Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Jaromír Bobek

Název práce: Forenzní analýza diskových úložišť – video tutoriály

Autor posudku: Ing. Tomáš Svoboda, Ph.D.

Cíl práce: Cílem práce je vytvořit videotutoriály v oblasti forenzní analýzy diskových úložišť

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☐	☒	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☐	☐	☒	☐	☐
Zpracování praktických aspektů tématu	☐	☐	☒	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☐	☐	☒	☐	☐
Hloubka a správnost provedené analýzy	☐	☐	☐	☒	☐	☐
Práce s literaturou	☐	☐	☐	☐	☒	☐
Logická stavba a členění práce	☐	☐	☒	☐	☐	☐
Jazyková a terminologická úroveň	☐	☐	☐	☐	☒	☐
Formální úprava a náležitosti práce	☐	☐	☐	☒	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☒	☐	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 0 %.

Dílčí připomínky a náměty:

Autor nevyužíval pravidelné konzultace s vedoucím bakalářské práce. Dopad této skutečnosti je patrný v následujících připomínkách a v celkovém posouzení práce.
Vedoucí práce má následující připomínky a náměty k předložené práci:

1. Předložená práce je v částech textu psaná s využitím 1. osoby jednotného čísla.
2. Metodika zpracování obsahuje následující otázky, na které ale nejsou uvedeny exaktní odpovědi:
    a. Jaké jsou hlavní rozdíly ve způsobu ukládání dat mezi HDD a SSD?
    b. Jaká data lze obvykle z disku získat běžně dostupnými forenzními nástroji?
    c. Jsou výrazné rozdíly v principu ukládání dat programu mezi jednotlivými webovými prohlížeči?
    d. Jsou získaná data uživatelsky čitelná? Nejsou nijak šifrovaná uživatelským programem?
3. Autor používá nekorektní typ citování.
4. Chybí zdroje u obrázků v teoretické části práce.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je rozdělena do osmi kapitol včetně úvodu a závěru. V kapitolách 4 a 5 autor z teoretického úhlu pohledu popisuje architekturu a principy diskových uložišť a principů forenzní analýzy. Představení principů forenzní analýzy je velice povrchní, bez vazby na relevantní a oficiální literaturu, např. ve formě RFC dokumentů. Autor dále obecně představuje programy, které jsou využitelné pro forenzní analýzu, přičemž nejsou zřejmá kritéria začlenění uvedených programů do výběru a zejména jejich vazba na forenzní analýzu diskových uložišť.
V praktické části se autor věnuje forenzní analýze zařízení útočníka a definuje počáteční podmínky pro provedení forenzní analýzy. Uvedení postupy autor rovněž zpracoval do formy videií dostupných na platformě Youtube. Počáteční podmínky však neobsahují definici dat, resp. artefaktů, které mají být zkoumány a mohou představovat např. malware nebo jiný vzorek dat, který má být zajištěn. Praktická část tak představuje namísto konkrétního postupu nalezení určitých artefaktů pouze abstraktní popis možností jednotlivých programů pro forenzní analýzu a jejich vlastnosti. Vhodná forma demonstrace programů pro forenzní analýzu diskových uložišť by představovala právě demonstraci programů na předem definovaných use-case s konkrétními artefakty.

Závěrem lze konstatovat, že i přes výše uvedené nedostatky práce splňuje požadavky kladené na závěrečnou práci.

Otázky k obhajobě:

1. Uveďte naplnění jednotlivých otázek, specifikovaných v metodice práce:
    a. Jaké jsou hlavní rozdíly ve způsobu ukládání dat mezi HDD a SSD?
    b. Jaká data lze obvykle z disku získat běžně dostupnými forenzními nástroji?
    c. Jsou výrazné rozdíly v principu ukládání dat programu mezi jednotlivými webovými prohlížeči?
    d. Jsou získaná data uživatelsky čitelná? Nejsou nijak šifrovaná uživatelským programem?

Práci doporučuji k obhajobě.

Navržená výsledná známka: D

V Hradci Králové**, dne 15. května 2023**

_____

podpis