UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

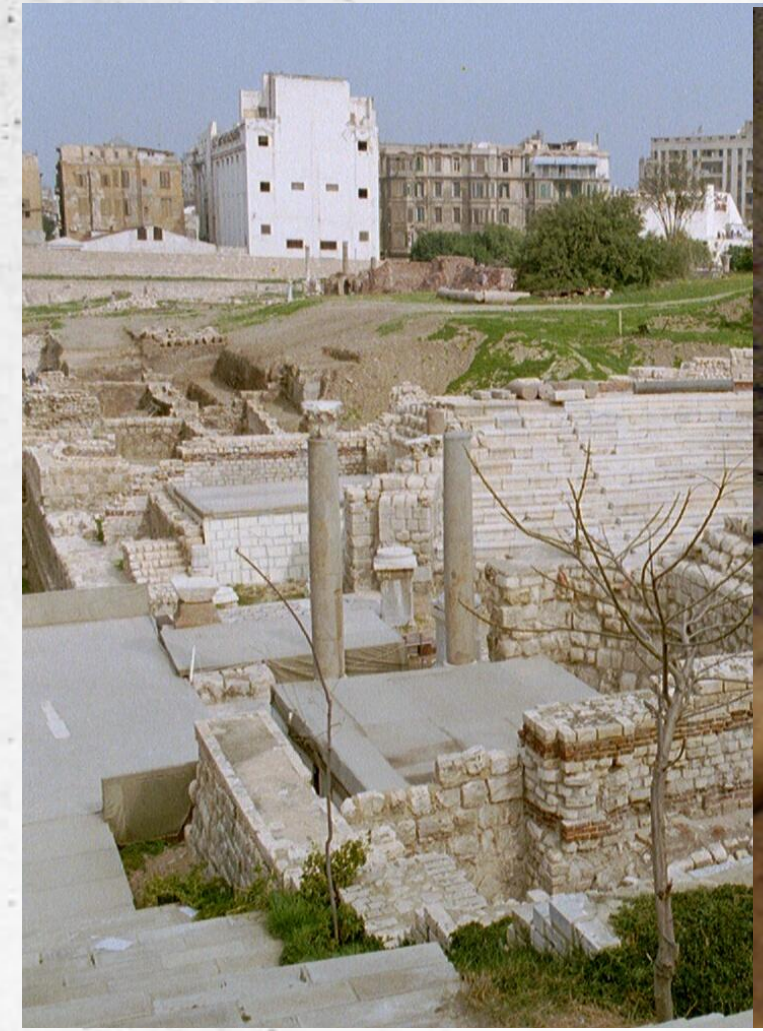
PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Analýza digitálnych stôp a znalecká činnosť

Meno a priezvisko
XX.XX.XXXX

Archeológia

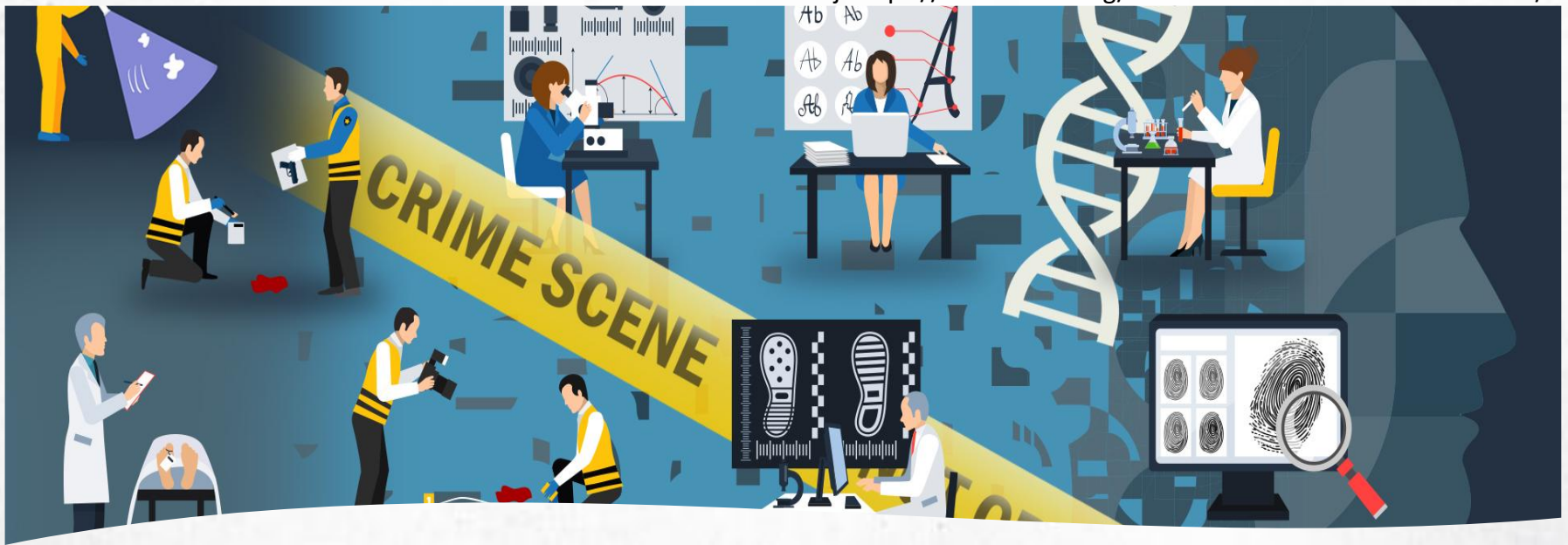


Zdroj: https://sk.wikipedia.org/wiki/Archeol%C3%B3gia, https://www.literama.sk/sk/knihy-kategoria/81/archeologia?_p_p=10, https://vedanadosah.cvtisr.sk/ludia/historia-a-archeologia/archeologovia-objavili-desiatky-vynimocne-zachovanych-vikinskych-kostier/

Forezná veda

- praktická aplikácia rôznych druhov vedy pre zodpovedanie otázok súvisiacich s právnym systémom
- "forenzná„ - v latinčine znamená "z fóra alebo pred ním".
- vzťahuje sa na proces získavania stôp, ktoré môžu byť prijaté ako dôkazy na súde
- forenzní vedci zhromažďujú, uchovávajú a analyzujú vedecké stopy

Zdroj: https://forensiccoe.org/webinar-human-factors-sourcebook/



Digitálna forezná analýza

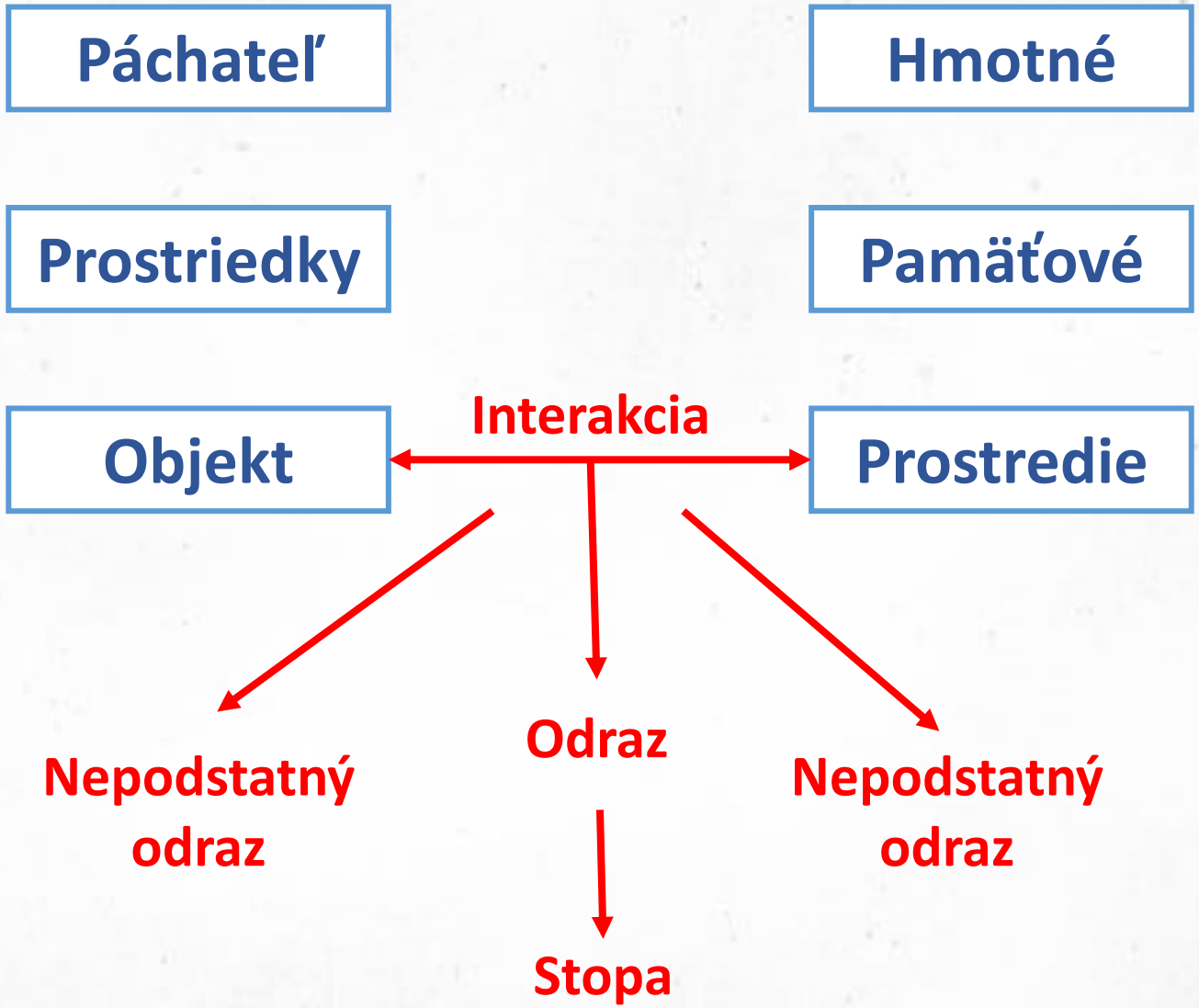
- je **viacstupňový proces** začínajúci identifikáciou digitálnych médií zo scény (možného trestného činu) ako potenciálneho dôkazu do fázy, v ktorej je predložený ako dôkaz odborným svedkom na súde (RAGHAVAN, 2013)

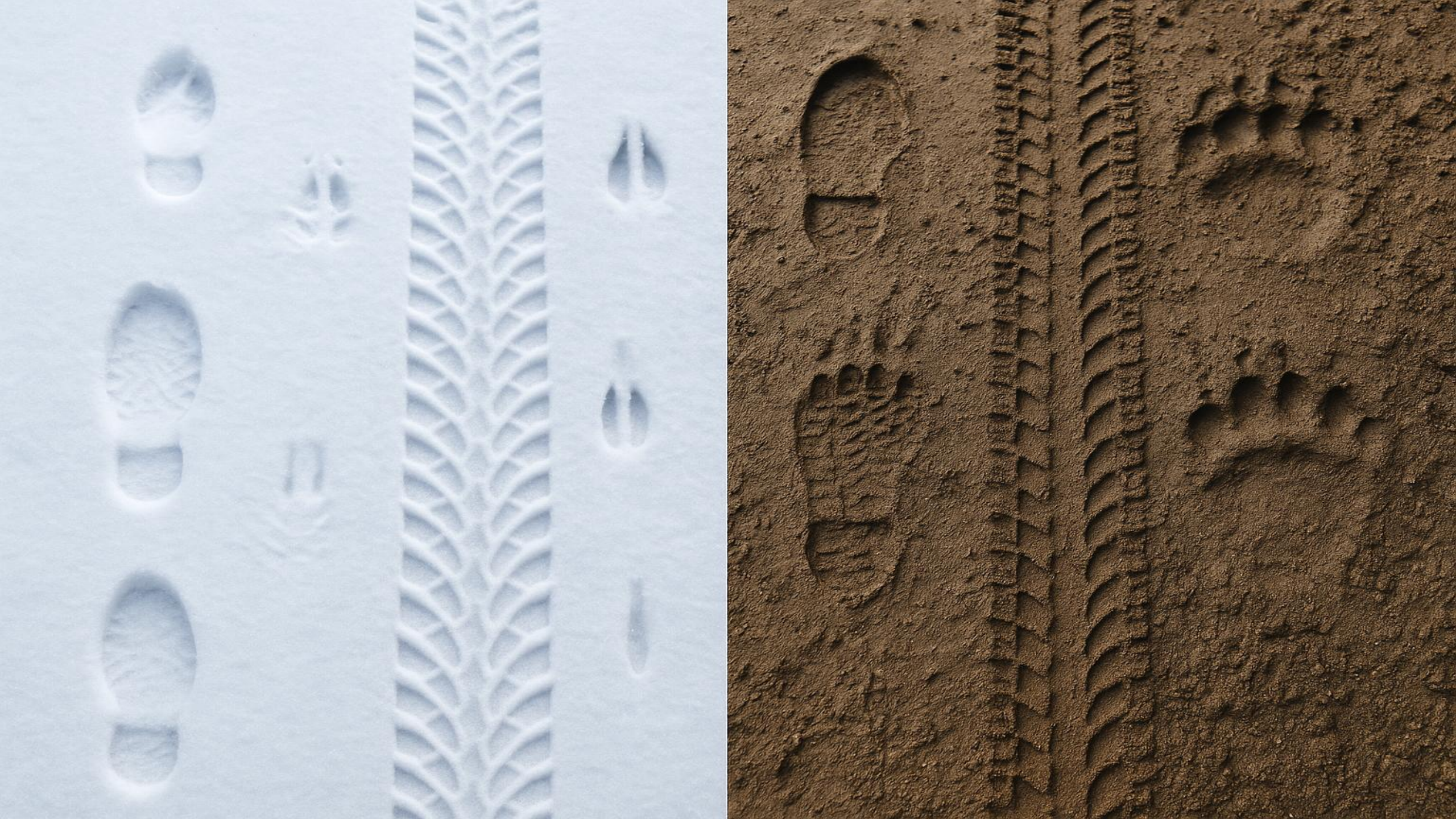
Locardov princíp výmeny

- **Locardov princíp výmeny**
  - „s kontaktom medzi dvoma body bude prebiehať výmena“
  - páchateľ priniesol niečo na miesto činu a odniesol niečo so sebou
  - napr. odtlačky, krv, vlasy a pod.

Zdroj: https://simplyforensic.com/edmond-locard/

Digitálna stopa (I.)





Digitálna stopa (III.)

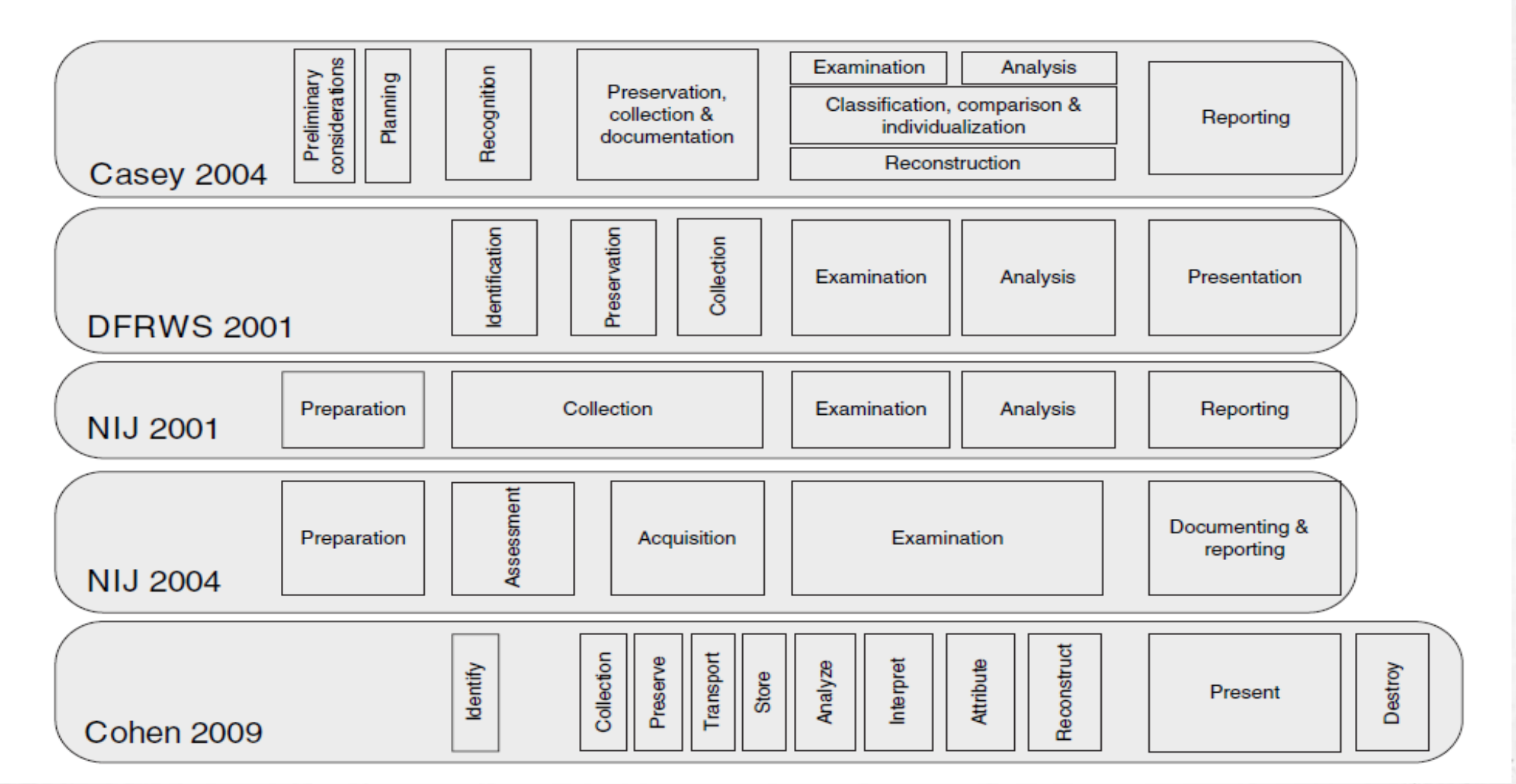
- je akákoľvek informácia s vypovedajúcou hodnotou uloženou alebo prenášanou v digitálnej podobe. **(Whitcomb, 2002)**

- je akákoľvek informácia uložená alebo prenášaná v binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz (**International Organization of Computer Evidence**)

- je akákoľvek informácia s vypovedacou hodnotou uložená alebo prenášaná v digitálnej binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz s vypovedacou hodnotou (**Scientific Working Group on Digital Evidence**)

Digitálna stopa (IV.)

Proces forenznej analýzy (I.)



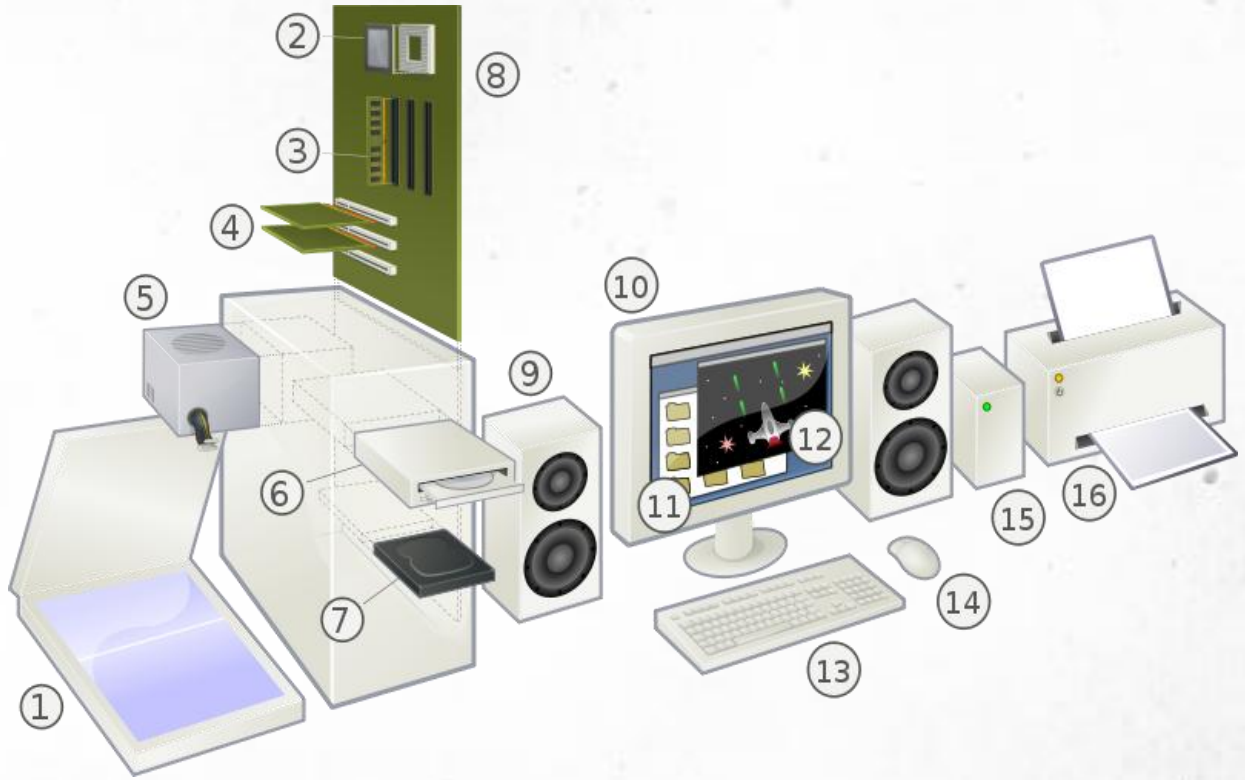
Zdroj: CASEY, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. 3. vydanie. Academic press, 2011. ISBN: 978-0123742681.

Proces forenznej analýzy (II.)

Fáza	Popis činností	Výstup fázy
Identifikácia (Identification)	▪ identifikácia účelu vyšetrovania a potrebných zdrojov ▪ vyhľadávanie, rozpoznávanie a dokumentáciu potenciálnych digitálnych stôp	▪ identifikované zariadenia
Zaisťovanie (Acquisition) a zber (Collection)	▪ zhromažďovanie údajov z digitálnych zariadení ▪ zhromažďovania zariadení, ktoré obsahujú potenciálne digitálne stopy	▪ forenzný image ▪ iné digitálne stopy
Uchovanie (Preservation)	▪ uloženie digitálnych stôp na vhodnom médií ▪ zaistenie integrity zaistených digitálnych stôp	▪ kryptografický haš
Vyťažovanie (Examination)	▪ extrakciu údajov (artefaktov) z digitálnych stôp ▪ redukcia a filtrovanie údajov (artefaktov) ▪ obnova súborov a získavanie (carving) údajov	▪ Výber relevantných digitálnych stôp (artefaktov)
Analýza (Analysis)	▪ Identifikujú sa nástroje a techniky, ktoré sa majú použiť ▪ prioritizácia, filtrácia, korelácia digitálnych stôp ▪ Interpretujú sa výsledky analýzy a potvrdzujú/vyvracajú hypotézy	▪ Potvrdenie/vyvrátenie hypotéz
Prezentácia (Presentation)	▪ sumarizácia a vysvetlenie výsledkov ▪ predloženie výsledkov zadávateľovi	▪ forenzná správa ▪ prezentácia

Identifikácia (I.)

- identifikácia účelu vyšetrovania a potrebných zdrojov
- vyhľadávanie, rozpoznávanie a dokumentáciu potenciálnych digitálnych stôp
- výstup: identifikované zariadenia



Identifikácia (II.)

- Dátové nosiče

Identifikácia (III.)

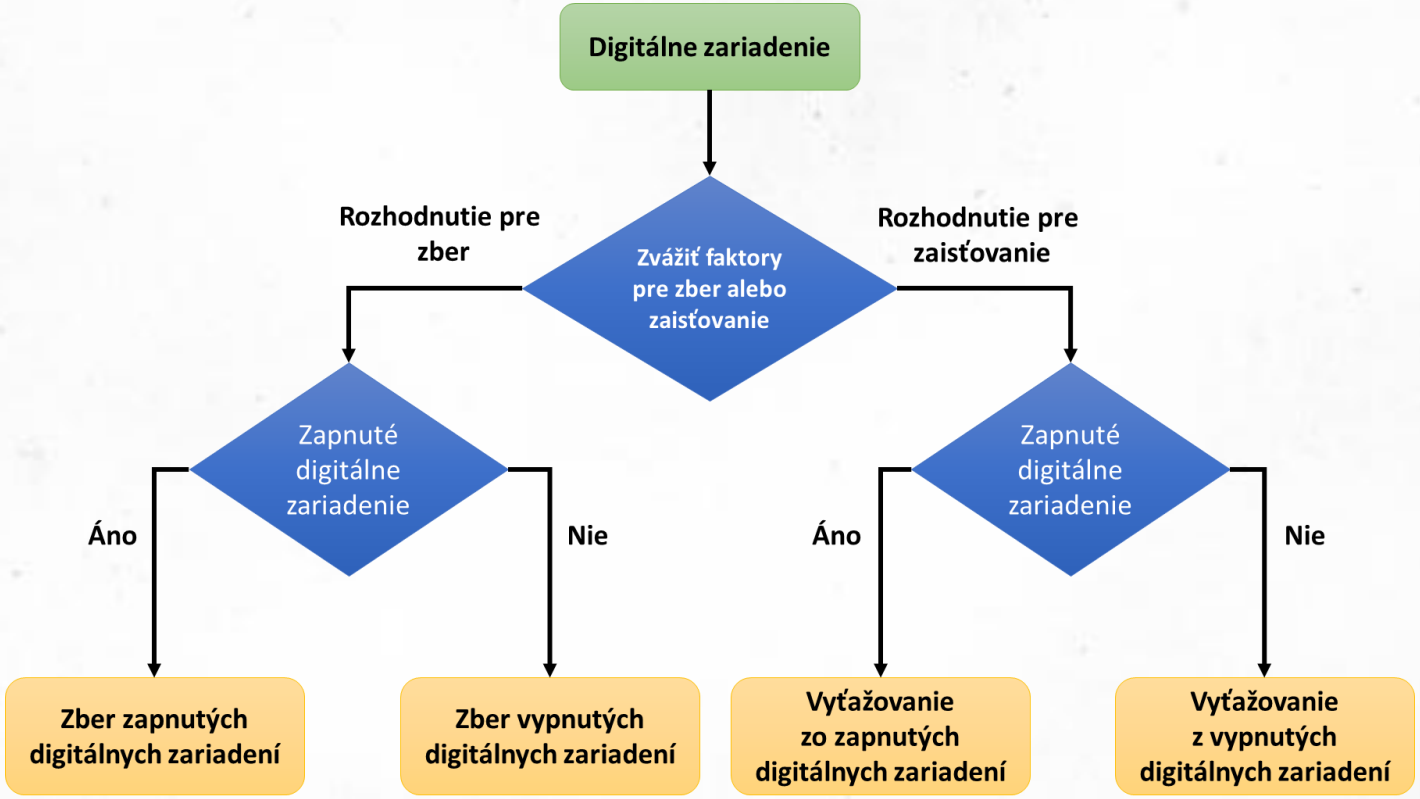
- Kde hľadať stopy?

Zdroj: http://web-cyb.org/hardware-info/elvn-desktop-progression.htm

Zdroj: https://www.flickr.com/photos/68800167@N07/6256946041

Zber a zaisťovanie (I.)

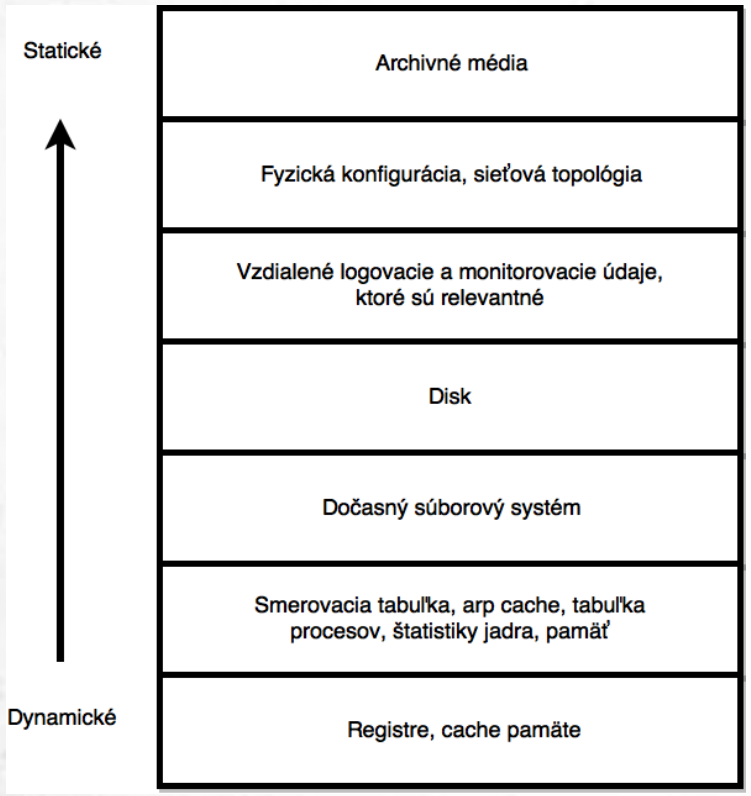
- cieľom tejto fázy je zhromažďovanie údajov z digitálnych zariadení za účelom vytvorenia digitálnej kópie s použitím riadnych forenzných metód a techník (Palmer, 2001).



ISO/IEC 27037:2012

Zber a zaisťovanie (II.)

- **Guidelines for Evidence Collection and Archiving** (RFC 3227), ktoré sa týkajú **poradia volatility** digitálnych stôp



Typ úložného média a údaje	Typická životnosť údajov
Registre, cache pamäte	nanosekundy
RAM	desiatky nanosekúnd
Stav siete	milisekundy
Procesy	sekundy
Údaje na disku (cache)	minúty
Cloudové úložisko	mesiace až roky
HDD úložisko	roky
Magnetické pásky	roky až dekády
CD-ROM, DVD, vytlačené údaje	dekády
Read-only pamäte, flash, SSD	dekády až storočia

Zber a zaisťovanie (III.)

Chain of Custody (reťazec uchovávania dôkazov)

- proces zabezpečujúci autentickosť, integritu
- dokumentácia zaisťovania stôp
- dokumentácia manipulácie s médiom s digitálnymi stopami

Číslo prípadu:			Číslo oddelenia:	
Vyšetrovateľ:				
Popis prípadu:				
Miesto získania dôkazu:				
Popis dôkazu		Výrobca	Výrobné číslo	Poznámky
Odtlačok dát	MD5			
	SHA2-256			
Dôkaz získaný:			Dátum a čas:	
Dôkaz zaznačovaný:			Dátum a čas:	
Dôkaz zabezpečený:			Dátum a čas:	
Dátum a čas	Akcia vykonaná s dôkazovým materiálom			Osoba + podpis
Strana:		Celkový počet strán:		Podpis:

Zber a zaisťovanie (IV.)

- používať **writeblocker**
  - špecializované zariadenia na zabránenie zápisu na zaistené médium počas kopírovania
  - pevné disky, USB kľúče, USB disky

Zdroj: https://amazon.com

Zber a zaisťovanie (V.)

Chyby pri zaisťovaní:

- **zlé zaistenie stôp** -> **znehodnotenie pre účely trestného konania**
- vypnutie zapnutého zariadenia bez zaistenia volatilných stôp
- **zle zapečatený hardvér** (napr. USB porty na na bokoch a vzadu na notebooku)
- **nepresné označenie** stôp (napr. obraz disku bieleho notebooku)
- **chaotické označenie** stôp (ak zaisťuje stopy viacero ľudí)
- **nezaistenie potrebného príslušenstva** (napr. dokumentácia, špecifické napájacie adaptéry)
- **nezaistenie ďalšieho príslušenstva** (napr. usb flash, CD/DVD)

Spôsob zaisťovania (I.)

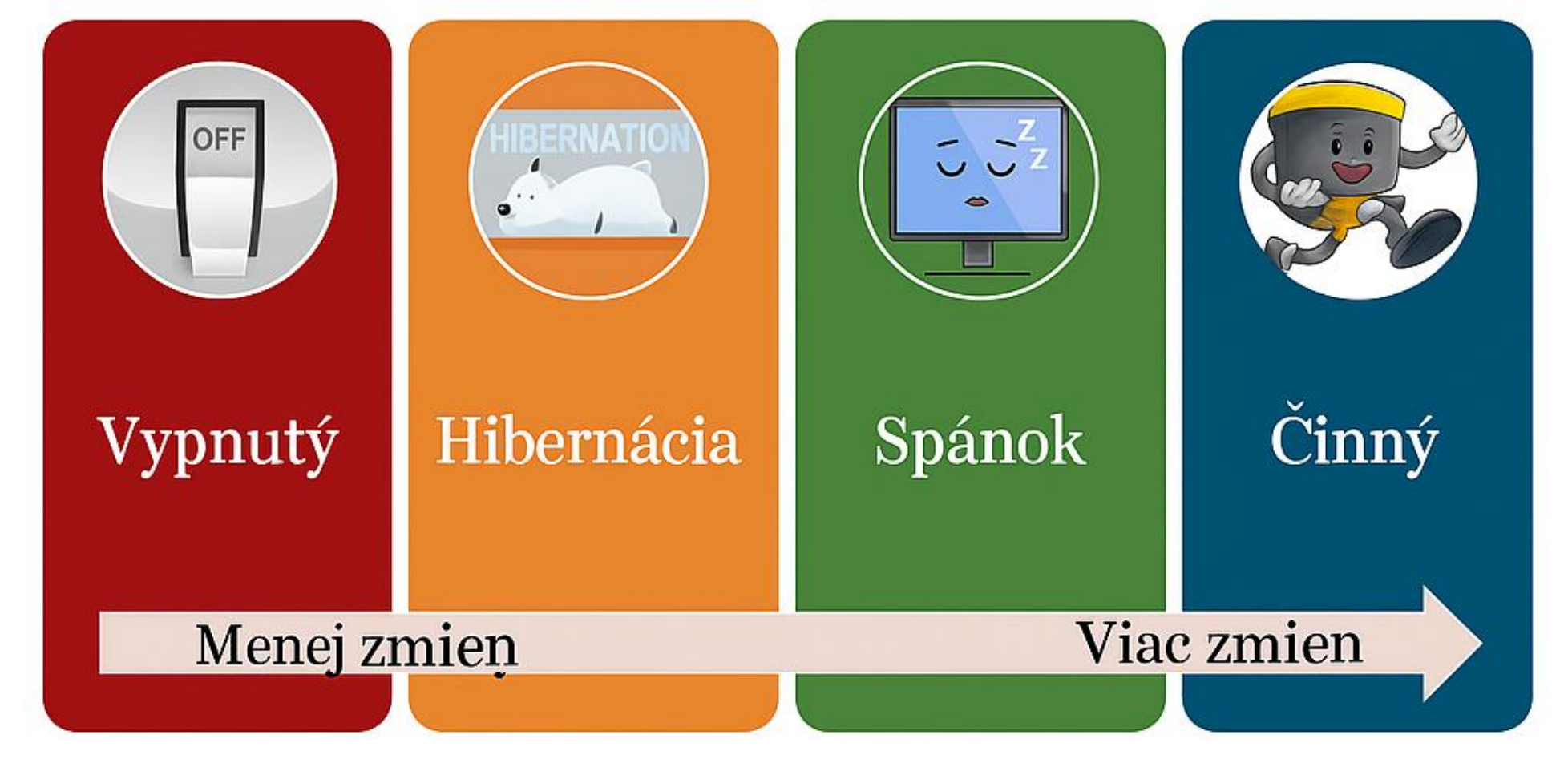
Live

- zariadenie je zapnuté
- dáta sa menia vplyvom zaisťovania aj bežnej činnosti systému
- RAM, swap, pripojené disky a pamäťové média, hardvérové
- kľúče, sieťová komunikácia

Post Mortem

- zariadenie je vypnuté
- bitové kópie zaistených médií cez writeblockery
- disky, pamäťové médiá

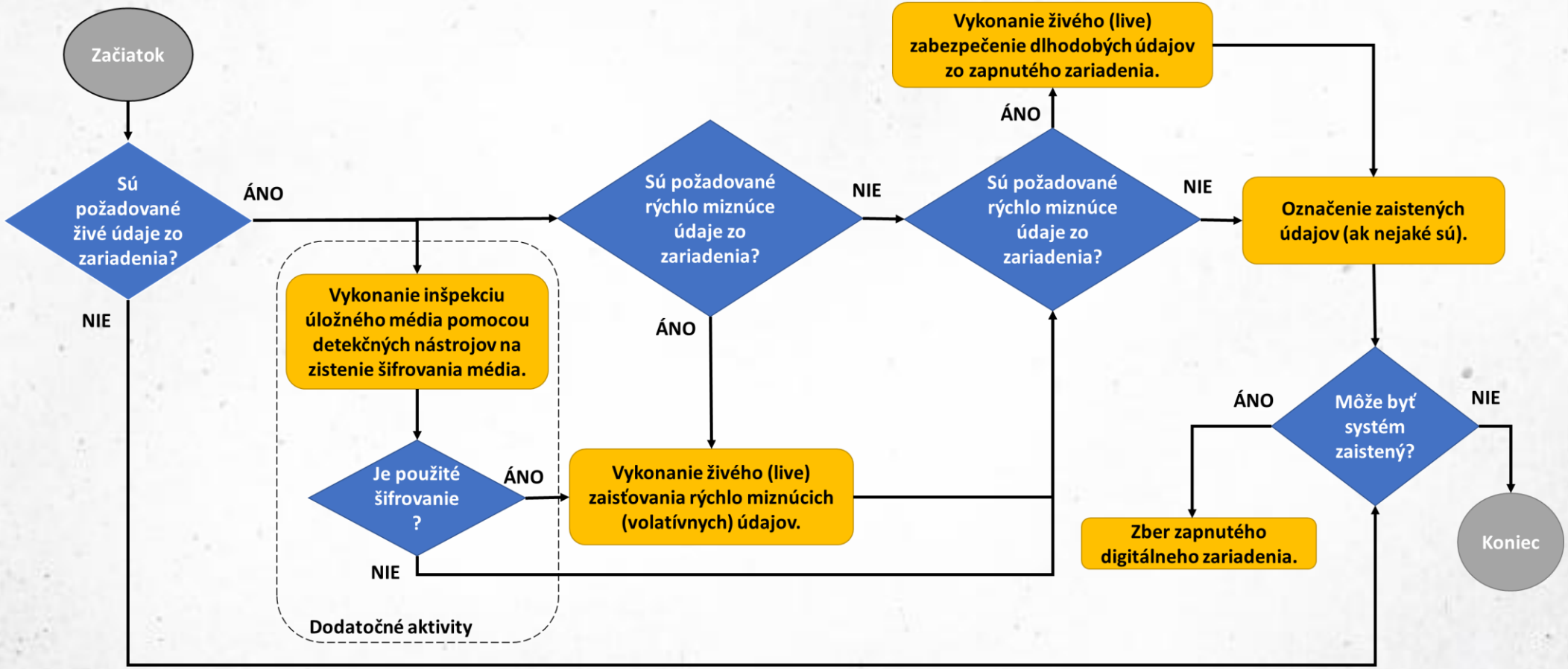
Spôsob zaisťovania (II.)



Zdroj: SANS materiál, FOR500

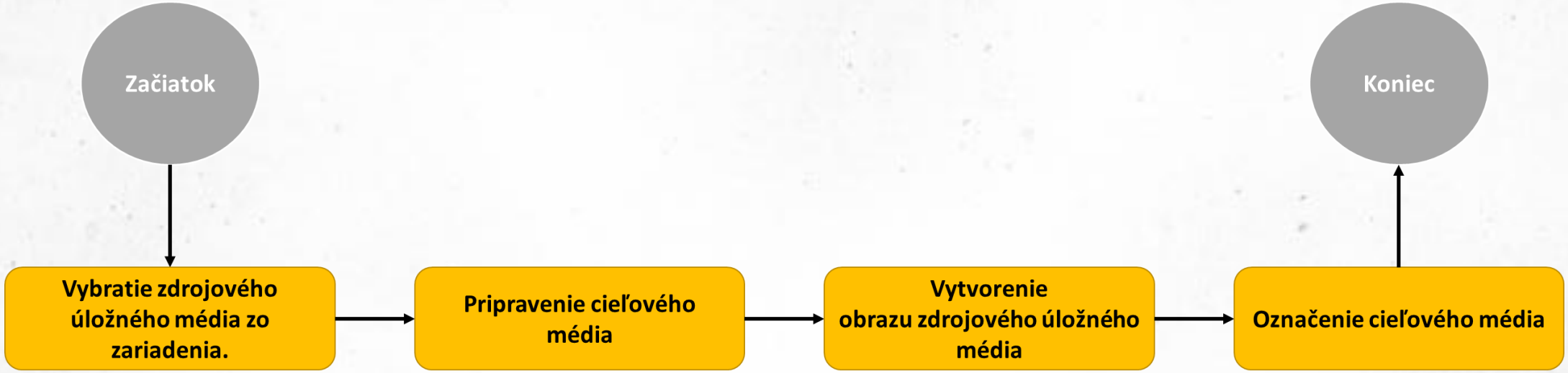
Spôsob zaisťovania (III.)

- **Zaisťovanie zo zapnutého zariadenia** (ISO/IEC 27037)



Spôsob zaisťovania (IV.)

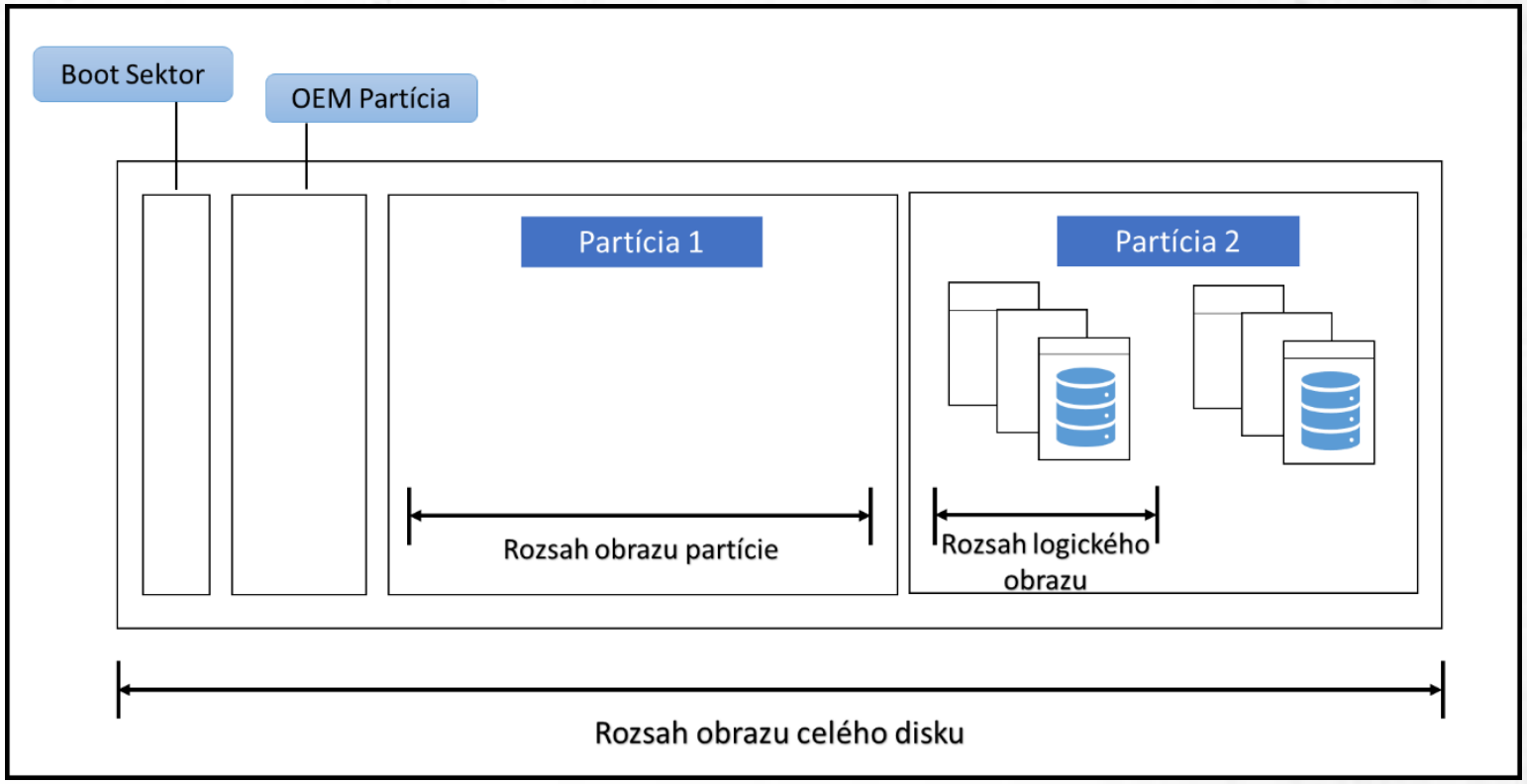
- **Zaisťovanie z vypnutého zariadenia** (ISO/IEC 27037)



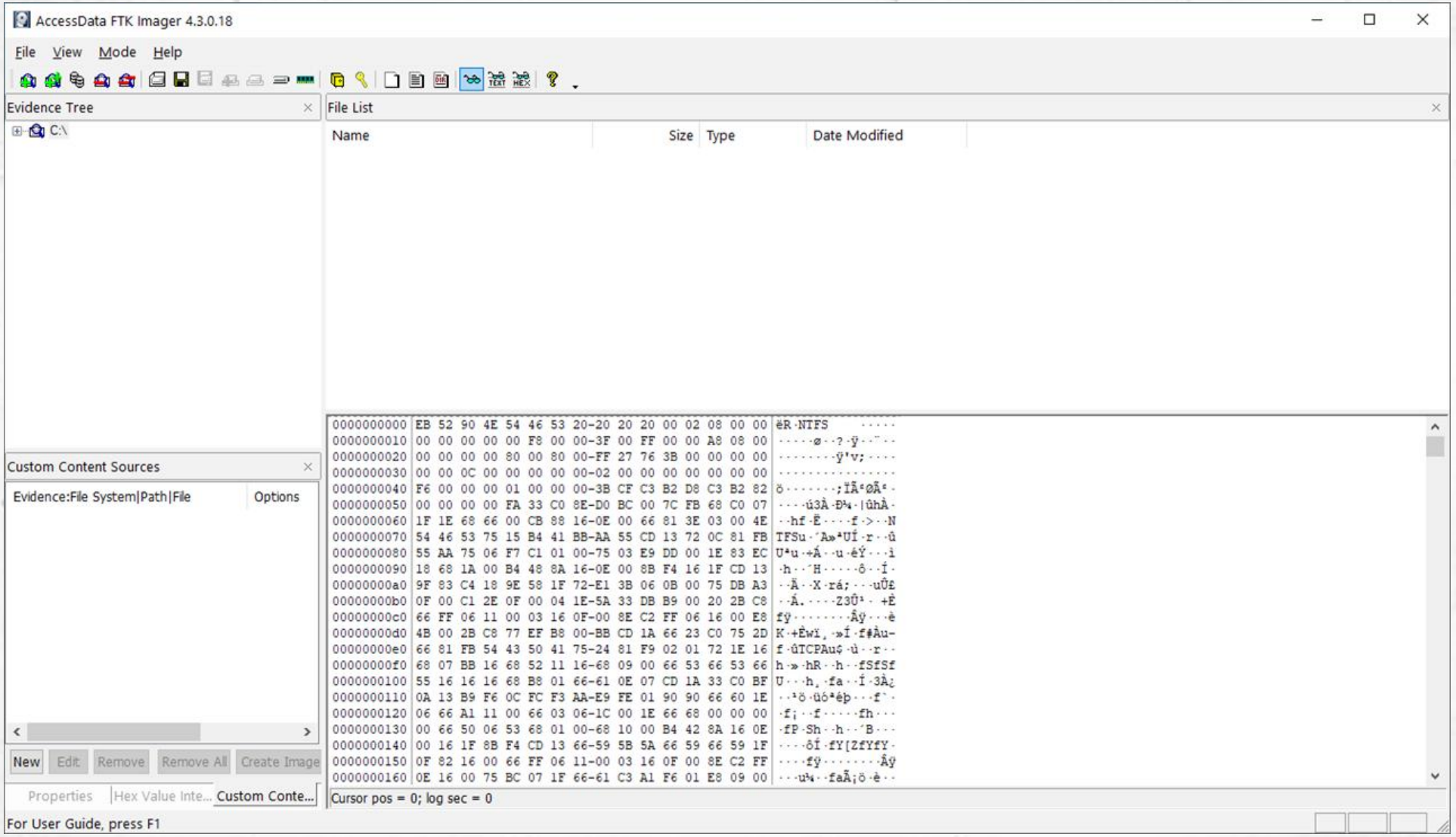
Zaisťovanie (I.)

3 typy forenzných imagov (obrazov):

- **Obraz kompletného disku**
- **Obraz partície**
- **súbory/adresáre – logický obraz**



Zaisťovanie (II.)



Uchovanie (I.)

- **dostatok úložnej kapacity**
  - disky
  - sieťové úložisko
- **zaistenie integrity dát**
  - napr. hash

Zdroj: http://www.vcfed.org/forum/showthread.php?24476-Sorting-floppy-disks-LOTS-of-floppy-disks

Integrita údajov

- Zabezpečenie integrity – Hash (digitálny odtlačok)

- **hašovacia funkcia** vytvára pre rovnaký vstup rovnaký výstup konštantnej dĺžky.
- checksum

- Známe hašovanie funkcie:
  - MD5 (Message-digest 5)
  - SHA-1 (Secure hash algorithm 1)
  - SHA-2 (256/384/512)
  - SHA-3 (256/384/512)
  - CRC32

Triáž

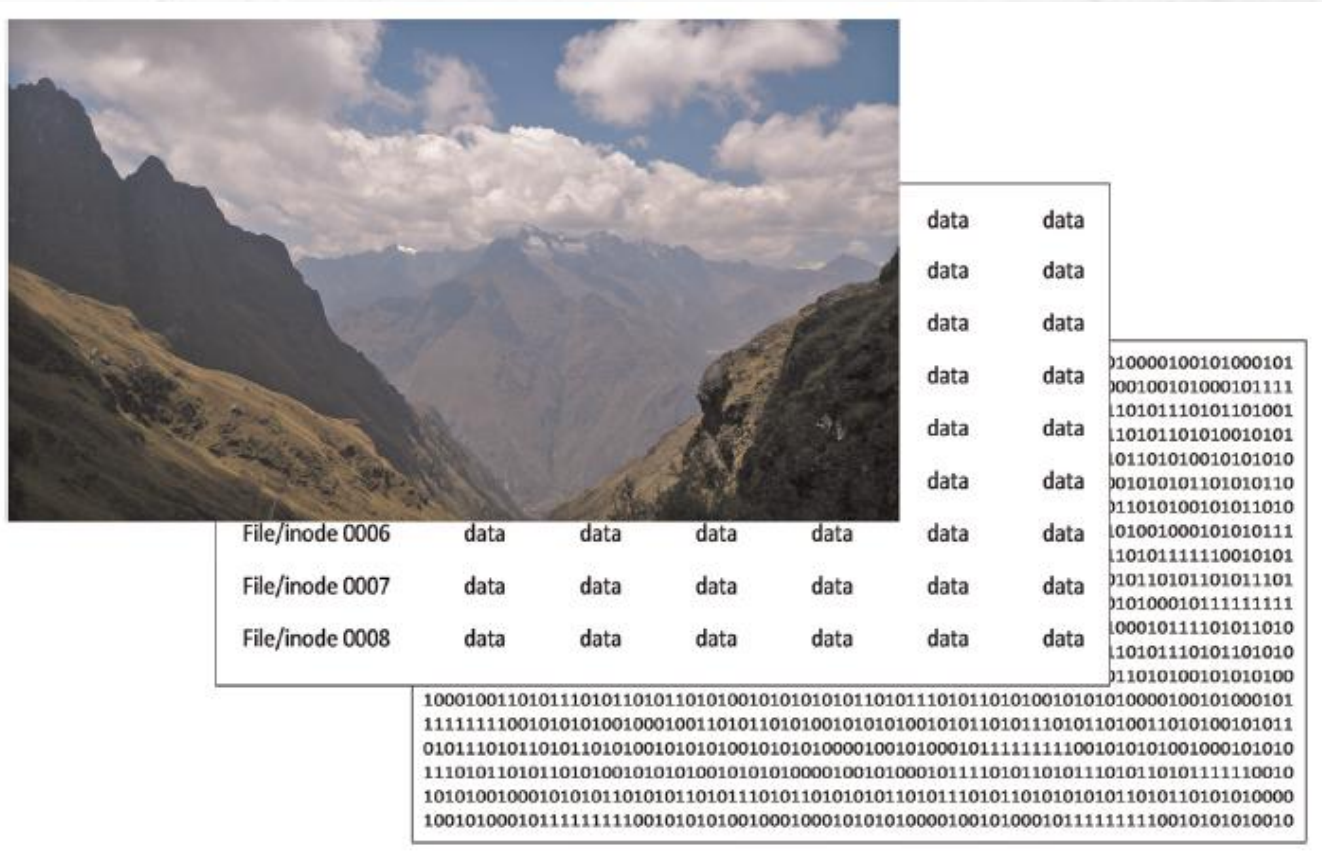
- Triáž (triedenie)

- Máme priestor na uloženie forenzného obrazu (imagu)?
- Máme čas na vytváranie forenzného obrazu (imagu)?
- Je nutné zaistiť celý disk?

- 99% forenzného vyšetrovania sa zameriava na 1% zaistených dát

Vyťaženie

- extrakciu údajov (artefaktov) z digitálnych stôp
- redukcia a filtrovanie údajov (artefaktov)
- obnova súborov a získavanie (carving) údajov
- Výstup: Výber relevantných digitálnych stôp (artefaktov)



Analýza (I.)

A	B	C	D	E	F	G	J	
date	time	timezon	MAC	source	sourcetype	type	short	desc
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998	Entry in log file: C:/Windows/
6/18/2009	22:36:15	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [L
6/18/2009	22:41:26	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [D
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F838A89.pf -
6/18/2009	22:41:59	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/	[DELETED] ???/{83da6326-97a
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed	PKMAILER.EXE-83FAD500.pf -
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7.p
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed	RUNDLL32.EXE-2E65B341.pf -
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windows
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences	LSO created -> File: C://mnt/v
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Firef
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe	UEME_RUNPATH:C:/Program
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E60C0AA7.pf - [
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/	[DELETED] ???/{83da6326-97a
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/	[DELETED] ???/00000008/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/	[DELETED] ???/{83da6326-97a

Analýza (II.)

Analýza (III.)

Postup analýzy:

- **pozorovanie** - digitálne dátové objekty čitateľné (alebo viditeľné) človekom majú obsah
- **hypotéza** - vypracovanie teórie na vysvetlenie digitálnych stôp.
- **predikcia** - na základe forenznej hypotézy forenzní vyšetrovatelia predpovedajú, kde by sa mohli nachádzať zaujímavé forenzné artefakty.
- **experiment/testovanie**
- **závery** - rekonštrukcia udalostí založenú na spojení a korelácii informácií.

Analýza (IV.)

- Koľko stoličiek je na obrázku?
- Koľko kresieb je na obrázku?

Zdroj: https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download

Analýza (V.)


User Comms
Web Based E-mail
E-mail
Calendar
Chat / Webmail Memory Artifacts
Chat and IM
File Download
Open / Save MRU
E-mail
Skype History
Index.dat/ Places.sqlite
Downloads.sqlite
Program Execution
UserAssist
LastVisited MRU
RunMRU Start->Run
MUI Cache
Win7 Jump Lists
Prefetch
Services (EVT)
File Opening/ Creation
Recent Files
Office Recent Files
Shell bags
Link Files
Jump Lists
Prefetch
Index.dat file://
Deleted File or File Knowledge
XP Search - ACMRU
Win7 Search – WordWheelQuery
Last Visited MRU
Thumbs.db
Vista/Win7 Thumbnails
Recycle Bin
Browser Artifacts
Physical Location
Timezone
Wireless SSID
VISTA/Win7 Network History
Cookies
Browser Search Terms
USB Key Usage
Key Identification
First/ Last Times
User
Volume Name
Drive Letter
Link Files
P&P Event Log
Account Usage (SAM)
Last Login
Last Failed Login
Last Password Change
Group Membership
Account Usage (EVT)
Success / Fail Logons
Logon Types
RDP Usage
Account Logon/ Authentication
Rogue Local Accounts
Browser Usage
History
Cookies
Cache
Session Restore
Flash & Super Cookies
Suggested Sites
Memory Fragments of Private Browsing

Prezentácia (I.)

Postup 5W 1H

- **Kto (Who)** – odpoveď na otázku, kto každý bol zapojený do procesu
  - zadávateľ, zamestnanci ...

- **Kedy (When)** - zaznamenanie dátumu a času, kedy sa začalo a kedy skončilo vyšetrovanie/incident/analýza
  - pozor na jednotlivé časy a časové pásma
  - používatejte štandardné časové zóny (UTC)

- **Kde (Where)** - uvedenie podrobnostiach informácie o umiestnení
  - napríklad kancelária, serverovňa a pod.

Prezentácia (II.)

Postup 5W 1H

- **Čo (What)** – zaznamenanie činnosti, ktoré boli vykonané
  - napríklad získanie pamäte alebo získanie záznamov z firewallu , vytvorenie imagu disku
- **Prečo (Why)** - odôvodnenie, prečo bola každá činnosť vykonaná.
- **Ako (How)** – uvedenie popisu spôsobu vykonávania akcie.
  - napr. ak CSIRT tím použil nejaký operačný postup, tak sa zahrnutie do výstupu
  - akákoľvek odchýlka od štandardných prevádzkových postupov by sa mala rovnako zaznamenať

Prezentácia (III.)

Písomné správy (Written reports)

- niektoré bezpečnostné incidenty si vyžadujú rozšírený písomný výstup

- 3 hlavné typy
  - **Zhrnutie (Executive summary)**
  - **Správa o incidente (Incident report)**
  - **Správa z forenznej analýzy (Forensic report)**

Číslo prípadu: 1405222/2018
Interné číslo prípadu: 123/2018
Forenzný znalec: Ján Mrkvička

Správa z forenznej analýzy

Číslo prípadu:	1405222/2018	Interné číslo prípadu:	123/2017

Forenzný znalec:	Ján Mrkvička		Evidenčné číslo znalca:	912344		
Adresa znalca:	Mesto:	Košice	Ulica:	Neznáma	PSČ:	04001
	Štát:	Slovenská republika	Číslo domu:	71		
Adresa inštitútu:	Mesto:	Košice	Ulica:	XXXX	PSČ:	0000
	Štát:	Slovenská republika	Číslo domu:	71		

Odbor:	10 00 00	Odvetvia:	10 04 00, 10 09 00, 10 10 00

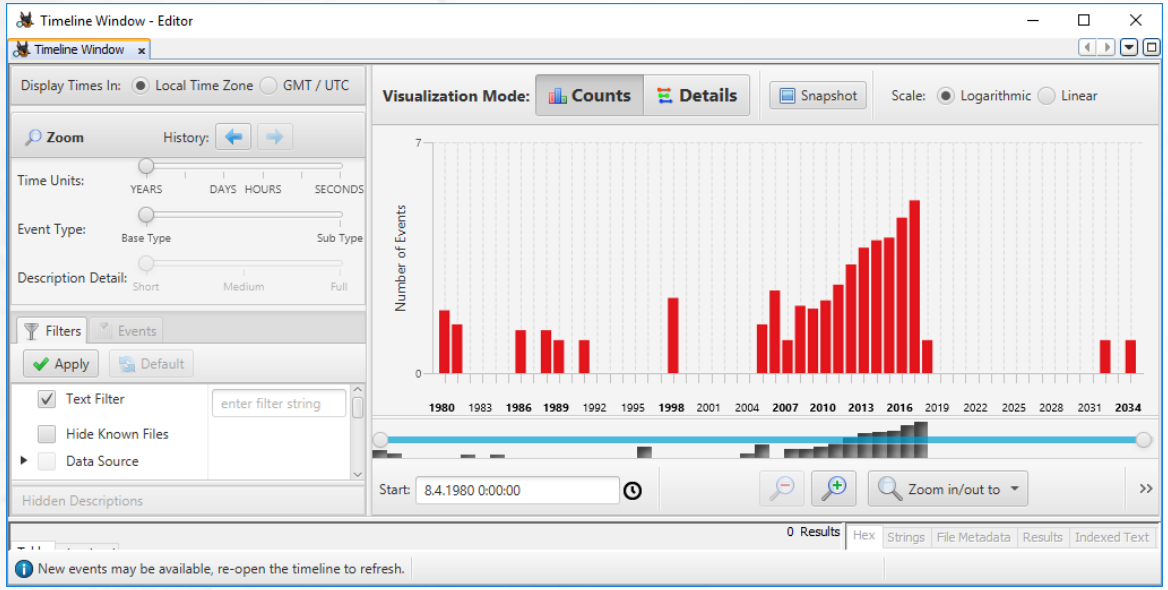
Dátum a čas nahlásenia incidentu (dd.mm.rrrr, hh:mm:ss):	24.05.2017 09:15:34	Dátum a čas vypracovania a ukončenia forenznej správy:	26.05.2017 17:30:00

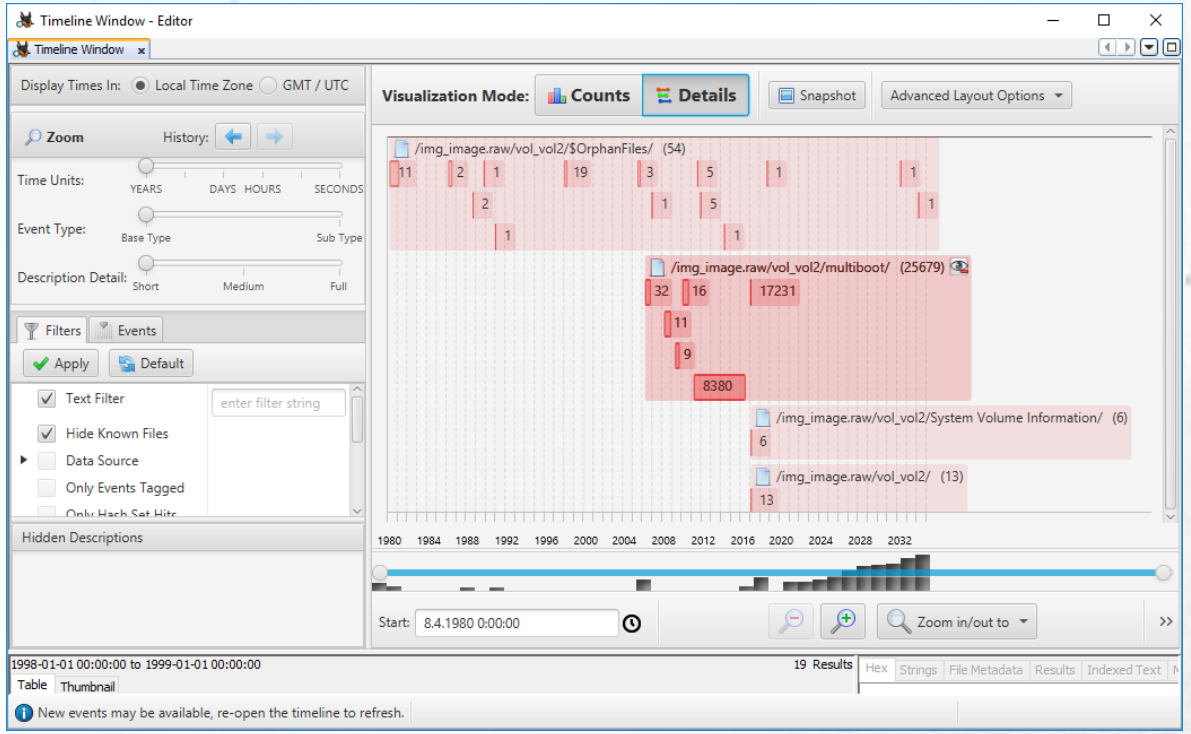
Osoby a subjekty

Číslo: 0001	☒ Svedok	☒ Zadávateľ	☐ Iné:		
Meno:	Ján	Priezvisko:	Admin	Titul:	Mgr.
Hodnosť:	----------	Národnosť:	Slovenská Republika		
Štátna príslušnosť:	Slovenská				
Identifikačné číslo:	o.p.: FA 547846989, číslo zamestnanca: 15254782				

Prezentácia (IV.)

- zostaviť zoznam všetkých udalostí, ktoré sa udiali v rámci operačného systému v chronologickom poradí bez ohľadu na jeho typ, umiestnenie alebo dokonca aplikáciu.





Znalec (I.)

- **Znalec**
  - je osoba rozdielna od procesných strán, ktorú orgán činný v trestnom konaní a súd priberá s tým účelom,
  - účel – na základe svojich odborných znalostí objasnila určitú skutočnosť, dôležitú pre trestné konanie, na objasnenie ktorej sa takéto odborné znalosti vyžadujú.

a) **znalecká organizácia -** ústavy špecializované na znaleckú činnosť podľa § 143 ods. 1 Trestného poriadku

b) **fyzická osoba zapísaná do zoznamu znalcov pre určitý odbor -** podľa zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch.

c) **fyzická osoba nezapísaná do zoznamu znalcov -** vo výnimočných prípadoch - tzv. "**znalci ad hoc**", po zložení sľubu znalca (§ 143 ods. 2 TP).

d) **znalecký ústav** (§ 147 TP)

Znalec (II.)

Zoznam znaleckých odborov (Príloha č. 1 vyhlášky MS SR č. 228/2018 Z. z.)

- relevantných z hľadiska kybernetickej bezpečnosti

10 00 00 Elektrotechnika

- 10 01 00 Elektro-energetické stroje a zariadenia
- 10 02 00 Elektronika
- 10 04 00 Riadiaca technika, výpočtová technika (hardvér)
- 10 06 00 Elektronické komunikácie
- 10 07 00 Odhad hodnoty elektrotechnických zariadení a elektroniky
- 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

49 00 00 Kriminalistika

- 49 20 00 Kriminalistická informatika

Znalecká činnosť (I.)

Zadávatelia znaleckých úkonov

- Fyzická osoba,
- Právnická osoba,
- OČTK
- Predseda senátu
- Súd
- Správny orgán

Právny základ pre zadanie znaleckého úkonu

- súkromný znalecký posudok, predložený stranou bez toho, aby znalecké dokazovanie nariadil súd, v zmysle § 209 ods. 1 zákona č. 160/2015 Z. z. CSP,
- znalecké dokazovanie, nariadené súdom, ktorý ustanoví znalca, v zmysle § 207 ods. 1 zákona č. 160/2015 Z. z. CSP,
- znalecký posudok, na základe ustanovenie znalca zo strany správneho orgánu, v zmysle § 36 ods. 1 zákona č. 71/167 Zb. o správnom konaní (správny poriadok),
- znalecký posudok, na základe pribratia znalca orgánom činným v trestnom konaní alebo predsedom senátu, v zmysle § 142 ods. 1 zákona č. 301/2005 Z. z. TP

Znalecká činnosť (II.)

Trestný poriadok - §142, ods. 1 – Znalecká činnosť

- Ak pre zložitosť objasňovanej skutočnosti nie je postup podľa § 141 (odborná činnosť) postačujúci, priberie orgán činný v trestnom konaní a v konaní pred súdom predseda senátu znalca na podanie znaleckého posudku. Ak ide o objasnenie skutočnosti obzvlášť zložitej, priberú sa **dvaja znalci**.

§ 11 Vylúčenie znalca

- (1) Znalec, tlmočník alebo prekladateľ je vylúčený, ak možno mať pre jeho pomer k veci, k zadávateľovi alebo k inej osobe, ktorej sa úkon týka, pochybnosť o jeho nezaujatosti.
- (3) Znalec, tlmočník alebo prekladateľ zapísaný v zozname nesmie vykonať úkon v odbore alebo odvetví, v ktorom nie je zapísaný; to sa nevzťahuje na znalca, tlmočníka alebo prekladateľa ustanoveného na účely súdneho alebo iného konania súdom alebo iným orgánom verejnej moci.
- (4) To, či úkon patrí do odboru alebo odvetvia, v ktorom je znalec, tlmočník alebo prekladateľ zapísaný do zoznamu, posudzuje ministerstvo.

Podmienky výkonu znaleckej činnosti (I.)

§ 11 Vylúčenie znalca

- (1) Znalec, tlmočník alebo prekladateľ je vylúčený, ak možno mať pre jeho pomer k veci, k zadávateľovi alebo k inej osobe, ktorej sa úkon týka, pochybnosť o jeho nezaujatosti.
- (3) Znalec, tlmočník alebo prekladateľ zapísaný v zozname nesmie vykonať úkon v odbore alebo odvetví, v ktorom nie je zapísaný; to sa nevzťahuje na znalca, tlmočníka alebo prekladateľa ustanoveného na účely súdneho alebo iného konania súdom alebo iným orgánom verejnej moci.
- (4) To, či úkon patrí do odboru alebo odvetvia, v ktorom je znalec, tlmočník alebo prekladateľ zapísaný do zoznamu, posudzuje ministerstvo.

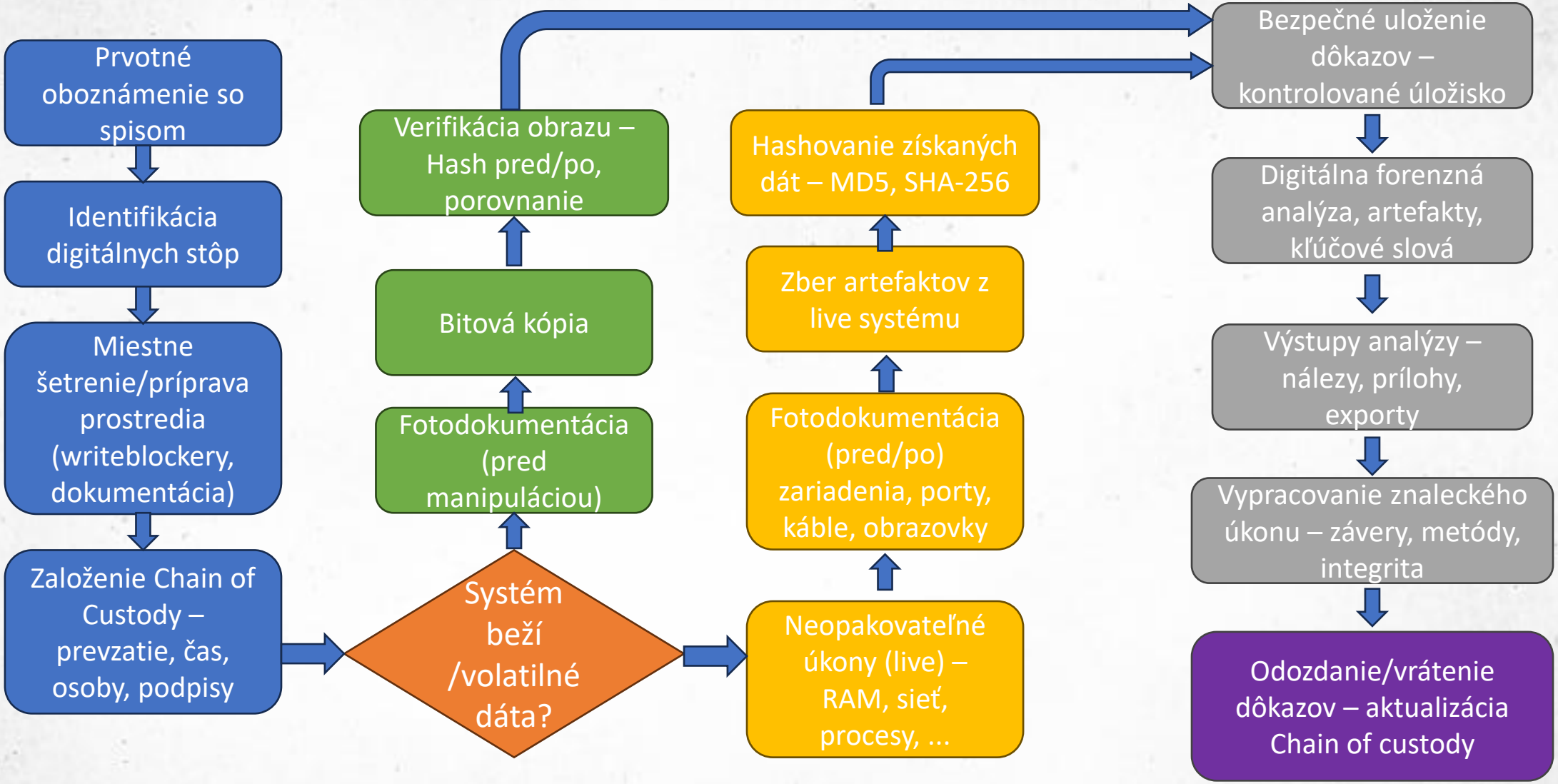
§ 12 Odmietnutie výkonu činnosti

- Znalec, tlmočník alebo prekladateľ zapísaný v zozname nesmie bezdôvodne odmietnuť vykonať úkon, ak je ustanovený súdom alebo iným orgánom verejnej moci.

Bežné úlohy znalca v trestnom konaní

- asistencia pri vykonávaní domových prehliadok (napr. získavanie a vyťažovanie dát priamo na mieste),
- účasť na výsluchoch v prípade potreby technickej konzultácie,
- zabezpečenie prístupu do počítačov alebo iných technických zariadení,
- dokumentovanie softvérového a hardvérového vybavenia,
- zisťovanie licenčných informácií operačných systémov a aplikácií,
- zaistenie dát z techniky použitej pri páchaní trestnej činnosti (napr. pre potreby znalcov iných odborov),
- obsahová analýza e-mailovej komunikácie vrátane príloh,
- vyhľadávanie konkrétnych dokumentov v dátových úložiskách,
- obnova vymazaných dát z dátových nosičov (HDD, USB, pamäťové karty),
- stanovenie všeobecnej hodnoty vecí alebo výšky spôsobenej škody,
- zásahy do účtovných systémov/dát,
- tvorba fiktívnych dokumentov.

Proces znaleckého skúmania



KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

meno.priezvisko@upjs.sk

https://cyberawareness.sk