FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Mgr. Dominik Novák
Student:	Šárka Nádvorníková
Název práce:	Forenzní analýza dat mobilní aplikace
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	6. června 2024

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Práce je vypracována v souladu se stanoveným zadáním. V úvodní části je popsán způsob ukládání dat v mobilních zařízeních s operačními systémy iOS a Android. V následujících kapitolách jsou obecně představeny možné způsoby zajištění dat z mobilních zařízení včetně ukázky analýzy aplikace. Tyto znalosti jsou dále použity v praktické části této práce.

2. Písemná část práce

70 / 100 (C)

Z formálního hlediska splňuje předaná práce všechny náležitosti. Kapitoly jsou logicky členěny a svým obsahem na sebe navazují. Z jazykového a typografického hlediska práce nebyly shledány zásadní nedostatky. Citace splňují požadavky.
Obsahově nelze vytknout podstatné nepřesnosti. V praktické části do jisté míry studentka využívá nabyté znalosti z teoretické části. Je však patrné, že některým tématům bylo vhodné věnovat více prostoru a jiné nebylo nutné studovat do hloubky. Jedná se zejména o kapitoly popisující způsob ukládání aplikačních dat, kde studentka vycházela zejména developerské dokumentace, která může posloužit jako základní zdroj, avšak většina obsahu je pro digitální forenzní analýzu zbytná. Zároveň úplně chybí příklady použití popsané teorie, čtenář tedy může postrádat souvislosti teoretického základu s praxí. Rovněž chybí bližší specifikace běžných artefaktů digitální forenzní analýzy v kombinaci s popsanými zdroji. V práci není blíže popsán ani rozsah zajištěných dat s ohledem na použitou metodu zajištění, která jak v ukázkové aplikaci WhatsApp, tak analyzované aplikaci Vinted může při analýze hrát zásadní roli.
Tyto nedostatky však studentka v praktické části překonala a jednotlivé kapitoly obsahově bez výhrad odpovídají stanoveným cílům práce v požadované kvalitě.

3. Nepísemná část, přílohy 75 /100 (C)

Pro účely zpracování nalezených dat byl vytvořen Python skript. Studentka vhodně zvolila výběr dat a skript tedy vybírá jen zájmové artefakty z identifikovaných souborů. Výstup ve formátu PDF je dobře strukturovaný a lze jej použít pro prezentaci analyzovaných dat. Díky tomu, že je skript jednoduchý, je možné jej upravovat pro konkrétní potřeby forenzního zkoumání, popř. při aktualizaci aplikace, tedy při možné změně organizace artefaktů.

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Praktická část práce ukazuje, že výsledný skript je použitelný pro analýzu dat aplikace Vinted. Přestože použití skriptu není plně automatizované, tedy neumí zájmové soubory nalézt přímo ve výstupu extrakce zařízení, je nástroj přímo použitelný pro potřeby analytiků s dalšími možnostmi personalizace. Vzhledem k tomu, že aplikace Vinted je hojně využívána v České republice a jejím blízkém okolí, kterou trh nástrojů s digitální forenzní analýzou často opomíjí, přináší práce nový jednoduchý nástroj použitelný pro potřeby místních odborníků.

Celkové hodnocení 75 /100 (C)

Přestože v úvodní části se studentka drobně odchylovala od teorie digitální forenzní analýzy, v praktické části se této úlohy zhostila ve velmi dobré kvalitě a výsledek práce naplňuje stanovený cíl.

Otázky k obhajobě

Proč je pravděpodobně pro zájmová data použita popsaná datová struktura a ne zmíněná SQLite databáze?
Lze tvrdit, že se jedná o kompletní uživatelská data aplikace Vinted?
Jaké metody extrakce by bylo nutné zvolit při potřebě zajištění obdobných dat z OS Android?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.