

D3 – Metodológia pre spracovanie digitálnych stôp



Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

OBSAH

1	Popis projektu	3
2	Úvod	3
3	Úloha KPB1.3.....	4
3.1.	Základné východiská.....	5
3.2.	Princípy získavania, uchovávaní a interpretácie digitálnych dôkazov.....	8
3.2.1.	Identifikácia nevyhnutného (primeraného) rozsahu skúmania.	8
3.2.2.	Akvízia dostatočného množstva relevantných informácií.....	9
3.2.3.	Evidencia a reťazenie (chain of custody), transparentnosť, preskúmateľnosť a hodnovernosť	10
3.2.4.	Nestrannosť a nezáujatosť	12
3.2.5.	Riziková analýza, taktika, profesionalita	13
3.3.	Štádia digitálnej analýzy	14
3.3.1.	Identifikácia digitálnych informácií	14
3.3.2.	Zhromažďovanie dát	15
3.3.3.	Uchovávanie dát.....	15
3.3.4.	Overovanie dát a postupov.....	16
3.3.5.	Analýza a interpretácia dát	17

1 Popis projektu

Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych dôkazov, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forenznych vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forenznych analytikov.** Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní.** Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné dôkazy pre vyšetrovanie a súdne konania.

2 Úvod

Cieľom pracovného balíka KPB1 je analyzovať a **reagovať na právne otázky súvisiace s navrhovaným projektom**. Tento pracovný balík definuje minimálne štandardy a právne záruky potrebné na zabezpečenie uplatňovania právneho rámca ochrany osobných údajov pri spracovaní digitálnych dôkazov a prípustnosti získaných výstupov automatizovanej forenznej analýzy ako dôkazov v trestnom konaní, pričom zohľadňuje aspekty etické, právne, ako aj otázky legitímnosti a proporcionality týkajúce sa extrakcie digitálnych dôkazov strojovým učením. Predmetom skúmania sú aj vlastnosti digitálnych dôkazov (integrita, autenticita, prípustnosť a relevantnosť).

Vzhľadom na absenciu ustanovení ktoré by sa venovali téme noriem zaistovania digitálnych dôkazov komplexne, uvedená metodológia stanovuje minimálny dokumentačný štandard aby bola analýza digitálnych stôp prípustná ako dôkaz bez ohľadu na skutočnosť, či boli spracované ručne znalcom, automatizovaným spôsobom na základe algoritmu alebo s použitím strojového učenia. Pojem dokazovania v trestnom konaní tvorí zákonom upravený postup subjektov trestného konania (orgánov činných v trestnom konaní, súdu, obvineného, poškodeného, zúčastnenej osoby atď.).

3 Úloha KPB1.3

Úloha KPB1.3 – Analýza podmienok prípustnosti spracovaných digitálnych dôkazov ako dôkazov v trestnom konaní. Etické pravidlá pre získavanie digitálnych dôkazov na základe strojového učenia. Taktiky kybernetickej obrany v súvislosti s forenzným vyšetrovaním a obnovou digitálnych dôkazov, vrátane využitia a prípustnosti automatizovanej analýzy (EISI).

Digitálne stopy môžu zahŕňať širokú škálu rôznych informácií s dôkaznou hodnotou uložených alebo prenášaných v digitálnej forme.¹ Konkrétne informácie obsiahnuté v digitálnych stopách môžu byť chránené právnou ochranou podľa rôznych právnych predpisov. Ak sa majú digitálne stopy skúmať a spracovávať orgánmi alebo iné subjektmi², na účely trestného konania, musia sa riadiť jednak osobitnými platnými predpismi ale i procesnými pravidlami trestného konania. V nasledujúcich kapitolách načrtávame potrebné kroky, ktoré je potrebné podniknúť, aby sa umožnilo ďalšie používanie digitálnych dôkazov v trestnom konaní.

Nasledovné kapitoly rozoberajú:

- Základné východiská
- Princípy získavania, uchovávaní a interpretácie digitálnych dôkazov
- Štádiá digitálnej analýzy

¹ Scientific Working Group on Digital Evidence (SWGDE). *Digital Evidence: Standards and Principles*. In *Forensic Science Communications*. 2000, No. 2. Available: <https://archives.fbi.gov/archives/about-us/lab/forensic-sciencecommunications/fsc/april2000/swgde.htm#Introduction>

² Ako konštatuje Dražová, „V rámci svojej pôsobnosti sa so zaistovaním dát ako potenciálnych elektronických dôkazov bežne potykajú aj rôzne subjekty mimo trestného konania, napríklad národné alebo vládne jednotky pre riešenie kybernetických bezpečnostných incidentov, orgány verejnej moci na účely civilného či správneho konania, tímy vykonávajúce digitálne vyšetrovanie pôsobiace v komerčnej sfére a podobne.“ Dražová, P. *Electronic evidence in criminal proceedings*. Dissertation thesis, 2021. Available: <https://opac.crzp.sk/?fn=detailBiblioFormChildA52T&sid=4BD9478A3A7038F60D223DAC8853&seo=CRZP-detail-kniha>

3.1. Základné východiská

Dokazovanie tvorí kľúčovú a neodmysliteľnú zložku trestného konania, pretože na podklade výsledkov vykonaného dokazovania súd rozhoduje o vine, respektíve nevine osoby obvinenej z trestného činu. Pojem dokazovanie tvorí zákonom upravený postup subjektov trestného konania (orgánov činných v trestnom konaní, súdu, obvineného, poškodeného, zúčastnenej osoby atď.), ktorého účelom je vyhľadať, zabezpečiť, vykonávať a zhodnotiť informácie dôležité pre poznanie skutkových okolností, na základe ktorých sa v trestnom konaní rozhoduje najmä o vine a treste obvineného, ale aj o ďalších právne relevantných skutočnostiach (napr. o nároku poškodeného na náhradu škody).³

Vzhľadom na absenciu ustanovení ktoré by sa venovali téme noriem zaistovania digitálnych dôkazov komplexne, je potrebné uviesť niekoľko systémových poznámok k postupu a minimálnym štandardom aby bola analýza digitálnych dôkazov prípustná ako dôkaz bez ohľadu na skutočnosť, či boli spracované ručne znalcom, automatizovaným spôsobom na základe algoritmu, alebo s použitím strojového učenia. Digitálne dôkazy zahŕňajú širokú škálu údajov pochádzajúcich z elektronických zariadení, alebo zaistených na diaľku, bez fyzickej držby resp. kontroly zariadenia, alebo nosiča informácií. **Zmyslom a princípom analýzy digitálnych stôp je vyhľadávanie a hodnotenie digitálnych informácií ako dôkazov.**

V porovnaní s inými druhmi kriminalistických stôp sa digitálne stopy vyznačujú špecifickými vlastnosťami, a to:

- nehmotnosť digitálnych stôp,
- latentnosť digitálnych stôp,
- časová trasovateľnosť digitálnych stôp,
- vysoká obsažnosť digitálnych stôp,
- veľmi nízka životnosť digitálnych stôp,
- uchovávanie a kvalita digitálnych stôp je ovplyvnená mnohými subjektívnymi faktormi,
- veľký dátový objem digitálnych stôp,
- dátová hustota digitálnych stôp v čase a s rozvojom nových technológií neustále klesá,
- extrémna dynamika prostredia digitálnych stôp,
- heterogénnosť a komplexnosť prostredia digitálnych stôp,
- veľký geografický rozsah priestoru s digitálnymi stopami,
- vysoký stupeň ochrany dát sťažuje alebo znemožňuje prácu s digitálnymi stopami,
- digitálna stopa je použitím špecializovaných prostriedkov automaticky identifikovateľná a spracovateľná,
- vysoká úroveň zahľadzovania digitálnych stôp kvalifikovanými páchatelmi,

³ ČENTĚŠ, J. a kol.: Trestné právo procesné. Všeobecná časť. Šamorín : Heuréka, 2016, s. 328.

- obnoviteľnosť zničených digitálnych stôp,
- originalnosť digitálnych stôp,
- nízka úroveň akceptácie digitálnych stôp zo strany súdov a orgánov činných v trestnom konaní.⁴

Digitálne stopy môžu mať pritom charakter fyzických stôp (pochádzajúcich zo zariadení, ktoré sú určené na spracovanie, uloženie alebo prenos dát, napríklad pevný disk počítača alebo pamäťová karta, ale v širšom význame aj počítač, tlačiareň a pod.), dátových stôp (pochádzajúce z rôznych databáz, adresátov, súborov) alebo stôp pochádzajúcich z metadát (metadáta sú v podstate dáta o dátach, teda súvisiace informácie týkajúce sa dátumu a času vytvorenia súboru, dátumu jeho modifikácie, vlastníka súboru, veľkosť súboru a pod.).

Fyzické a dátové objekty sa stávajú dôkazom až vtedy, ak sú akceptované orgánom činným v trestnom konaní, respektíve súdom. Kľúčovou otázkou je preto otázka preukázateľnosti axiómy, že digitálna stopa sa nachádzala na určitom mieste a že v priebehu procesu od jej zaistenia až do ukončenia znaleckého skúmania nebola žiadnym spôsobom modifikovaná. Preto sa pracuje s duplikátom digitálnej stopy, čo je presná digitálna reprodukcia všetkých dátových objektov nachádzajúcich sa na pôvodnom fyzickom objekte vyhotovená na fyzicky rovnaký typ dátového média.⁵ Objem dát a informačný obsah všetkých dátových objektov sú v pomere 1:1 medzi originálom a duplikátom. Duplikáty digitálnych stôp sa vytvárajú pre potreby znaleckého dokazovania, aby mohol byť pôvodný materiál kedykoľvek predložený k opätovnému skúmaniu iným znalcom (pozn. najčastejšie pôjde o prípady, kedy si dá vyhotoviť znalecký posudok obvinený), ak samotný fyzický objekt (napríklad počítač) nemožno z rôznych dôvodov zaistiť. V praxi sa v prípade počítačov bežne vytvára obraz (*image*) disku, ktorý je verným duplikátom obsahu disku, teda zrkadlom jeho pôvodného obsahu uložený v digitálnej podobe.⁶

Analýzou stôp súvisiacich s informačno-komunikačnými technológiami za účelom ich použitia ako elektronického dôkazu v trestnom konaní sa zaoberá **digitálna forenzná analýza**. Nastupuje po tom, čo orgán činný v trestnom konaní, resp. súd dospel k záveru, že za účelom preukázania skutočností podľa ustanovenia § 119 TP bude potrebné obstaráť isté penzum dát, ktoré za splnenia určitých kritérií, môže nadobudnúť povahu elektronického dôkazu.

Elektronický dôkaz by mal preto spĺňať tieto podmienky:

- zákonnosť (dôkaz musí byť získaný zákonom predpísaným spôsobom),
- autentickosť (pravosť, musí existovať príčinná súvislosť medzi dôkazom a skutkom),

⁴ Ibid.

⁵ SMEJKAL, V.: Současné možnosti boje proti počítačové kriminalitě. In Data Security Management. 2016, č. 4, s. 18 – 23.

⁶ PORADA, V., RAK, R.: Digitální stopy v kriminalistice a forenzních vědách. In Soudní inženýrství. 2006, č. 17, s. 3- 23.

- integrita (dôkaz musí byť ucelený a nezmenený),
- spoľahlivosť (spôsob získania dôkazu a manipulácia s ním nesmie v žiadnom prípade vzbudzovať dôvodné pochybnosti o autentickeosti a hodnovernosti dôkazu),
- hodnovernosť (za hodnoverný dôkaz možno považovať iba taký dôkaz, ktorý bol získaný zákonom predpísaným spôsobom, a zároveň neexistujú dôvodné pochybnosti o jeho pravosti, integrity a spoľahlivosti).

Postupy naznačené touto metodológiou majú viesť k tomu, aby pri ich dodržaní, bolo možné považovať digitálnu stopu za dôkaz a tak ho aj hodnotiť. Na to aby použitie tejto metodológie naplnilo svoj účel a zaistené digitálne stopy boli dôkazmi je však v prvom rade potrebné splniť základnú požiadavku zákonnosti získania digitálnych stôp, pričom v zmysle § 119 ods. 2 zákona č. 301/2005 Z.z. Trestný poriadok v znení neskorších predpisov (ďalej len "TP") *za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona*. S poukazom na uvedené je možné digitálne stopy zaisťovať v rôznych zákonných režimoch, nielen v režime zaisťovania digitálnych dôkazov orgánmi činnými v trestnom konaní a súdmi podľa TP.

Jednou z možností je advokát konajúci v procesnom postavení obhajcu / splnomocnenca poškodeného / opatrovníka poškodenej osoby s obmedzenou spôsobilosťou na právne úkony, ak jej zákonný zástupca nemôže vykonávať svoje práva, pretože s poukazom na § 2 ods. 10 TP právo obstarávať dôkazy majú aj strany (generálna splnomocňujúca klauzula). Podľa § 7 ods. 1 Advokátskeho poriadku *advokát má právo vyhľadávať a získavať dôkazné prostriedky (svedkov, listiny, znalecké posudky, atď.), zisťovať skutkové okolnosti prípadu, nesmie však svedkov ovplyvňovať a zistené dôkazy a skutočnosti pozmeňovať alebo skresľovať. O zistených skutkových okolnostiach môže vyhotoviť písomný záznam a môže ho nechať svedkom podpísať. Advokát môže o zistených okolnostiach so súhlasom dotknutých osôb vyhotoviť aj zvukový, obrazový alebo zvukovoobrazový záznam za predpokladu, že bude použitý v súlade so zákonom a bude dodržaná zásada mlčanlivosti advokáta. Advokát môže vyhľadávať svedkov, zisťovať dôkazy a skutkové okolnosti prípadu aj prostredníctvom tretích osôb*.

Ďalším prípadom je subjekt poskytujúci právne služby prevádzkovateľovi základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov (ďalej len "ZKB") jednou zo základných povinností prevádzkovateľa základnej služby podľa §19 ods.6, písm. d) ZKB je v zabezpečiť v čase kybernetického incidentu dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní. Pre tieto účely je obzvlášť potrebné postupovať podľa uvedenej metodiky, nakoľko zákon ustanovuje právnu povinnosť konať tak, aby zaistené digitálne stopy kybernetického bezpečnostného incidentu boli použiteľné v trestnom konaní ako dôkazy, pričom však nestanovuje postup ako má prevádzkovateľ základnej služby postupovať, aby túto zákonnú povinnosť splnil.

Ďalším možným právnym režimom, v ktorom sa zaisťujú digitálne dôkazy je prípad právneho zástupcu poskytovateľa služieb podľa § 4 zákona č. 329/2025 Z. z. o niektorých administratívnych opatreniach súvisiacich so zhromažďovaním elektronických dôkazov v

trestnom konaní, ktorý je transpozíciou smernice (EÚ) 2023/1544, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych
V ďalších situáciách podľa ustanovení §135a zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, kedy sú konatelia povinní vykonávať svoju pôsobnosť s odbornou starostlivosťou a v súlade so záujmami spoločnosti a všetkých jej spoločníkov, alebo podľa §82 zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov pri plnení úloh vedúcich zamestnancov.

3.2. Princípy získavania, uchovávania a interpretácie digitálnych dôkazov

Vo väčšine právnych poriadkov a organizácií sa digitálne dôkazy riadia tromi základnými princípmi: relevantnosťou⁷, spoľahlivosťou⁸ a dostatočnosťou⁹. Vzhľadom na chýbajúce jednotné normy a definície sme sa rozhodli riadiť technickými normami a usmerneniami stanovenými v norme ISO 27037 – Usmernenia pre identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov¹⁰, keďže kľúčovými zložkami, ktoré zabezpečujú dôveryhodnosť vyšetrovania, sú metodiky uplatňované počas procesu¹¹, bez zameriavania sa na konkrétne nástroje alebo metódy ako i spôsob identifikácie, získavania a analýzy, ktorý môže byť vykonaný ručne odborne spôsobilou osobou, automatizovane na základe algoritmov, alebo s použitím strojového učenia. Preto je potrebné pri získavaní digitálnych dôkazov dodržiavať určité zásady:

3.2.1. Identifikácia nevyhnutného (primeraného) rozsahu skúmania.

Proces identifikácie zahŕňa vyhľadávanie dostupných úložísk a adries, ktoré obsahujú potenciálne informácie o hľadanom objekte, ktorý by mal byť v nevyhnutný na dosiahnutie účelu. Tento proces zahŕňa aj stanovenie priorít pri zbere informácií na základe ich volatility¹², čo môže zabrániť ich strate alebo minimalizovať škody s cieľom získať najlepšie a originálne informácie vrátane metadát a systémových údajov.¹³

⁷ Relevantnosťou sa rozumie údaj o hodnote informácie pre vyšetrovanie a ktorá predstavuje dôvod na jej získanie, ako je stanovené v norme ISO-EIC 27037, s. 6.

⁸ Atribút konzistentného výsledku a očakávateľných postupov ISO EIC 27037, Pojmy a definície, 3.15

⁹ Informácie odôvodňujúce záver, že bolo zhromaždené také množstvo materiálu na vykonanie analýzy s odôvodnenými závermi. ISO-EIC 27037, s. 6

¹⁰ Publikované v 2012

¹¹ ISO EIC 27037, Úvod

¹² ISO EIC 27037, s.8.

¹³ ISO- EIC 27037, s. 8.

Správna identifikácia a stanovenie priorít informácií týkajúcich sa hľadaného objektu by mali viesť k označeniu iba relevantných informácií. Identifikáciu relevantných informácií by bolo treba vnímať skôr ako mapovanie než ako jednoduché vyhľadávanie, keďže správna dokumentácia identifikácie relevantných informácií sa použije aj v ďalších krokoch.

Nevyhnutný a primeraný rozsah môže byť:

- časový (relevantný interval skúmania), alebo
- obsahový (vyhľadávanie podľa kľúčových atribútov)
- osobný (analýza by nemala pokrývať získavanie informácií o osobách mimo rámec zadania a ak áno, mal by byť tento vzťah jasný a zrozumiteľný- napr. spoločník, osoba žijúca v spoločnej domácnosti atď.).¹⁴

V prípade automatizovaného algoritmu pre identifikáciu je potrebné, aby bolo zdokumentované a vysvetliteľné osobou, ktorá ho používa, na základe čoho a prečo algoritmus dospel k identifikovanému rozsahu. Uvedené je primerané použiteľné i na automatizovanú identifikáciu digitálnych stôp s použitím strojového učenia, tak aby tieto postupy boli overiteľné, transparentné. Nie je teda možné napr. akceptovať, že v prípade postupov strojového učenia využitých na identifikáciu digitálnych stôp ide o obchodné tajomstvo subjektu, ktorý túto identifikáciu vykonal, alebo poskytol aplikáciu resp. Software s týmito prvkami.¹⁵

3.2.2. Akvizícia dostatočného množstva relevantných informácií

Pre lepšie pochopenie je potrebné poznamenať, že norma ISO 27037 rozlišuje medzi zberom a získavaním digitálnych dôkazov:

- zber sa týka fyzického zhromažďovania/odstraňovania fyzických predmetov, ktoré obsahujú potenciálne digitálne dôkazy, a
- získanie znamená vytvorenie kópie údajov z určeného súboru (výsledkom je kópia digitálnych dôkazov)¹⁶

Budeme sa riadiť touto terminológiou a ďalej používať pojem získanie, keďže predmetom digitálnych analýz je získavanie digitálnych údajov, nie fyzických zariadení.

¹⁴ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 13, available on 10.03.2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

¹⁵ US DOJ vs. Sterlingov, Misty Fog, dostupné dňa 29.08.2026 na: <https://caselaw.findlaw.com/court/us-dis-crt-dis-col/115886148.html>

¹⁶ ISO EIC 27037, Pojmy a definície, p. 2

Získanie dostatočného množstva informácií znamená, že je zhromaždené také množstvo materiálu na vykonanie riadnej digitálnej analýzy a odôvodnené zodpovedanie položených otázok, alebo zistených skutočností. Expert, vykonávajúci digitálnu analýzu by mal byť schopný uviesť, koľko materiálu bolo celkovo zohľadnené a zozbierané a aké postupy sa použili na rozhodnutie, koľko a aký materiál sa vyhľadával na účely analýzy vrátane použitia automatického systému zberu s pomocou algoritmov, alebo spôsobov strojového učenia.

Pri získavaní relevantných informácií počas digitálnej analýzy by sa mal *použiť* hash¹⁷, aby sa zachovala integrita a pôvodný stav informácií v čase¹⁸, tak a aby nebolo možné dôkazy po ich získaní upravovať.¹⁹

3.2.3. Evidencia a reťazenie (chain of custody), transparentnosť, preskúmateľnosť a hodnovernosť

Uvádzanie presných údajov a záznamov o využití nosiča informácie ako i identifikácia osoby, ktorá tento nosič informácie využila je nevyhnutné pre možnosť spätného preskúmania²⁰ digitálnej analýzy a jej použiteľnosti ako dôkazu v trestnom konaní.²¹

Princíp evidencie taktiež vyžaduje uvádzať v analýze konkrétne nástroje²², ktoré sa použili pre akvizíciu, obnovu či vyhľadávanie informácií. Účelom je dokumentácia celého postupu

¹⁷ Reťazec bitov, ktorý je výstupom hashovej funkcie . In: ISO EIC 27037, Pojmy a definície

¹⁸ See also Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 58 dostupné 10.03.2026 na:

<https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

¹⁹ ISO-EIC 27037, s. 9

²⁰ Preskúmateľnosť v súlade s ISO 27037, s. 7 znamená i to, že v ktoromkoľvek časovom okamihu počas vykonávania digitálnej analýzy, alebo neskôr pri jej hodnotení, je možné (napr. tretej osobe) sa v tomto procese získavania relevantných informácií pre digitálnu analýzu vrátiť a zopakovať ho, za predpokladu, že uvedené zdroje sú dostupné.

²¹ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 11-12,15 dostupné 10.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

²² Základným predpokladom je využívanie licencovaných nástrojov a postupov, ktorými sa neporušuje právo duševného vlastníctva. Otvorená otázka je pri používaní free verzií forenzných nástrojov, ktoré sú dostupné obmedzený čas, alebo na obmedzený počet úkonov resp. s obmedzenými funkcionalitami. Toto samo

a použitých nástrojov pre prípadné následné preskúmanie a overiteľnosť. Princíp evidencie taktiež vyžaduje, ak analýzu vykonáva viacej osôb, aj dokumentáciu rozsahu konania týchto osôb a spôsobu odovzdávania si informácií a zadaní v čase.²³

Overiteľnosť a hodnotenie digitálnej analýzy nie je možné bez základných údajov o období (kedy sa vykonávala analýza), miestach a zdrojoch použitých v analýze a časovom zakonzervovaní zistených informácií. Uvedené je potrebné najmä preto, že samotná digitálna analýza sa môže použiť ako dôkaz i s väčším časovým odstupom od jej spracovania, kedy určité nástroje použité v čase spracovania už nie sú funkčné, alebo určitý poskytovateľ (najmä sociálna sieť) danú funkcionality už verejne, alebo vôbec nepodporuje.²⁴ Súčasne samotná preskúmateľnosť v spojení s odôvodnením a identifikáciou relevantných informácií pre digitálnu analýzu majú priamy odraz v samotnej hodnovernosti digitálnej analýzy, resp. jej spoľahlivosti.²⁵

Reťazenie evidencie pri identifikovaní a akvizícií dostatočného množstva relevantných informácií je vo svojej podstate chronologická dokumentácia, pozostávajúca z evidencií prístupu osôb a ich činností na tieto digitálne dôkazy v jednotlivých štádiách tak ako bolo uvedené vyššie a ako bude uvedené ďalej.

ISO normy neustanovujú ako dlho sa majú tieto evidencie uchovávať. Vychádzajúc z logiky vecí mali by sa uchovávať rovnakú dobu ako samotná digitálna analýza, najmä v prípade, ak je predpoklad, že takáto digitálna analýza bude zdieľaná aj s inými justičnými alebo vyšetrovacími autoritami, ako dôkaz.²⁶ V zásade možno konštatovať, že doba uchovávanie tejto dokumentácie je determinovaná taktiež partikulárnymi registratúrnymi lehotami pre konkrétny štátny orgán ako pôvodcu registratúry²⁷, ktoré sú stanovené v rezortnom registratúrnym poriadku.²⁸ Pre úplnosť dodávame, že uchovávanie tejto dokumentácie je taktiež potrebné skúmať aj s pohľadu charakteru informácií napr. účtovná

nepredstavuje problém, pokiaľ je tento postup touto free verziou spätne verifikovateľný a jeho použitie nemá vplyv na hodnovernosť záverov.

²³ ISO 27037, s.10-11.

²⁴ Open source investigations in the age of Google / editors, Henrietta Wilson, SOAS University of London, UK & King's College London, UK, Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK. Description: New Jersey : World Scientific, [2024] | Series: Security science and technology, 2059-1063 ; Vol. 4, s. 47

²⁵ ISO 27037, s.6.

²⁶ ISO EIC 27037, s. 10.

²⁷ §16 zákona č. 392/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

²⁸ §17 zákona č. 392/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.

dokumentácia²⁹ resp. zdravotnícka dokumentácia.³⁰ Pre všeobecnú informáciu dodávame, že zákon č. 382/2004 Z.z. o znalcoch , tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v §17 ods. 10 stanovuje povinnosť znalca uchovávať znalecký posudok 10 rokov.

3.2.4. Nestrannosť a nezaujatosť

Tak ako pri akomkoľvek inom vyhľadávaní dôkazov, osoba vyhľadávajúca a hodnotiaca digitálne dôkazy, musí k týmto pristupovať bez zaujatosti a objektívne, bez konfliktu záujmov³¹, ktorý nie len, že nesmie existovať, ale sa nesmie ani javiť- tzv. teória zdania.³²

S poukazom na uvedené je nevyhnutné, aby sa v digitálnej analýze objavilo i zdôvodnenie, ak sa určitý zdroj informácie, alebo nosič nepoužil alebo sa na neho neprihliadalo. V spojení s evidenciou a chain of custody by požiadavku nestrannosti a nezaujatosti digitálnej analýzy mala garantovať osoba, ktorá zodpovedá za celkovú digitálnu analýzu.

²⁹ §35 ods. 1, ods. 2 zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov; §76 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov

³⁰ §22 ods.2, ods.4 až ods. 5 zákona o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

³¹ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 12,15 dostupné 10.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

³² ESĽP rozsudok vo veci PARLOV-TKALČIĆ proti Chorvátsku, č.24810/06, para. 86, dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-96426%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-96426%22]}) ; ESĽP rozsudok vo veci MOISEYEV proti RUSKU, č- 62936/00, para. 184 dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-88780%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-88780%22]}) ; ESĽP rozsudok vo veci ŠAHINER proti TURECKU, č. 29279/95, para: 44 dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-59666%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59666%22]}) ; ESĽP rozsudok vo veci KYPRIANOU proti CYPRUS, č. 73797/01, para: 118 dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-71671%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-71671%22]}) ; ; ESĽP rozsudok vo veci MIKHAIL MIRONOV proti Rusku, č. 58138/09, para: 36 dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-204834%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-204834%22]}) ; ESĽP rozsudok vo veci, KHODORKOVSKIY a LEBEDEV proti RUSKU, č 51111/07 a 42757/07, para: 430 dostupné dňa 11.06.2026 na: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-200333%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200333%22]})

3.2.5. Riziková analýza, taktika, profesionalita³³

Za dodržanie bezpečnosti zvolených forénznych postupov, ktoré by mali byť otestované ešte pred ich aplikáciou na reálny prípad,³⁴ a dotknutých osôb zodpovedajú všetky dotknuté osoby, nielen na digitálnej analýze podieľajúci sa znalec, kriminalistický technik alebo odborník. Profesionalita zúčastnených osôb na digitálnej analýze vyplýva z ich opatrnosti, vedomostí a zručností.³⁵ Za týmto účelom je potrebné prijať opatrenia týkajúce sa infraštruktúry, vrátane hardvéru, softvéru a sietí zapojených do digitálnej analýzy a opatrenia týkajúce sa správania osôb, ktoré sa zúčastňujú v určitej miere tvorby digitálnej analýzy vrátane orgánov činných v trestnom konaní, či operatívnych zložiek.

Riziková analýza, urobená pred samotným vyšetrovaním, taktika a plánovanie digitálnej analýzy by mali zohľadňovať všetky druhy rizík, vrátane technologických, finančných, právnych, fyzických, psychosociálnych. Riziková analýza použitia digitálnych postupov sa musí vysporiadať najmä s otázkami primeranosti odoberania celých nosičov a zariadení, kopírovaním digitálnych informácií a ich rozsahu. oddelia svoje profesionálne aktivity od osobných online aktivít. Osobné zariadenia by sa nemali používať na profesionálne digitálne analýzy a profesionálne zariadenia by sa nikdy nemali používať na osobné aktivity. Všeobecné požiadavky na bezpečnosť zariadení, na ktorých bude osoba vykonávať digitálnu analýzu by sa mali riadiť zásadami kybernetickej bezpečnosti podľa ISO 27001 a to najmä v s prijatím vhodných opatrení na vstupe a prístupových bodoch³⁶, vrátane fyzickej bezpečnosti kancelárií, miestností a zariadení,³⁷ najmä monitoringu z hľadiska neoprávneného fyzického prístupu³⁸ a odpočúvania³⁹ vrátane životného cyklu pamäťových médií počas ich získavania, používania, prepravy a likvidácie a požiadavkami na manipuláciu s nimi⁴⁰. V zásade možno zhrnúť, že pokiaľ uvedená entita, oddelenie, laboratórium je certifikované podľa ISO 27001,

³³ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 44 dostupné 10.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

³⁴ ISO EIC 27037, s. 6

³⁵ Príloha A ISO EIC 27037 Odborník je schopný v priebehu procesu identifikácie informácií definovať informácie, ktoré môžu pomôcť pri vyšetrovaní, ako aj právne predpisy týkajúce sa nakladania s potenciálnymi dôkazmi z OSINT. Určuje požiadavky na nástroje potrebné na zber a získavanie údajov a zariadení a vykonáva posúdenie rizík. V fáze získavania je schopný uplatňovať požiadavky na zabezpečenie opakovateľnosti a auditovateľnosti.

³⁶ Článok 7.2. Fyzický prístup ISO 27001

³⁷ Článok 7.3. Fyzický prístup ISO 27001

³⁸ Článok 7.4. a 7.12 Fyzický prístup ISO 27001

³⁹ Článok 7.10. Fyzický prístup ISO 27001

⁴⁰ Článok 7.6. a 7.13 Fyzický prístup ISO 27001

alebo spĺňa požiadavky ISO 27001, sú splnené i základné požiadavky na digitálnu analýzu v zmysle uvedeného vyššie resp. v zmysle ISO 27037 a ISO 27042.

Identifikácia zraniteľností a ich závažnosti má vplyv na samotné poznanie rizík v procese digitálnej analýzy, ktoré sa týkajú samotnej infraštruktúry a pripojenia, používaných zariadení a úložísk, reputačných rizík ako i samotnej bezpečnosti osôb.

V prípade určenia potreby anonymizácie skúmaných údajov, nasledujúcim nevyhnutným krokom je zabezpečenie, že proces anonymizácie je uskutočnený v súlade s aplikovateľnou právnou úpravou ochrany osobných údajov.

3.3. Štádia digitálnej analýzy

Proces digitálnej analýzy pozostáva z piatich štádií. Sú to:⁴¹

3.3.1. Identifikácia digitálnych informácií

Existujú dva hlavné prístupy pri otvorenom vyšetovaní a vyhľadávaní:⁴²

- vyhľadávanie prostredníctvom všeobecných alebo pokročilých (aktívnych) vyhľadávacích metód; dopyty, algoritmy a parametre by mali byť štruktúrované presne a jasne s určitou mierou kreativity pri prehľadávaní rôznych nosičov. Je potrebné pracovať s rôznymi kľúčovými slovami a domnienkami a predpokladmi, i keď neboli ešte preukázané. Tieto hypotézy však musia vychádzať z vykonaného vyšetovania a musia byť odôvodnené.
- monitoring (sledovanie a pravidelné prehliadanie) obsahu stálych zdrojov; ide o postup, v ktorom sa používajú pravidelne aktualizované kľúčové slová, ktoré spolu súvisia⁴³. Spravidla sa využívajú automatizované nástroje na pravidelný monitoring určitých zdrojov, s cieľom dopĺňania už známych informácií.

⁴¹ Takto uvedené štádia sú v súlade i s technickými normami zaistovania digitálnych dôkazov ISO 27042, str. 4-11 a ISO 27037 str. 6-18, pokiaľ je možné z dokumentácie digitálnej analýzy dovodiť predpísané štandardy, viď vyššie.

⁴² Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 55-56 dostupné 27.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁴³ Tzv. Topic. (poznámka autora)

- *predbežné posúdenie/hodnotenie dát*; pred samotným zberom dostatočného množstva relevantných informácií, je potrebné ich vyhodnotiť a toto hodnotenie zdokumentovať. V prvom rade je potrebné posúdiť relevantnosť informácie a jej kontextových údajov pre dané vyšetrovanie.⁴⁴ Najmä v počiatočných fázach toto určenie môže byť problematické, avšak bez ohľadu na to, by mal byť znalec, alebo odborne spôsobilá osoba vykonávajúci digitálnu analýzu schopný vysvetliť, prečo je alebo by mal byť údaj pre vyšetrovanie relevantný.

Rovnako je potrebné posúdiť spoľahlivosť resp. hodnovernosť dát, čo zahŕňa hodnotenie metadát, prepojených informácií a pôvodného zdroja.

Odborník vykonávajúci digitálnu analýzu by mal posudzovať digitálne informácie a ich nosiče aj z pohľadu, či je pravdepodobné, že digitálna informácia bude odstránená, alebo k nej bude zamedzený prístup. Pravdepodobnosť odstránenia obsahu možno posúdiť na základe viacerých faktorov, charakteru nosiča, umiestnenia obsahu a súladu obsahu s podmienkami používania poskytovateľa služieb.

3.3.2. Zhromažďovanie dát

Ide o postup, ktorý je opísaný vyššie a zahŕňa v sebe viaceré spôsoby akvizície dát.

3.3.3. Uchovávanie dát

Vo všeobecnosti platí, že dáta sa uchovávajú z dôvodu ich dostupnosti a použiteľnosti vo vyšetrovaní tak aby bola zachovaná ich pôvodnosť, dostupnosť, určiteľnosť.⁴⁵ Toto sa dosahuje práve reťazením dokumentácie, dôkaznými, záložnými a pracovnými kópiami údajov, hashovaním.⁴⁶ Aby bolo možné toto zachovať, je potrebné jednotlivé informácie ako digitálne dôkazy označovať a dokumentovať, kto, kedy k nim pristupoval a čo s nimi vykonal.⁴⁷ Platí pravidlo, že samotná analýza a práca s digitálnou informáciou sa vykonáva na pracovnej kópii, nie na originály alebo dôkaznej kópii.⁴⁸ Dosiahnutie pôvodnosti, dostupnosti

⁴⁴ Pozri vyššie

⁴⁵ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s 61 dostupné 27.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁴⁶ Vid' vyššie.

⁴⁷ ISO EIC 27037, s.10

⁴⁸ ISO EIC 27037, s. 25

a určiteľnosti dát sa spravuje vo všeobecnej rovine zásadami kybernetickej bezpečnosti, tak ako sú stanovené v ISO 27001. Na dosiahnutie súladu uchovávaných dát so všeobecnými štandardmi kybernetickej bezpečnosti podľa ISO 27001 je potrebné aby boli informácie uložené v koncových zariadeniach používateľa, spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich chránené⁴⁹, najmä pridelovaním a používaním obmedzených a riadených privilegovaných prístupových práv⁵⁰ a technológií a postupov bezpečnej autentizácie,⁵¹ opatrenia na prevenciu úniku údajov,⁵² vytvárania záložných kópií a pravidelne testovania v súlade s dohodnutou špecifickou politikou zálohovania,⁵³ vytvárania, uchovávanía, ochrany a analýzy logov o činnosti, poruchách a výnimkách,⁵⁴ synchronizácie systémových hodín,⁵⁵ segregácia rolí⁵⁶, manažmentu prístupu k externým webovým stránkam,⁵⁷ pravidiel efektívneho používania kryptografie vrátane správy kryptografických kľúčov,⁵⁸ a zásad bezpečného kódovania,⁵⁹ oddelených a zabezpečených vývojových, testovacích a produkčných prostredí musia byť oddelené a zabezpečené.⁶⁰

3.3.4. Overovanie dát a postupov

Overovanie dát sa uskutočňuje jednak vo vzťahu k iným zdrojom alebo nosičom.. Vo všeobecnosti sa pri overovaní informácií posudzuje najmä spoľahlivosť zdroja a overiteľnosť (dôveryhodnosť) informácie v matici 4x4 resp. 6x6⁶¹, kde A1 je informácia od vždy spoľahlivého zdroja, ktorá je potvrdená, alebo potvrditeľná iným zdrojom, pričom kategória informácie D4

⁴⁹ Článok 8.1. Technologické opatrenie ISO 27001

⁵⁰ Článok 8.2. Technologické opatrenie ISO 27001

⁵¹ Článok 8.5. Technologické opatrenie ISO 27001

⁵² Článok 8.12. Technologické opatrenie ISO 27001

⁵³ Článok 8.13. Technologické opatrenie ISO 27001

⁵⁴ Článok 8.15. Technologické opatrenie ISO 27001

⁵⁵ Článok 8.17. Technologické opatrenie ISO 27001

⁵⁶ Článok 8.20. a 8.22. Technologické opatrenie ISO 27001

⁵⁷ Článok 8.23. Technologické opatrenie ISO 27001

⁵⁸ Článok 8.24. Technologické opatrenie ISO 27001

⁵⁹ Článok 8.28. Technologické opatrenie ISO 27001

⁶⁰ Článok 8.31. Technologické opatrenie ISO 27001

⁶¹NATO AJP-2.1 Source Reliability and Information Credibility Scales, available at: https://cld.pt/dl/download/40e71e02-28d0-4c6e-b2f4-248aebd8ca49/CPOS_HERANCA/Fase%20Conjunta/Anexos/6-AEOM/%28DCM%29%20-%20Doutrina%20Militar%20Conjunta/Refer%C3%A2ncias%20Bibliogr%C3%A1ficas%20Gerais/AJP-2.1%20EDB%20V1%20E_JUN16.pdf?download=true

resp. F6 pochádza od predtým neznámeho zdroja a ktorá sa nedá inak overiť.⁶² Taktiež je súčasťou tohto posudzovania určitosť (resp. presnosť) alebo vágnosť informácie.⁶³

3.3.5. Analýza a interpretácia dát

Samotná analýza pozostáva z:

- analýzy meta dát a
- analýzy obsahu.

Metadáta sú údaje, ktoré opisujú iné údaje a poskytujú o nich informácie. Môžu ich vytvoriť používateľ, ktorý daný objekt vytvoril, iní používatelia, poskytovateľ komunikačných služieb alebo akékoľvek zariadenie, na ktorom sa údaje vytvárajú, prenášajú, prijímajú alebo prezerajú. Metadáta sú dôležité pre opis objektu a okolností jeho vytvorenia, šírenia alebo úpravy. Metadáta môžu zahŕňať autora súboru, dátum jeho vytvorenia, údaje o nahratí, úpravy, veľkosť súboru a lokalizačné dáta. Ďalej sú súčasťou meta dát i obrázkové formáty s doplnkovými údajmi o fotoaparátoch, scanneroch apod, či informácie o zdrojových kódach programovaných stránok, ktoré môžu obsahovať skrytý či upravený obsah a zobrazí štruktúru odkazov a nefunkčné odkazy.⁶⁴

Analýza obsahu predstavuje napr. geolokáciu podľa polohy objektu, činnosti alebo miesta, z ktorého bol určitý prvok vytvorený, Takéto techniky môžu zahŕňať napríklad identifikáciu jedinečných geografických prvkov na fotografii a ich skutočnú polohu na mape. Pre samotnú analýzu obsahu môže byť nevyhnutné ďalšie spracovanie údajov, napr. preklady, zmeny formátov. Akékoľvek spracovanie digitálneho objektu musí byť dokumentované (chain of

⁶² Tamtiež.

⁶³ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s 63 dostupné 10.03.2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁶⁴ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s 64 dostupné 10.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

custody).^{65 66} Tento postup predpokladá i digitálna analýza a vyťaženie dát ako „príprava“ pre ďalšiu odborne spôsobilú osobu napr. antropológa, pediatra, audítora, účtovníka, lingvistu, prekladateľa apod.

Ide o cyklus, ktorý sa môže opakovať i viackrát, keďže môžu vyjsť najavo nové informácie. Osoby vykonávajúce digitálnu analýzu sú povinné dokumentovať svoje činnosti počas každej fázy.⁶⁷

Pre analýzu a interpretáciu digitálnych stôp, ktoré majú byť použiteľné ako dôkazy v trestnom konaní platí, že táto musí byť v poslednom kroku vždy posúdená odborne spôsobilou osobou, hoci s pomocou algoritmov automatizovaným spôsobom alebo zásad a postupov strojového učenia. Je nevyhnutné boli analytické výstupy vždy verifikované človekom a súčasne vysvetliteľné, transparentné a overiteľné. Nie je teda možné napr. akceptovať, že v prípade postupov strojového učenia využitých na identifikáciu digitálnych stôp ide o obchodné tajomstvo subjektu, ktorý túto identifikáciu vykonal, alebo poskytol aplikáciu resp. software s týmito prvkami.⁶⁸

Zistenia digitálnej analýzy, ktoré sa týkajú buď zhromaždených údajov, alebo záverov vyvođených z týchto údajov, môžu byť v trestnom stíhaní využité dôkazným prostriedkom pri dodržaní horeuvedených zásad, prostredníctvom:⁶⁹

- výsluchu osoby (ústne) vrátane výsluchu prostredníctvom videokonferencie. Pri výsluchu je možné použiť i vizualizácie digitálnej analýzy formou poznámok.

⁶⁵ Vid' vyššie

⁶⁶ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s 65-67

dostupné 10.03.2026 na: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁶⁷ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s 66 dostupné na 10.03.2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁶⁸ US DOJ vs. Sterlingov, Misty Fog, dostupné dňa 29.08.2026 na: <https://caselaw.findlaw.com/court/us-dis-crt-dis-col/115886148.html>

⁶⁹ Acc. Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Center and UN Human Rights Office of the High Commissioner; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, s. 82 dostupné 10.03.2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

- alebo písomne prostredníctvom odborného vyjadrenia, či znaleckého posudku. Súčasťou písomného odborného vyjadrenia, znaleckého posudku môžu byť i vizualizácia výsledkov a postupov pri tvorbe digitálnej analýzy, doplnený o prípadný výsluch osoby podľa bodu vyššie.

Z pohľadu právneho posúdenia je pritom irelevantné, či bola identifikácia, zber a uchovanie vykonané manuálne odborne spôsobilou osobou, alebo automatizovaným spôsobom. Zmyslom a účelom horeuvedených postupov je najmä zákonnosť získania, autenticitu, integritu, hodnovernosť, zachovanie dokumentácie postupu a možnosť jeho následného preskúmania.

Hore uvedené rozobraté postupy zabezpečia, že elektronický dôkaz bude spĺňať tieto podmienky:

- zákonnosť- dôkaz musí byť získaný zákonom predpísaným spôsobom;
- autentickosť -pravosť, musí existovať príčinná súvislosť medzi dôkazom a skutkom;
- integrita- dôkaz musí byť ucelený a nezmenený;
- spoľahlivosť- spôsob získania dôkazu a manipulácia s ním nesmie v žiadnom prípade vzbudzovať dôvodné pochybnosti o autenticnosti a hodnovernosti dôkazu);
- hodnovernosť - za hodnoverný dôkaz možno považovať iba taký dôkaz, ktorý bol získaný zákonom predpísaným spôsobom, a zároveň neexistujú dôvodné pochybnosti o jeho pravosti, integrity a spoľahlivosti).

Použitie uvedenej metodiky poskytne prevádzkovateľovi základnej služby určitú mieru právnej istoty podľa §19 ods.6, písm. d) ZKB v postupe riešenia kybernetického bezpečnostného incidentu, tak aby digitálne stopy z riešeného kybernetického incidentu boli použiteľné ako dôkazy v trestnom konaní. Pre tieto účely je obzvlášť potrebné postupovať podľa uvedenej metodiky, nakoľko zákon ustanovuje právnu povinnosť konať tak, aby zaistené digitálne stopy kybernetického bezpečnostného incidentu boli použiteľné v trestnom konaní ako dôkazy, avšak nestanovuje postup ako má prevádzkovateľ základnej služby postupovať, aby túto zákonnú povinnosť splnil.