

Digitální forenzní analýza

***e*FOCUS**

Digitální forenzní analýza

Ing. Marián Svetlík

svetlik@rac.cz

Risk Analysis Consultants, s.r.o.



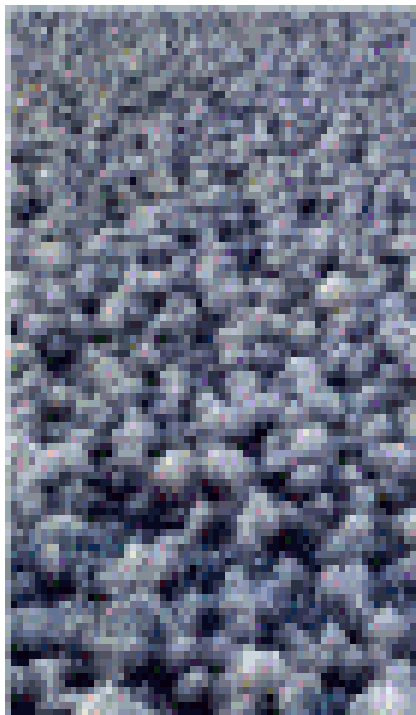
RISK ANALYSIS CONSULTANTS



Obsah

- Co lze forenzní analýzou odhalit?
- Jaké chyby se vyskytují?

Co to je Digitální Forenzní Analýza?



Analýza

Za použití našich forenzních neboli vyšetřovacích technik analyzujeme získaná data. Výsledkem naší činnosti v této fázi jsou zprávy o konkrétních zjištěních včetně identifikace klíčových problémů a závěrečných doporučení v záležitostech, které náš tým posuzoval.

„Za použití našich forenzních neboli vyšetřovacích technik analyzujeme získaná data“

Co to je Digitální Forenzní Analýza?

- **Obecné zásady forenzní práce**

1. Kroky podniknuté pro zajišťování a shromažďování digitálních důkazů by neměly ovlivnit jejich integritu
2. Osoby provádějící zkoumání digitálních důkazů by měly být pro tuto činnost vyškoleni a pravidelně proškoleni
3. Všechny prováděné činnosti by měly být zdokumentovány a záznamy zabezpečeny tak, aby byly dostupné pro případné přezkoumání

ACPO - Good Practice Guide for Computer-Based Electronic Evidence

Co to je Digitální Forenzní Analýza?

- Atributy forenzní analýzy
 - Integrita
 - Opakovatelnost/Přezkoumatelnost
 - Legalita
 - Nezávislost
 - Odbornost
 - Dokumentace

Digitální Forenzní Analýza

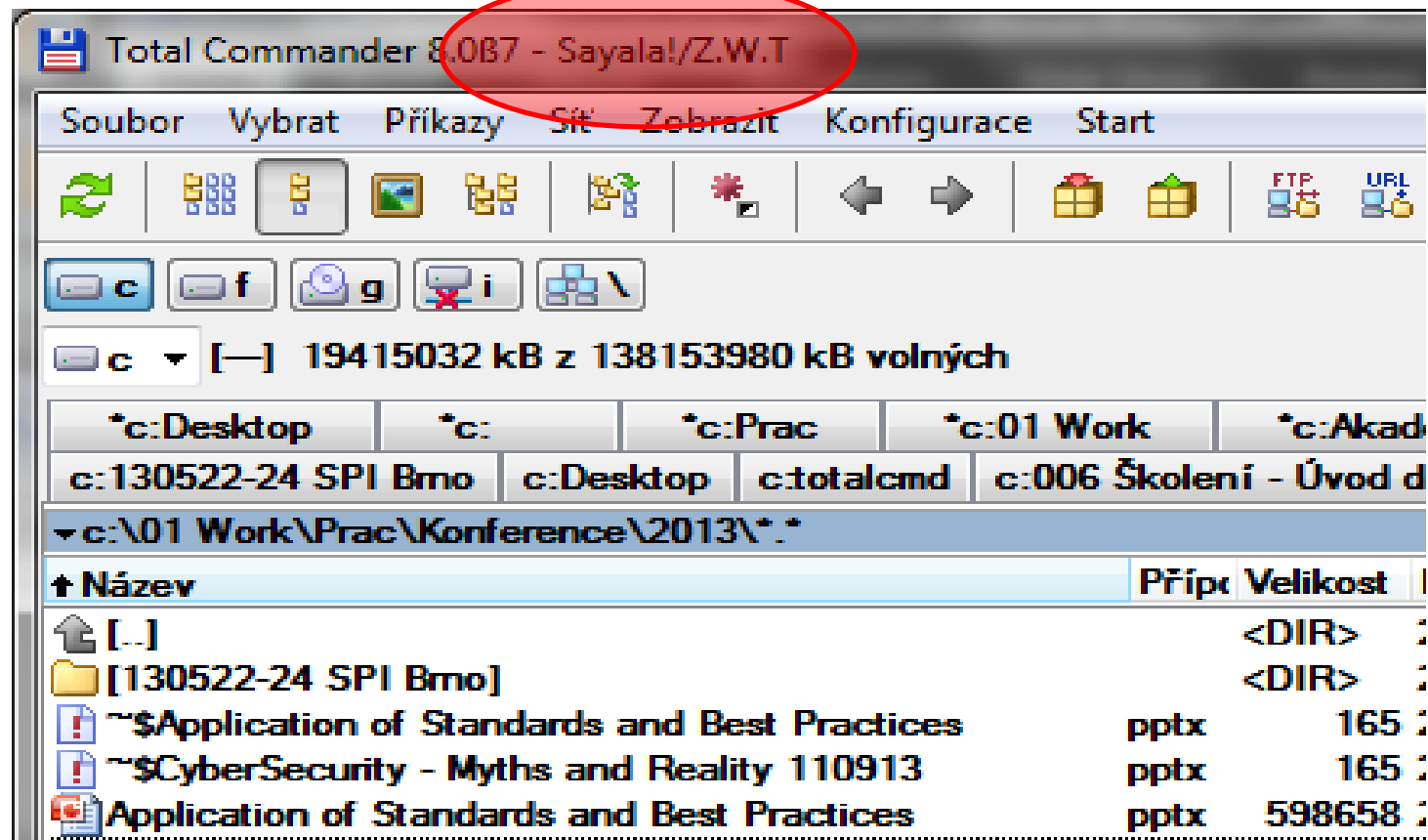
- Integrita

Digitální Forenzní Analýza

- Opakovatelnost /Přezkoumatelnost

Digitální Forenzní Analýza

- Legalita



Digitální Forenzní Analýza

- Nezávislost

a postupu zkoumání není možné tento opakovat a ověřit správnost tvrzení.

Příklad pravděpodobného narušení zásady Nepodjatosti

BOX 4

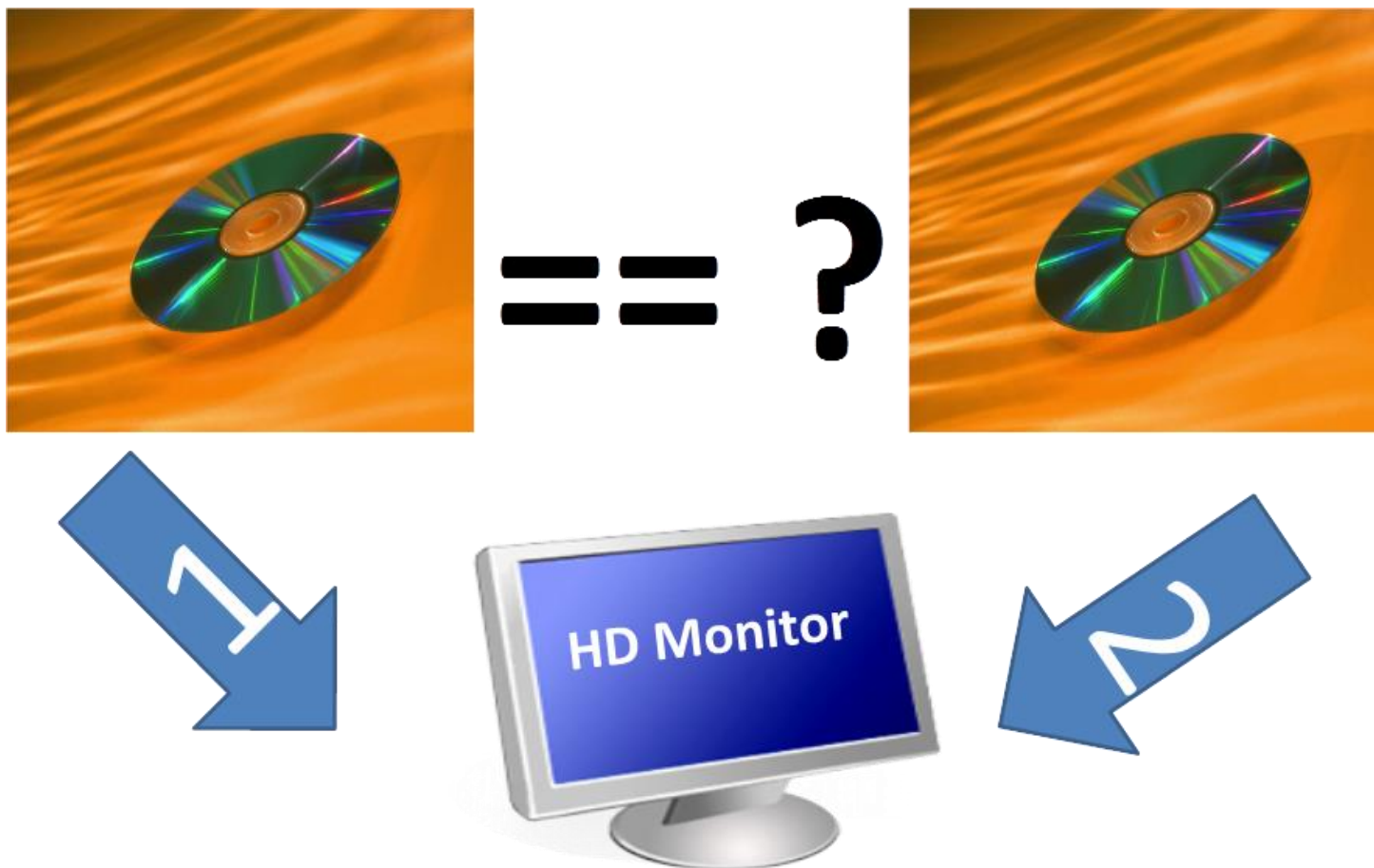
Znalec ve vyjádření k nezávislosti na zkoumaném objektu a subjektu píše, že sice instaloval posuzovaný systém u klienta, avšak toto bylo prováděno na základě smlouvy o dílo a zpracování znaleckého posudku na tento systém se řídí trestním řádem, tudíž se jedná o úplně jiný právní vztah. Podjatost je tedy z jeho strany vyloučena.

Příklad nedostatečné dokumentace

BOX 5

Digitální Forenzní Analýza

- Odbornost



Digitální Forenzní Analýza

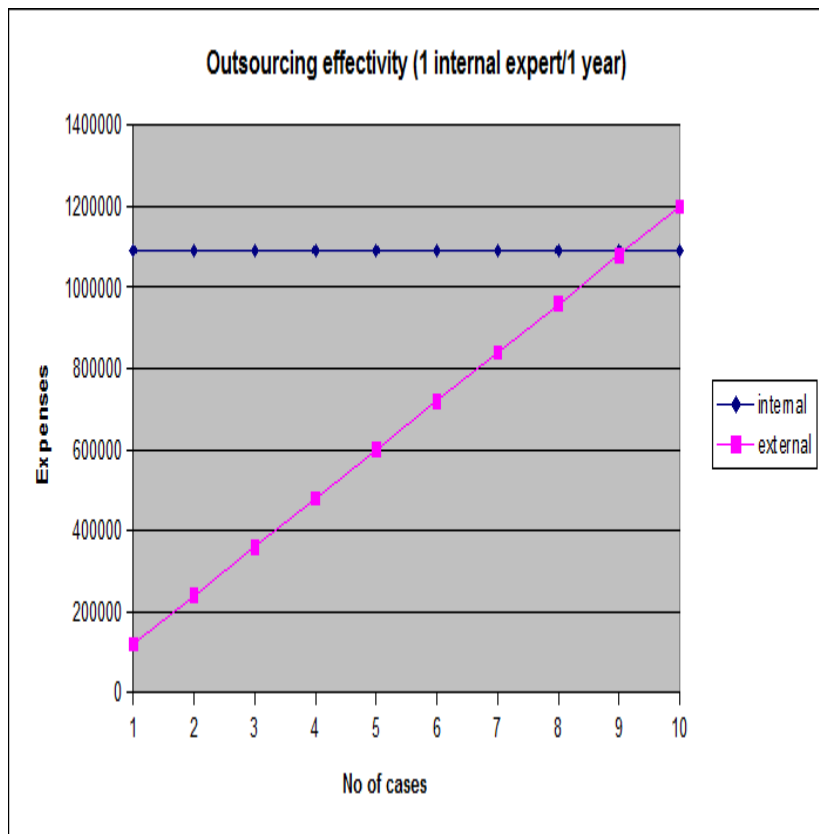
- Dokumentace



Co dokáže odhalit?

- Cokoliv, co lze v digitálních datech najít

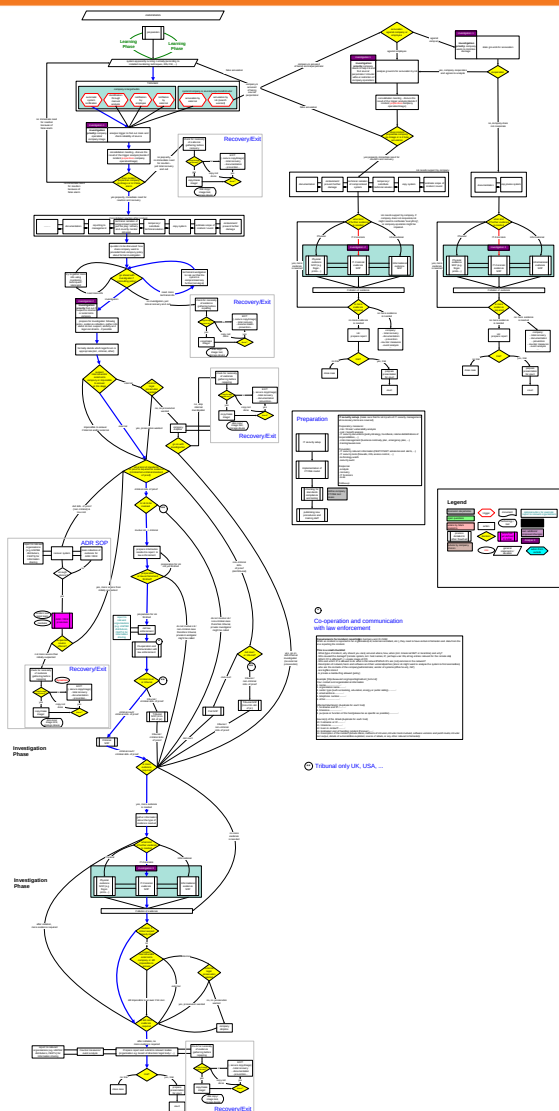
Kdy dělat forenzní analýzu?



- Podezření z trestného činu
- Regulatorní požadavky
- Interní incidenty a jejich šetření
- Pojištění rizik ICT

Interní forenzní tým – zjednodušená kalkulace nákladů

Mít interní forenzní tým?



- Ano, když na to máte
 - Pozor na podjatost
 - Pozor na ekonomickou efektivitu
 - V zásadě jen pro interní šetřerní

Workflow šetření interního incidentu

Jaké chyby se vyskytují?

- Nedělá se když je potřeba
- Nesplňuje atributy forenzní analýzy



Děkuji za pozornost

***e*FOCUS**
