

Posudek práce

předložené na Ústavu Aplikované Informatiky Přírodovědecké fakulty JU

posudek oponenta bakalářské práce

Autor: Martin Dobiáš

Název práce: Automatizace forenzního zkoumání – forenzní audit pro účely zjištění porušování autorských práv

Studijní obor: Aplikovaná informatika – specializace Bezpečnost a sítě

Datum odevzdání: 24.4.2015

Jméno a tituly oponenta: Ing. Tomáš Machala

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

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

Odborná úroveň práce:	vynikající
Věcné chyby:	téměř žádné
Výsledky:	originální
Rozsah práce:	standardní
Grafická, jazyková a formální úroveň:	velmi dobrá
Tiskové chyby:	téměř žádné
Celková úroveň práce:	velmi dobrá

Slovní vyjádření, komentáře a připomínky vedoucího práce:

Cílem práce bylo vytvoření aplikace umožňující provádění analýzy instalovaného software a hledání možných cracků z bitové kopie disku s OS Windows za účelem forenzního zkoumání, ve vztahu k možnému porušování autorských práv.

Aplikace nazvaná pyAnalyzator byla navrhována na platformě OS Linux Ubuntu v programovacím jazyce Python. Jedná se o malou, přehlednou a stabilní aplikaci s jednoduchým ovládáním. Testováním aplikace nebyly zjištěny žádné závažné chyby a výsledky odpovídaly exportům z jiných forenzních nástrojů. Nevýhoda aplikace je možnost načtení pouze bitové kopie s příponou img, neboť v praxi jsou hojně využívány i jiné formáty (např. dd, 000, atd.).

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:

Je možné, aby program mohl načítat bitové kopie i jiných formátů vytvořených příkazem dd, jako jsou přípony dd, 000, či komprimovanou image EnCase Image File s příponou E01?

Práci **doporučuji** uznat jako **bakalářskou**.

Navrhuji hodnocení stupněm: výborně

Místo, datum a podpis oponenta: České Budějovice: 11.5.2015

