

Digitálna forenzná analýza: Pašerák ľudí a digitálne dôkazy

Prípado:

Policačná jednotka zadržala podozrivého muža, ktorý je podozrivý z organizovania nelegálneho prevozu ľudí cez hranice. Počas domovej prehliadky boli zaistené nasledovné digitálne zariadenia:

- **Notebook** používaný podozrivým
- **USB kľúč**, ktorý bol nájdený ukrytý v tajnej priehradke auta
- **Mobilný telefón**, ktorý bol vypnutý a pravdepodobne obsahuje šifrované dáta

Vyšetovatelia predpokladajú, že podozrivý využíval tieto zariadenia na komunikáciu s klientmi a organizovanie prevozov. Cieľom digitálnej forenznej analýzy je identifikovať dôkazy, ktoré potvrdia alebo vyvrátia podozrenia.

Ciele vyšetovania:

1. **Identifikovať dôkazy o pašovaní ľudí** – chaty, dokumenty, zoznamy osôb, trasy.
2. **Zistiť spôsob komunikácie** – šifrované aplikácie, anonymizačné technológie.
3. **Analyzovať USB kľúč** – získať súbory, históriu úprav, možné skryté dáta.
4. **Obnova zmazaných dát** – extrakcia zmazaných správ, e-mailov, obrázkov.
5. **Overenie geografických dát** – získanie GPS súradníc z fotografií alebo aplikácií.

Hypotézy:

Hypotéza 1: Podozrivý používal USB kľúč na uchovávanie citlivých informácií o pašovaní.

- Na USB kľúči sa môžu nachádzať súbory obsahujúce zoznamy osôb, trasy prevozu alebo informácie o platbách.
- Podozrivý mohol vymazať súbory v snahe zničiť dôkazy.

Hypotéza 2: Notebook bol použitý na plánovanie operácií a komunikáciu s klientmi.

- História prehliadača môže obsahovať prístupy na darknet alebo šifrované e-mailové služby.
- Dokumenty alebo tabuľky môžu obsahovať informácie o trasách alebo poplatkoch.
- Záznamy o použití anonymizačných nástrojov (VPN, TOR).

Hypotéza 3: Mobilný telefón obsahuje kľúčovú komunikáciu medzi podozrivým a prevádzanými osobami.

- Aplikácie ako WhatsApp, Signal alebo Telegram mohli byť použité na koordináciu.
- SIM karta alebo IMEI môže odhaliť spojenie s inými podozrivými.
- Geolokácia môže odhaliť pohyb podozrivého v čase pašovania.

Hypotéza 4: Dáta boli úmyselne šifrované alebo skryté pomocou pokročilých metód.

- Možné použitie skrytých oddielov na USB.
- Skúmanie zmazaných súborov pomocou forenzných nástrojov.

Hypotéza 5: Únik informácií odhalil pašerácku sieť.

- V prípade, že na zariadeniach sa nachádzajú mená spolupracovníkov alebo kontakty na iné osoby, môže byť odhalená širšia zločinecká sieť.

Metodológia forenzného vyšetrovania:**1. Forenzné klonovanie dát:**

- Vytvorenie digitálnych obrazov notebooku, USB a mobilu.
- Hashovanie na zachovanie integrity dát.

2. Analýza USB kľúča:

- Obnova zmazaných súborov.
- Skúmanie metadát súborov.
- Hľadanie šifrovaných alebo skrytých oddielov.

3. Skúmanie notebooku:

- Kontrola histórie prehliadača, nainštalovaných aplikácií.
- Vyhľadanie potenciálnych dokumentov týkajúcich sa pašovania.
- Preskúmanie e-mailovej komunikácie a cloudových úložísk.

4. Forenzná analýza mobilného telefónu:

- Extrakcia dát zo SIM karty a histórie hovorov.
- Analýza chatovacích aplikácií.
- Skúmanie GPS súradníc uložených vo fotografiách alebo v histórii polohy.

5. Krížová analýza získaných dôkazov:

- Porovnanie zoznamov kontaktov, IP adries, e-mailových adries.
- Overenie časových značiek súborov s pohybom podozrivého.
- Pokus o identifikáciu ďalších podozrivých osôb na základe komunikácie.

Výsledky vyšetrovania (očakávané):

- **Identifikácia zapojených osôb** – nájdenie mien, čísel, e-mailov.
- **Potvrdenie trasy pašovania** – GPS údaje, mapy, letenky.
- **Obnova zmazaných dôkazov** – obnovenie súborov z USB, mobilu, notebooku.

- **Zistenie spôsobu komunikácie** – analýza šifrovaných aplikácií a VPN.
 - **Zachovanie reťazca dôkazov** – správa pre vyšetrovanie a súd.
-

5WH

Kto:

Podozrivý muž, ktorý organizoval pašovanie ľudí, a osoby, ktoré s ním komunikovali, ako aj obeť pašovania.

Kde:

Miesto, kde boli zaistené zariadenia (domová prehliadka) a miesta prevodu ľudí cez hranice.

Kedy:

Čas, kedy bol muž zadržaný, a čas nelegálnych aktivít.

Čo:

Organizovanie nelegálneho prevodu ľudí cez hranice, využívanie digitálnych zariadení na komunikáciu a plánovanie.

Prečo:

Podozrivý sa mohol zapojiť do pašovania kvôli finančným ziskom alebo iným motiváciám.

Ako:

Použitie digitálnych zariadení ako USB kľúč, notebook a mobil na organizáciu pašovania, komunikáciu s klientmi, a možná šifrovaná komunikácia.



Zariadenie:

- Typ: USB flash drive

- Model: SanDisk Ultra Fit USB 3.1
- Farba: Čierna
- Rozhranie: USB 3.1 (kompatibilné s USB 3.0)
- Kapacita: 64 GB
- Rýchlosť čítania: Až 130 MB/s
- Podporované operačné systémy: Windows, MacOS
- Sériové číslo: (0S 8063477)



Notebook

- Typ: Prenosný počítač
- Model: Dell XPS 15
- Displej: 15.6" FHD
- Procesor: Intel Core i7
- RAM: 16 GB
- Úložisko: 512 GB SSD
- Operačný systém: Windows 10 Pro



Mobil

- Typ: Smartfón
- Model: Samsung Galaxy S21
- Displej: 6.2" Dynamic AMOLED
- Procesor: Exynos 2100
- RAM: 8 GB
- Úložisko: 128 GB
- Operačný systém: Android 11
- Batéria: 4000 mAh

Vytvorenie kópií a zabezpečenie

Bitové kópie RAM z notebooku boli získané pomocou nástrojov FTK Imager (verzia 4.7.1.2) a Magnet RAM Capture (verzia 1.2.0). Na vytvorenie bitovej kópie úložného zariadenia bol využitý FTK Imager. Kópie boli následne uložené na externý pracovný disk určený na uchovávanie a prácu s obrazmi diskov. Všetky originály aj kópie sú bezpečne uložené v anti-statickej skrinke, aby sa predišlo poškodeniu vlhkosťou, a táto krabica je následne umiestnená v trezore, ktorý sa nachádza v monitorovaných priestoroch s vysokou úrovňou bezpečnosti.

Literatúra

<https://www.hackingarticles.in/usb-forensics-detection-investigation/>

Článok sa zaobera metódami detekcie a vyšetrovania USB flash diskov v digitálnej forenznej analytike. Popisuje nástroje ako Windows registry, PowerShell a USBDeview na identifikáciu pripojených zariadení. Ďalej sa venuje obnovovaniu zmazaných súborov pomocou diskového obrazu a analýze dát pomocou nástrojov ako FTK Imager.

Záver:

Tento prípad digitálnej forenznej analýzy sa sústreďí na identifikáciu dôkazov, ktoré môžu potvrdiť zapojenie podozrivého do pašovania ľudí. Analýza notebooku, USB a mobilného telefónu môže odhaliť dôležité informácie vedúce k ďalším podozrivým osobám a umožniť úspešné ukončenie vyšetrovania.