení.
- Hashovanie (SHA-1 a MD5) bolo použité na overenie integrity získaného forenzného obrazu zariadenia.
- Zálohovanie dôkazov bolo vykonané uložením forenzného obrazu do zabezpečeného úložiska určeného pre digitálne dôkazy.
- Katalogizácia dôkazov bola vykonaná v rámci forenzného prípadu, kde bol zaznamenaný názov dôkazu, dátum vytvorenia obrazu a použitý nástroj.
- Retenčné pravidlá boli stanovené na dobu minimálne 5 rokov v súlade s internými pravidlami a legislatívou pre uchovávanie digitálnych dôkazov.

Nástroje použité pri uchovaní dôkazov:

FTK Imager – nástroj použitý na vytvorenie forenzného obrazu zariadenia.

E01 (EnCase Evidence Format) – formát použitý na uloženie digitálneho dôkazu.

Autopsy – nástroj použitý na následnú analýzu získaných dát.

Analýza bola vykonaná na pracovnej stanici s operačným systémom Windows

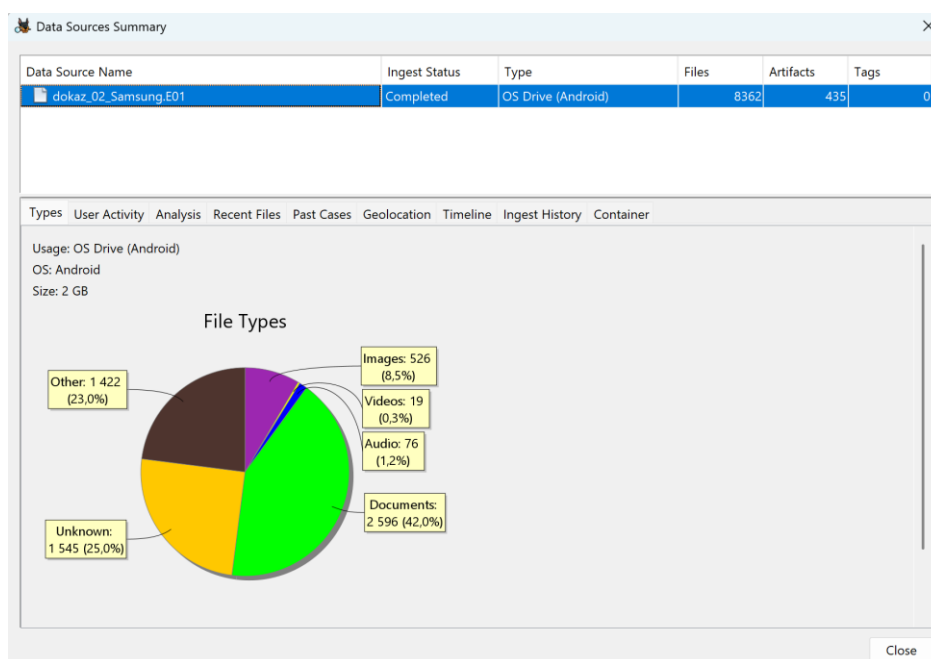
Detailný reťazec dôkaznej väzby (**chain of custody**) je uvedený v tabuľke 1.

Tabuľka 1 Chain of custody: Mobilné zariadenie Samsung Galaxy S26 Ultra

Číslo: 01	Typ súboru: E01	Obnovený súbor: nie	Veľkosť: 2152 MB												
Popis prípadu:		Neautorizované finančné transakcie z bankového účtu													
Názov súboru:		dokaz_02_Samsung.E01													
Miesto získania Digitálnej stopy:		Mobilné zariadenie používateľa, z ktorého boli vykonané neautorizované finančné transakcie													
Poznámky:		Forenzný obraz interného úložiska mobilného zariadenia													
Časové pečiatky															
Access: Mar 16, 2026 – 17:50:32		Modify: Mar 16, 2026 – 17:50:39	Change: -												
Digitálny odtlačok (heš)	MD5	31743dffa88639b4fa7e5157f183389													
	SHA1	b3fc67f8304e4b3840685975c5d912198ca936ec													
Časová pečiatka		Akcia vykonaná s digitálnou stopou													
Mar 14, 2026 15:00		Zaistenie mobilného zariadenia a jeho uloženie do ochranného obalu													
Mar 16, 2026 17:50		Vytvorený forenzný obraz mobilného zariadenia pomocou nástroja FTK Imager													
Mar 16, 2026 17:51		Vytvorené 2 pracovné kópie digitálnej stopy pomocou nástroja FTK Imager pre účely analýzy a archivácie													
Mar 16, 2026 17:53		Import forenzného obrazu do nástroja Autopsy													
Mar 16, 2026 17:55		Kontrola integrity digitálneho dôkazu pomocou hash MD5 a SHA1													
Image Verification Results: Verification started: Mon Mar 16 17:50:39 2026 Verification finished: Mon Mar 16 17:50:45 2026 MD5 checksum: 31743dffa88639b4fa7e5157f183389 : verified SHA1 checksum: b3fc67f8304e4b3840685975c5d912198ca936ec : verified															
Listing dokaz_02_Samsung.E01_1 Host Table Thumbnail Summary <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Size (Bytes)</th> <th>Sector Size (Bytes)</th> <th>Timezone</th> <th>Device ID</th> </tr> </thead> <tbody> <tr> <td>dokaz_02_Samsung.E01</td> <td>Image</td> <td>2256535552</td> <td>512</td> <td>Europe/Bratislava</td> <td>e051d44b-0958-4b42-9644-4535fbceb005</td> </tr> </tbody> </table> Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Metadata Name: /img_dokaz_02_Samsung.E01 Type: E01 Size: 2256535552 MD5: 31743dffa88639b4fa7e5157f183389 SHA1: b3fc67f8304e4b3840685975c5d912198ca936ec				Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID	dokaz_02_Samsung.E01	Image	2256535552	512	Europe/Bratislava	e051d44b-0958-4b42-9644-4535fbceb005
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID										
dokaz_02_Samsung.E01	Image	2256535552	512	Europe/Bratislava	e051d44b-0958-4b42-9644-4535fbceb005										

7. Analýza

Všetky získané dáta boli analyzované pomocou forenzného nástroja **Autopsy**, ktorý umožňuje prehliadať súborový systém zariadenia a analyzovať jednotlivé súbory a databázy aplikácií. Po načítaní forenzného obrazu do nástroja Autopsy bol vykonaný základný prehľad dát uložených v zariadení. Podľa obrázka 1 celkovo bolo identifikovaných 8362 súborov a 435 artefaktov. Najväčší podiel tvorili dokumenty (42 %), nasledované neznámymi typmi súborov (25 %) a ostatnými súbormi (23 %). Menší podiel predstavovali obrázky, audio a video súbory.



Obrázok 1 Prehľad dát v zariadení

Pri otvorení forenzného obrazu mobilného zariadenia bola identifikovaná štruktúra súborového systému Android. Dáta zariadenia sa nachádzali v oddieloch označených ako **Linux (0x83)**. Tieto oddiely obsahovali systémové priečinky a priečinky jednotlivých aplikácií.

V rámci analýzy bol preskúmaný najmä vol 92, kde sa nachádzal priečinok data, ktorý obsahuje dáta aplikácií nainštalovaných v zariadení. Každá aplikácia mala vlastný priečinok, napríklad:

- **com.android.browser**
- **com.android.phone**
- **com.amazon.mp3**

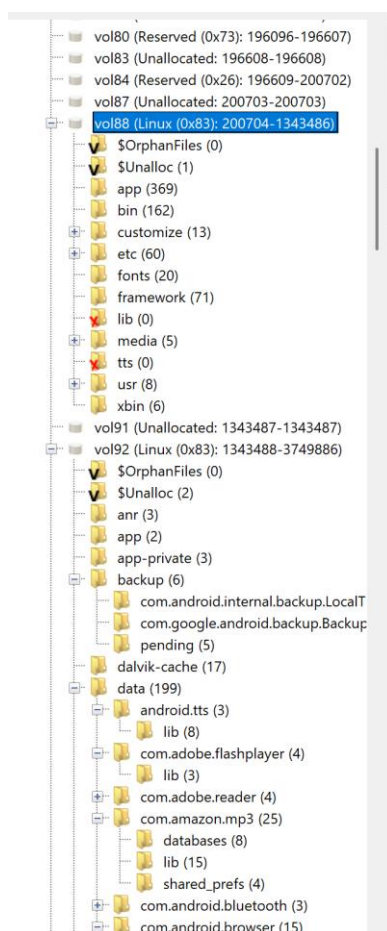
- **com.adobe.reader**

Tieto priečinky obsahovali ďalšie podpriečinky ako napríklad:

- **databases** – databázové súbory aplikácií
- **shared_prefs** – konfiguračné nastavenia aplikácií
- **lib** – knižnice aplikácií

Tieto súbory boli následne prehliadané pomocou nástroja Autopsy s cieľom identifikovať informácie o aktivite používateľa a potenciálne digitálne dôkazy súvisiace s vyšetrovaným incidentom.

Obrázok 2 zobrazuje štruktúru súborového systému mobilného zariadenia zobrazenú v nástroji Autopsy.



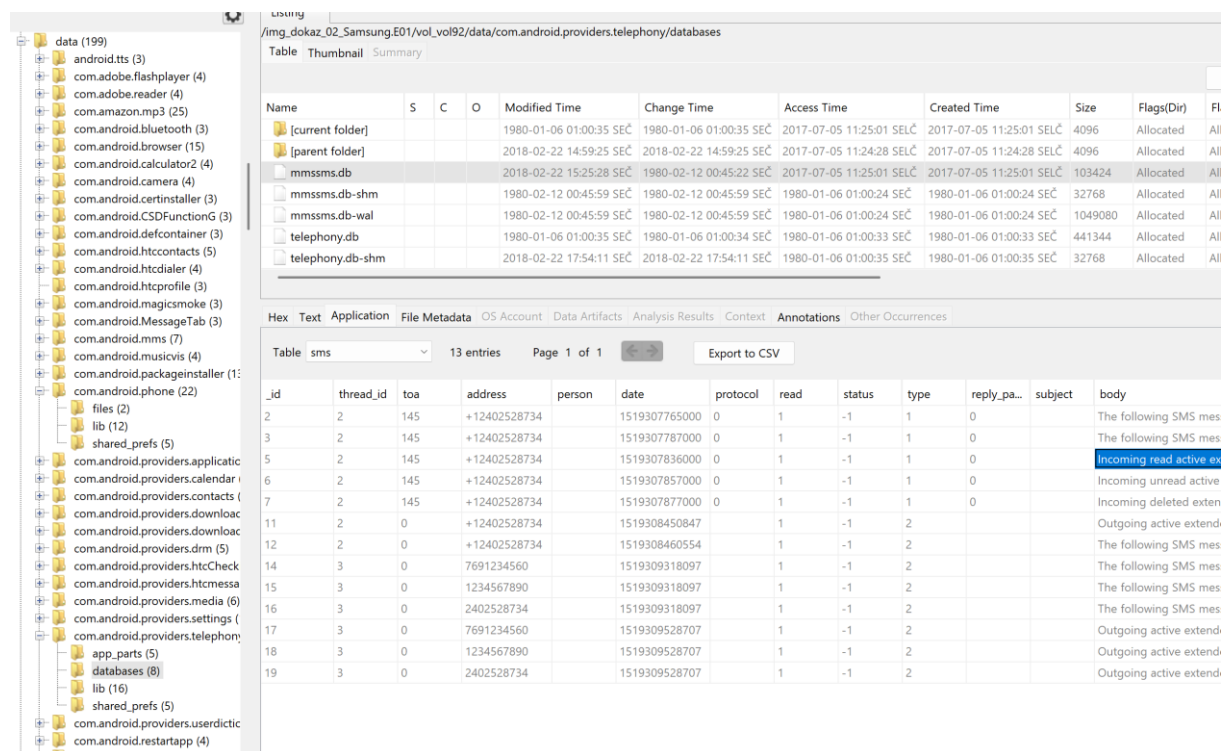
Obrázok 2 Štruktúra súborového systému Samsung

7.1 Analýza SMS správ

V prvom kroku som venovala pozornosť SMS správam uloženým v mobilnom zariadení. Tieto správy sú uložené v databáze mmssms.db, ktorá obsahuje informácie o prijatých a odoslaných textových správach vrátane telefónneho čísla odosielateľa, času prijatia a obsahu správy.

Analýzou tejto databázy je možné identifikovať správy, ktoré môžu obsahovať internetové odkazy alebo text typický pre phishingové útoky, napríklad výzvy na prihlásenie do bankovej služby alebo overenie používateľského účtu.

Ako je znázornené na obrázku 3, v databáze správ je možné zobraziť jednotlivé záznamy vrátane obsahu správy (body), telefónneho čísla odosielateľa a časovej pečiatky. Tieto údaje umožňujú identifikovať potenciálne podvodné správy zaslané používateľovi zariadenia.



The screenshot shows a file explorer interface with a sidebar on the left displaying a directory tree of Android data files. The main pane shows the contents of the mmssms.db database file. Below the file list, there is a table view of the SMS messages stored in the database. The table has columns for _id, thread_id, toa, address, person, date, protocol, read, status, type, reply_pa..., subject, and body. The table contains 13 entries, with the first entry having _id 2 and the last entry having _id 19. The body column contains text snippets of the messages, such as 'The following SMS mes' and 'Incoming read active ex'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	FI
[current folder]				1980-01-06 01:00:35 SEČ	1980-01-06 01:00:35 SEČ	2017-07-05 11:25:01 SELČ	2017-07-05 11:25:01 SELČ	4096	Allocated	All
[parent folder]				2018-02-22 14:59:25 SEČ	2018-02-22 14:59:25 SEČ	2017-07-05 11:24:28 SELČ	2017-07-05 11:24:28 SELČ	4096	Allocated	All
mmssms.db				2018-02-22 15:25:28 SEČ	1980-02-12 00:45:22 SEČ	2017-07-05 11:25:01 SELČ	2017-07-05 11:25:01 SELČ	103424	Allocated	All
mmssms.db-shm				1980-02-12 00:45:59 SEČ	1980-02-12 00:45:59 SEČ	1980-01-06 01:00:24 SEČ	1980-01-06 01:00:24 SEČ	32768	Allocated	All
mmssms.db-wal				1980-02-12 00:45:59 SEČ	1980-02-12 00:45:59 SEČ	1980-01-06 01:00:24 SEČ	1980-01-06 01:00:24 SEČ	1049080	Allocated	All
telephony.db				1980-01-06 01:00:35 SEČ	1980-01-06 01:00:34 SEČ	1980-01-06 01:00:33 SEČ	1980-01-06 01:00:33 SEČ	441344	Allocated	All
telephony.db-shm				2018-02-22 17:54:11 SEČ	2018-02-22 17:54:11 SEČ	1980-01-06 01:00:35 SEČ	1980-01-06 01:00:35 SEČ	32768	Allocated	All

_id	thread_id	toa	address	person	date	protocol	read	status	type	reply_pa...	subject	body
2	2	145	+12402528734		1519307765000	0	1	-1	1	0		The following SMS mes
3	2	145	+12402528734		1519307787000	0	1	-1	1	0		The following SMS mes
5	2	145	+12402528734		1519307836000	0	1	-1	1	0		Incoming read active ex
6	2	145	+12402528734		1519307857000	0	1	-1	1	0		Incoming unread active
7	2	145	+12402528734		1519307877000	0	1	-1	1	0		Incoming deleted exten
11	2	0	+12402528734		1519308450847		1	-1	2			Outgoing active extend
12	2	0	+12402528734		1519308460554		1	-1	2			The following SMS mes
14	3	0	7691234560		1519309318097		1	-1	2			The following SMS mes
15	3	0	1234567890		1519309318097		1	-1	2			The following SMS mes
16	3	0	2402528734		1519309318097		1	-1	2			The following SMS mes
17	3	0	7691234560		1519309528707		1	-1	2			Outgoing active extend
18	3	0	1234567890		1519309528707		1	-1	2			Outgoing active extend
19	3	0	2402528734		1519309528707		1	-1	2			Outgoing active extend

Obrázok 3 SMS databáza

Pri analýze databázy mmssms.db podľa obrázka 4 bol identifikovaný záznam SMS správy s _id = 124, odoslanej z telefónneho čísla +421903556221. Hodnota v poli date = 1768176000000 zodpovedá dátumu 12.1.2026. Obsah správy obsahoval internetový odkaz smerujúci na externú webovú stránku, ktorá sa vydávala za prihlasovaciu stránku banky.

_id	thread_id	to_a	address	person	date	protocol	read	status	type	reply_path_present	subject	body
124	7	NULL	+421903556221	NULL	1768176000000	0	0	-1	1	0	NULL	Security alert; zaznamenali sme podozrivú aktivitu na vašom účte. Overté prihlásenie na http://secure-banka-login.com

Obrázok 4 Podozrivá sms

Hodnota uložená v databáze date = 1768176000000 je uložená vo formáte Unix timestamp v milisekundách. Po konverzii na čitateľný čas zodpovedá dátumu 12.1.2026 10:00:00. Tento čas predstavuje moment prijatia SMS správy obsahujúcej phishingový odkaz.

7.2 Analýza prehliadača

Po identifikovaní podozrivej SMS správy obsahujúcej phishingový odkaz som pokračovala v analýze dát mobilného zariadenia preskúmaním aplikácie internetového prehliadača com.android.browser. Cieľom tejto analýzy bolo zistiť, či používateľ na uvedený odkaz zo správy klikol a či sa v databázach prehliadača nachádzajú záznamy o návšteve webovej stránky uvedenej v SMS správe alebo iných podozrivých stránok súvisiacich s phishingovým útokom.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2017-07-05 11:25:30 SEČ	2017-07-05 11:25:30 SEČ	4096	Allocated
[parent folder]				1980-03-26 04:08:37 SEČ	1980-03-26 04:08:37 SEČ	2017-07-05 11:24:52 SEČ	2017-07-05 11:24:52 SEČ	4096	Allocated
browser.db				2017-11-01 18:29:45 SEČ	1980-03-27 09:04:28 SEČ	2017-11-01 18:29:45 SEČ	2017-11-01 18:29:45 SEČ	60416	Allocated
browser.db-shm				1980-03-27 09:04:29 SEČ	1980-03-27 09:04:29 SEČ	2017-11-01 18:29:45 SEČ	2017-11-01 18:29:45 SEČ	32768	Allocated
browser.db-wal				1980-03-27 09:04:29 SEČ	1980-03-27 09:04:29 SEČ	2017-11-01 18:29:45 SEČ	2017-11-01 18:29:45 SEČ	240024	Allocated
carousel.db				2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2018-02-23 11:50:55 SEČ	2018-02-23 11:50:55 SEČ	12288	Allocated
carousel.db-shm				2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	32768	Allocated
carousel.db-wal				2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	2018-02-27 13:13:08 SEČ	3176	Allocated
webview.db				2017-11-01 18:29:30 SEČ	1980-03-27 09:04:28 SEČ	2017-07-05 11:25:30 SEČ	2017-07-05 11:25:30 SEČ	15360	Allocated
webview.db-shm				1980-03-27 09:04:28 SEČ	1980-03-27 09:04:28 SEČ	2017-11-01 18:29:30 SEČ	2017-11-01 18:29:30 SEČ	32768	Allocated
webview.db-wal				2018-03-29 13:50:59 SEČ	2018-03-29 13:50:59 SEČ	2017-11-01 18:29:30 SEČ	2017-11-01 18:29:30 SEČ	136272	Allocated
webviewCache.db				2017-11-01 18:29:31 SEČ	1980-03-29 09:04:28 SEČ	2017-07-05 11:25:30 SEČ	2017-07-05 11:25:30 SEČ	6144	Allocated
webviewCache.db-shm				1980-03-27 09:04:28 SEČ	1980-03-27 09:04:28 SEČ	2017-11-01 18:29:31 SEČ	2017-11-01 18:29:31 SEČ	32768	Allocated
webviewCache.db-wal				1980-03-25 23:57:10 SEČ	1980-03-25 23:57:10 SEČ	2017-11-01 18:29:31 SEČ	2017-11-01 18:29:31 SEČ	240024	Allocated

_id	title	url	bookmark	hostoffset	host_onechar	host_twochar	host_threechar
98	Amazon.de GmbH	http://www...	2	11	a	am	ama
99	The Pirate Bay	http://www...	2	11	t	th	the
100	Skyrock	http://www...	2	11	s	sk	sky
102	Hotfile.com	http://www...	2	11	h	ho	hot
103	Nasza-klasa.pl	http://www...	2	11	n	na	nas
105	Clicksor	http://www...	2	11	c	cl	cli
106	Answers.com	http://www...	2	11	a	an	ans
108	Tagged	http://www...	2	11	t	ta	tag

Obrázok 5 Zobrazenie tabuľky httpbookmarks z databázy browser.db v nástroji Autopsy

Po identifikovaní databázových súborov v priečinku databases bol otvorený súbor browser.db obrázok 5, ktorý obsahuje údaje o používaní internetového prehliadača zariadenia.

Databáza bola analyzovaná priamo v nástroji Autopsy, kde je možné zobrazovať jednotlivé tabuľky a ich obsah. Jednou z analyzovaných tabuliek bola tabuľka httpbookmarks, ktorá obsahuje informácie o uložených záložkách prehliadača.

Ako je možné vidieť na obrázku 5, medzi záznamami sa nachádza aj webová stránka <http://secure-banka-login.com>, ktorá sa vydáva za prihlasovaciu stránku bankovej služby.

_id	title	url	bookmark	hostoffset
124	Bank account verification	http://secure-banka-login.com	0	11

Obrázok 6 Podozrivá url stránky

Následne bola vykonaná analýza databáz webview.db a webviewCache.db, ktoré môžu obsahovať dočasne uložené údaje z webových formulárov alebo prihlasovacích polí. Cieľom tejto analýzy bolo zistiť, či sa v zariadení nachádzajú uložené prihlasovacie údaje alebo iné údaje zadané používateľom na analyzovanej webovej stránke. Po preskúmaní obsahu týchto databáz však neboli identifikované žiadne uložené prihlasovacie údaje ani údaje z formulárov, ktoré by bolo možné priamo spojiť s phishingovou stránkou.

Následne bol analyzovaný obsah priečinkov app_cache, app_appcache a databáza webviewCache.db, ktoré obsahujú dočasne uložený obsah webových stránok načítaných v internetovom prehliadači. Cieľom analýzy bolo identifikovať prípadné fragmenty HTML stránok, obrázky alebo iné súbory súvisiace s phishingovou webovou stránkou. Po preskúmaní obsahu týchto priečinkov však neboli identifikované žiadne súbory ani dáta, ktoré by bolo možné priamo spojiť s analyzovanou phishingovou stránkou.

Porovnaním časových údajov z databázy správ mmssms.db a databázy prehliadača browser.db bolo možné potvrdiť časovú súvislosť medzi prijatím phishingovej SMS správy a následným otvorením podozrivej webovej stránky. SMS správa bola prijatá 12.1.2026 o 10:00:00, zatiaľ čo záznam v databáze prehliadača ukazuje návštevu stránky <http://secure-banka-login.com> v čase 12.1.2026 o 10:02:05. Tento časový rozdiel naznačuje, že používateľ krátko po prijatí správy klikol na odkaz uvedený v SMS správe a otvoril phishingovú stránku v internetovom prehliadači zariadenia.

8. Záver

Na základe vykonanej digitálno-forenznej analýzy mobilného zariadenia používateľa bolo možné identifikovať relevantné digitálne stopy súvisiace s neoprávnenou finančnou transakciou.

Analýzou databázy SMS správ bola identifikovaná podozrivá správa obsahujúca internetový odkaz smerujúci na externú webovú stránku, ktorá sa vydávala za prihlasovaciu stránku banky. Táto správa bola prijatá dňa 12.1.2026 o 10:00:00.

Následnou analýzou databázy internetového prehliadača bolo zistené, že krátko po prijatí tejto správy došlo k otvoreniu webovej stránky <http://secure-banka-login.com>, a to v čase 12.1.2026 o 10:02:05. Táto časová súvislosť naznačuje, že používateľ reagoval na prijatú SMS správu a otvoril odkaz vedúci na podvodnú stránku.

Hoci sa v zariadení nepodarilo identifikovať uložené prihlasovacie údaje ani obsah formulárov, zistené skutočnosti podporujú scenár phishingového útoku (smishing), pri ktorom mohol používateľ zadať svoje prihlasovacie údaje na podvodnej webovej stránke.

V rámci analýzy neboli identifikované žiadne známky prítomnosti škodlivého softvéru ani podozrivej aktivity v iných aplikáciách, čím boli hypotézy o kompromitácii zariadenia prostredníctvom malvéru alebo iných služieb zamietnuté.

Na základe uvedených zistení možno konštatovať, že neoprávnený prístup k bankovému účtu bol s vysokou pravdepodobnosťou spôsobený phishingovým útokom prostredníctvom SMS správy, na ktorú používateľ reagoval otvorením odkazu a následným zadaním prihlasovacích údajov. Na základe zistení, banka nie je povinná vrátiť poškodenému sumu, ktorá mu bola bez jeho vedomia stiahnutá z účtu.