Posudek práce

předložené na Přírodovědecké fakultě JU

☐posudek vedoucího ☑posudek oponenta
☐ bakalářské práce ☑ diplomové práce

Autor/ka:	**Bc. Vojtěch Novotný**
Název práce:	**Forenzní analýza mobilních zařízení s operačním systémem Android**
Studijní program a obor:	Aplikovaná informatika
Rok odevzdání:	2016

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@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 bylo zhodnocení, popis a metodika forenzního zkoumání na zařízeních s operačním systémem Android. Navržený postup forenzní analýzy byl následně porovnáván s komerčně využívanými forenzními nástroji.

V první části práce byla popsána architektura operačního sytému Android a rozdělení používaných souborových systémů pamětí zařízení. Dále byly dostatečně popsány druhy dat, které zařízení obsahují, a je možné tyto získat forenzní analýzou.

Další část práce se již zabývá samotnou přípravou a zpřístupněním dat z mobilního zařízení pro potřeby forenzního zkoumání. Autor zde popsal postupy pro získání dat z pamětí zkoumaných zařízení, jejich specifika a následně možnosti zpřístupnění a analýzy těchto dat. Jsou zde detailně rozebrány umístění a vlastnosti dat jednotlivých aplikací jako jsou Kontakty, Zprávy SMS a MMS, Výpis hovorů, ale i například Facebook, Skype či další komunikační programy, které jsou důležité vzhledem k zajištění digitálních důkazů při forenzní analýze, ale i umístění základních dat o mobilním zařízení.

V závěru práce jsou představeny komerčně využívané forenzní nástroje, se kterými jsou následně porovnány výsledky zkoumání.

Text je napsán přehledně, bez závažných chyb a je doplněn přehlednou grafikou. Celkově hodnotím práci jako zdařilou, byla dostatečně zvládnuta teorie, navržen postup vytěžení zařízení a nalezena všechna důležitá data.

Z uvedených důvodů hodnotím práci výborně a doporučuji k obhajobě.

Případné otázky při obhajobě a náměty do diskuze:

- V práci byla zmíněna duplicitní SIM karta. Je možné tuto kartu vytvořit bez znalosti PIN nebo PUK kódu karty originální?
- Odebrání paměťové karty ze zapnutého systému může způsobit zničení tohoto paměťového média, navrhněte jiný, než popsaný způsob analýzy a pořadí zkoumání jednotlivých částí z vypnutého mobilního telefonu.
- Komerční systém UFED umožňuje provádět u některých typů zařízený tzv. „Výpis souborového systému". Jaká data z tohoto výpisu je možné získat?

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou.

Navrhuji hodnocení stupněm:
☑ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta: Ing. Tomáš Machala
V Českých Budějovicích dne 11. 5. 2016

Posudek práce

předložené na Přírodovědecké fakultě JU

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

Autor/ka:	**Bc. Vojtěch Novotný**
Název práce:	**Forenzní analýza mobilních zařízení s operačním systémem Android**
Studijní program a obor:	Aplikovaná informatika
Rok odevzdání:	2016

Jméno a tituly vedoucího/oponenta:	Mgr. Jakub Kothánek
Pracoviště:	Ústav aplikované informatiky, PřF JČU
Kontaktní e-mail:	jakub.kothanek@it-znalec.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 zhodnocení, popis a vytvoření metodiky pro forenzní zkoumání na zařízeních s operačním systémem Android. Navržený postup forenzní analýzy byl následně porovnáván s komerčně využívanými forenzními nástroji.

V prvé části byl detailně rozebrán operační systém Android, jeho totožné rozdílné znaky s operačními systémy vytvořenými s jádrem Linuxu. Dále se autor zabýval možnostmi vytěžení jednotlivých typů dat.

Ve druhé části práce se autor zabývá přípravou zařízení pro forenzní analýzu a samotné analýze a jejími možnostmi. Velice kvituji popsanou možnost tzv. Rootnutí zařízení, díky kterému lze využít fyzickou analýzu na jakémkoli zařízení s operačním systémem Linux. Dále se autor zabývá umístěním jednotlivých typů dat a aplikací.

Nakonec autor představuje komerční řešení forenzní analýzy (nástroje jako UFED, apod.), se kterými své výsledky porovnává.

Vynikající odbornou úroveň práce znehodnocuje veliké množství gramatických chyb a chybějící interpunkce v souvětích. Jinak je text napsán přehledně, členění textu se jeví také logicky. Zdařilé se jeví i obrázky, které dokreslují výsledky diplomové práce.

Celkově hodnotím práci jako velice zdařilou, veliká škoda je gramatických chyb a chybějící interpunkce, kdy toto znevažují kvalitu práce.

Z uvedených důvodů hodnotím práci velmi dobře a doporučuji k obhajobě.

Případné otázky při obhajobě a náměty do diskuze:

Probíhá instalace podpůrné aplikace u všech typů extrakcí?
Lze nějakým způsobem dosáhnout možnosti fyzické analýzy i u oficiálně nepodporovaných zařízení?

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 13.5.2016 Mgr. Jakub Kothánek