Posudek práce

předložené na Přírodovědecké fakultě JU

❑posudek vedoucího ☑posudek oponenta
☑ bakalářské práce ❑ diplomové práce

Autor/ka: **Marek Šobra**
Název práce: **Vytvoření forenzní live distribuce Linuxu za použití volně šiřitelných aplikací**
Studijní program a obor: Aplikovaná informatika, Kriminalisticko-technická činnost v IT
Rok odevzdání: 2017

Jméno a tituly vedoucího/oponenta: Ing. Tomáš Machala
Pracoviště: Krajské ředitelství policie Jihočeského kraje
Odbor kriminalistické techniky a expertíz
České Budějovice
Kontaktní e-mail: tomas.machala@pcr.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 bylo vytvoření funkční forenzní live distribuce linuxového systému, který obsahuje volně dostupné základní forenzní aplikace a zastřešení těchto aplikací pod jeden obslužný program, jenž by usnadnil jejich spouštění. Jako výchozí jazyk pro linuxovou distribuci a aplikace byl zvolen jazyk český.

První část práce je věnována základnímu seznámení s problematikou digitálních stop, jejich zajišťování v rámci trestního řízení a popisu přípravy před jejich zajištěním v závislosti na jejich umístění.

Další část práce představuje použitou distribuci systému Linux a volně dostupné forenzní aplikace pro systémy Linux. Ty jsou chronologicky řazené podle postupu při zajišťování dat, a to od zajištění bytové kopie paměťového média či operační paměti a aplikace pro výpočet kontrolních součtů, zajišťující úplnost a správnost dat, přes aplikace pro extrakci dat z paměťového média, až po analytické nástroje. Samotná obslužná aplikace je popsána v poslední části práce.

Live distribuce Lubuntu byla prověřena z hlediska funkčnosti. Všechny popsané aplikace byly funkční a obsahovaly popisy a návody v českém jazyce.

Text práce je sestaven přehledně, bez závažných chyb a je doplněn přehlednou grafikou a popisy. Celkově hodnotím práci jako zdařilou, byla výborně zvládnuta teorie a následné sestavení live distribuce.

Z uvedených důvodů hodnotím práci výborně a doporučuji k obhajobě.

Případné otázky při obhajobě a náměty do diskuze:

- Jaké jiné volně dostupné live forenzní distribuce linuxu znáte?
- Existují volně dostupné linuxové aplikace pro získání dat z messengerů či mobilních telefonů?

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 9.5.2017 Ing. Tomáš Machala