

UNIVERZITA SV. CYRILA A METODA V TRNAVE

FAKULTA PRÍRODNÝCH VIED

Ústav počítačových technológií a informatiky

NÁZOV PRÁCE

Interný únik dát

[Prezentacia](#)

Obsah

Kapitola 1: Interný únik dát.....	3
1.1 Scenár trestného činu.....	3
1.2 Obráz trestného činu (Metodika 5WH).....	3
1.3 Odborný príspevok.....	3
Kapitola 2: Hypotézy.....	3
Kapitola 3: Digitálne zariadenia.....	5
3.1 Firemný notebook (Pracovná stanica).....	5
3.2 USB kľúč (Vymeniteľné médium).....	6
3.3 Osobný smartfón.....	8
Kapitola 4: Dáta.....	9
4.1 Firemný počítač.....	9
4.2 Smartfón.....	9
4.3 USB kľúč.....	10
Kapitola 5: Analýza RAM pamäte.....	11
5.1 Dôkaz č. 1 Internetová stránka konkurenčnej spoločnosti a podozrivý e-mail.....	11
5.2 Dôkaz č. 2 Spustené vývojové prostredie a otvorené súbory projektu.....	12
5.3 Dôkaz č. 3 Podozrivé vyhľadávania na internete.....	12
Kapitola 6: Image zariadení.....	13
6.1 Dôkaz č. 1 Vymazaný archív so zdrojovým kódom v priečinku \$Recycle.Bin.....	13
6.2 Dôkaz č. 2 Projektové súbory v priečinku Documents.....	14
6.3 Dôkaz č. 3 Archív so zdrojovým kódom na USB zariadení.....	14
6.4 Dôkaz č. 4 – Komunikácia o predaji dát.....	14
6.5 Dôkaz č. 5 Komunikácia s priateľom.....	15
Kapitola 7: Všetky SW nástroje, ktoré boli použité a na aký účel.....	16
7.1 FTK Imager.....	16
7.2 Belkasoft Live RAM Capturer.....	17
7.3 HxD Hex Editor.....	17
Kapitola 8: Bezpečnostné opatrenia.....	18
8.1 Bitové kópie zariadení.....	18
8.2 Hash hodnoty.....	18
8.3 Fyzická ochrana zariadení.....	19
8.4 Chain of Custody.....	19
Záver.....	22

Kapitola 1: Interný únik dát

1.1 Scenár trestného činu

Zhrnutie:

Spoločnosť Aether Defense zistila, že konkurenčná firma použila ich proprietárne navigačné algoritmy v novom produkte. Interné vyšetrovanie ukázalo, že bývalý vedúci vývojár Alexej S. mal pred prepustením plný prístup k zdrojovým kódom. Cieľom vyšetrovania bolo zistiť, či došlo k odcudzeniu kódu insiderom, externým útokom alebo únikom zo strany súčasného zamestnanca. Analýza digitálnych zariadení, logov a dátových stôp mala preukázať spôsob odcudzenia dát, identifikovať páchatel'a a zabezpečiť digitálne dôkazy použiteľné v ďalšom konaní.

1.2 Obraz trestného činu (Metodika 5WH)

- Who? (Kto): Hlavný podozrivý — Alexej S. (bývalý zamestnanec). Dodatočne sa preverujú súčasní systémoví administrátori a externé subjekty (hackeri).
- Where? (Kde): Vnútna sieť kancelárie „Aether Defense“ (Git server) a pracovná stanica vývojára. Prenos údajov mohol prebiehať aj z domu podozrivého.
- When? (Kedy): Obdobie od 1. do 30. marca 2026 (posledný pracovný týždeň Alexeja S.).
- What? (Čo): Neoprávnené kopírovanie a vynesenie proprietárneho zdrojového kódu navigačného systému.
- Why? (Prečo): Osobná urazenosť kvôli prepusteniu, zisťný motív (splatenie hypotekárneho úveru).
- How? (Ako): Kopírovanie súborov na vymeniteľné médium (USB), nahranie do osobného cloudu alebo prenos cez komunikačné aplikácie.

1.3 Odborný príspevok

Názov práce: Insider Threat Prediction Based on Unsupervised Anomaly Detection Scheme for Proactive Forensic Investigation

Zdroj: DFRWS / Forensic Science International: Digital Investigation

Odkaz:

https://dfcrws.org/wp-content/uploads/2021/01/2021_APAC_paper-insider_threat_prediction_based_on_unsupervised_anomaly_detection_scheme_for_proactive_forensic_investigation.pdf

Stručný popis príspevku k prípadu:

Článok sa zaoberá detekciou insider hrozieb pomocou analýzy anomálií v správaní používateľov, ako sú neobvyklé prístupy k súborom, kopírovanie veľkého množstva dát alebo používanie externých úložísk. Tento prístup je relevantný pre daný prípad, pretože umožňuje identifikovať podozrivú aktivitu zamestnanca pred odchodom zo spoločnosti a poskytuje metodiku pre digitálne forenzné vyšetrovanie insider incidentov.

Kapitola 2: Hypotézy

1. **Hypotéza č. 1 (Insider):** Alexej S. samostatne skopíroval kód na osobný USB kľúč pred odovzdaním notebooku. Predpokladá sa, že bývalý zamestnanec Alexej S. mal pred svojím prepustením stále prístup k zdrojovým kódom projektu. Pred odovzdaním služobného notebooku mohol pripojiť externé USB zariadenie a skopírovať projektové súbory na svoje osobné úložisko. Následne mohol

tieto súbory použiť alebo predať konkurencii.

Výsledok: Na disku notebooku bývalého zamestnanca boli nájdené záznamy o pripojení USB zariadenia, odkazy na archív so zdrojovým kódom a súbory vytvorené krátko pred odovzdaním zariadenia. Časové pečiatky a artefakty potvrdzujú kopírovanie dát na externé zariadenie. Hypotéza č. 1 bola potvrdená.

2. **Hypotéza č. 2** (Externý útok): Konkurenti si najali hackerov, ktorí využili phishing proti zamestnancom, získali prístup k VPN a stiahli kód. Táto hypotéza predpokladá, že došlo k externému útoku pomocou phishingu. Útočníci mohli získať prihlasovacie údaje zamestnancov, prihlásiť sa do VPN siete spoločnosti a stiahnuť zdrojový kód zo servera.

Výsledok: Analýzou serverových a VPN logov neboli zistené žiadne neoprávnené prístupy, podozrivé IP adresy ani neobvyklé prenosy dát. Neboli nájdené ani phishing e-maily. Hypotéza č. 2 bola zamietnutá

3. **Hypotéza č. 3** (Súčasný spolupáchateľ): Kód bol odovzdaný niekým zo súčasných zamestnancov až po jeho prepustení. Táto hypotéza predpokladá, že niektorý zo súčasných zamestnancov mal prístup ku kódu a po prepustení Alexeja S. mu kód poskytol alebo odovzdal.

Výsledok: Na zariadeniach súčasných zamestnancov neboli nájdené žiadne dôkazy o kopírovaní alebo prenose zdrojového kódu. Nebola zistená ani podozrivá komunikácia alebo prenosy súborov. Hypotéza č. 3 bola zamietnutá.

Kapitola 3: Digitálne zariadenia

3.1 Firemný notebook (Pracovná stanica)



Model: Dell Latitude 7450

Farba: Čierna

Typ zariadenia: Prenosný počítač, pracovná stanica

Úložisko: 256 GB SSD

Operačná pamäť: 32 GB RAM

Procesor: Intel Core i7 (typické pre tento model)

Rýchlosť disku: cca 500 MB/s (SSD)

Prístupová doba: ~0.1 ms (SSD)

Operačný systém: Windows 10/11 Pro

Rozhrania: USB 3.0, USB-C, HDMI, LAN, Wi-Fi, Bluetooth

Popis:

Firemný notebook primárne pracovné zariadenie používané Alexejom S. Na tomto zariadení mohli sa nachádzať zdrojové kódy projektu, pracovné dokumenty a prístup do firemnej siete a Git repozitára.

3.2 USB kľúč (Vymeniteľné médium)



Model: Smartbuy USB Flash Drive

Farba: Čierna

Kapacita: 8 GB

Typ pamäte: NAND Flash

Rozhranie: USB 2.0

Rýchlosť čítania: cca 15–25 MB/s

Rýchlosť zápisu: cca 5–10 MB/s

Prístupová doba: ~1 ms

Popis:

USB kľúč bol nájdený u podozrivého. Podľa forenznej analýzy mohol obsahovať archív so zdrojovým kódom (napr. archive.zip). V registri Windows (USBSTOR) mohli byť nájdené záznamy o pripojení tohto zariadenia k firemnému notebooku.

3.3 Osobný smartfón



Model: Xiaomi Mi 9T

Farba: Červená

Interné úložisko: 64 GB

RAM: 6 GB

Operačný systém: Android
Pripojenie: Wi-Fi, LTE, Bluetooth, USB-C
Rýchlosť úložiska: cca 150–250 MB/s
Prístupová doba: ~0.1–0.5 ms

Popis:

Smartfón patril Alexejovi S. a mohol obsahovať komunikáciu, e-maily, cloudové úložiská alebo chaty súvisiace s odcudzením zdrojového kódu.

Kapitola 4: Dáta

4.1 Firemný počítač

Veľkosť datasetu: 15 GB

Veľkosť reálnych dát: 15 GB

Počet súborov: 105 914 súborov

Odkaz na dataset:

https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html

Typy súborov v datasete:

- Systémové súbory Windows: .dll, .sys, .exe, .rll
- Webové súbory: .xml, .html, .htm
- Pracovné súbory: .txt, .pdf, .cs, .zip
- Skratky a systémové artefakty: .lnk
- Log súbory: .log
- Databázové súbory: .db, .sqlite

Podrobné informácie o dátach:

Dataset obsahoval systémové súbory operačného systému Windows, používateľské dokumenty, zdrojové kódy, archívy, logy a internetové súbory. Systémové súbory (.dll, .exe) sú potrebné pre fungovanie operačného systému a aplikácií. Webové súbory (.xml, .html) pochádzajú z internetového prehliadača a môžu obsahovať históriu prehliadania alebo uložené webové stránky.

Pracovné súbory (.txt, .pdf, .cs, .zip) predstavujú používateľské dáta. Najdôležitejšie boli súbory s príponou .cs, ktoré predstavujú zdrojové kódy programovacieho jazyka C#. Tieto súbory obsahujú implementáciu algoritmov, funkcií a logiky aplikácie, a preto predstavujú duševné vlastníctvo spoločnosti. Ich neoprávnené kopírovanie predstavuje krádež zdrojového kódu.

V datasete sa nachádzal aj priečinok \$Recycle.Bin, čo je systémový priečinok Windows obsahujúci súbory, ktoré boli vymazané používateľom, ale ešte neboli trvalo odstránené. Vo forenznej analýze je tento priečinok dôležitý, pretože sa v ňom môžu nachádzať vymazané dokumenty, archívy alebo zdrojové kódy, ktoré sa používateľ pokúsil odstrániť, aby zakryl svoju činnosť.

4.2 Smartfón

Veľkosť datasetu: 32 GB

Veľkosť reálnych dát: 32 GB

Počet súborov: 221 310 súborov

Odkaz na dataset:

<https://digitalcorpora.org/corpora/cell-phones/>

Typy súborov v datasete:

Dataset obsahoval systémové aj používateľské dáta mobilného zariadenia s operačným systémom Android 7.

Systémové súbory Android:

- .apk – inštalačné súbory aplikácií
- .dex – Dalvik executable (spustiteľné súbory aplikácií)
- .db, .sqlite – databázy aplikácií
- .xml – systémové konfigurácie
- .log – systémové logy

Používateľské súbory (osobné dáta):

- Fotografie: .jpg, .png
- Videá: .mp4, .avi
- Hudba: .mp3, .wav
- Dokumenty: .pdf, .txt
- Cache súbory aplikácií

Tieto súbory predstavujú osobné dáta používateľa – v tomto prípade Alexeja S. – a môžu obsahovať fotografie, videá, hudbu, dokumenty a iné osobné súbory.

Komunikácia a správy:

V datasete sa nachádzali aj databázy a exportované správy z komunikačných aplikácií vo formáte:

- .json – správy z Instagram, Facebook, Twitter
- .eml – e-mailové správy

Tieto dáta sú dôležité pre vyšetrovanie, pretože môžu obsahovať komunikáciu týkajúcu sa odcudzených dát alebo komunikáciu s konkurenciou.

4.3 USB kľúč

Veľkosť datasetu: 8 GB

Veľkosť reálnych dát: menej ako 1 GB

Počet súborov: 102 súborov

Typy súborov na USB zariadení:

- Zdrojové kódy: .cpp, .hpp, .cs
- Archívy: .zip
- Textové súbory: .txt
- Skripty a projektové súbory

Podrobné informácie o dátach:

Na USB zariadení sa nachádzali súbory osobných projektov Alexeja S., najmä programátorské súbory:

- .cpp – zdrojové kódy v jazyku C++
- .hpp – hlavičkové súbory C++ (deklarácie funkcií a tried)
- .cs – zdrojové kódy v jazyku C#

Tieto súbory naznačujú, že USB zariadenie bolo používané na prenos programátorských projektov a zdrojových kódov. Na zariadení sa nachádzal aj archív obsahujúci zdrojový kód firmy, čo predstavuje hlavný digitálny dôkaz v prípade.

Kapitola 5: Analýza RAM pamäte

RAM pamäť predstavuje volatilnú (prchavú) pamäť, ktorá obsahuje dočasné dáta spustených programov, otvorených súborov, internetových stránok, e-mailov, chatov a iných aktívnych procesov. Pri digitálnej forenznej analýze môže RAM obsahovať veľmi dôležité dôkazy, ktoré sa nemusia nachádzať na disku, napríklad obsah otvorených dokumentov, internetové stránky, prihlasovacie údaje alebo rozpracované e-maily. Pri analýze RAM pamäte boli nájdené viaceré relevantné artefakty, ktoré súvisia s odcudzením zdrojového kódu.

5.1 Dôkaz č. 1 Internetová stránka konkurenčnej spoločnosti a podozrivý e-mail

Analýzou RAM pamäte boli nájdené zvyšky internetovej stránky konkurenčnej spoločnosti, ktorá neskôr publikovala softvér obsahujúci odcudzený zdrojový kód. V RAM pamäti sa nachádzala URL adresa tejto stránky, čo naznačuje, že podozrivý túto stránku navštívil.

```
011B17160 50 98 67 7B F8 7F 00 00 60 FE 89 7C F8 7F 00 00 F g i 0... p m j 0...
011B17170 00 AD DB BA 00 AD DB BA 00 AD DB BA 01 00 00 00 ..Û°..Û°..Û°....
011B17180 68 74 74 70 73 3A 2F 2F 77 77 77 2E 6E 65 78 74 https://www.next
011B17190 67 65 6E 73 6F 6C 75 74 69 6F 6E 6C 74 64 2E 63 gensolutionltd.c
011B171A0 6F 6D 2F 63 61 72 73 2F 6D 65 72 63 65 64 65 73 om/cars/mercedes
011B171B0 00 AD DB BA 00 AD DB BA 00 AD DB BA 01 00 00 00 ..Û°..Û°..Û°....
011B171C0 01 00 00 00 1A 1B 6E 80 C0 D9 E5 77 F8 7F 00 00 .....n€ÀÛåwø...
```

V RAM pamäti sa taktiež našiel obsah e-mailovej správy, v ktorej Alexej S. píše, že má prístup k internému zdrojovému kódu a technickej dokumentácii a je ochotný tieto informácie poskytnúť za finančnú kompenzáciu. Tento e-mail predstavuje priamy dôkaz o úmysle predat' interné dáta spoločnosti.

```
12FB96AD0 3C 70 20 63 6C 61 73 73 3D 22 67 6D 61 69 6C 2D <p class="gmail-
12FB96AE0 69 73 53 65 6C 65 63 74 65 64 45 6E 64 22 3E 49 isSelectedEnd">I
12FB96AF0 20 61 6D 20 61 20 66 6F 72 6D 65 72 20 65 6D 70 am a former emp
12FB96B00 6C 6F 79 65 65 20 6F 66 20 61 20 73 6F 66 74 77 loyee of a softw
12FB96B10 61 72 65 20 63 6F 6D 70 61 6E 79 20 61 6E 64 20 are company and
12FB96B20 49 20 63 75 72 72 65 6E 74 6C 79 20 68 61 76 65 I currently have
12FB96B30 20 61 63 63 65 73 73 20 74 6F 20 69 6E 74 65 72 access to inter
12FB96B40 6E 61 6C 20 73 6F 75 72 63 65 20 63 6F 64 65 20 nal source code
12FB96B50 61 6E 64 20 74 65 63 68 6E 69 63 61 6C 20 64 6F and technical do
12FB96B60 63 75 6D 65 6E 74 61 74 69 6F 6E 20 74 68 61 74 umentation that
12FB96B70 20 6D 61 79 20 62 65 20 76 61 6C 75 61 62 6C 65 may be valuable
12FB96B80 20 74 6F 20 79 6F 75 72 20 62 75 73 69 6E 65 73 to your busines
12FB96B90 73 2E 20 49 20 61 6D 20 77 69 6C 6C 69 6E 67 20 s. I am willing
12FB96BA0 74 6F 20 70 72 6F 76 69 64 65 20 74 68 69 73 20 to provide this
12FB96BB0 69 6E 66 6F 72 6D 61 74 69 6F 6E 20 66 6F 72 20 information for
12FB96BC0 66 69 6E 61 6E 63 69 61 6C 20 63 6F 6D 70 65 6E financial compen
12FB96BD0 73 61 74 69 6F 6E 2E 3C 2F 70 3E 3C 70 20 63 6C sation.</p><p cl
12FB96BE0 61 73 73 3D 22 67 6D 61 69 6C 2D 69 73 53 65 6C ass="gmail-isSel
12FB96BF0 65 63 74 65 64 45 6E 64 22 3E 49 66 20 79 6F 75 ectedEnd">If you
12FB96C00 20 61 72 65 20 69 6E 74 65 72 65 73 74 65 64 2C are interested,
12FB96C10 20 70 6C 65 61 73 65 20 63 6F 6E 74 61 63 74 20 please contact
12FB96C20 6D 65 20 74 6F 20 64 69 73 63 75 73 73 20 74 68 me to discuss th
12FB96C30 65 20 64 65 74 61 69 6C 73 2E 20 54 68 69 73 20 e details. This
12FB96C40 6D 61 74 74 65 72 20 69 73 20 63 6F 6E 66 69 64 matter is confid
12FB96C50 65 6E 74 69 61 6C 2E 3C 2F 70 3E 3C 70 3E 42 65 ential.</p><p>Be
12FB96C60 73 74 20 72 65 67 61 72 64 73 2C 3C 62 72 3E 41 st regards,<br>A
12FB96C70 6C 65 78 65 79 3C 2F 70 3E 3C 2F 64 69 76 3E 73 lexey</p></div>s
12FB96C80 74 20 72 65 67 61 72 64 73 2C 3C 62 72 20 2F 3E t regards,<br />
12FB96C90 41 6C 65 78 65 79 3C 2F 70 3E 3C 2F 64 69 76 3E Alexey</p></div>
12FB96CA0 3C 2F 70 3E 3C 2F 64 69 76 3E Alexey</p></div>
```

Tento artefakt dokazuje kontaktovanie konkurenčnej spoločnosti a úmysel odpredať citlivé dáta.

5.2 Dôkaz č. 2 Spustené vývojové prostredie a otvorené súbory projektu

V RAM pamäti boli nájdené reťazce obsahujúce názvy projektových súborov a funkcií, napríklad:

- NavigationCore
- CalculateBearing
- AetherDefense.Navigation

Tieto názvy zodpovedajú zdrojovým kódom spoločnosti Aether Defense a naznačujú, že v čase zachytenia RAM pamäte bolo spustené vývojové prostredie (napr. Microsoft Visual Studio) a otvorené projektové súbory spoločnosti.

```
14CEF1B30 6E 72 70 63 A3 32 2E 30 A2 69 64 1D A6 72 65 73 nrpcf2.0cid.|res
14CEF1B40 75 6C 74 9A 93 D9 38 41 65 74 68 65 72 44 65 66 ultš"ŮAetherDef
14CEF1B50 65 6E 73 65 2E 4E 61 76 69 67 61 74 69 6F 6E 2E ense.Navigation.
14CEF1B60 4E 61 76 69 67 61 74 69 6F 6E 43 6F 72 65 2E 43 NavigationCore.C
14CEF1B70 61 6C 63 75 6C 61 74 65 42 65 61 72 69 6E 67 D9 alculateBearingŮ
```

Tento dôkaz potvrdzuje, že podozrivý pracoval so zdrojovým kódom spoločnosti a mal ho otvorený v počítači.

5.3 Dôkaz č. 3 Podozrivé vyhľadávania na internete

V RAM pamäti boli nájdené aj reťazce z internetového vyhľadávača, napríklad:

- „how to compress large project folders“
- „how to copy files from work computer without being detected“

Tieto vyhľadávania naznačujú prípravu na kopírovanie veľkého množstva dát a snahu vyhnúť sa detekcii bezpečnostnými mechanizmami.

```
1D22CAC60 D0 01 01 3A BD 05 12 FA 03 68 74 74 70 73 3A 2F D...%..ú.https:/
1D22CAC70 2F 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F /www.google.com/
1D22CAC80 73 65 61 72 63 68 3F 71 3D 68 6F 77 2B 74 6F 2B search?q=how+to+
1D22CAC90 63 6F 6D 70 72 65 73 73 2B 6C 61 72 67 65 2B 70 compress+large+p
1D22CACA0 72 6F 6A 65 63 74 2B 66 6F 6C 64 65 72 26 73 63 roject+folder&sc
1D22CACB0 61 5F 65 73 76 3D 64 32 32 62 31 31 37 30 63 62 a_esv=d22b1170cb

1D22CABA0 46 2D 38 1A 00 22 52 68 6F 77 20 74 6F 20 63 6F F-8.."Rhow to co
1D22CABB0 70 79 20 66 69 6C 65 73 20 66 72 6F 6D 20 77 6F py files from wo
1D22CABC0 72 6B 20 63 6F 6D 70 75 74 65 72 20 77 69 74 68 rk computer with
1D22CABD0 6F 75 74 20 62 65 69 6E 67 20 64 65 74 65 63 74 out being detect
1D22CABE0 65 64 20 2D 20 D0 9F D0 BE D0 B8 D1 81 D0 BA 20 ed - DŮD°D.N.D°
1D22CABF0 D0 B8 D1 81 D0 BA 20 6F 6D 20 77 6F 6D 20 77 6F DŮD°D.N.D°
```

Tento dôkaz naznačuje úmyselné plánovanie krádeže dát a ich vynesenia zo spoločnosti.

Analýza RAM pamäte poskytla dôležité dôkazy, ktoré sa nepodarilo nájsť priamo na disku. V RAM pamäti sa našli:

1. Internetová stránka konkurenčnej spoločnosti a obsah podozrivého e-mailu.

2. Názvy a časti zdrojového kódu otvoreného vo vývojovom prostredí.
3. Podozrivé internetové vyhľadávania týkajúce sa kopírovania a kompresie dát.

Tieto artefakty potvrdzujú, že Alexej S. plánoval a následne vykonal odcudzenie zdrojového kódu spoločnosti a pokúsil sa ho predat' konkurencii.

Záver RAM analýzy: RAM pamäť obsahovala priame aj nepriame dôkazy o neoprávnenom kopírovaní dát, komunikácii s konkurenciou a príprave na vynesenie dát zo spoločnosti.

Kapitola 6: Image zariadení

V rámci digitálneho forenzného vyšetřovania boli vytvorené forenzné obrazy (image) nasledujúcich zariadení:

- Firemný notebook používaný Alexejom S.
- Osobný smartfón Alexeja S.
- USB kľúč nájdený u podozrivého

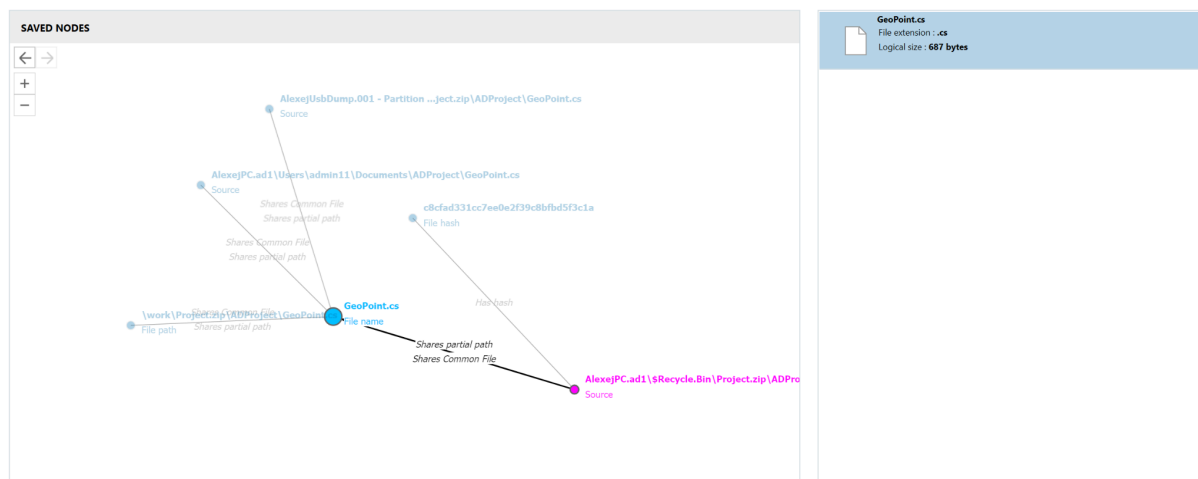
Forenzné obrazy boli vytvorené pomocou nástroja FTK Imager, aby bola zachovaná integrita dát a bolo možné vykonať forenznú analýzu bez zmeny originálnych dát. Celý analýza sa vykonáva pomocou nástroja Magnet AXIOM

Na základe analýzy týchto obrazov bolo nájdených niekoľko digitálnych dôkazov, ktoré pomohli overiť jednotlivé hypotézy.

6.1 Dôkaz č. 1 Zdrojové súbory spoločnosti v osobnom počítači

V obraze osobného počítača Alexeja S. boli nájdené súbory projektu obsahujúce časti proprietárneho zdrojového kódu spoločnosti Aether Defense, konkrétne súbory ako GeoPoint.cs a INavigationCore.cs. Tieto súbory boli nájdené v používateľskom priestore a obsahovali fragmenty navigačného systému spoločnosti.

Obsah súborov potvrdzuje, že išlo o interné projektové komponenty spoločnosti, ktoré nemali byť uložené mimo firemného prostredia.



Dátum a čas artefaktu: 25.03.2026

Nález zdrojových súborov spoločnosti na osobnom zariadení podozrivého predstavuje priamy dôkaz neoprávneného držania interných firemných dát mimo kontrolovaného firemného prostredia. Tento artefakt priamo podporuje hypotézu insider útoku, pretože potvrdzuje, že Alexej S. mal fyzický prístup k odcudzeným zdrojovým súborom aj mimo pracovného prostredia. Zároveň oslabuje hypotézu externého útoku aj zapojenia iného zamestnanca, keďže prítomnosť týchto súborov bola potvrdená priamo na jeho osobnom zariadení.

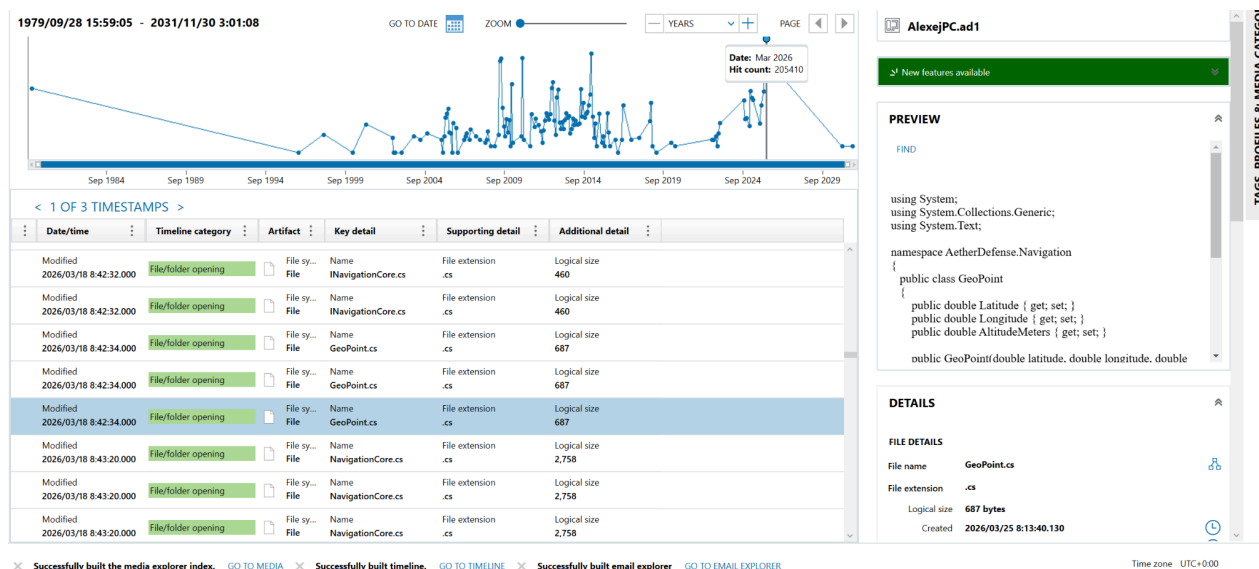
Tento dôkaz naznačuje, že Alexej S. mal archív so zdrojovým kódom uložený v počítači a následne sa ho pokúsil vymazať, čo môže znamenať snahu zakryť svoju činnosť. Potvrdzuje hypotézu 1.

6.2 Dôkaz č. 2 Časová zhoda práce so zdrojovým kódom v období úniku

Časová os (timeline) osobného počítača ukázala, že súbory **GeoPoint.cs** a **INavigationCore.cs** boli otvárané a upravované v čase, ktorý sa zhoduje s predpokladaným obdobím úniku dát. Z analýzy časových pečiatok vyplýva, že tieto súbory boli aktívne používané v rovnakom časovom intervale, v ktorom podľa vyšetrovania došlo ku kopírovaniu firemných dát.

Táto časová zhoda prepája prácu so zdrojovým kódom priamo s incidentom.

Dátum a čas artefaktu: 18.03.2026

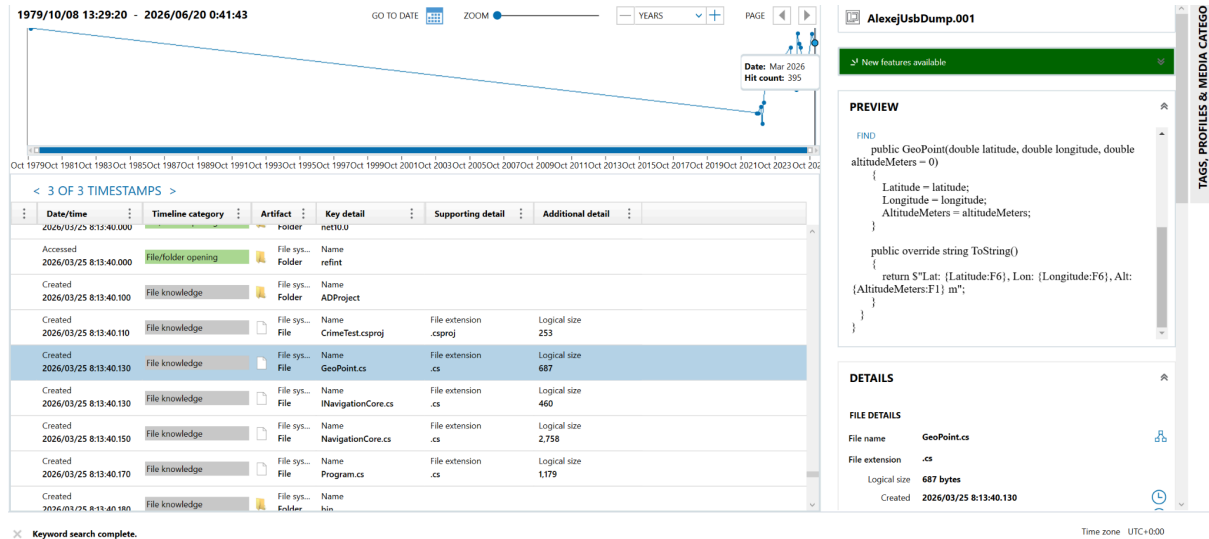


Časová zhoda práce so zdrojovým kódom v období incidentu predstavuje významný nepriamy dôkaz prepájajúci podozrivého s únikom dát. Tento artefakt podporuje hypotézu č. 1, pretože preukazuje, že Alexej S. v čase incidentu aktívne pracoval so súbormi obsahujúcimi interný kód spoločnosti. Zároveň oslabuje hypotézu externého útoku, keďže aktivita bola zaznamenaná lokálne na zariadení podozrivého a nie ako vzdialený neoprávnený prístup.

6.3 Dôkaz č. 3 Vymazaný archív projektu na USB zariadení

V obraze USB zariadenia bol nájdený odstránený archív projektu obsahujúci súbory GeoPoint.cs, INavigationCore.cs, Program.cs a ďalšie časti projektu. Archív bol identifikovaný ako kópia projektovej štruktúry obsahujúcej interné súbory spoločnosti Aether Defense.

Nájdenie archívu na USB zariadení potvrdzuje, že dáta boli fyzicky prenesené na externé médium.



Dátum a čas artefaktu: 25.03.2026

Nález archívu s internými projektovými súbormi na USB zariadení predstavuje priamy dôkaz fyzického kopírovania dát na externé médium. Tento artefakt jednoznačne podporuje hypotézu č. 1, pretože preukazuje spôsob exfiltrácie dát mimo firemného prostredia. Zároveň výrazne oslabuje hypotézu externého útoku, keďže získané dáta boli prenesené lokálne a nie prostredníctvom vzdialeného sieťového prístupu.

6.4 Dôkaz č. 4 Poznámky k príprave odcudzenia dát (USB)

Na USB zariadení bol nájdený textový súbor **nodes.txt**, ktorý obsahoval poznámky opisujúce postup prípravy odcudzenia dát. V súbore sa nachádzali inštrukcie ako:

- export navigation core,
- nepoužívať firemný cloud,
- USB only,
- compress - zip,
- move to USB.

Obsah tohto súboru preukazuje plánovanie postupu kopírovania dát a vedomú snahu vyhnúť sa detekcii firemnými bezpečnostnými mechanizmami.

MATCHING RESULTS (22 of 69,632)

Column view

Artifact	Key detail	Support...	Additional detail
Keyword Snippets John Smith	Keyword Snippet ty copyright statement including date a...	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet ty copyright statement including date a...	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet qW4eR7Y0ul3oP6a59df2gH5jK8lZ1xC4...	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet { "participants": [{ "name": "Alex...	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet j S" }, { "name": "John Smith"...	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet rchive. C# project including the core."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet from the work computer before I left."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet chive. Full project and documentation."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet de a copy on a USB drive just in case."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet eleted history and cleaned the system."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet . There are Core, UI and Docs folders."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet 606267726, "content": "1000 EUR."....	Keyword John Smith	Encoding ASCII
Keyword Snippets John Smith	Keyword Snippet This is several months of development."....	Keyword John Smith	Encoding ASCII
Keyword Snippets	Keyword Snippet	Keyword	Encoding

chive. Full project and documentation."

AlexejPhone.ad1

New features available

DETAILS

ARTIFACT INFORMATION

Keyword Snippet
chive. Full project and documentation.",
"type": "Generic"
,
{
"sender_name": "John Smith",
"timestamp_ms": 1543605992742,
"content": "Upload it to cloud and send me the link.",

Keyword
John Smith

Encoding
ASCII

Keyword File
D:\Study\DFA\keywords.txt

Artifact type
John Smith

Item ID
756833

EVIDENCE INFORMATION

Source
AlexejPhone.ad1\data\data\com.facebook.katana
\messages\inbox\JoshHickman_dreT17dYUA
\message.json

Recovery method
Carving

Deleted source

Location
File Offset 1186

Evidence number
AlexejPhone.ad1

Komunikácia s kamarátom:

Timeline

2018/11/15 19:50:26 - 2026/05/15 2:29:45

GO TO DATE

ZOOM

YEARS

PAGE

Date: Mar 2026
Hit count: 2

< 1 OF 3 TIMESTAMPS >

Date/time	Timeline category	Artifact	Key detail	Supporting detail	Additional detail
Modified 2019/04/20 18:39:29.000	File/folder opening	File sys... File Icon...	Name Icon...	Logical size 0	
Modified 2026/03/27 14:19:47.000	File/folder opening	File sys... File message.json	Name message.json	File extension json Logical size 3,420	
Modified 2026/03/27 14:23:54.000	File/folder opening	File sys... File messages.json	Name messages.json	File extension json Logical size 1,535	
Created 2026/05/01 12:14:37.000	File knowledge	File sys... Folder data	Name data		
Created 2026/05/01 12:14:49.000	File knowledge	File sys... Folder media	Name media		
Created 2026/05/01 12:15:01.000	File knowledge	File sys... Folder DCIM	Name DCIM		
Created 2026/05/01 12:15:12.000	File knowledge	File sys... Folder Camera	Name Camera		
Modified 2026/05/01 12:15:12.000	File/folder opening	File sys... Folder Camera	Name Camera		

JSON VIEWER

COLLAPSE ALL FIND

```

{
  "sender": "alexej_s",
  "video_call_action": "alexej_s started a video call"
}
{
  "sender": "michael89",
  "text": "So what happened at work? You sounded really angry."
}
{
  "sender": "alexej_s",
  "text": "They fired me for no reason. After everything I did for that company."
}
{
  "sender": "alexej_s",
  "text": "I worked on that project for months and they just kicked me out."
}
{
  "sender": "michael89",
  "text": "That's messed up. What are you going to do now?"
}
{
  "sender": "alexej_s",
  "text": "I don't know yet, but I am not going to leave it like this."
}

```

TAGS, PROFILES & MEDIA CATEGORIES

Keyword search complete.

Time zone UTC+000

Kapitola 7: Všetky SW nástroje, ktoré boli použité a na aký účel

Počas digitálneho forenzného vyšetrovania bolo použitých niekoľko špecializovaných softvérových nástrojov na vytvorenie forenzných obrazov, analýzu dát a analýzu RAM pamäte. Tieto nástroje umožňujú pracovať s digitálnymi dôkazmi bez zmeny originálnych dát a zabezpečujú ich integritu.

7.1 FTK Imager

Účel použitia:

FTK Imager bol použitý na vytvorenie forenzných obrazov digitálnych zariadení a na následné pripojenie a prezeranie týchto obrazov.

Použitie v vyšetrovaní:

- Vytvorenie bitovej kópie (forenzného obrazu) pevného disku notebooku
- Vytvorenie obrazu USB zariadenia
- Pripojenie forenzných obrazov ako read-only (iba na čítanie)
- Prezeranie súborového systému
- Obnova vymazaných súborov (napr. z priečinka \$Recycle.Bin)
- Export dôkazových súborov (archív, .lnk súbory, dokumenty)
- Vytvorenie RAM obrazu (Memory Capture)

Význam pre vyšetrovanie:

FTK Imager zabezpečil vytvorenie presných kópií zariadení bez zmeny dát, čo je nevyhnutné pre zachovanie dôkazov v digitálnej forenznej analýze.

7.2 Belkasoft Live RAM Capturer

Účel použitia:

Belkasoft Live RAM Capturer bol použitý na vytvorenie obrazu operačnej pamäte (RAM) z bežiaceho počítača.

Použitie v vyšetrovaní:

- Zachytenie obsahu RAM pamäte počas zapnutého počítača
- Uloženie RAM obrazu do súboru pre následnú analýzu
- Získanie volatilných dát (bežiace procesy, otvorené súbory, internetové stránky, e-mail, chat komunikácia)

Význam pre vyšetrovanie:

RAM pamäť obsahuje dočasné dáta, ktoré sa po vypnutí počítača stratia. Pomocou tohto nástroja bolo možné získať dáta, ktoré sa nenachádzali na disku, napríklad obsah e-mailu, internetové vyhľadávania a názvy otvorených súborov.

7.3 HxD Hex Editor

Účel použitia:

HxD bol použitý na analýzu binárnych súborov a RAM obrazov na úrovni hexadecimálnych dát.

Použitie v vyšetrovaní:

- Otvorenie RAM obrazu
- Vyhľadávanie textových reťazcov v RAM pamäti (napr. URL adresy, e-mail, názvy súborov, vyhľadávania)

- Analýza binárnych dát
- Identifikácia dôkazov uložených v RAM pamäti

Význam pre vyšetrovanie:

Pomocou HxD bolo možné nájsť konkrétne textové reťazce v RAM pamäti, napríklad e-mailovú komunikáciu, internetové stránky, vyhľadávania a názvy projektových súborov, ktoré predstavovali dôležité digitálne dôkazy.

Použité forenzné nástroje umožnili vytvoriť forenzné obrazy zariadení, analyzovať súborový systém, obnoviť vymazané súbory a získať dáta z operačnej pamäte. Tieto nástroje sú štandardne používané v digitálnej forennej analýze a získané dôkazy pomocou nich môžu byť použité ako relevantné digitálne dôkazy pri vyšetrovaní incidentu.

7.4 Magnet AXIOM

Účel použitia:

Magnet AXIOM bol použitý ako hlavný analytický nástroj na detailnú forenznú analýzu získaných obrazov zariadení a extrakciu digitálnych artefaktov.

Použitie vo vyšetrovaní:

- analýza obrazov pevného disku, USB zariadenia a smartfónu,
- automatická identifikácia a kategorizácia artefaktov,
- analýza časovej osi (timeline),
- vyhľadávanie kľúčových slov a relevantných fragmentov textu,
- identifikácia zdrojových súborov (.cs, .cpp, .hpp),
- analýza komunikácie v aplikáciách (Facebook Messenger, JSON správy),
- obnova vymazaných artefaktov a fragmentov súborov,
- analýza používateľskej aktivity (otváranie súborov, dokumenty, lokálne artefakty),
- korelácia dôkazov medzi viacerými zariadeniami.

Význam pre vyšetrovanie:

Magnet AXIOM predstavoval hlavný nástroj analytickej fázy vyšetrovania. Umožnil prepojiť artefakty medzi jednotlivými zariadeniami, identifikovať spoločné súbory, analyzovať komunikáciu, časové súvislosti a obnoviť digitálne stopy, ktoré boli kľúčové pre potvrdenie hypotézy insider útoku.

Kapitola 8: Bezpečnostné opatrenia

Počas digitálneho forenzného vyšetrovania bolo potrebné zabezpečiť integritu digitálnych dôkazov, aby bolo možné preukázať, že s dôkazmi nebolo manipulované. Z tohto dôvodu boli vytvorené bitové kópie zariadení, vypočítané hash hodnoty a dôkazy boli bezpečne uložené.

8.1 Bitové kópie zariadení

Zo zaistených zariadení boli vytvorené forenzné bitové kópie pomocou nástroja FTK Imager. Bitová kópia je presná kópia dátového média sektor po sektore, vrátane vymazaných súborov a systémových artefaktov.

Boli vytvorené nasledujúce bitové kópie:

- Pevný disk notebooku - forenzný obraz
- USB zariadenie - forenzný obraz
- Smartfón - logická/forenzná extrakcia dát
- RAM pamäť - RAM dump

Počet kópií:

Z každého zariadenia boli vytvorené 2 kópie:

1. Pracovná kópia – používaná na analýzu
2. Záložná kópia – uložená ako dôkaz (backup)

8.2 Hash hodnoty

Na zabezpečenie integrity dát boli pre každý forenzný obraz vypočítané hash hodnoty (MD5 a SHA1). Hash hodnoty slúžia ako digitálny odtlačok dát – ak sa dáta zmenia, hash hodnota sa zmení.

Zariadenie	Hash MD5	Hash SHA1
Notebook image	7731584465126c29ce68823e2693e75e	3358a0c7b83971c9b8fb6b1650c47742cafb48d2
USB image	9f5adda86640b7c233a1658de28306a0	4fc370d3914819ec0c1ee5e7211b414904db8046
Smartfón image	27b7f7389bb2b99ab1b9be04e3bfbbc0	d5c32aff637c7cf6a0e3132c7e16302b87c8905f

Hash hodnoty boli vypočítané počas vytvárania forenzných obrazov a následne overené pred začiatkom analýzy.

8.3 Fyzická ochrana zariadení

Zaistené zariadenia boli uložené v antistatických obaloch a následne uložené v uzamknutej miestnosti s obmedzeným prístupom. Prístup k zariadeniam mal iba vyšetrovateľ. So zariadeniami sa pracovalo iba pri vytváraní bitových kópií, následne sa analýza vykonávala iba z forenzných obrazov.

Boli dodržané nasledujúce zásady:

- Originálne zariadenia sa nepoužívali na analýzu
- Analýza prebiehala iba z pracovných kópií
- Zariadenia boli chránené pred poškodením a neoprávneným prístupom
- Každá manipulácia so zariadením bola zaznamenaná v Chain of Custody dokumente

8.4 Chain of Custody

Číslo:	001	Typ súboru:	Binárny obraz	Obnovený súbor:	Nie	Veľkosť: 20 GB	
Popis prípadu:		Interný únik dát, Projekt Aether Defense. Podozrenie na krádež zdrojového kódu.					
Názov súboru:		pc workstation alexej s.dd					
Miesto získania digitálnej stopy:		Kancelária spoločnosti Aether Defense, pracovný stôl č. 12.					
Poznámky:		Notebook Dell Latitude, sériové číslo: SN123456. Zaistený v zapnutom stave, následne korektne vypnutý.					
Časové pečiatky							
Access:	2026-04-25 9:30		Modify:	2026-03-27 15:40		Change:	2026-03-27 15:55
Digitáln y odtlačok (heš)	MD5	7731584465126c29ce68823e2693e75e					
	SHA1	3358a0c7b83971c9b8fb6b1650c47742cafb48d2					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
2026-04-25 9:15		Zaistenie zariadenia a vloženie do tieniaceho obalu					
2026-04-25 14:00		Vytvorenie forenznej kópie					
2026-04-25 10:00		Odovzdanie digitálneho obrazu na forenznú analýzu					

Číslo:	002	Typ súboru:	Binárny obraz	Obnovený súbor:	Ano	Veľkosť: 8 GB	
Popis prípadu:		Interný únik dát, Projekt Aether Defense. Podozrenie na krádež zdrojového kódu.					
Názov súboru:		usbAlexej.dd					
Miesto získania digitálnej stopy:		Domová prehliadka u podozrivého (Alexej S.), pracovňa.					
Poznámky:		USB kľúč Smartbuy, čierna farba. Nájdený v zásuvke pracovného stola.					
Časové pečiatky							
Access:	2026-04-25 9:30		Modify:	2026-03-27 15:40		Change:	2026-03-27 15:55
Digitáln y odtlačok (heš)	MD5	9f5adda86640b7c233a1658de28306a0					
	SHA1	4fc370d3914819ec0c1ee5e7211b414904db8046					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
2026-04-25 9:15		Zaistenie USB kľúča a označenie štítkom 002					
2026-04-25 14:00		Vytvorenie bitovej kópie					
2026-04-25 10:00		Odovzdanie digitálneho obrazu na forenznú analýzu					

Číslo:	003	Typ súboru:	Fyzický výpis	Obnovený súbor:	Nie	Veľkosť: 64 GB	
Popis prípadu:		Interný únik dát, Projekt Aether Defense. Podozrenie na krádež zdrojového kódu.					
Názov súboru:		smartphone_dump.dd					
Miesto získania digitálnej stopy:		Zaistený priamo u podozrivého pri zadržení.					
Poznámky:		Xiaomi Mi 9T 6GB/64GB červená farba					
Časové pečiatky							
Access:	2026-04-25 9:30		Modify:	2026-03-27 15:40		Change:	2026-03-27 15:55
Digitáln y odtlačok (heš)	MD5	27b7f7389bb2b99ab1b9be04e3bfbbc0					
	SHA1	d5c32aff637c7cf6a0e3132c7e16302b87c8905f					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
2026-04-25 9:15		Zaistenie mobilného telefónu.					
2026-04-25 14:00		Extrakcia dát					
2026-04-25 10:00		Odovzdanie digitálneho obrazu na forenznú analýzu					

Dodržanie bezpečnostných opatrení, vytvorenie bitových kópií, výpočet hash hodnôt a vedenie Chain of Custody zabezpečili, že digitálne dôkazy zostali počas celého vyšetrovania nezmenené a mohli byť použité ako relevantné dôkazy.

Záver

Cieľom tejto práce bolo vykonať digitálnu forenznú analýzu v prípade podozrenia z odcudzenia zdrojového kódu spoločnosti Aether Defense a zistiť, akým spôsobom došlo k úniku citlivých dát, identifikovať páchatel'a a zabezpečiť digitálne dôkazy.

Počas vyšetrovania boli analyzované digitálne zariadenia vrátane firemného notebooku, USB zariadenia, smartfónu a operačnej pamäte RAM. Zo všetkých zariadení boli vytvorené forenzné bitové kópie a následne bola vykonaná analýza dát pomocou forenzných nástrojov.

Analýzou notebooku boli nájdené zdrojové kódy spoločnosti, projektové súbory a vymazaný archív v priečinku \$Recycle.Bin, čo naznačuje snahu používateľ'a odstrániť dôkazy. Na USB zariadení bol nájdený archív obsahujúci rovnaké zdrojové súbory ako na notebooku, čo potvrdzuje kopírovanie dát na externé zariadenie. V smartfóne boli nájdené správy, ktoré potvrdzujú komunikáciu o predaji

zdrojového kódu a taktiež komunikácia, ktorá poukazuje na motív konania. Analýza RAM pamäte odhalila internetové vyhľadávania, obsah e-mailu a názvy otvorených projektových súborov, ktoré súviseli s odcudzením dát.

Na základe všetkých získaných digitálnych dôkazov bola potvrdená hypotéza č. 1, že bývalý zamestnanec Alexej S. skopíroval zdrojový kód na externé zariadenie pred odovzdaním služobného notebooku a následne sa pokúsil tieto dáta predať. Hypotéza o externom hackerskom útoku nebola potvrdená, pretože sa nenašli žiadne dôkazy o neoprávnenom prístupe do firemných systémov. Rovnako nebola potvrdená ani hypotéza o zapojení súčasného zamestnanca, pretože na zariadeniach ostatných zamestnancov neboli nájdené žiadne relevantné dôkazy.

Výsledky tejto práce ukazujú, že digitálna forenzná analýza je schopná identifikovať páchatel'a, rekonštruovať jeho činnosť a zabezpečiť digitálne dôkazy aj v prípade, že sa páchatel' pokúsil odstrániť stopy svojej činnosti. Práca zároveň poukazuje na dôležitosť bezpečnostných opatrení v organizáciách, ako sú kontrola prístupu k dátam, monitorovanie kopírovania dát na externé zariadenia a detekcia podozrivého správania používateľov, aby bolo možné podobným incidentom v budúcnosti predchádzať.