

# Posudek práce

předložené na Přírodovědecké fakultě JU

- |  |   |
|--|---|
| <input type="checkbox"/> posudek vedoucího           | <input type="checkbox"/> posudek oponenta |
| <input checked="" type="checkbox"/> bakalářské práce | <input type="checkbox"/> diplomové práce  |

Autor/ka: Doule František

Název práce: Zařízení pro dokumentaci a analýzu forenzních stop z oblasti informačních technologií

Studijní program a obor: Měřicí a výpočetní technika

Rok odevzdání: 2013

Jméno a tituly vedoucího/opponenta: Ing. Machala Tomáš

Pracoviště: Krajské ředitelství policie Jihočeského kraje, Odbor kriminalistické techniky a expertíz, České Budějovice

Kontaktní e-mail: tomas.machala@atlas.cz

## Odborná úroveň práce:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

## Věcné chyby:

- téměř žádné  vzhledem k rozsahu přiměřený počet  méně podstatné četné  závažné

## Výsledky:

- originální  původní i převzaté  netriviální kompilace  citované z literatury  opsané

## Rozsah práce:

- veliký  standardní  dostatečný  nedostatečný

## Grafická, jazyková a formální úroveň:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

## Tiskové chyby:

- téměř žádné  vzhledem k rozsahu a tématu přiměřený počet  četné

## Celková úroveň práce:

- vynikající  velmi dobrá  průměrná  podprůměrná  nevyhovující

### **Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:**

Cílem práce je vytvoření jednoduchého zařízení umožňující provádění bitových kopií paměťových médií za účelem forenzního zkoumání.

V první části byl dostatečně popsán problém zálohování paměťových médií pro účely forenzního zkoumání s prostředky systému GNU/Linux, které jsou běžně používané pro praxi a byly zde představeny softwarové prostředky pro forenzní zkoumání. V druhé části je popsáno samotné zařízení a jeho návrh, které je navrženo s důrazem na jednoduchost a přehlednost při pořizování bitových kopií paměťových médií. V případě nahrazení hardware za rozměrově menší by toto zařízení mohlo plně nahradit v práci zmíněný duplikátor.

Práce je napsána přehledně, velikost jednotlivých kapitol je úměrná jejich významu. Po formální stránce (jazykové, terminologické, grafické) je předložená práce vypracována pečlivě, bez hrubých nedostatků. Cíle práce byly splněny a v rámci forenzního zkoumání je zařízení plně použitelné.

### **Případné otázky při obhajobě a náměty do diskuze:**

- V návrhu je prováděn test velikosti cílového média. Jakým způsobem musí být testována velikost kapacitně stejně velkých paměťových médií (zdrojového i cílového), tak aby byla korektně provedena záloha zdrojového média?
- Zařízení využívá příkaz `dcfldd`. Jaký parametr tohoto příkazu zamezí ukončení procesu, pokud se při běhu zálohy vyskytne na paměťovém médiu chyba, např. nečitelný sektor a jak uživatel pozná, že nedošlo k přečtení tohoto sektoru?

**Práci**

doporučuji

nedoporučuji

uznat jako diplomovou/bakalářskou.

**Navrhuji hodnocení stupněm:**

výborně  velmi dobře  dobře  neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích dne 17.května 2013

Ing. Machala Tomáš



