Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Špecialista kybernetickej bezpečnosti vo verejnej správe

Stretnutie 6

KC KYB UNIZA, https://kc.uniza.sk/

kckyb@uniza.sk, kcskolenia@uniza.sk

Harmonogram – deň 6

Hodina	Začiatok	Koniec	Rozsah
1	8:00	8:45	0:45
2	8:45	9:30	0:45
3	9:45	10:30	0:45
4	10:30	11:15	0:45
5	11:30	12:15	0:45
6	13:00	13:45	0:45
7	13:45	14:30	0:45
8	14:45	15:30	0:45
9	15:30	16:15	0:45
10	16:30	17:15	0:45

20	Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)	Digitálna forenzná analýza	Uramová	1	Deň 6
21	Moderné technológie, bezpečnosť cloudu a IoT (Blok VII)	Bezpečnosť cloudu	Moravčík	2,3	
22		Spravodajstvo o hrozbách (CTI)	Uramová	4	
23		Umelá inteligencia v KB	Škvarek	5	
24		Bezpečnosť IoT	Papán	6	
25	Zvyšovanie povedomia o KB a testovanie bezpečnosti (Blok VIII)	Bezpečnostné povedomie a tréningy zamestnancov	Uramová	7,8	
26		Bezpečnostné testovanie a ofenzívne zručnosti	Uramová	9,10	

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálna forenzná analýza

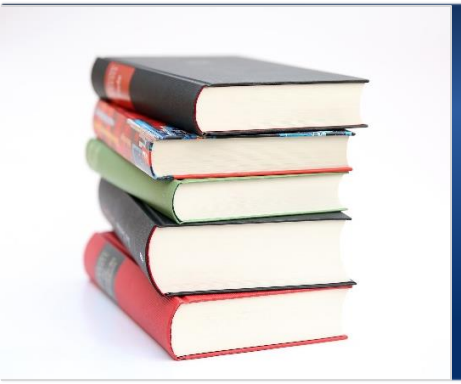
Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Obsah

- **Techniky a nástroje na zber, analýzu a uchovávanie digitálnych dôkazov**
- **Zber digitálnych dôkazov z rôznych zariadení, zachovanie integrity dôkazov**
- **Analýza dát z počítačov a pevných diskov, obnova zmazaných súborov a analýza súborových systémov.**
- Identifikácia a analýza malvéru, reverzné inžinierstvo na pochopenie fungovania malvéru, sandboxing
- **Právne a etické aspekty (dodržiavanie právnych predpisov a etických noriem pri zbere a analýze dôkazov), príprava dôkazov pre súdne konania**

Úvod do digitálnej forenznej analýzy

Terminológia

- **Forenzia**
  - z lat. „Forensis“ - súdne, od „Forum“ - verejné priestranstvá, kde sa konali súdy
- „**Forenzné**“ znamená „**súdne**“
  - preto „Forenzia“ zvyčajne označuje postupy a vedy, súvisiace s vyšetrovaním a súdnym dokazovaním
- **Forenzná veda** (alebo skrátene forenzika, forensics)
  - je vedný odbor, ktorý sa zaoberá vyšetrovaním, získavaním stôp a dokazovaním bezpečnostného incidentu alebo porušenia práva štátu či pravidiel organizácie
- **Digitálna forenzná analýza** (DFA)
  - je odbor forenznej vedy, ktorý sa zaoberá identifikáciou, získavaním, uchovávaním a analýzou digitálnych dôkazov.

Čo to je DFA

- Digitálna forenzná analýza:
  - je **proces identifikácie, získavania, uchovávania, analýzy a prezentácie digitálnych dôkazov**
  - cieľom je, aby boli použiteľné v **právnom alebo internom vyšetrovaní**
  - zaoberá sa dokazovaním kybernetických bezpečnostných incidentov
  - postupy musia zabezpečiť **integritu dôkazov** (chain of custody, nemodifikovanie dát)
- Zaoberá sa:
  1. **Identifikáciou** digitálnych dôkazov
  2. **Zhromažďovaním** digitálnych dôkazov
  3. **Analýzou** digitálnych dôkazov
  4. **Uchovávaním** digitálnych dôkazov




- **DFIR (Digital Forensics and Incident Response)**
  - kombinácia forenznej analýzy a reakcie na incident.
  - v rámci interného riešenia incidentu sa bežne robí "forenzná analýzu", aj keď dôkazy nechceme použiť na súde.
  - nemusíme striktne dodržať všetky právne požiadavky na dôkazný materiál,
  - ale je výhodné dodržať základné forenzné princípy (nemeniť originálne dáta, robiť si záznamy, pracovať s kópiou).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálna forenzná veda

- je neustále sa rozvíjajúca **vedná disciplína** s viacerými odbormi:
  1. **Počítačová forenzná analýza** (Computer Forensics)
     - cieľom tohto odboru je identifikácia, uchovávanie, zhromažďovanie, analýza a podávanie správ o stopách nájdených v zariadeniach a pamäťových médiách.
  2. **Sieťová forenzná analýza** (Network Forensics)
     - cieľom tohto odboru je za pomoci nástrojov a technológií, ktoré monitorujú sieťovú prevádzku, analyzovať a odhaliť zdroj bezpečnostných útokov, vniknutí alebo neobvyklého sieťového prenosu.
  3. **Forenzná analýza mobilných zariadení** (Mobile Devices Forensics)
     - tento odbor sa zameriava na zaisťovanie, interpretáciu a tiež obnovu elektronických stôp mobilných zariadení.
  4. **Forenzná analýza pamäte** (Memory Forensics)
     - vedný odbor zaoberajúci sa zaisťovaním a analýzou pamäte z bežiacich zariadení.
  5. **Forenzná analýza cloudov** (Cloud Forensics)
     - vedný odbor zaoberajúci sa zaisťovaním digitálnych stôp pri používaní cloudových služieb.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zainteresované strany forenznej analýzy

Osoby typicky zodpovedné za identifikáciu, zber, získanie a uchovanie potenciálnych (digitálnych) dôkazov:

- V pracovno-právnych vzťahoch:
  - špecialisti informačnej bezpečnosti
  - špecialisti na riešenie incidentov
  - manažéri kybernetickej bezpečnosti
  - manažéri forenzných laboratórií
  - audítori
- Vo vyšetrovaniach a súdnych sporoch:
  - forenzní technici (z angl. „Digital Evidence First Responders“ - **DEFR**),
  - forenzní špecialisti (z angl. „Digital Evidence Specialists - **DES**),
  - **súdni znalci** zapísaní v príslušnom odvetví a znaleckom odbore

Osoby typicky účastné na konaní (vo všeobecnosti osoby ktoré potrebujú určiť a preukázať spoľahlivosť predložených digitálnych dôkazov):

- V pracovno-právnych vzťahoch:
  - špecialisti na systém riadenia podvodov (fraud management)
  - HR špecialisti
  - audítori
- Vo vyšetrovaniach a súdnych sporoch:
  - orgány činné v trestnom konaní (v zmysle §10 ods. 1 TP - prokurátor a policajt)
  - súdy
  - obhajcovia, advokáti
  - strany sporu, poškodený, obvinený, obžalovaný, osoby s obhajovacími právami (zákonný zástupca, opatrovník, orgány starostlivosti o mládež, a.i.)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Postup pri zbere a akvizícií digitálnych dôkazov

Zber digitálnych dôkazov z rôznych zariadení, zachovanie integrity dôkazov

Vrátane techník a nástrojov na zber, analýzu a uchovávanie digitálnych dôkazov

Postup pri zbere a akvizícií digitálnych dôkazov

1. Právne a organizačné predpoklady
2. Zber a Akvizícia digitálnych dôkazov
   - Zber - proces zaisťovania fyzických zariadení, ktoré obsahujú digitálne dôkazy.
   - Akvizícia - proces vytvárania kópie údajov v rámci definovanej množiny.
     - Produktom akvizície je potenciálna kópia digitálneho dôkazu.
   - Systém po incidente stále beží => Life forensics
   - Systém po incidente je vypnutý => Dead forensics
   - Plus: zber špeciálnych zariadení (kamera a iné)
3. Verifikácia integrity digitálnych dôkazov
4. Dokumentácia celého vyšetrovania (Chain of Custody Record)
5. Analytické a následné kroky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1. Právne a organizačné predpoklady

- Získanie **autorizácie**
  - **Súdny príkaz**, **interné oprávnenie**, **zmluvný súhlas klienta**
    - Dôvodom je súlad so zákonom **GDPR**
  - Súhlas musí definovať: **kde**, **čo** sa smie získať a **na aký účel**
- Definovanie **cieľa a rozsahu** vyšetrovania
  - Určenie cieľa forenzného zásahu
    - Reakcia na incident, dôkazové konanie, preventívna kontrola
  - Stanovanie rozsahu zberu
- Vyhodnotenie **rizík**
  - Môže sa systém po vypnutí poškodiť alebo stratiť dáta?
  - Je zariadenie súčasťou produkčnej infraštruktúry?
- Príprava **vybavenia a forenzných pomôcok**
  - Sada nástrojov pre riešenie kybernetických bezpečnostných incidentov
- Príprava **dokumentačných formulárov** na okamžité označenie dôkazov

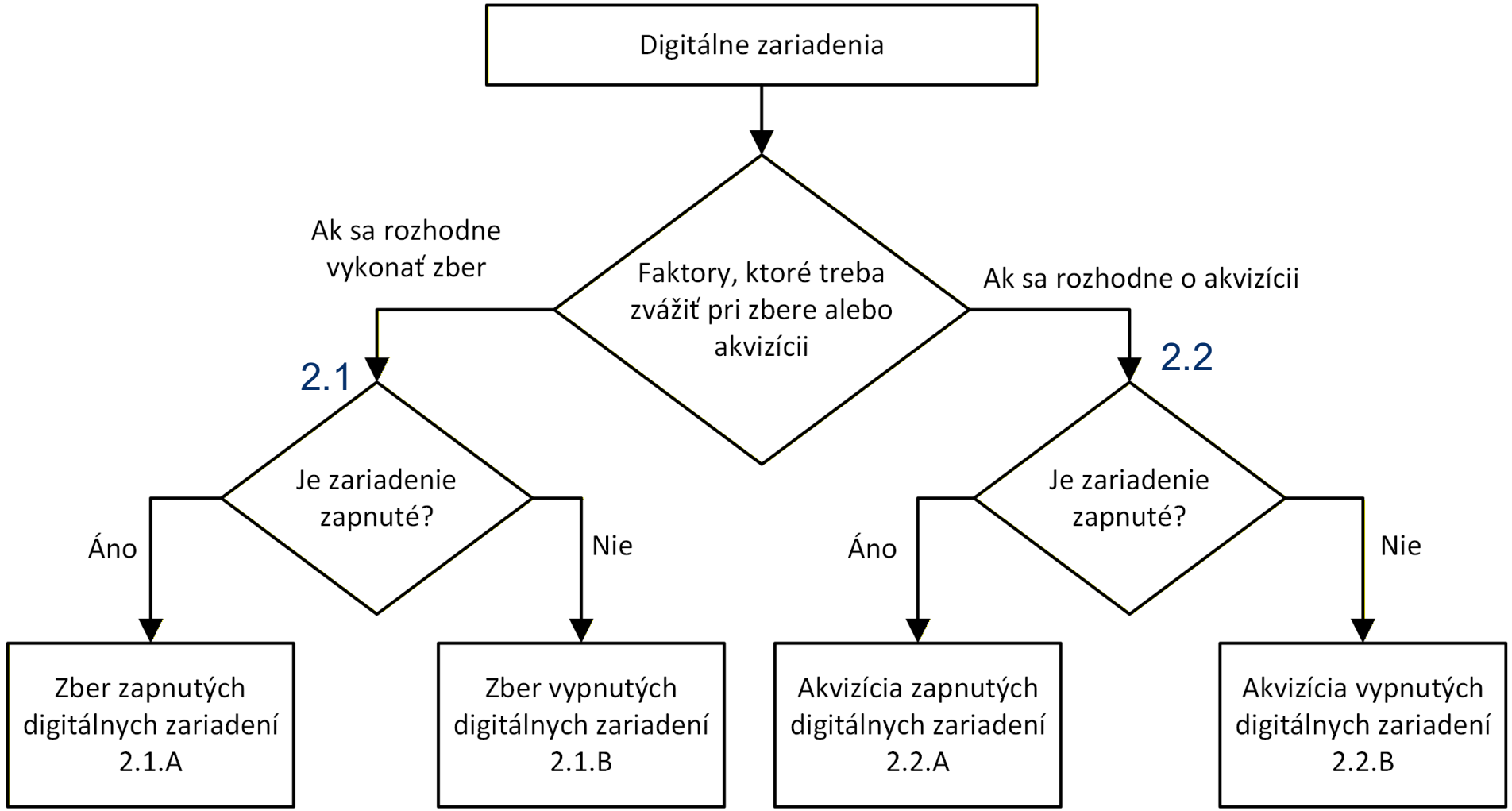
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Postup pri zbere a akvizícií digitálnych dôkazov

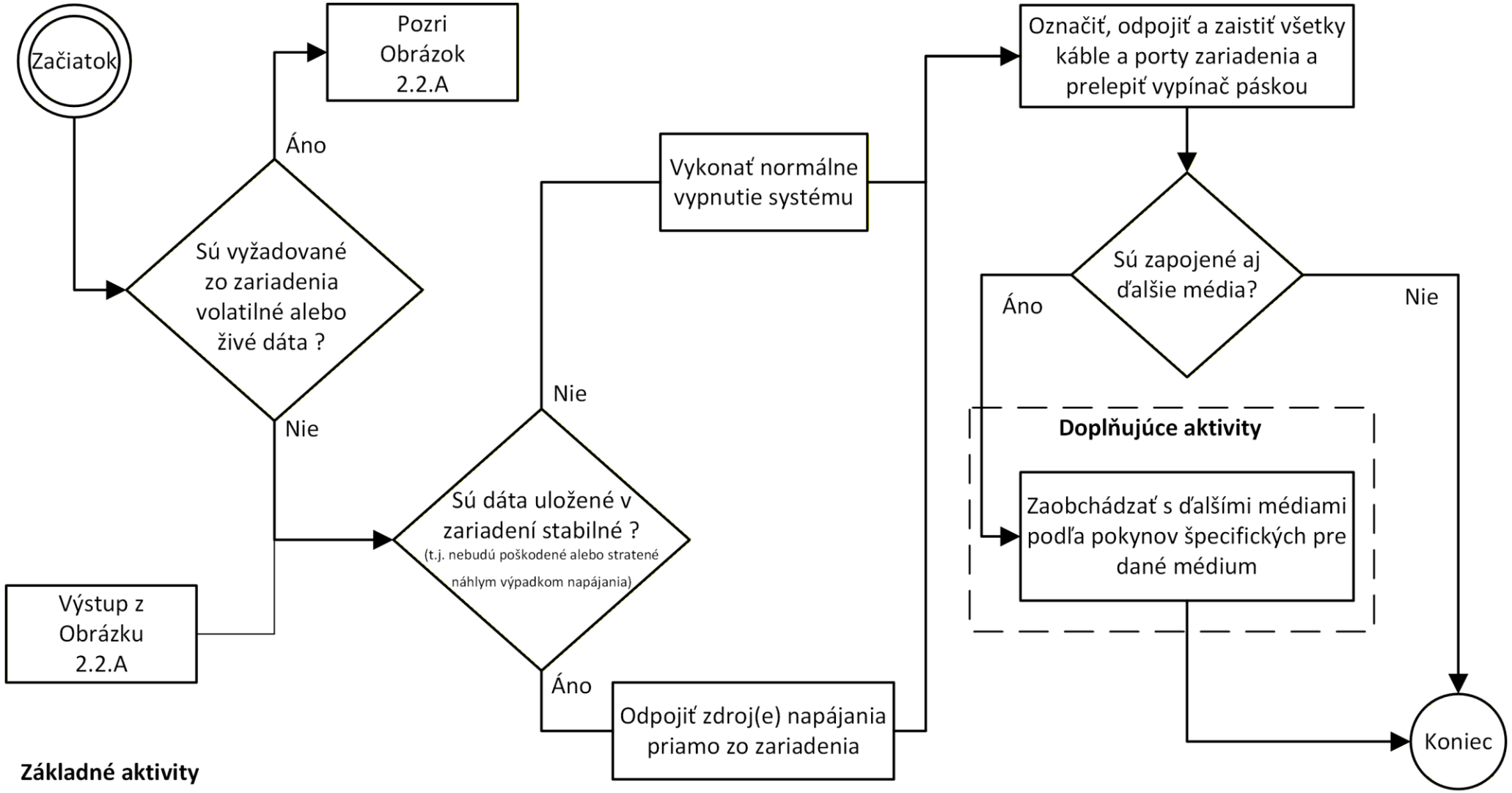
1. Právne a organizačné predpoklady
2. Zber a akvizícia digitálnych dôkazov
   - Zber - proces zaisťovania fyzických zariadení, ktoré obsahujú digitálne dôkazy.
   - Akvizícia - proces vytvárania kópie údajov v rámci definovanej množiny.
     - Produktom akvizície je potenciálna kópia digitálneho dôkazu.
   - Systém po incidente stále beží => Life forensics
   - Systém po incidente je vypnutý => Dead forensics
   - Plus: zber špeciálnych zariadení (kamera a iné)
3. Verifikácia integrity digitálnych dôkazov
4. Dokumentácia celého vyšetrovania (Chain of Custody Record)
5. Analytické a následné kroky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

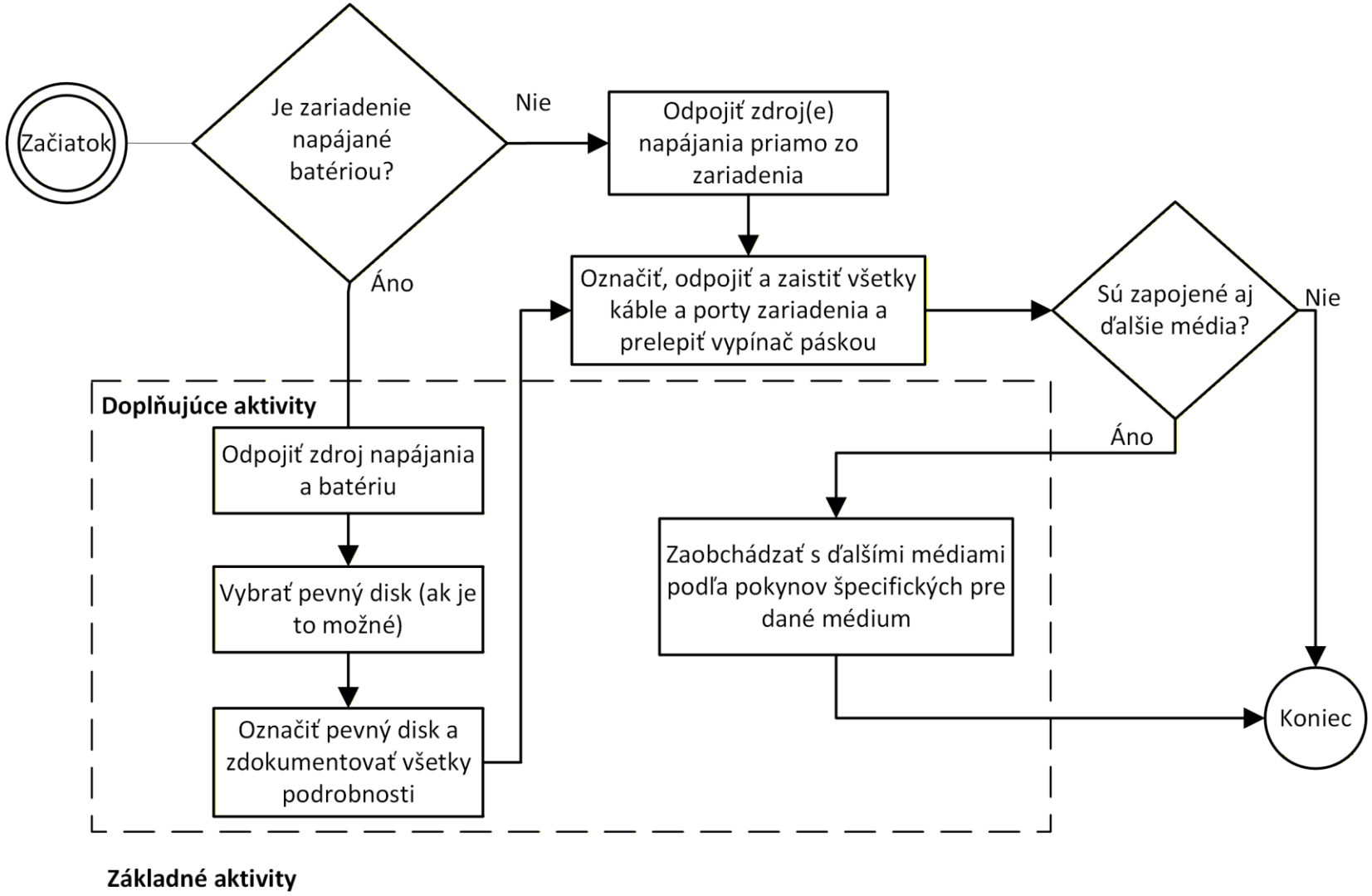
2. Postup rozhodnutia o zbere alebo akvizícií digitálnych dôkazov



2.1.A Proces zberu zo zapnutého zariadenia



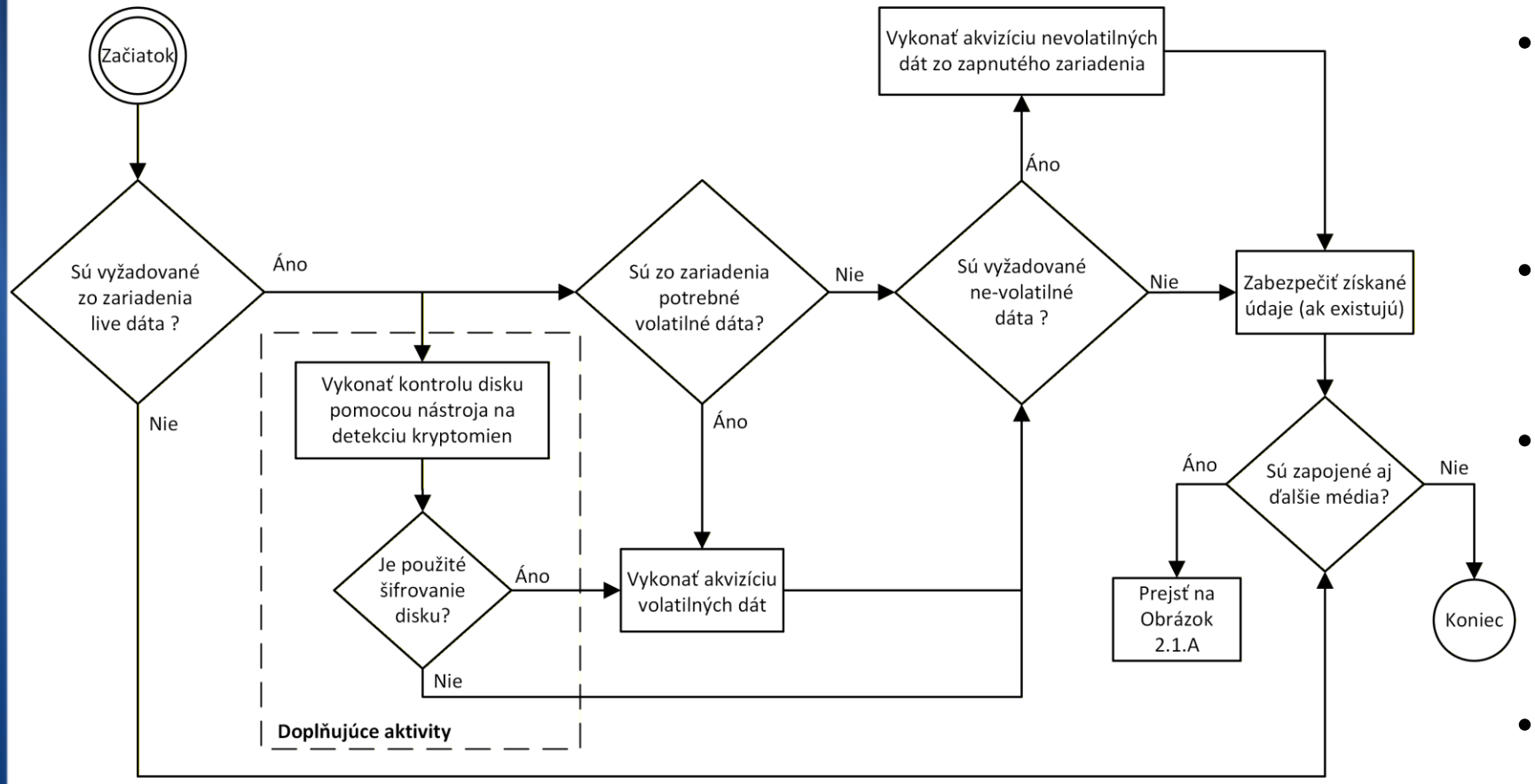
2.1.B Proces zberu z vypnutého zariadenia



- Po vykonaní zberu, digitálne zariadenia sú následne bezpečne premiestnené do laboratória alebo iného kontrolovaného prostredia na neskoršiu akvizíciu a analýzu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2.2.A Proces akvizície zo zapnutého zariadenia

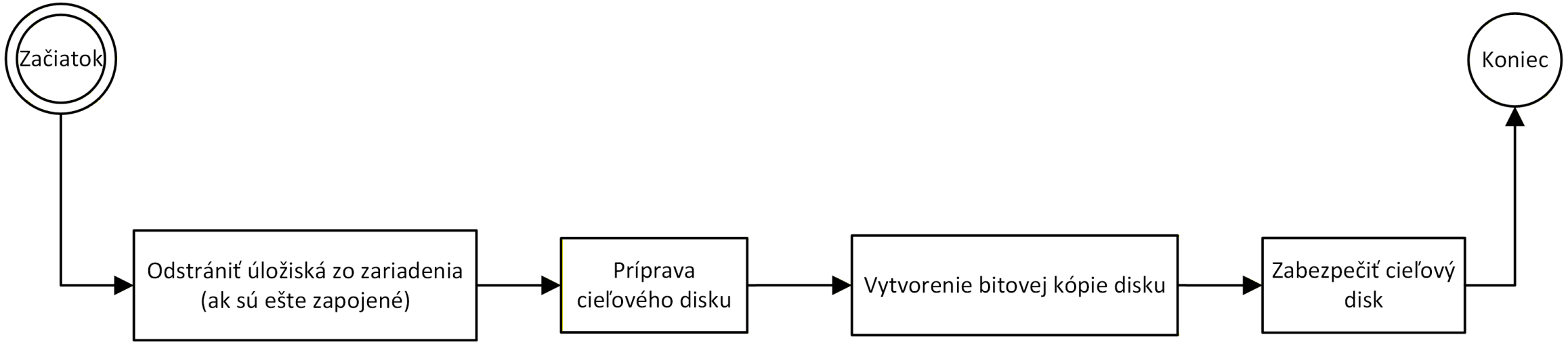


- Zachytenie RAM
  - Nástroje: winpmem, avml...
- Vypočítanie kontrolného súčtu (hash)
- Zber sieťových spojení a bežiacich procesov
  - Nástroje: nestat, ss, ps...
- Zaznamenanie každej operácie
  - Čas a kto spustil aké príkazy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2.2.B Postup akvizície z vypnutého zariadenia

- HDD alebo SSD zapojiť cez HW write-blocker
- Bitová kópia disku
  - Nástroje: dc3dd, guigamer, ewfacquire
  - hash
- Duplikovať kópie disku
  - Dôležité pre analýzu dôkazov
- Disk kompromitovaného zariadenia
  - Označiť, uschovať, zabezpečiť pred neoprávneným zásahom



Rozhodnutie o akvizícii vypnutého a zapnutého zariadenia

Dead (systém je vypnutý)

- HDD alebo SSD zapojiť cez HW write-blocker
- Bitová kópia disku
  - Nástroje: dc3dd, guigamer, ewfacquire
  - hash
- Duplikovať kópie disku
  - Dôležité pre analýzu dôkazov
- Disk kompromitovaného zariadenia
  - Označiť, uschovať, zabezpečiť pred neoprávneným zásahom

Live (systém je zapnutý)

- Zachytenie RAM
  - Nástroje: winpmem, avml...
  - Vytvorenie hash reportu
- Zber sieťových spojení a bežiacich procesov
  - netstat - zobrazuje sieťové spojenia, štatistiky rozhraní, smerovacie tabuľky a otvorené porty
  - ss - modernejšia a rýchlejšia náhrada za netstat
  - ps - zobrazuje bežiace procesy v systéme
- Zaznamenanie každej operácie
  - Čas a kto spustil aké príkazy

Akvizícia digitálnych dôkazov

Vlastnosť	A. Dead-box forensics	B. Live-box forensics
Stav systému	Vypnutý	Zapnutý
Primárny účel	Analýza trvalých dát	Zachytenie volatilných dát
Zachytené dáta	Disk, FS, metadáta	RAM, procesy, spojenia
Riziko modifikácie	Minimálne	Vysoké
Nutné vybavenie	Write-blocker, imaging	Live acquisition nástroje
Výhody	Forenzne čisté	Zachytenie RAM dát
Nevýhody	Žiadne RAM dáta	Riziko zmeny systému
Typické použitie	Súdne prípady	Incident response
Šifrované disky	Zvyčajne zamknuté	Často odomknuté v RAM
Príklady nástrojov	Autopsy, TSK, EnCase	Volatility, FTK Imager Lite

- Digitálne stopy sú typicky volatilného (krehkého) charakteru
- Nesprávnym skúmaním môžu byť zmenené, manipulované alebo zničené

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Akvizícia digitálnych dôkazov

Základné best practices

A. **Dead-box** forensics
   - vypnutie zariadenia a priamy zber dôkazov

B. **Live-box** forensics
   - Zber živej pamäte – RAM image

C. **Sieťový** zber
   - Zachytenie paketov, logov z firewallu...

D. Zber z **mobilných** zariadení

E. Timeline analýza
   - Rekonštrukcia udalostí

Čo sa môže zbierať

1. Pamäťové média
   - HDD alebo SSD disk
   - USB
2. Pamäť (RAM)s
3. Logy
4. Sieťové záznamy a procesy
5. E-maily a archívy
6. Metadáta súborov
7. Odstránené súbory (obnoviteľné)
8. Súbory prehliadača a cache

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje na zber a analýzu digitálnych dôkazov

- **Disk imaging**
  - **dd**
    - Klasický unixový kopírovací nástroj (CLI)
  - **dc3dd**
    - Forenzne orientované riešenie dd (CLI)
  - **Guymager**
    - Nástroj pre disk imaging s GUI
  - **ewfacquire**
    - vytváranie EWF/E01 obrazov (kompatibilné s EnCase)

- Môžu existovať prípady, v ktorých nie je možné alebo prípustné vytvoriť kópiu digitálneho dôkazu zdroja dôkazov,
  - napríklad keď je zdroj údajov príliš objemný
  - v týchto prípadoch môže analytik vykonať logickú akvizíciu, ktorá sa zameriava iba na:
    - konkrétne dátové typy, adresáre alebo lokality.
  - toto spravidla prebieha na úrovni súborového systému resp. diskových oddielov.

- **Formát EWF/E01:**
  - EWF = Expert Witness Format
    - všeobecný názov pre formát obrazov používaný v digitálnej forenzike.
  - E01 je najrozšírenejšia implementácia EWF
    - prípona súborov .E01, .E02, … pre segmenty.
  - Tento formát vytvoril Guidance Software (EnCase) a je de-facto priemyselný štandard pre forenzné obrazy diskov.

- **Kľúčové vlastnosti E01**
  - obsahuje *sektorový obraz* zdroja (bit-for-bit/ bitstream)
  - **metadata header** (informácie o akvizícii: kto, kedy, zariadenie, poznámky)
  - podporuje **segmentovanie** (E01, E02… ak je obraz rozdelený na časti)
  - často obsahuje **kontrolné súčty** (MD5 / SHA1 alebo iné) pre overenie integrity
  - môže obsahovať **kompresiu** (znižuje veľkosť obrazu)
  - široká **kompatibilita** s EnCase a mnohými forenznými nástrojmi

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Postup pri zbere a akvizícií digitálnych dôkazov

1. Právne a organizačné predpoklady
2. Zber a akvizícia digitálnych dôkazov
   - Zber - proces zaisťovania fyzických zariadení, ktoré obsahujú digitálne dôkazy.
   - Akvizícia - proces vytvárania kópie údajov v rámci definovanej množiny.
     - Produktom akvizície je potenciálna kópia digitálneho dôkazu.
   - Systém po incidente stále beží => Life forensics
   - Systém po incidente je vypnutý => Dead forensics
   - Plus: zber špeciálnych zariadení (kamera a iné)
3. Verifikácia integrity digitálnych dôkazov
4. Dokumentácia celého vyšetrovania (Chain of Custody Record)
5. Analytické a následné kroky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

3. Verifikácia integrity

- Ak sa pre digitálny dôkaz (bitová kópia disku, pamäťová snímka, logy) **nepreukáže, že nebol zmenený** od momentu získania, môže jeho hodnota v súdnom alebo internom konaní výrazne poklesnúť.
- Ako to preukázať:
  - pomocou použitia časových pečiatok a hash reportu
    - Odporúčaný min. štandard SHA-256
    - SHA-1 & MD5 iba ako doplnok

1. Hash originálneho pamäťového média pred vytvorením bitovej kópie (image)
2. Po vytvorení bitovej kópie sa porovná s pôvodným
3. Zaznamenanie výsledkov a dokumentácia

+ časové pečiatky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aj malá zmena rozhodne o vierohodnosti dôkazu !

„Toto je hash SHA-256.“

3158d941eaacd1117557ad1694d6cd0f0c63c27b2ed5bb022b9591e01063c9d1

„Toto je hash SHA256.“

2026d28e78656ba757c1bd8f86044566abc4c9578d0feb26151efefab3d2d849

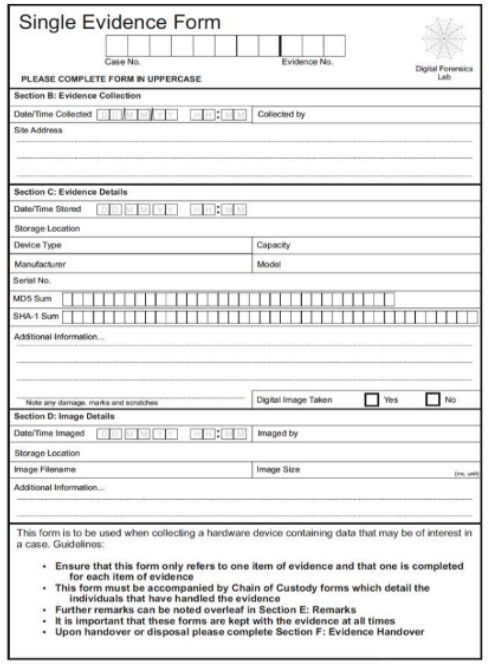
Postup pri zbere a akvizícií digitálnych dôkazov

1. Právne a organizačné predpoklady
2. Zber a akvizícia digitálnych dôkazov
   - Zber - proces zaisťovania fyzických zariadení, ktoré obsahujú digitálne dôkazy.
   - Akvizícia - proces vytvárania kópie údajov v rámci definovanej množiny.
     - Produktom akvizície je potenciálna kópia digitálneho dôkazu.
   - Systém po incidente stále beží => Life forensics
   - Systém po incidente je vypnutý => Dead forensics
   - Plus: zber špeciálnych zariadení (kamera a iné)
3. Verifikácia integrity digitálnych dôkazov
4. Dokumentácia celého vyšetrovania (Chain of Custody Record)
5. Analytické a následné kroky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zber digitálnych dôkazov z rôznych zariadení

4. Dokumentácia - Chain of custody


Single Evidence Form

Case No. Evidence No.

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected Collected by

Site Address

Section C: Evidence Details

Date/Time Stored

Storage Location

Device Type Capacity

Manufacturer Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches Digital Image Taken Yes No

Section D: Image Details

Date/Time Imaged Imaged by

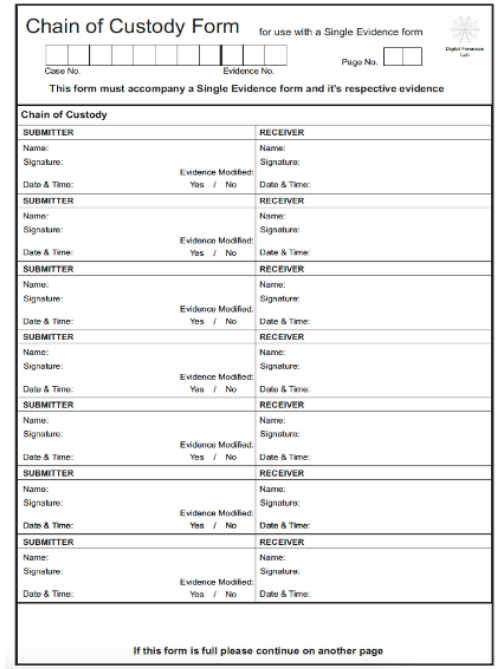
Storage Location

Image Filename Image Size

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover


Chain of Custody Form for use with a Single Evidence form

Case No. Evidence No. Page No.

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:
SUBMITTER		RECEIVER
Name:		Name:
Signature:	Evidence Modified:	Signature:
Date & Time:	Yes / No	Date & Time:

If this form is full please continue on another page

- Pri zbere dôkazov treba zaznamenať
  - Jedinečný identifikátor získanej stopy
    - ID
  - Stručný popis predmetu
    - Typ, sériové číslo, stav
    - napr. identifikácia média, umiestnenie, sériové číslo, číslo modelu, MAC adresa, súvisiace IP adresy, atď.
  - Dátum a čas získania
  - Miesto získania
  - Použitý nástroj pre zber
    - Napr. dc3dd...
  - Zoznam osôb, ktoré pristupovali ku získaným stopám, čas a miesto prístupu
  - Osoba, ktorá dôkaz zobrala
  - Komu bol dôkaz odovzdaný
    - Dátum a čas, účel prenosu
    - Zoznam osôb, ktoré kontrolujú pohyb potenciálnych dôkazov z úschovy a do úschovy a čas tohto presunu, od momentu keď digitálne zariadenie a / alebo potenciálne digitálne dôkazy boli získané
  - Nevyhnutné zmeny potenciálnych digitálnych dôkazov, rovnako ako meno osoby zodpovednej teda aj zdôvodnenie pre zavedenie zmeny

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Opatrenia na mieste incidentu

- Forenzný technik by mal vykonať činnosti na zabezpečenie a ochranu umiestnenia potenciálnych digitálnych dôkazov, ihneď po príchode na miesto.
- Činnosti by mali obsahovať nasledujúce úkony, v súlade s národnou legislatívou:
  - Zaistenie a **prevzatie kontroly** nad oblasťou v ktorej sa nachádzajú zariadenia
  - Určiť, kto je najvyššia **zodpovedná** osoba
  - Uistiť sa, že sa všetky **osoby vzdialili** od zariadení a zdrojov napájania
  - **Legitimovať** každého, kto má prístup k lokácii a každého, kto by mohol mať dôvod byť prítomný na mieste incidentu
  - V prípade, že je zariadenie **zapnuté nevypínať ho** a ak je zariadenie **vypnuté nezapínať ho**
  - Pokiaľ je to možné, zdokumentovať (napr. zakresliť, odfotografovať) scénu, všetky komponenty a kabeláže v ich pôvodnej polohe. Označiť porty a káble tak, aby konfigurácia systému mohla byť zrekonštruovaná neskôr
  - Ak je to možné, prehľadať priestor či sa v ňom nevyskytujú také položky, ako sú lístky s poznámkami, denníky, doklady, zápisníky, alebo hardvérové a softvérové príručky so zásadnými detailami o zariadení (napr. heslá a PIN čísla)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Postup pri zbere a akvizícii digitálnych dôkazov

1. Právne a organizačné predpoklady
2. Zber a akvizícia digitálnych dôkazov
   - Zber - proces zaisťovania fyzických zariadení, ktoré obsahujú digitálne dôkazy.
   - Akvizícia - proces vytvárania kópie údajov v rámci definovanej množiny.
     - Produktom akvizície je potenciálna kópia digitálneho dôkazu.
   - Systém po incidente stále beží => Life forensics
   - Systém po incidente je vypnutý => Dead forensics
   - Plus: zber špeciálnych zariadení (kamera a iné)
3. Verifikácia integrity digitálnych dôkazov
4. Dokumentácia celého vyšetrovania (Chain of Custody Record)
5. Analytické a následné kroky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

5. Analýza dôkazov

- Používať iba kópie (forenzné obrazy)
  - Prečo ? : Originálny disk musí zostať v nezmenenej podobe ako dôkaz
- Indexovanie a dokumentácie analýzy
  - Z ktorého pamäťového média pochádzajú
  - Ktorý nástroj ich našiel
- Vytvorenie forenzného reportu
  - Report je oficiálny výstup analýzy (Dokument)
    - Čo bolo získané
      - Typ média, veľkosť...
    - Ako bolo získané
      - Použitý nástroj, verzia, hash...
    - Kto to robil
      - Meno, funkcia...
    - Čo sa zistilo

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje na analýzu dôkazov

- **Analýza zozbieraných dôkazov**
  - **Autopsy** ako GUI pre súbor nástrojov The Sleuth Kit
    - kompletné rozhranie pre analýzu obrazov, timeline analýzu, prehliadanie súborov
    - (neskôr bude ukážka z nástroja)
  - **Sleuth Kit** (fls, ils, icat, mactime)
    - CLI nástroje na prieskum súborového systému (FS), carving, timeline
    - (pokrač. na ďalšom snímku)
  - **EnCase** Forensic
    - komerčný štandard pre súdne prípady, robustné reportovanie a scripting.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

The Sleuth Kit (TSK) nástroje

- TSK nástroje
  - pracujú priamo so súborovým systémom (*FS)*,
  - nie s logickými súbormi ako bežné OS.
- V kontexte Sleuth Kit to znamená:
  - **typ súborového systému** (NTFS, FAT32, Ext4, APFS…)
  - **štruktúra súborov a adresárov**
  - **metadata** (inódy, časové pečiatky, oprávnenia…)
  - **alokácia a fragmentácia dát**
- Carving
  - je proces, pri ktorom sa z disku (alebo iného média) snažíme **nájsť a zrekonštruovať súbory iba na základe ich obsahu**, nie na základe:
    - názvu súboru
    - cesty v adresárovej štruktúre
    - MFT (NTFS) alebo inode (ext4)
    - iných metadát
  - Používa sa hlavne, keď:
    - súborový systém je **poškodený**
    - útočník **zmazal metadáta**
    - došlo k **preformátovaniu**
    - existujú len **fragmenty súborov**

- **TSK nástroje –** fls, ils, icat, mactime
  - **fls** – File List
    - **F = file**, **ls = list**
    - Vypisuje zoznam súborov a adresárov z diskového obrazu alebo súborového systému.
    - Vie zobraziť aj zmazané položky a metadata.
  - **ils** – Inode List
    - **i = inode**, **ls = list**
    - Listuje všetky inódy (metadata záznamy) v súborovom systéme.
    - Neprezerá názvy súborov, ale *raw* inódy.
  - **icat** – Inode Cat
    - **i = inode**, **cat = concatenate / zobraz obsah**
    - Z inódu vytiahne obsah súboru priamo z FS, aj keď je súbor zmazaný alebo bez mena.
  - **mactime** – Modified, Accessed, Changed, Created time
    - **M = Modified**
      A = Accessed
      C = Changed metadata
      (T)ime = časová os
    - Vytvára časovú os (timeline) udalostí na základe MAC časov súborov.
    - Používa výstup z fls alebo ils.

Nástroje na zber a analýzu digitálnych dôkazov

- Obnova zmazaných súborov
  - **Foremost**
- Analýza pamäte (RAM)
  - **Volatility**
    - štandardná platforma na analyzovanie RAM image (procesy, sieť, DLL)
  - **Rekall**
    - alternatíva k Volatility s inými pluginmi a prístupmi
- Sieťová analýza
  - **Wireshark, tshark**
    - analýza pcap súborov, dekódovanie protokolov
  - **tcpdump**
    - CLI nástroje na zachytávanie a filtrovanie paketov
- Analýza malvéru
  - **Ghidra**
    - bezplatný disassembler/ Reverse Engineering rámec od NSA, silná statická analýza
  - **Any.Run**
    - interaktívne online sandboxovanie
  - **Cuckoo Sandbox**
    - dynamicky spustí malware a vygeneruje report

Jump kit

Sada nástrojov pre riešenie KBI

Alias: „Jump-kit“

- prenosná súprava nástrojov a zariadení

Cieľom je:

- umožniť rýchlu, efektívnu a pripravenú reakciu na incident

- Obsahuje hardware, software a príslušenstvo potrebné na vyšetrovanie incidentu
- Používa sa na zber dôkazov, analýzu incidentu a obnovu systémov.
- Musí byť vždy pripravený na použitie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sada nástrojov pre riešenie KBI – Obsah kufríka

Obsah Jump kitu	
Notebook	Lenovo ThikPad E14
Externé pamäťové médiá	HDD / SSD / USB
Patch káble	1 m
Write-Blocker	Forensics UltraDock
Dokumenty	
Response plán	Postup pri riešení incidentu
	Kontaktné informácie
	Postup pri zbere dôkazov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sada nástrojov pre riešenie KBI – Write-blocker

- Hardvérový write-blocker
- Blokuje zápis na pripojené pamäťové médium

Funkcie zobrazenia:

- Sériové číslo disku
- Kapacita
- Teplota disku
- Rýchlosť pripojenia
- Počet chybných sektorov

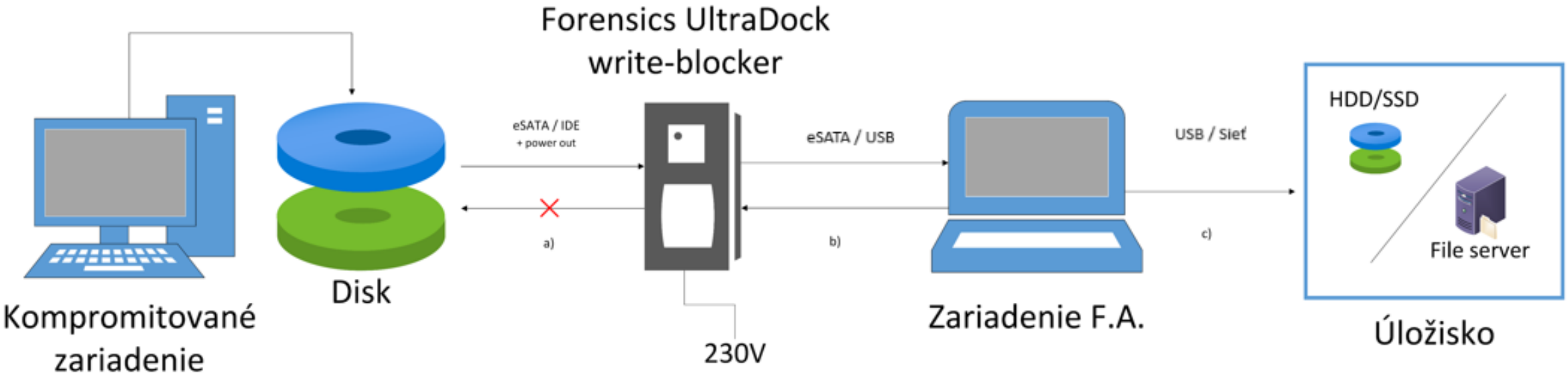
- Cena: ~500€

- Prepojenie s diskom
  - eSATA
  - IDE
- Prepojenie s forenzným počítačom
  - USB
  - SATA Power In

Forensic Ultradock v6

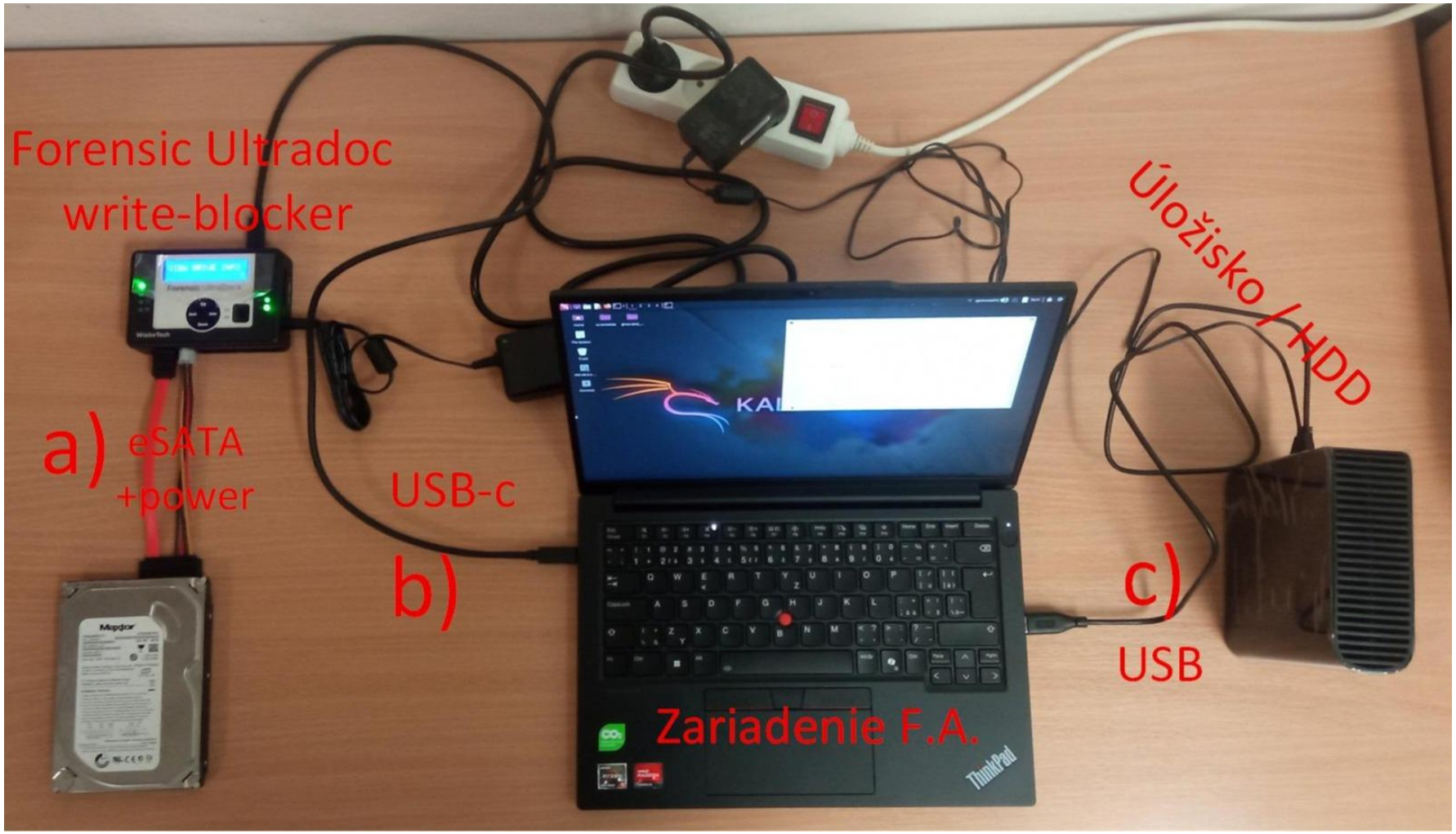
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tvorba bitovej kópie disku - zapojenie



Ukážka zberu dôkazu

Tvorba bitovej kópie disku - zapojenie



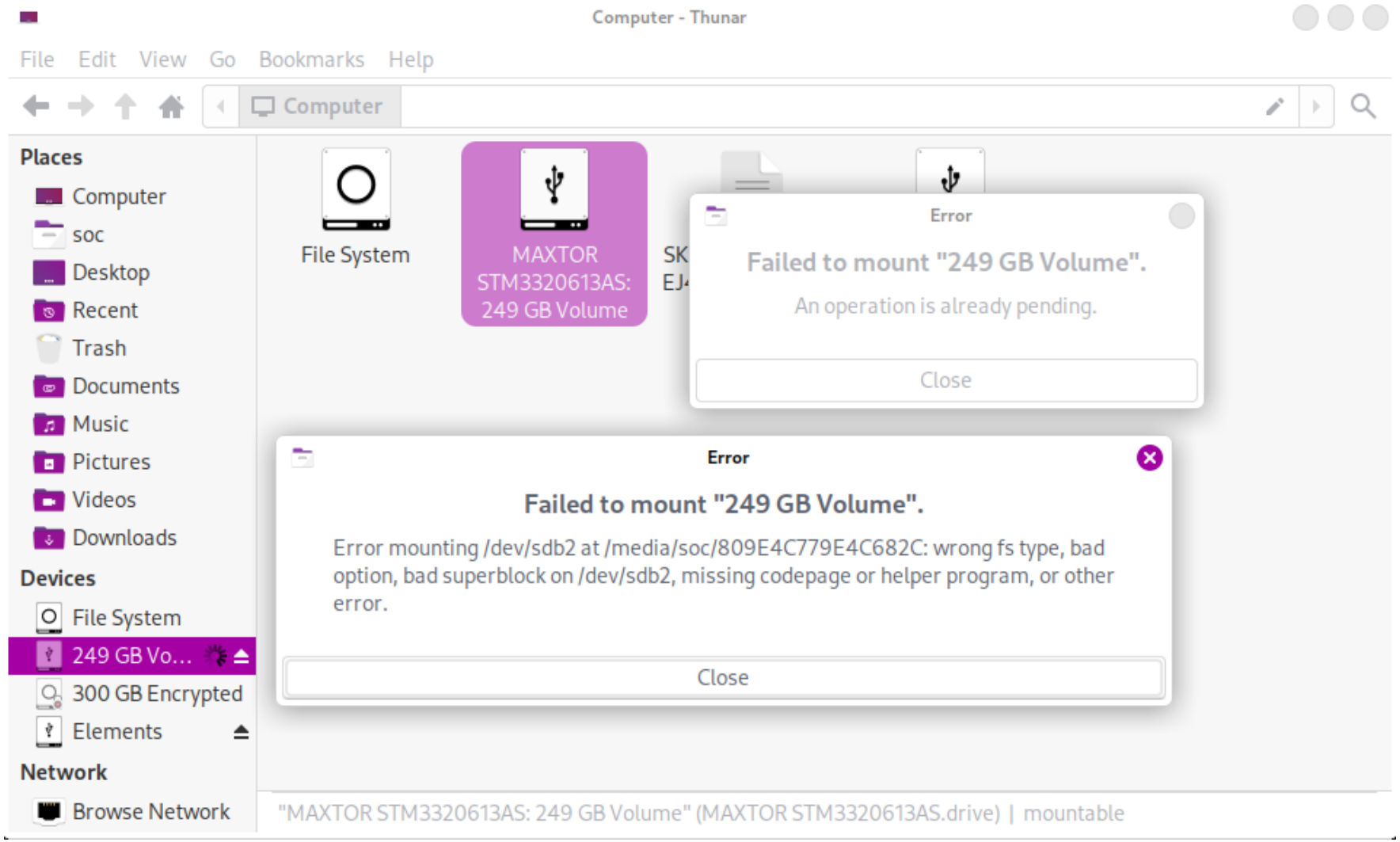
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

```
t-kali)-[~]

MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
  8:0    0   5.5T  0 disk
  8:1    0   5.5T  0 part /media/soc/Elements
  8:16   0 298.1G  0 disk
  8:17   0   500M  0 part
  8:18   0 231.5G  0 part
  8:19   0   850M  0 part
259:0    0 476.9G  0 disk
259:1    0   260M  0 part
259:2    0    16M  0 part
259:3    0 279.4G  0 part
259:4    0     2G  0 part
259:5    0   977M  0 part /boot/efi
259:6    0 184.3G  0 part /
259:7    0  10.1G  0 part [SWAP]

t-kali)-[~]
```

Ukážka tvorby bitovej kópie

Tvorba bitovej kópie disku

- Správca súborov nedokáže otvoriť disk kompromitovaného zariadenia, ktoré je prepojené cez write-blocker.
- Systém sa snaží spraviť zápis o prístupe do disku
  - to sa mu nepodarí vďaka WB
  - vypíše chybu.



Tvorba bitovej kópie disku - zobrazenie diskov a partícií

```
┌──(soc㉿soc-kali)-[~]
└─$ lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda           8:0    0   5.5T  0 disk
└─sda1        8:1    0   5.5T  0 part /media/soc/Elements
sdb           8:16   0 298.1G  0 disk
├─sdb1        8:17   0   500M  0 part
├─sdb2        8:18   0 231.5G  0 part
└─sdb3        8:19   0   850M  0 part
nvme0n1     259:0    0 476.9G  0 disk
├─nvme0n1p1 259:1    0   260M  0 part
├─nvme0n1p2 259:2    0    16M  0 part
├─nvme0n1p3 259:3    0 279.4G  0 part
├─nvme0n1p4 259:4    0     2G  0 part
├─nvme0n1p5 259:5    0   977M  0 part /boot/efi
├─nvme0n1p6 259:6    0 184.3G  0 part /
└─nvme0n1p7 259:7    0  10.1G  0 part [SWAP]

┌──(soc㉿soc-kali)-[~]
└─$
```

Zelený = Externý disk (kde sa bitová kópia disku uloží)

Červený = Disk kompromitovaného zariadenia

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tvorba bitovej kópie disku - disk hash

Príkaz:

sudo md5sum /zdroj/hashu > cesta/kde/sa/uloží/subor.txt

```
┌──(soc㉿soc-kali)-[~]
└─$

┌──(soc㉿soc-kali)-[~]
└─$ sudo md5sum /dev/sdb2 > /home/soc/Desktop/generated_hash/hashMD5-sda2.txt

[sudo] password for soc:
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tvorba bitovej kópie disku

Príkaz:

sudo dc3dd **if**=/dev/sdb2 **of**=/media/soc/Elements/test_disk_imaging/sdb2_dc3dd.img **hash**=md5 **log**=/media/soc/Elements/test_disk_imaging/sdb2_dc3dd.txt

```
┌──(soc㉿soc-kali)-[~]
└─$ sudo dc3dd if=/dev/sdb2 of=/media/soc/Elements/test_disk_imaging/sdb2_dc3dd.img hash=md5 log=/media/soc/Elements
/test_disk_imaging/sdb2_dc3dd.txt

[sudo] password for soc:

dc3dd 7.2.646 started at 2025-10-21 18:35:34 +0200
compiled options:
command line dc3dd if=/dev/sdb2 of=/media/soc/Elements/test_disk_imaging/sdb2_dc3dd.img hash=md5 log=/media/soc/Elem
ents/test_disk_imaging/sdb2_dc3dd.txt
device size: 485507487 sectors (probed),   248,579,833,344 bytes
sector size: 512 bytes (probed)
165442650112 bytes ( 154 G ) copied ( 67% ), 4492 s, 35 M/s
```

Tvorba bitovej kópie disku -kontrola

```
┌──(soc㉿soc-kali)-[~/Desktop/generated_hash]
└─$ cat README.txt
hashmd5-sdb2.txt                // prvy vygenerovany hash z fyz. disku
hashmd5-sdb2-img.txt            // hash vygenerovany pocas bitovej kopie
hashmd5-from-img-test.txt       // hash vygenerovany zo suboru bitovej kopie
hashmd5-from-copy.txt           // hash vygenerovany z duplikatu bitovej kopie

┌──(soc㉿soc-kali)-[~/Desktop/generated_hash]
└─$ ls
hashmd5-from-copy.txt  hashmd5-from-img-test.txt  hashmd5-sdb2-img.txt  hashmd5-sdb2.txt  README.txt

┌──(soc㉿soc-kali)-[~/Desktop/generated_hash]
└─$ cat hashmd5-sdb2.txt && cat hashmd5-sdb2-img.txt && cat hashmd5-from-img-test.txt && cat hashmd5-f
rom-copy.txt
b9fb8e468f82bc5ee50e8ace102bee5a /dev/sdb2
b9fb8e468f82bc5ee50e8ace102bee5a
b9fb8e468f82bc5ee50e8ace102bee5a  sdb2_dc3dd.img
b9fb8e468f82bc5ee50e8ace102bee5a  sdb2_dc3dd_v2.img
```

Analýza súborových systémov

Ukážka analýzy dát z bitovej kópie disku pomocou nástroja Autopsy

Možnosti pre obnovu zmazaných súborov

Analýza súborových systémov – Ciele analýzy

- Prehľad súborového systému
  - získať celkový obraz o štruktúre disku
- Vyhľadávanie kľúčových slov
  - nájsť relevantné informácie (IP adresy, mená, e-mail, názvy súborov)
- Časová analýza (timeline)
  - zrekonštruovať časovú postupnosť udalostí
- Obnova zmazaných súborov
  - získať prístup k dátam, ktoré boli vymazané, ale ešte **neprepísané**
- Detekcia neobvyklých súborov alebo skriptov
  - Identifikovať škodlivé alebo skryté dáta

Príprava analýzy disku - Mountnutie obrazu

- Príkaz pri FA, keď chceme bezpečne prehliadať a analyzovať obsah bitovej kópie:

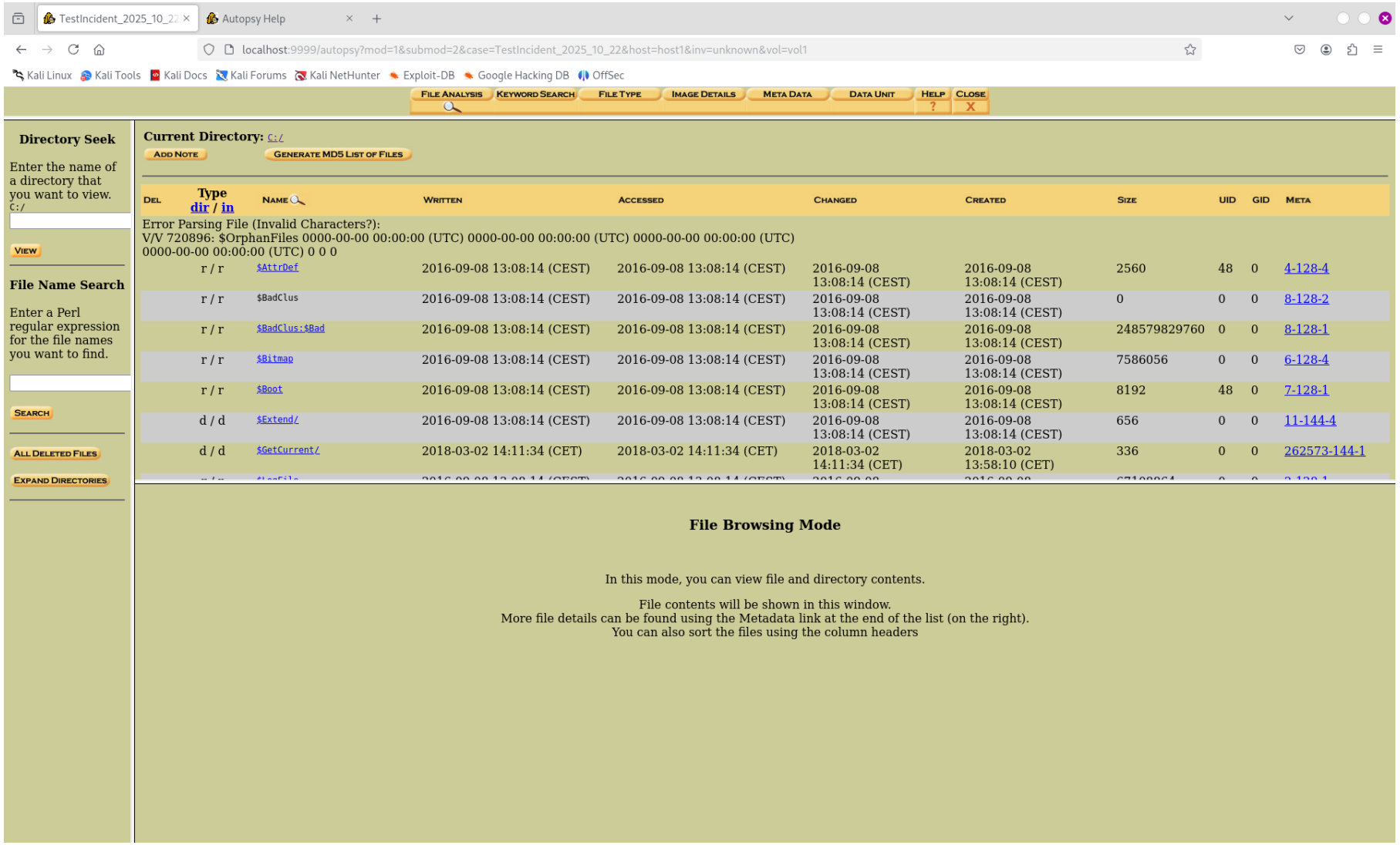
  sudo mount –o ro, loop </cesta/ku/suboru.img> /mnt/disk-image

  - „Pripoj diskový obraz suboru.img v režime iba na čítanie pomocou loop zariadenia do adresára /mnt/disk-image. “
    - t.j. súbor, ktorý má byť interpretovaný ako blokové zariadenie - tzn. správať sa ako disk

```
┌──(soc㉿soc-kali)-[~]
└─$ sudo mkdir /mnt/disk-image
[sudo] password for soc:

┌──(soc㉿soc-kali)-[~]
└─$ ls /mnt
disk-image

┌──(soc㉿soc-kali)-[~]
└─$ sudo mount -o ro,loop /media/soc/Elements/test_disk_imaging/sdb2_dc3dd_v2.img /mnt/disk-image

┌──(soc㉿soc-kali)-[~]
└─$ ls /mnt/disk-image
'$GetCurrent'   BOOTNXT          MSOCache          'Program Files (x86)'   Users
'$Recycle.Bin'  fog.log          pagefile.sys       Qt                     Windows
'$WINDOWS.~BT'  hiberfil.sys     PerfLogs           Recovery               Windows10Upgrade
 AMD            inetpub          ProgramData        swapfile.sys           Windows.old
 bootmgr        Intel           'Program Files'    'System Volume Information'

┌──(soc㉿soc-kali)-[~]
└─$ ls /mnt/disk-image/Users
 Administrator   Default          'Default User'   lendelv   sotek1   student.RB001-13
'All Users'      Default_00        desktop.ini     Public    spravca  zivicka1
 cervenik        DefaultAppPool    hatalova3       skolenie  student
```

```
┌──(soc㉿soc-kali)-[~]
└─$ lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0         7:0    0 231.5G  1 loop /mnt/disk-image
sda           8:0    0   5.5T  0 disk
└─sda1        8:1    0   5.5T  0 part /media/soc/Elements
nvme0n1     259:0    0 476.9G  0 disk
├─nvme0n1p1 259:1    0   260M  0 part
├─nvme0n1p2 259:2    0    16M  0 part
├─nvme0n1p3 259:3    0 279.4G  0 part
├─nvme0n1p4 259:4    0     2G  0 part
├─nvme0n1p5 259:5    0   977M  0 part /boot/efi
├─nvme0n1p6 259:6    0 184.3G  0 part /
└─nvme0n1p7 259:7    0  10.1G  0 part [SWAP]

┌──(soc㉿soc-kali)-[~]
└─$
```

Príprava analýzy disku – import kópie napr. do Autopsy



Čo je Autopsy

- Grafické rozhranie pre forenzný rámec nástrojov Sleuth Kit
  - open-source

Sleuth Kit = súbor príkazových nástrojov

Autopsy = používateľsky prívetivé prostredie

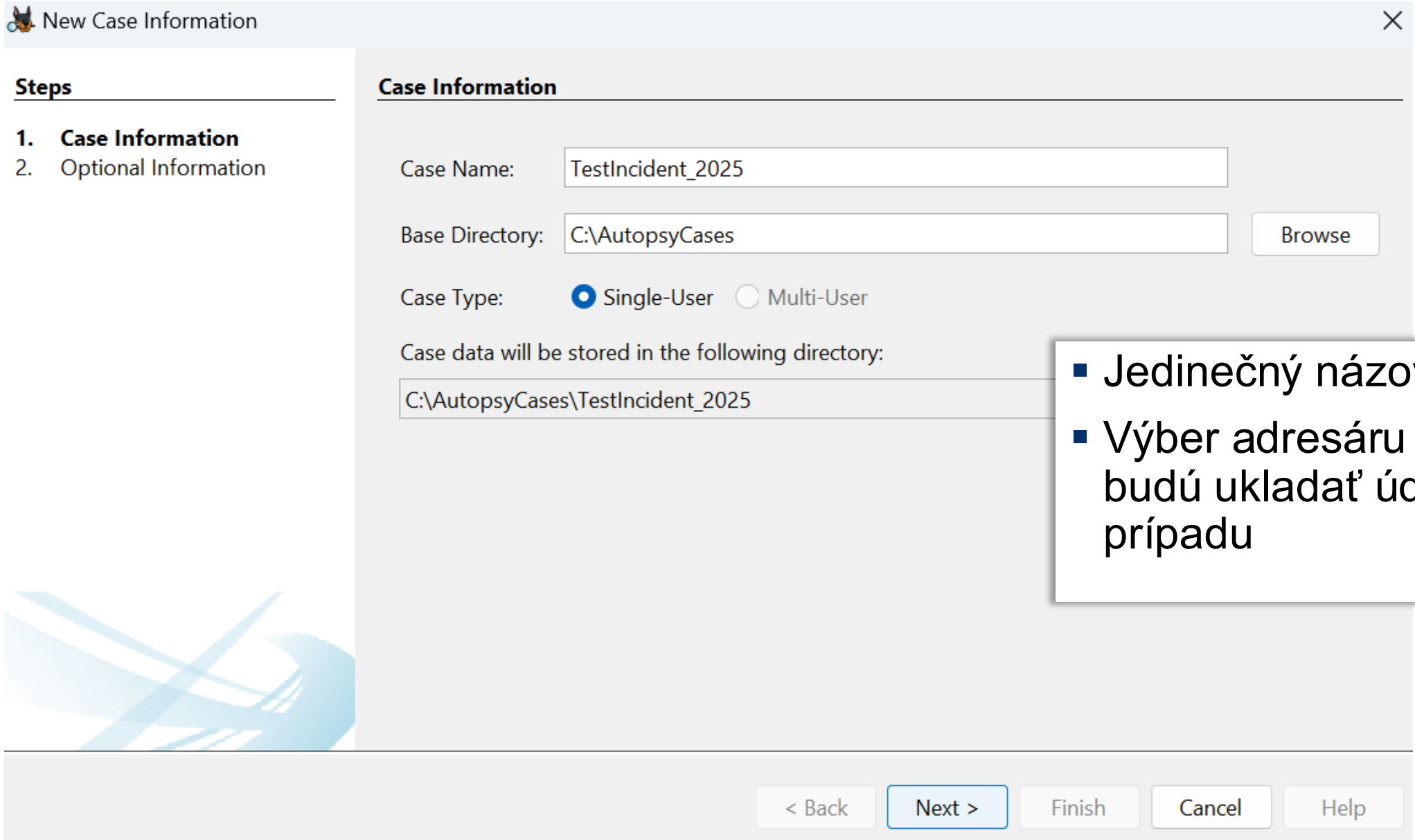
- Najnovšia verzia: **4.22.1** pre Windows (vydaná v apríly 2025)

Načo sa používa:

- Vyhľadávanie dôkazov
- Obnova zmazaných súborov
- Analýza súborového systému
- Korelácia udalostí
- Tvorba časovej osi
- Generovanie reportov

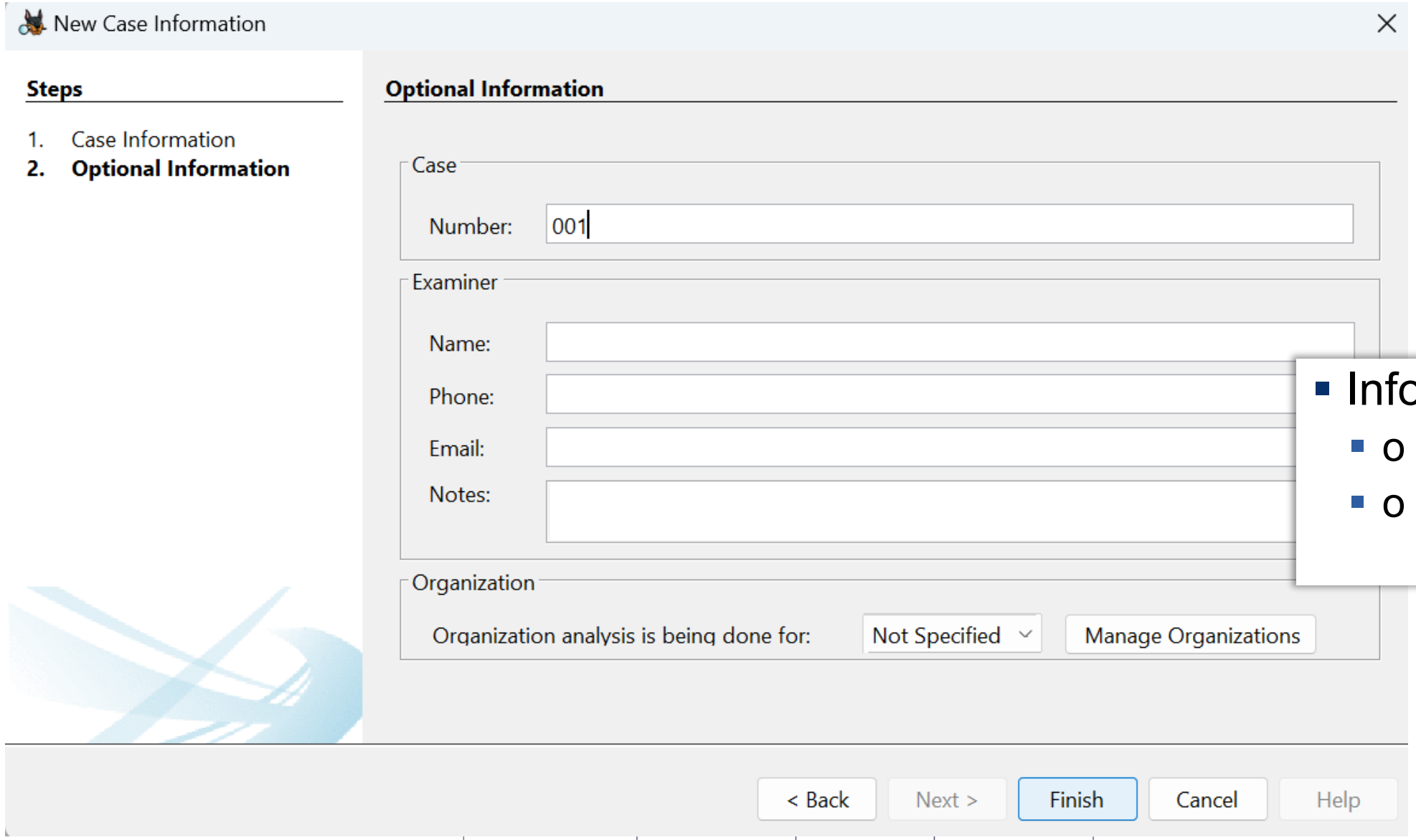
Príprava nástroja Autopsy

Vytvorenie nového prípadu



- Jedinečný názov prípadu
- Výber adresáru kde sa budú ukladať údaje k prípadu

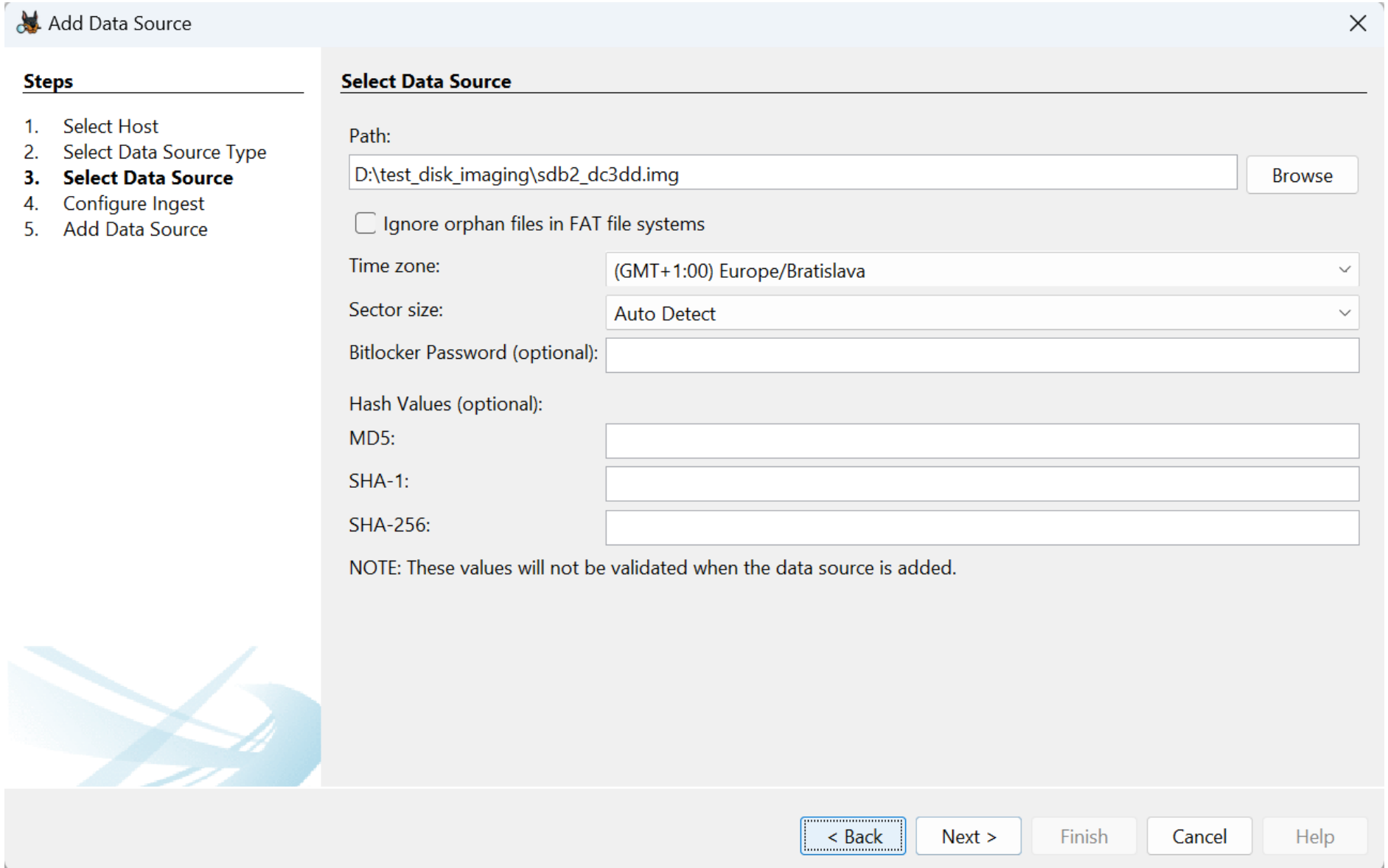
Vytvorenie nového prípadu – Doplňujúce informácie



- Informácie
  - o analytikovi
  - o organizácii

Príprava nástroja Autopsy

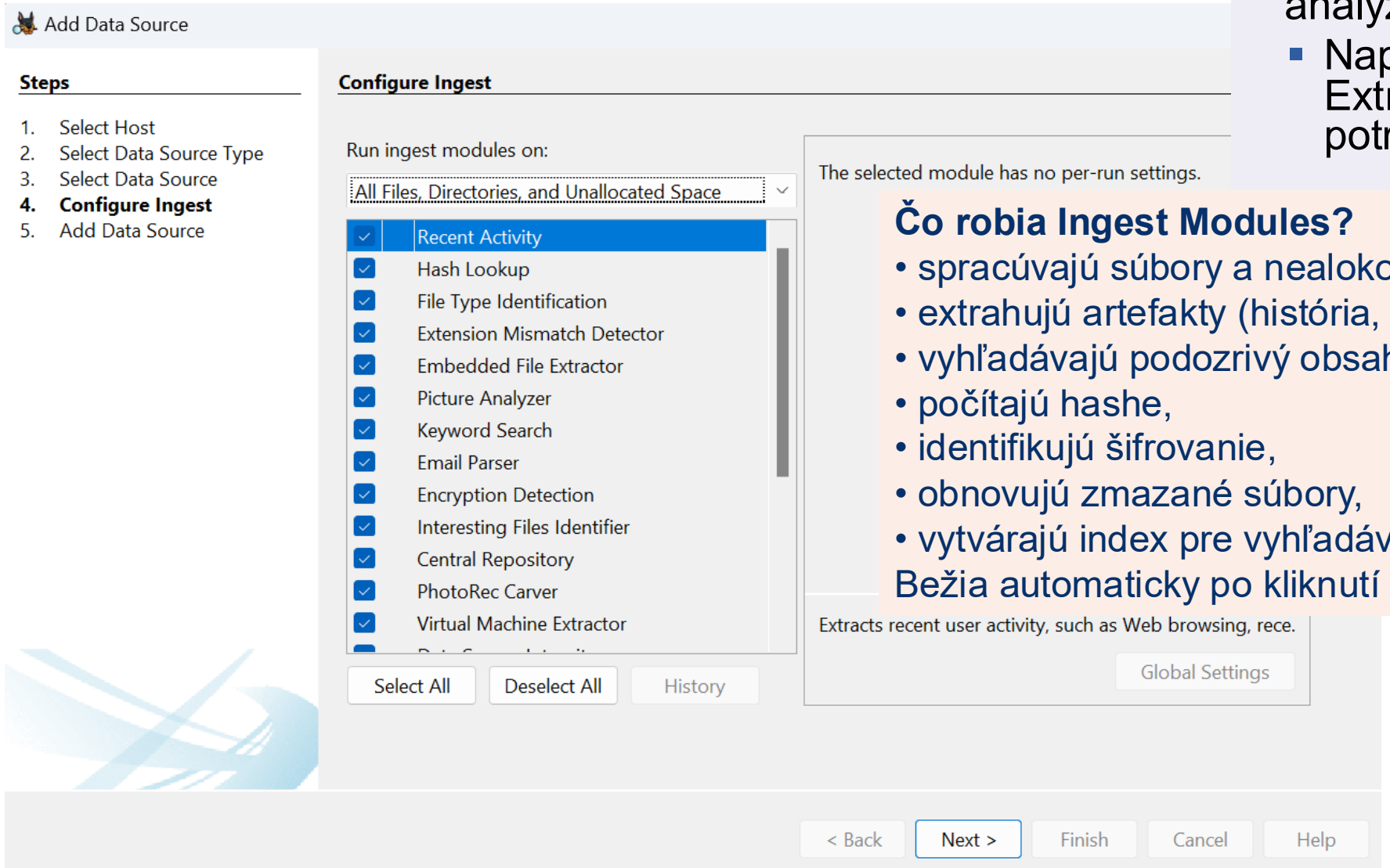
Pridanie dátového zdroja (kópie disku)



Príprava nástroja Autopsy

Výber analyzátorov (ingest modules)

- Pri výbere všetkých modulov celková analýza trvá dlhšie
- Nie všetky moduly musia byť zapnuté stačí si vybrať čo bude potrebné na základe cieľu analýzy
  - Napríklad (Virtual Machine Extractor nemusí byť vždy potrebný)

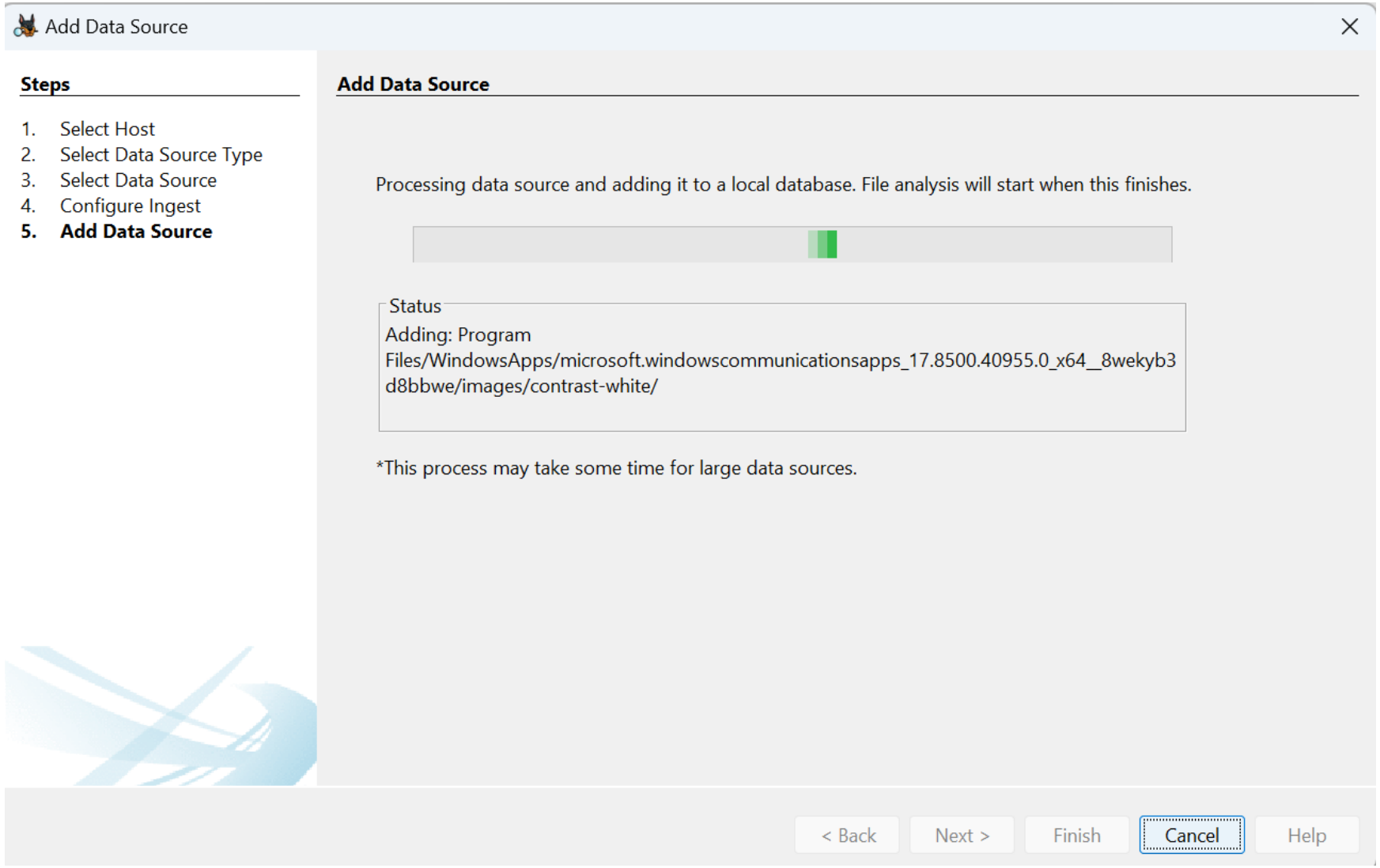


Čo robia Ingest Modules?

- spracúvajú súbory a nealokovaný priestor,
- extrahujú artefakty (história, e-maily, registry, logy…),
- vyhľadávajú podozrivý obsah,
- počítajú hashe,
- identifikujú šifrovanie,
- obnovujú zmazané súbory,
- vytvárajú index pre vyhľadávanie.

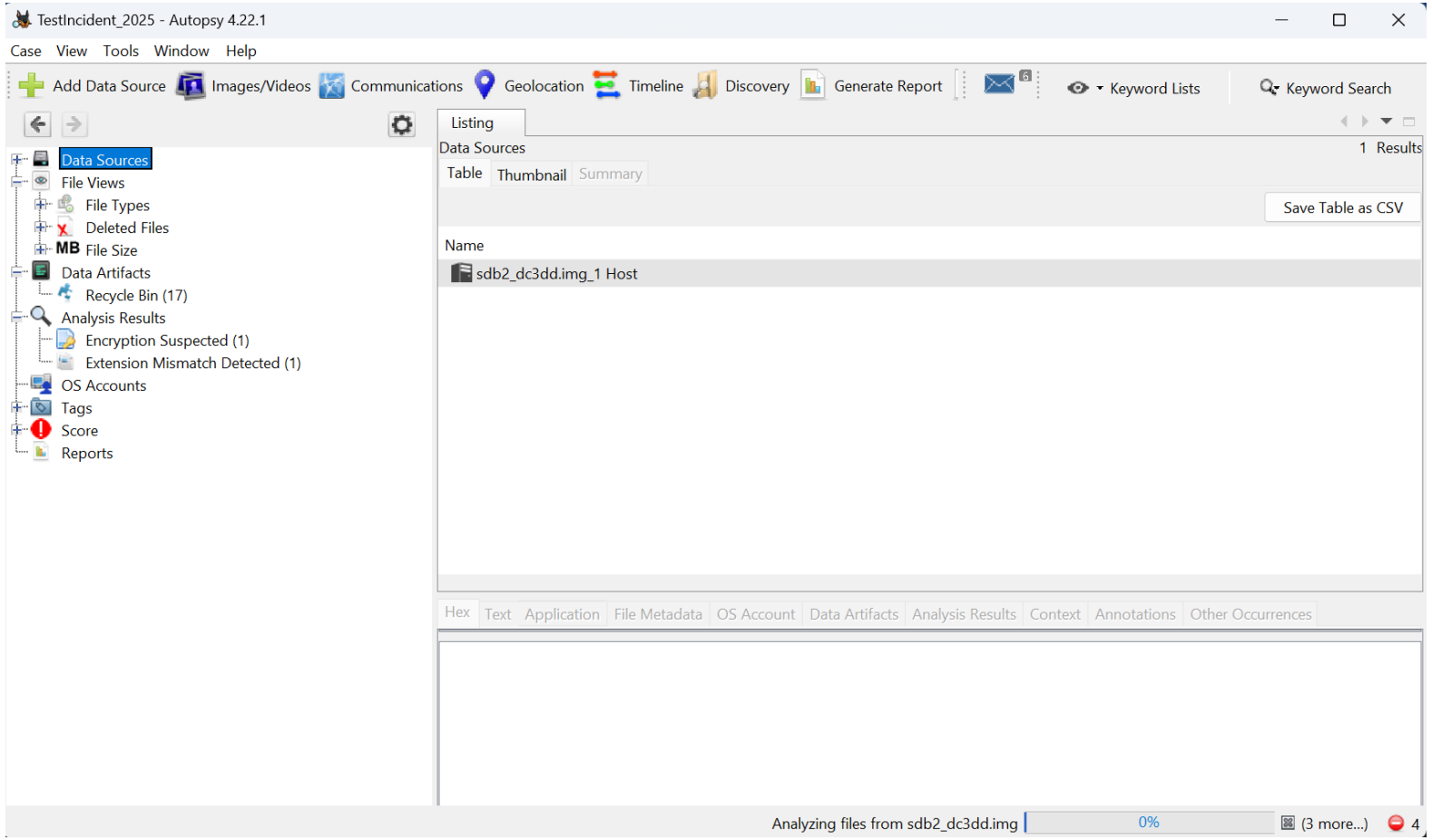
Bežia automaticky po kliknutí na **Next** pri pridávaní zdroja.

Spustenie nástroja Autopsy



- Po spracovaní zdroja údajov, spustíme analýzu cez tlačidlo „finish“

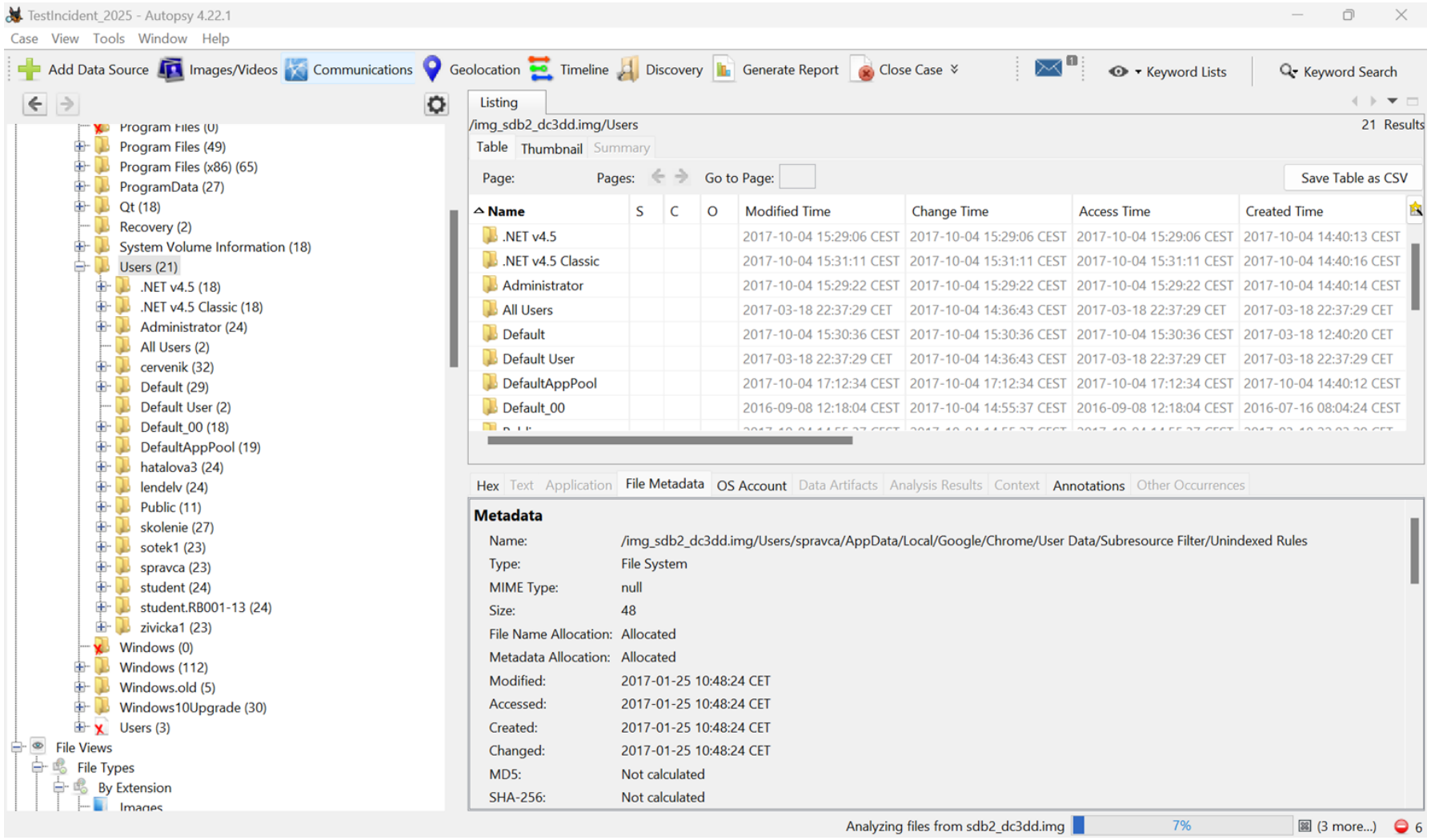
Spustenie nástroja Autopsy



Vpravo dole (0%) je vidieť spustenie analýzy všetkých vybraných modulov.

Môže to trvať dlhší časť

Príprava analýzy disku – import kópie napr. Autopsy



- Data sources po analýze
- Novšia verzia aj na Windows (aplikácia) 4.22.1

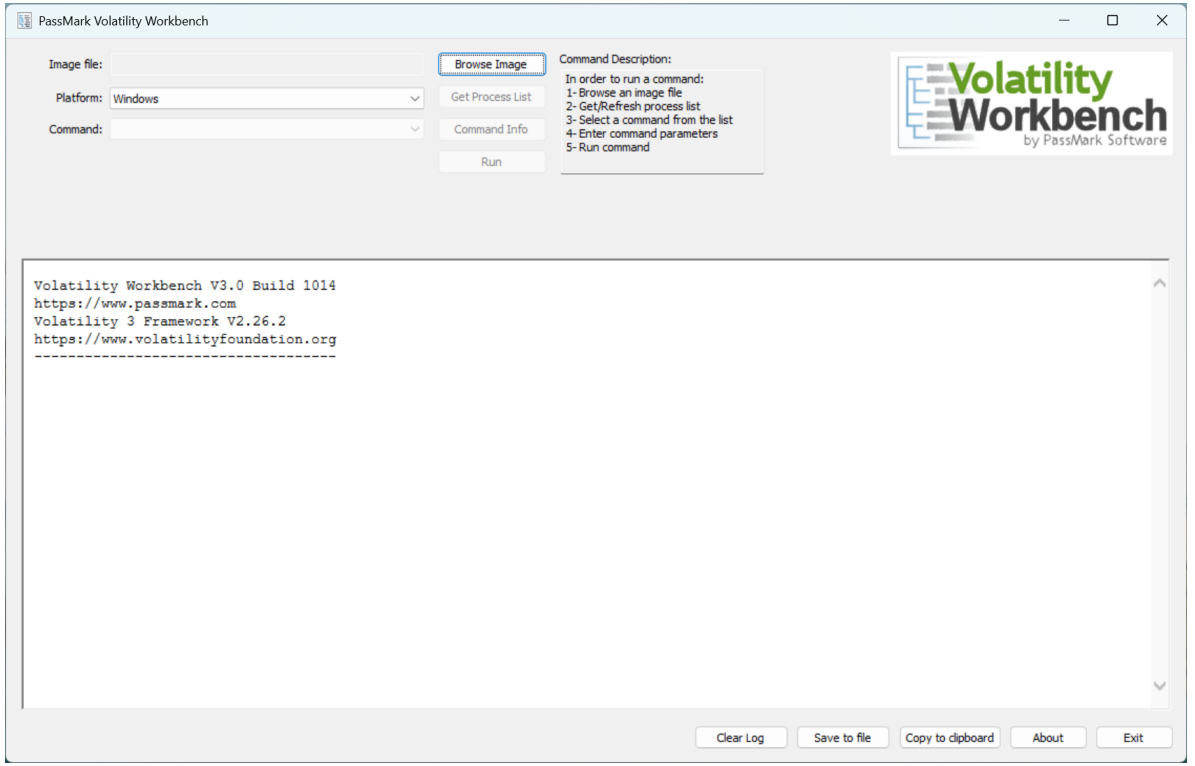
Akvizícia a analýza obrazu RAM

Proces akvizície obrazu RAM

- Ak je zariadenie stále zapnuté
  - Nesmie sa vypnúť
- Príprava prenosného pamäťového média
  - Obsahuje:
    - Nástroj na tvorbu bitovej kópie pamäte RAM (winpmem, DumpIt ...)
      - Spúšťa sa z externého média (nie je potrebná inštalácia)
    - Spúšťací skript
      - Automatický proces tvorby bitovej kópie RAM
    - Voľné miesto na uloženie bitovej kópie obrazu RAM
- Dokumentácia
- Analýza digitálneho dôkazu

Postup akvizície obrazu RAM

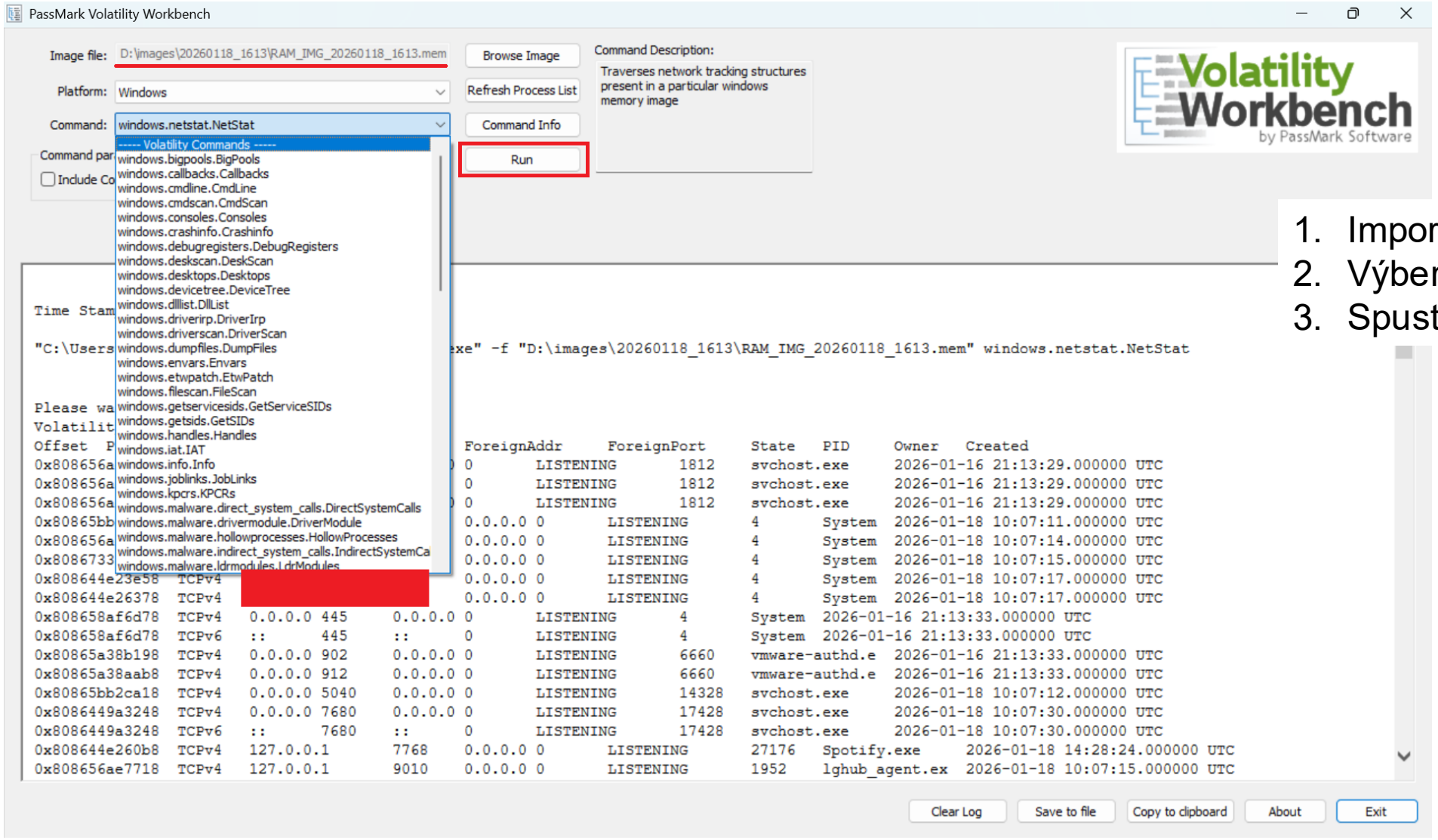
- 1. Vloženie externého pamäťového úložiska (USB)
- 2. Zaznamenanie aktuálnej sieťovej komunikácie
- 3. Spustenie tvorby bitovej kópie
- 4. Vypočítať hash bitovej kópie
- 5. Dokumentácia – Chain of Custody



- Analýza bitovej kópie RAM
  - Volatility 3.0 – (Volatility Workbench - GUI)

Analýza bitovej kópie RAM

Volatility Workbench



1. Import bitovej kópie RAM
2. Výber príkazu
3. Spustenie

Nástroj pre DFIR, live forenznú analýzu a hunting

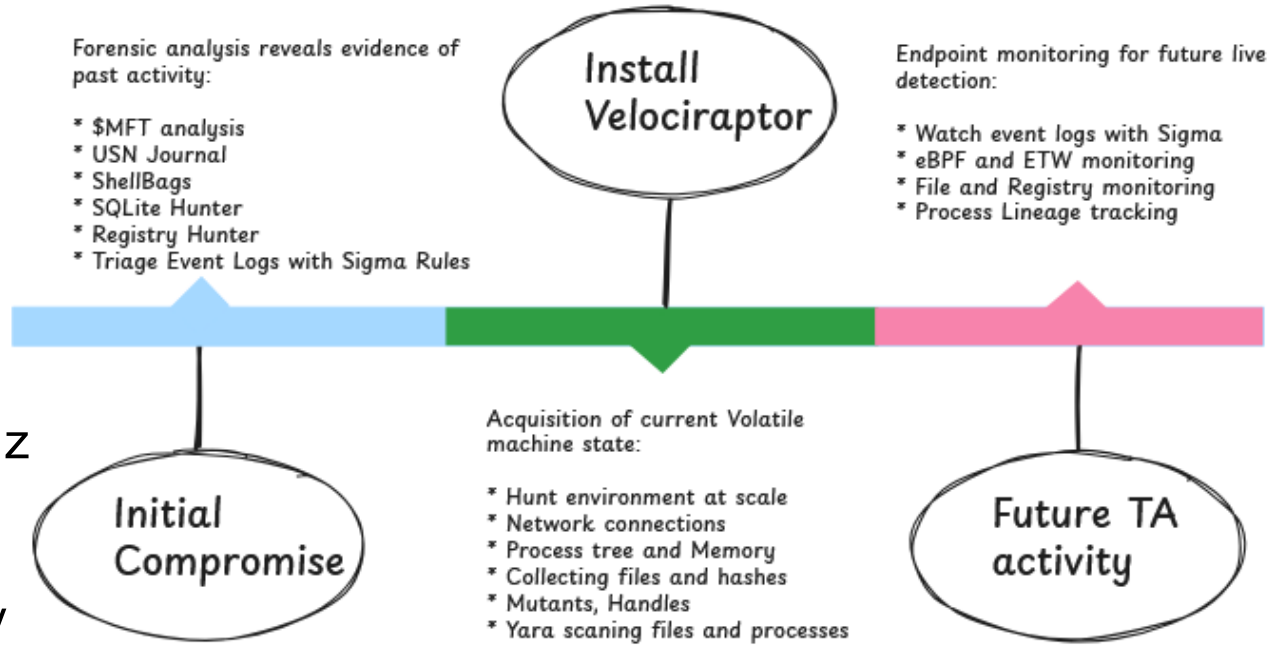
Ako získať „volatile“ dáta?

... informácie uložené len počas behu systému, ako RAM, bežiace procesy, otvorené handles, obsah registra, aktuálne sieťové spojenia, ...

Velociraptor

Účel a funkcie nástroja

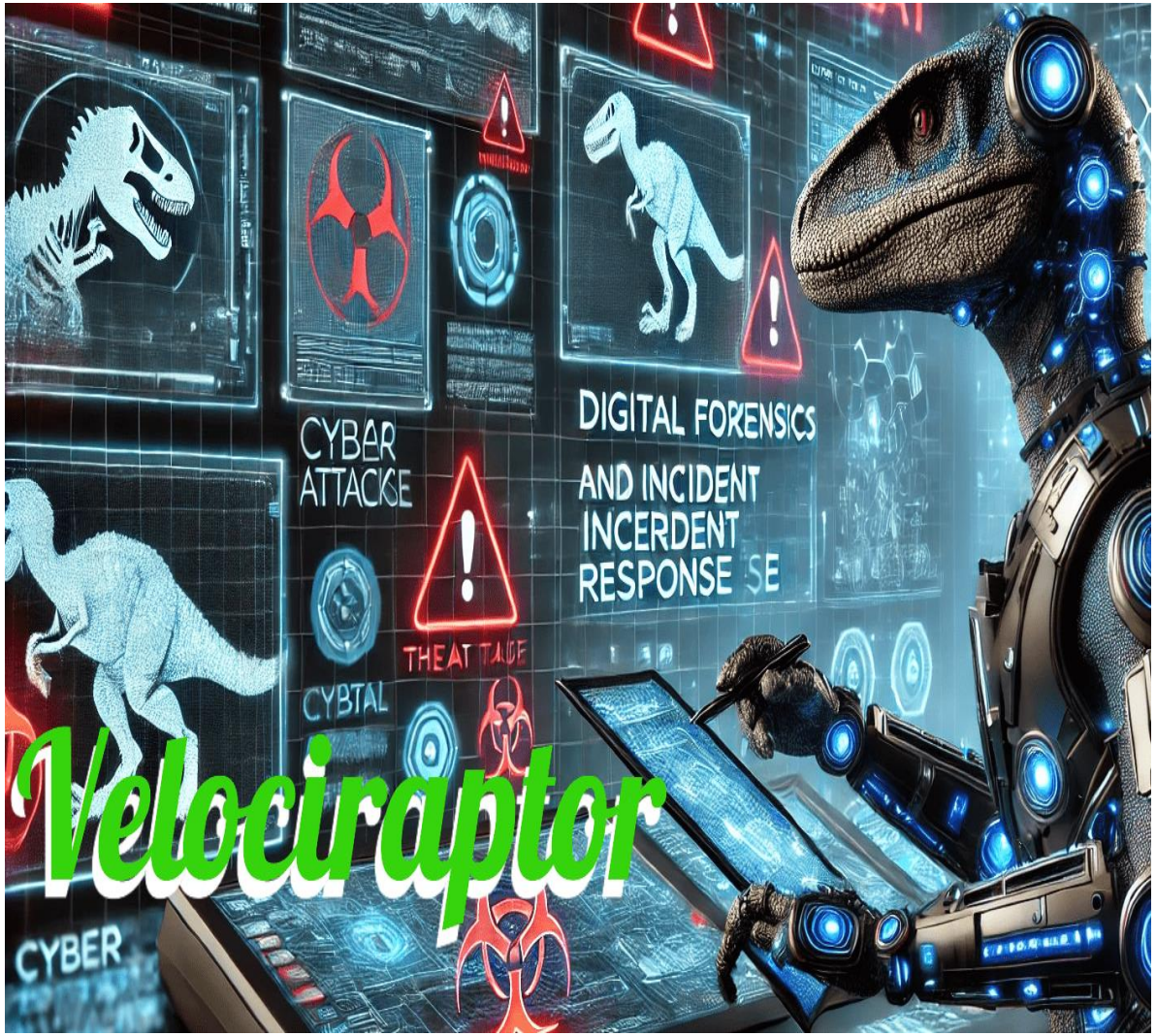
- Pokročilá open-source platforma na:
  - Monitorovanie zariadení
  - Digitálnu forenznú analýzu
  - Reakciu na incidenty
- Pokrýva celý životný cyklus útoku
- Hlavné funkcie:
  - Zber dôkazov
    - Umožňuje rýchly, cielený zber dôkazov z viacerých zariadení naraz
  - Kontinuálny zber udalostí
    - Neustále sleduje udalosti – logy, zmeny súborov, spúšťanie procesov
  - Centrálne a dlhodobé ukladanie dát
    - vhodné pre spätnú analýzu
  - Aktívne vyhľadávanie podozrivých aktivít
  - Obsahuje knižnicu forenzných artefaktov
    - dajú sa upraviť podľa potrieb



Velociraptor

Hunting

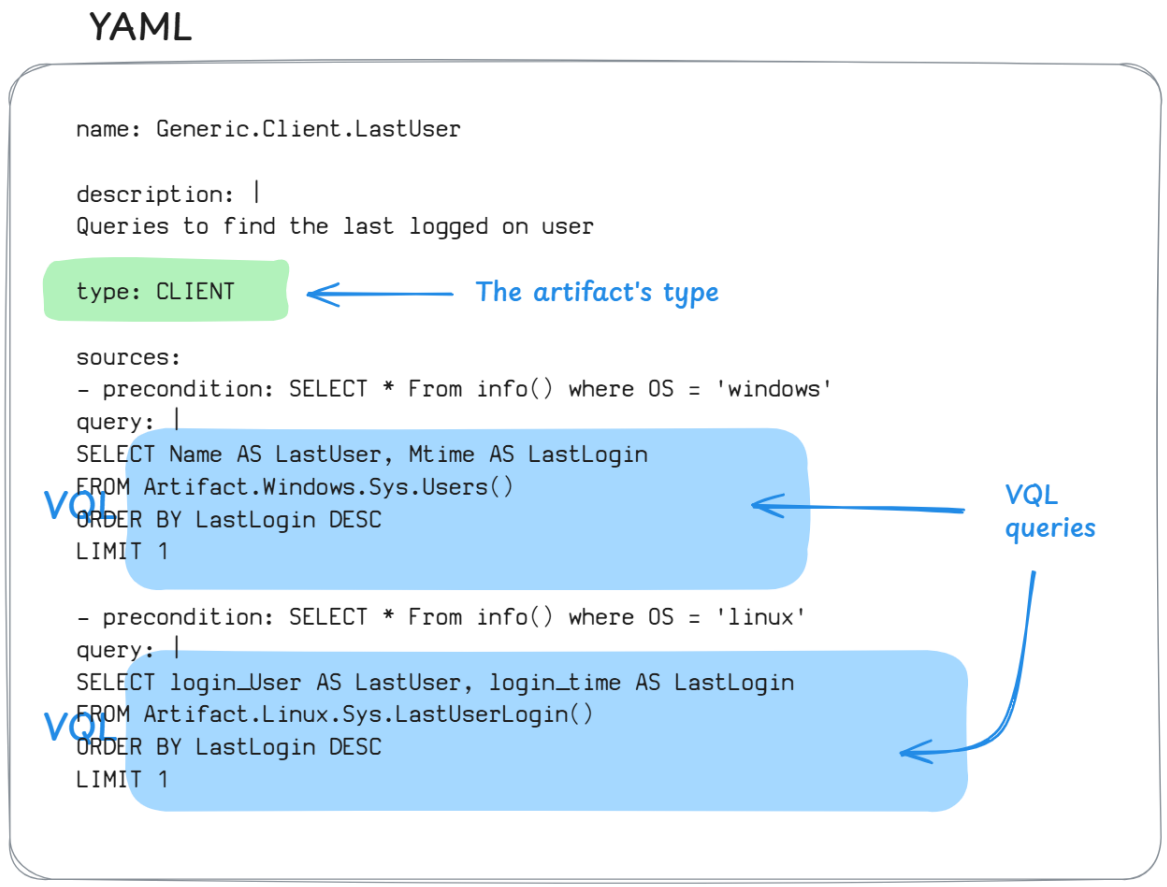
- je škálovateľný, centralizovaný zber artefaktov v celej infraštruktúre
  - z jedného alebo viacerých zariadení naraz
  - s možnosťou automatizácie
- Ak chceme napr. získať systémové logy, RAM dump, spustené procesy, sieťové pripojenia, alebo súbory z viacerých strojov po incidente
  - T.j. vrátane volatile data!
- Výsledky sa dajú porovnávať naprieč klientmi
- Umožňuje monitorovať aj offline zariadenia
  - Hunt počká, zber sa vykoná, keď sa znova pripoja
- Hunt Manager riadi plánovanie, zber a sledovanie priebehu
  - zabraňuje duplicitám – teda nezbiera ten istý artefakt dvakrát z rovnakého zariadenia



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Velociraptor Artifacts (nie forenzné artefakty)

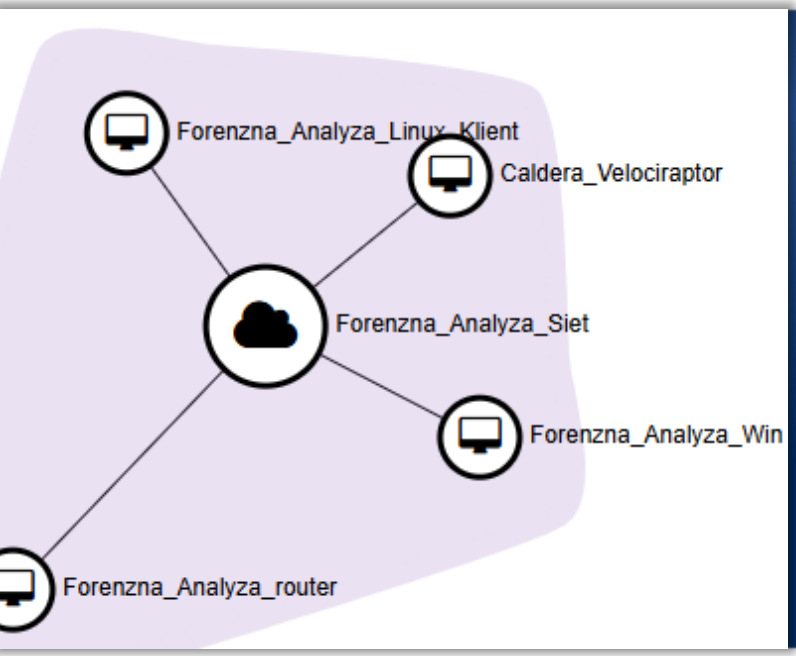
- Artefakty sú predpripravené skripty alebo **VQL (Velociraptor Query Language)** moduly, ktoré vykonávajú konkrétne úlohy
  - od jednoduchého zisťovania informácií o systéme
  - až po komplexnú detekciu a forenznú analýzu
- Môžu byť spustené na klientovi alebo na serveri
- Slúžia na rôzne účely: detekcia škodlivého správania, prehľad o systéme, zbieranie súborov, analýza pamäte, správa používateľov a udalostí,...
- hlavnou výhodou je **automatizácia a štandardizácia** zberu dát
  - čím znižujú potrebu manuálnych zásahov
  - a urýchľujú analýzu bezpečnostných incidentov
- 400+ built-in artifacts



Prehľad artefaktov

- **Zber súborov a VFS**
  - umožňuje rýchle vyhľadanie súborov a spravovanie virtuálneho súborového systému
  - Príklady: Windows.Search., *Windows.VFS*
- **Detekcia a monitorovanie**
  - sa zameriava na zistenie podozrivých aktivít, ako sú nové procesy, registrácie služieb, zmeny v registri alebo udalosti Windows Event Log
  - Príklady: Windows.Detection., *Windows.Events.*, Windows.ETW.*
- **Forenzná analýza**
  - umožňuje hlbšie skúmanie systému, pamäte, súborov, UEFI alebo časovej osi
  - Príklady: Windows.Forensics., *Windows.Memory.*, Windows.NTFS.*
- **Remediácia**
  - slúži na automatické zastavenie alebo obmedzenie škodlivého správania
  - Príklady: Windows.Remediation.*
- **Systémové informácie**
  - poskytujú prehľad o procesoch, službách, používateľoch, pripojeniach a certifikátoch
  - Príklady: Windows.System., *Windows.Sys.*, Windows.Sysinternals.*
- **Registre a konfigurácia**
  - umožňujú sledovať kľúče a hodnoty, ktoré môžu indikovať malvér alebo perzistenciu
  - Príklady: Windows.Registry.*
- **Networking a monitorovanie**
  - monitorujú otvorené porty, ARP cache, PCAPy alebo DNS dotazy
  - Príklady: Windows.Network., *Windows.ETW.DNS*, Windows.EventLogs.*
- **Timeline a audit**
  - pomáhajú rekonštruovať históriu udalostí, ako sú spustené procesy, prihlásenie alebo prehliadanie súborov
  - Príklady: Windows.Timeline., *Windows.EventLogs.*, Windows.Events.*

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Ukážka tvorby hunt-u vo Velociraptor

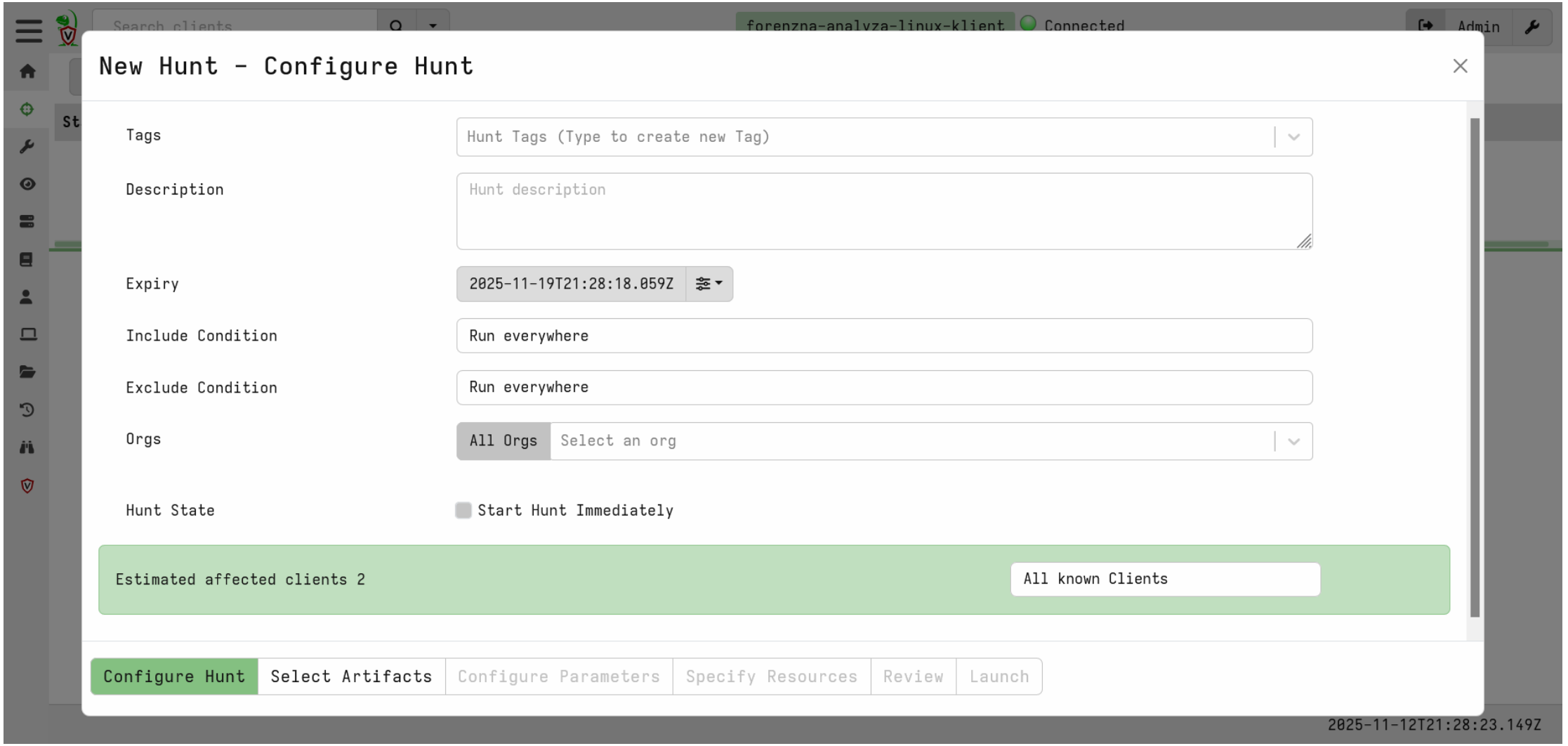
Testovacia topológia v CC OpenStack na KIS FRI UNIZA

Velociraptor

Sekcia Hunts

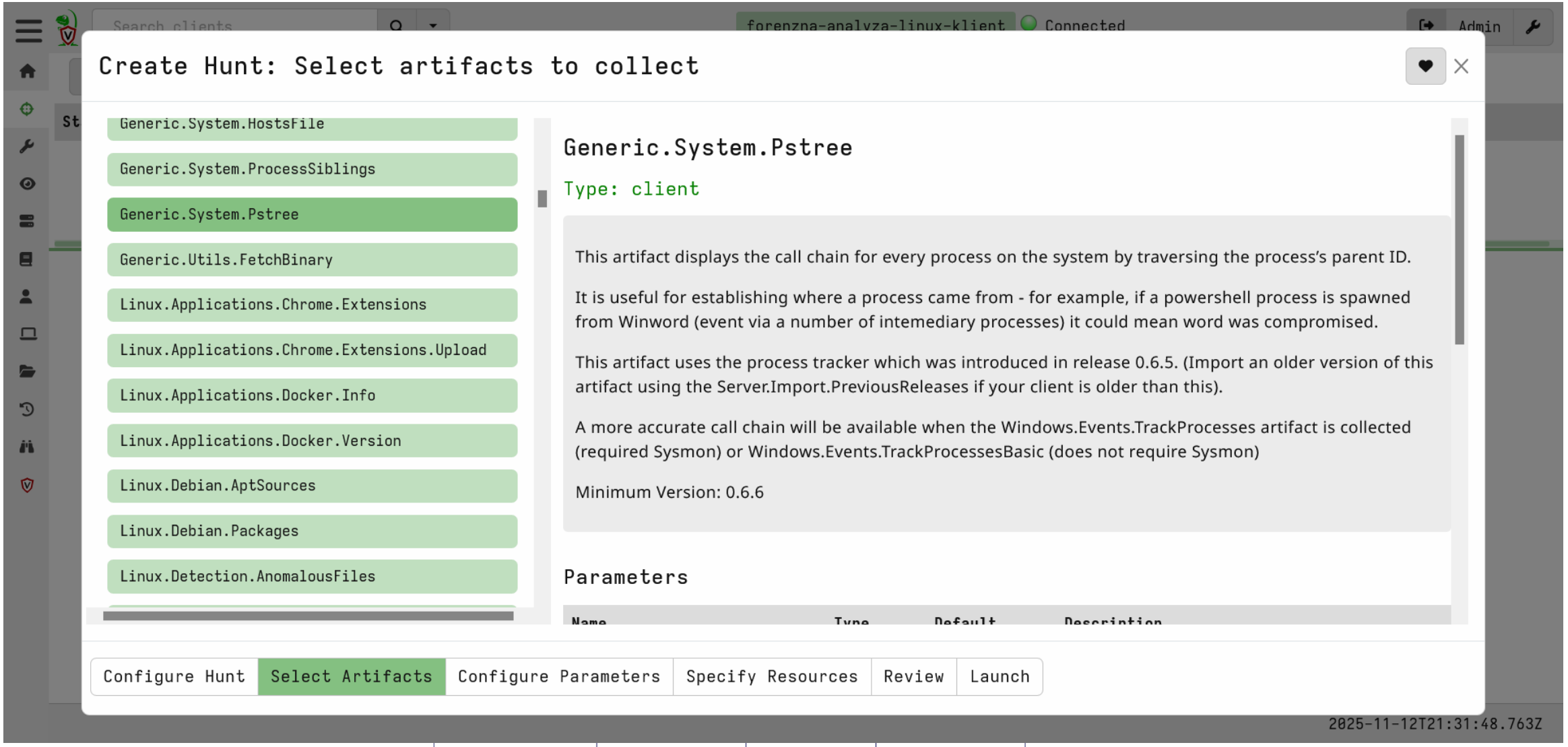
Velociraptor

Vytvorenie nového hunt-u



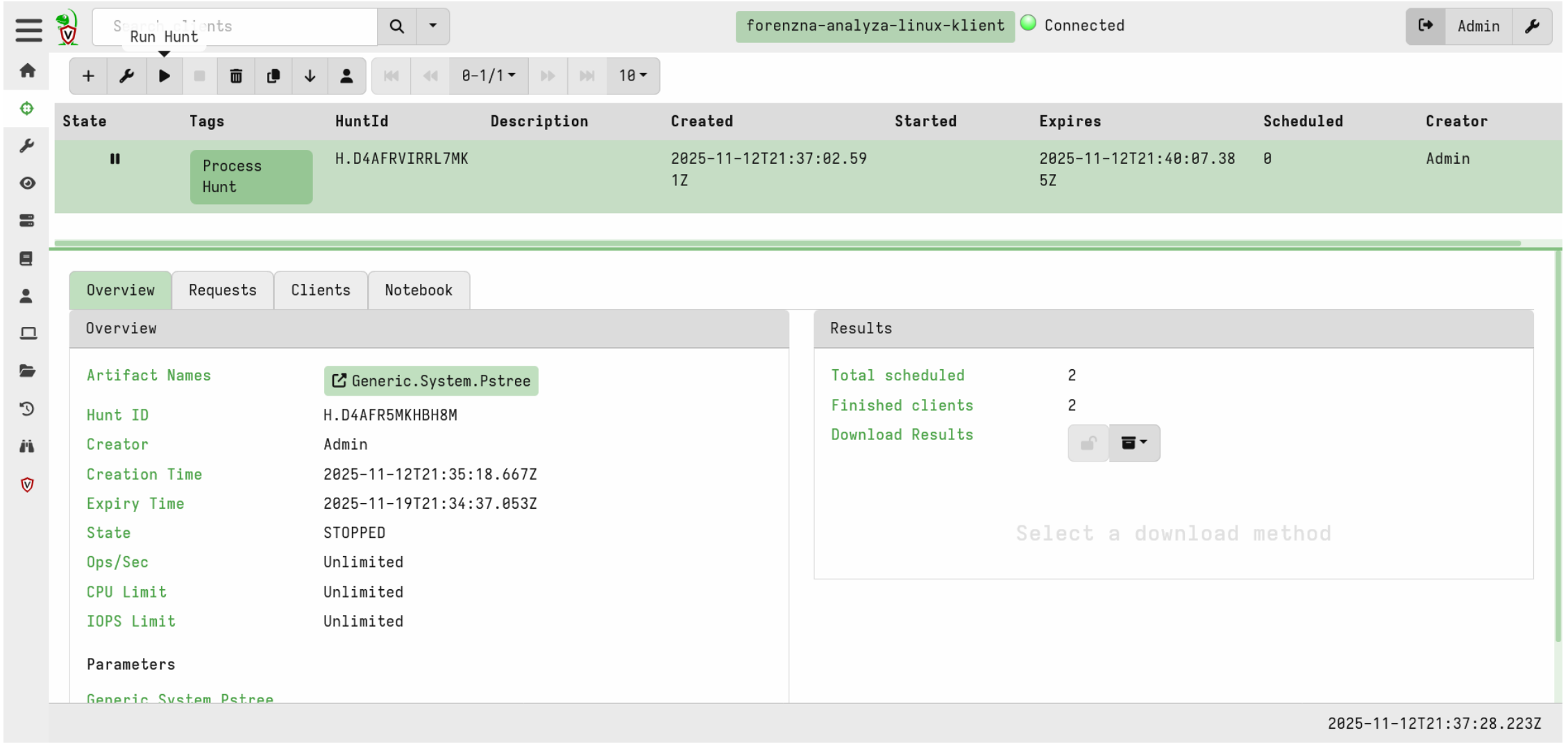
Velociraptor

Výber artefaktov



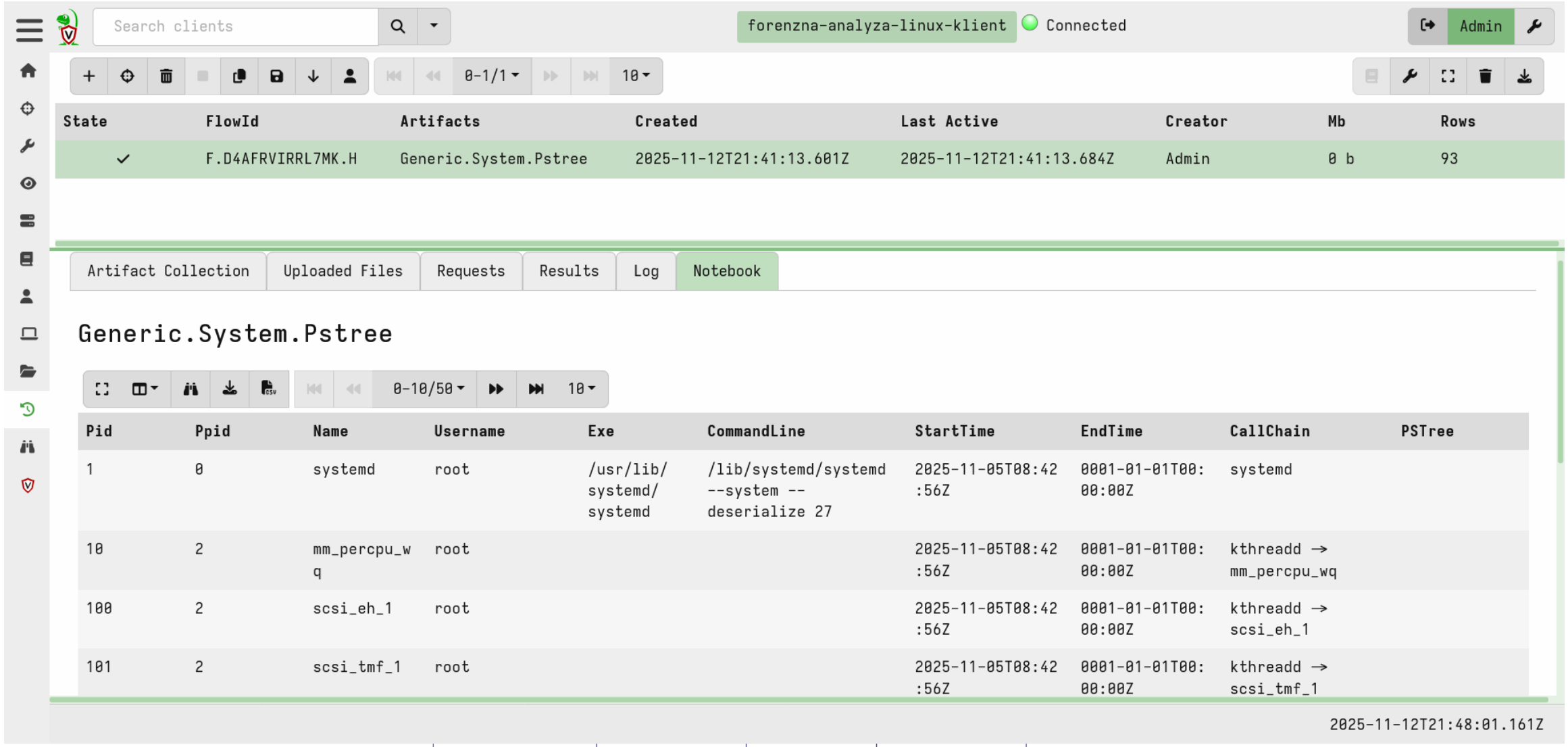
Velociraptor

Spustenie hunt-u



Velociraptor

Zobrazenie artefaktov



Identifikácia a analýza malvéru

Reverzné inžinierstvo na pochopenie fungovania malvéru, sandboxing

Krátka pripomienka pojmu

- angl. malware, skratka zo slov malicious software
- **škodlivý softvér** alebo **kód**
- Cieľ:
  - poškodiť zariadenie
  - zneužiť údaje
  - získať neoprávnený prístup
  - narušiť bežnú činnosť systému.

- Vírus
- Červ (Worm)
- Trójsky kôň
- Ransomvér
- Spyvér
- Advér
- Rootkit
- Keylogger

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Identifikácia malvéru

Hľadať:

- Spustiteľné alebo binárne súbory (napr.: .exe, .dll, .sys, .bin)
- Skripty a makrá (.ps1, .vbs, .js, .docm, .xlsm)
- Súbory, kde typ nesedí s príponou

- EDR /SIEM logy

- Vypočítať hash SHA-256
- Porovnať hash s databázou (napr.: VirusTotal, MalwareBazar)
- Statická analýza
  - Nevyžaduje spustenie
- Dynamická analýza
  - Vyžaduje spustenie → sandboxing

Reverzné inžinierstvo malvéru

- Je proces, pri ktorom sa snažíme pochopiť čo daný malvér robí a prečo:
  - spôsob infekcie
  - metódy šifrovania konfigurácie
  - komunikačné kanály (C2)
  - moduly, ktoré sťahuje
  - aké dáta exfiltruje

- Statická analýza → skúmanie súboru bez jeho spustenia
- Dynamická analýza → spustenie vzorky v izolovanom prostredí

Statická analýza

- Skúmanie súboru bez jeho spustenia
  - Nie je potrebné izolované prostredie

Zameriava sa na:

- Metadáta súboru
  - Timestamp
  - Veľkosť
  - Formát
- Vnútorné artefakty
  - String
  - Importované API
  - Štruktúry
  - Čo malvér používa
    - Sieťové volania
    - Kryptografiu
    - Manipulácia procesov

- Ghidra
  - Analýza kódu, dekompilácia a pochopenie funkčnosti
- YARA
  - Pravidlá na identifikáciu malvéru

Dynamická analýza - Sandbox

- Sandbox je izolované prostredie na bezpečné spustenie a sledovanie podozrivých súborov
- Sleduje aké:
  - Súbory vytvára
  - Procesy spúšťa
  - Záznamy v registri mení
  - Sieťovú komunikáciu nadväzuje
- Všetky aktivity sa zaznamenávajú a vyhodnocujú

- Cuckooo sandbox
  - Open-source nástroj
    - technicky stále existuje a je používaný — má aktívnu komunitu modulov.
    - nie veľmi živý v pôvodnej verzii (2.x) — hlavné repo je archív, aktívny vývoj je obmedzený, a nové vydanie (2.0) je momentálne RC (release candidate).

Online:

- Any.Run
- Joe Sandbox
- Hybrid analysis

- Windows sandbox
  - Zabudovaný v novších verziách
    - Windows 10 (od verzie 1903 ďalej) – ale iba v edíciách Pro, Enterprise a Education.
    - Windows 11 – tiež v edíciách Pro, Enterprise a Education, nie je podporovaný v Home verzii.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Open-source alternatívy nástrojov pre analýzu malvéru

- CAPEv2
  - je to sandbox odvodený od Cuckoo, špecializovaný na dynamickú analýzu malvéru (unpacking) a extrakciu konfiguračných údajov a payloadov.
    - Config And Payload Extraction
  - Poskytuje: behaviorálna analýza API - monitorovanie správania cez odchytávanie API volaní (API hooking), zachytávanie sieťovej komunikácie, screenshoty, memory dump, atď.
  - Modularita a REST API robia CAPEv2 vhodným aj pre väčšie analýzy.
  - GitHubExistuje aj Docker verzia pre jednoduchšiu nasaditeľnosť.
- DRAKVUF Sandbox
  - Agentless sandbox na úrovni hypervízora (Virtual Machine Introspection, VMI).
  - Analyzuje správanie malvéru bez inštalácie agenta vo virtuálnom systéme – to znižuje možnosť, že malvér zistí, že je sandboxovaný.
  - Podporuje Windows aj Linux.
  - Webové rozhranie pre upload súborov a zobrazenie výsledkov analýzy.

https://blog.gjorge.com/drakvuf-vs-capev2/

- SaMOSA
  - Novší sandbox navrhnutý pre side-channel analýzu malvéru, najmä pre OT/CPS (operačné technológie, embedded systémy).
  - Snímka viacerých side-kanálov (systémové volania, sieť, disk, hardvérové performance counters) pre lepšiu analýzu správania.
  - Podporuje viac architektúr:
    - x86-64, ARM64, PowerPC.

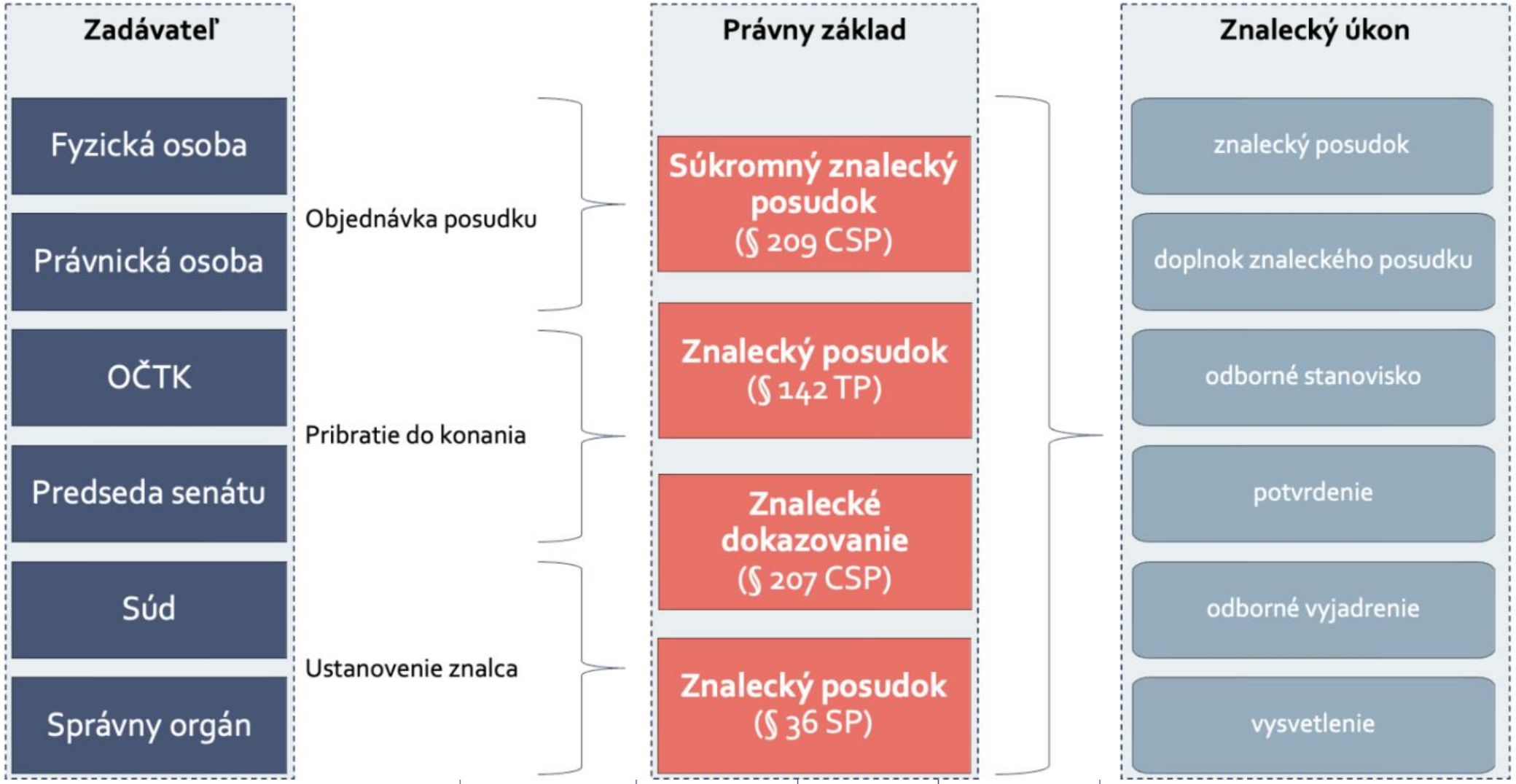
https://arxiv.org/html/2508.14261v1

Právne a etické aspekty

Právne a etické aspekty

- Výsledky digitálnej forenznej analýzy často vstupujú do:
  - Právnych procesov
  - Interných disciplinárnych procesov
  - Korporačných rozhodnutí
- Protiprávne alebo neeticky získané dôkazy môžu:
  - Byť neprípustné vo vyšetrovaní
  - Prezentovanie výsledkov môže viesť k strate reputácie organizácie
    - Vyvodené právne následky
- Zákon č. 382/2004 Z.z. o znalcoch, tlmočníkoch a prekladateľoch:
  - Znalecká činnosť:
    - špecializovaná odborná činnosť vykonávaná za podmienok ustanovených v zákone znalcami pre zadávateľa
    - úlohou znalca je **zodpovedať položené otázky** v písomnom znaleckom posudku
    - znalec **nie je oprávnený vyjadrovať sa** k **právnemu** posúdeniu veci
    - v každom znaleckom úkone musí byť **odôvodnený postup** a musí byť zabezpečená jeho preskúmateľnosť
    - civilný sporový poriadok spresňuje inštitút tzv. „**súkromného znaleckého posudku**“ (§209 CSP), ktorý definuje ako znalecký posudok predložený stranou bez toho, aby znalecké dokazovanie nariadil súd. Pri vykonávaní tohto dôkazu sa bude postupovať rovnako akoby išlo o znalecký posudok súdom ustanoveného znalca.
  - Znalec:
    - fyzická osoba alebo právnická osoba splnomocnená štátom na vykonávanie činnosti podľa tohto zákona, ktorá je zapísaná **v zozname znalcov**, tlmočníkov a prekladateľov

Znalecké úkony



Znalecké odvetvia relevantné z hľadiska DFA

10 00 00 Elektrotechnika

- 10 01 00 Elektro-energetické stroje a zariadenia
- 10 02 00 Elektronika
- 10 03 00 Elektrotechnické materiály
- 10 04 00 Riadiaca technika, výpočtová technika (hardvér)
- 10 05 00 Robotické a mechatronické systémy
- 10 06 00 Elektronické komunikácie
- 10 07 00 Odhad hodnoty elektrotechnických zariadení
- 10 08 00 Nosiče zvukových a zvukovoobrazových záznamov
- 10 09 00 Počítačové programy (softvér)
- 10 10 00 Bezpečnosť a ochrana informačných systémov
- 10 11 00 Kybernetická bezpečnosť

27 00 00 Písmoznalectvo

- 27 01 00 Ručné písmo
- 27 02 00 Strojové písmo
- 27 03 00 Jazyková analýza

49 00 00 Kriminalistika

- 49 06 00 Kriminalistické skúmanie ručného písma a podpisov
- 49 08 00 Kriminalistické skúmanie dokumentov
- 49 20 00 Kriminalistická informatika
- 49 21 00 Kriminalistická fotografia a video

- Kybernetická bezpečnosť **je nové znalecké odvetvie vymedzené** vo Vyhláške Ministerstva spravodlivosti SR č. 228/2018 Z.z, (od 07/2023)
- KB je **komplexná disciplína**, ktorá si zvyčajne vyžaduje uplatnenie niekoľkých rôznych znaleckých odvetví

https://www.justice.gov.sk/registre/znalci

Právne predpisy

- Zákon č. 300/2005 Z. z. – Trestný zákon
  - § 247 – Neoprávnený prístup k počítačovému systému
  - § 247a – Neoprávnený zásah do systému
  - § 247b – Neoprávnené zachytávanie údajov
  - § 247c – Výroba a používanie nástrojov na počítačovú kriminalitu

- Zákon č. 301/2005 Z. z. – Trestný poriadok
  - upravuje postup orgánov činných v trestnom konaní a súdov pri dokazovaní, zbieraní dôkazov vrátane údajov z počítačových systémov.

- Zákon č. 69/2018 Z. z. – o kybernetickej bezpečnosti
  - stanovuje povinnosti v oblasti kybernetickej bezpečnosti, riadenia a zabezpečenia informačných a komunikačných technológií, správcov základných služieb a poskytovateľov digitálnych služieb.

- Zákon č. 18/2018 Z. z. – o ochrane osobných údajov
  - zásadne dôležitý pri spracovaní osobných údajov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Normy a štandardy

- NIST SP 800-86 - Sprievodca integráciou **forenzných techník** pre reakciu na incidenty (Guide to Integrating Forensic Techniques into Incident Response).
- RFC 3227 - Pokyny pre **zber** a **archiváciu** dôkazov pri počítačovej bezpečnosti.
- RFC 3161 - Štandard pre **časové pečiatky** (Time-Stamp Protocol), ktorý zabezpečuje dôkaz o existencii dát v určitom čase.
- ISO/IEC 27037 - Smernica pre identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov.
- ISO/IEC 27041 - Smernica zameraná na zabezpečenie **vhodnosti** a **primeranosti** metód forenzného vyšetrovania incidentov.
- ISO/IEC 27042 - Smernica pre **analýzu** a **interpretáciu** digitálnych dôkazov.
- ISO/IEC 27043 - Princípy a procesy forenzného **vyšetrovania** incidentov.
- ISO/IEC 27050 - Štandard pre **elektronické objavovanie** (eDiscovery), zahŕňa identifikáciu, uchovávanie, zber, spracovanie, preskúmanie a prezentáciu elektronicky uložených informácií.

Uplatňovanie noriem si vyžaduje súlad s národnou legislatívou, pravidlami a reguláciou.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

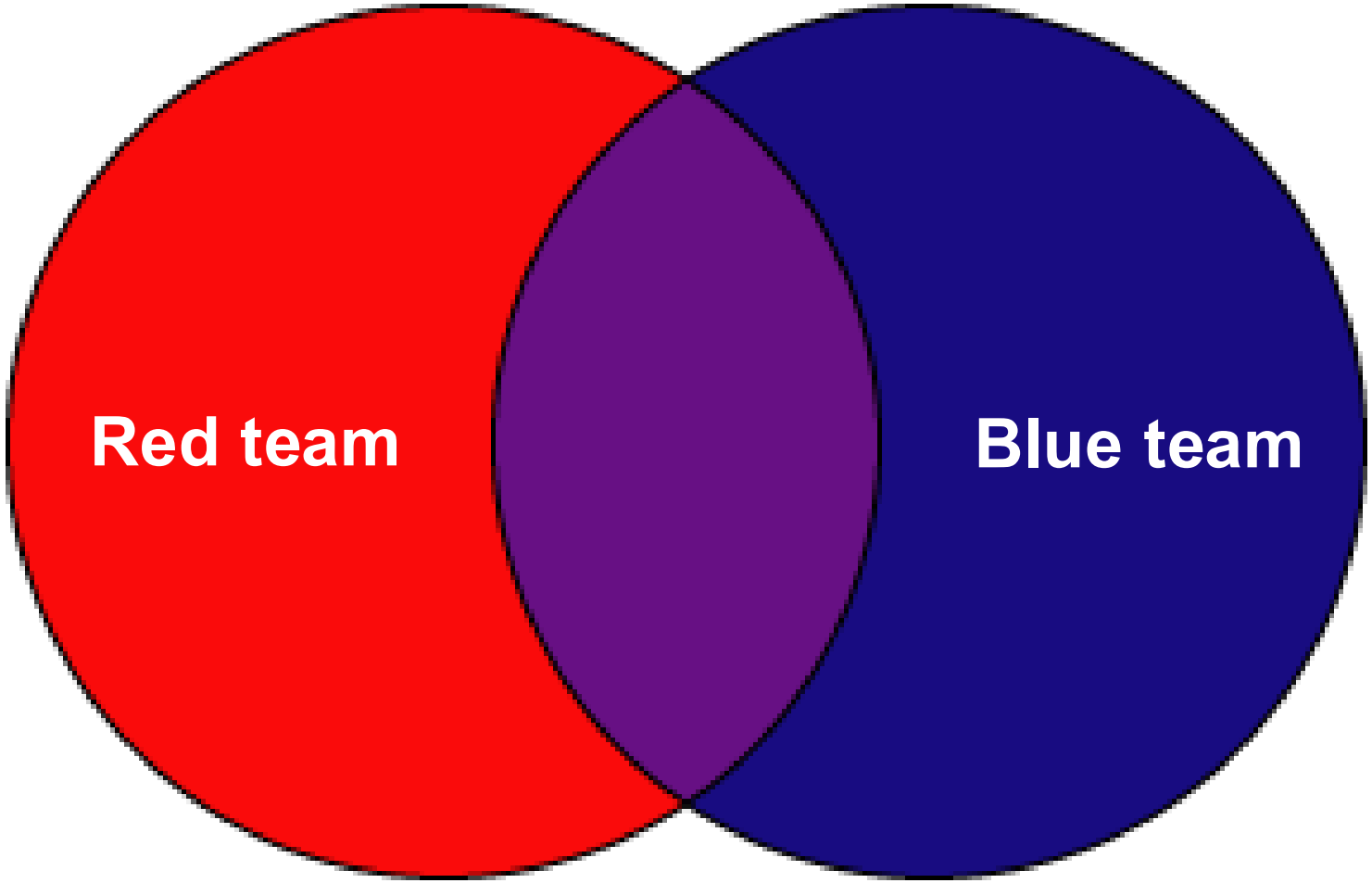
Dokumenty a praktické návody

- SWGDE – (Scientific Working Group on Digital Evidence)
  - Konkrétne postupy pre rôzne typy zariadení
- ACPO – (Association of Chief Police Officers)
  - Britský praktický sprievodca pre zaobchádzanie s digitálnymi dôkazmi
- EnCase Dokumentácia - Oficiálna príručka pre komerčný nástroj EnCase
- Autopsy/Sleuth Kit Dokumentácia
  - Kompletná dokumentácia pre populárny open-source forenzný nástroj
- FTK (Forensic Toolkit) Dokumentácia
  - Príručky od AccessData

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kali - Purple

Prečo „Purple“?



Kali - Purple - OS

- špeciálna distribúcia Linuxu založená na **Kali Linux**, ktorá je zameraná na **defenzívnu bezpečnosť**

- Kali-Purple bol predstavený v roku 2023
- Najnovšia verzia: 2025.3

Zameranie:

- SOC (Security Operations Center) operácie
- Monitoring a detekciu hrozieb
- Incident response
- Analýzu malware
- Forenzné vyšetrovanie

Kategórie nástrojov:

- Identifikácia
- Obrana
- Detekcia
- Reakcia
- Obnova

Kali - Purple – Nástroje (100+)

- Bitová kópia disku
  - dc3dd
  - ewfacquire
  - guymager
- Analýza malwaru
  - Ghidra
  - Ollydbg
  - Yara
- Analýza Disku
  - Autopsy
  - Nástroje sleuthkit
- Rekonštrukcia udalostí
  - galleta
    - analýza cookies z web prehliadača
  - mac-robber
    - extrakcia dát zo súborového systému
  - foremost
    - obnova zmazaných súborov
- Packet analyzér
  - Wireshark
  - Netsniff-ng

Ďalšie nástroje: ....

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Digitálna forenzná analýza

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk