Review of Master's Thesis

Student: Zembjaková Martina, Bc.
Title: Network Forensics Tools Survey and Taxonomy (id 23022)
Reviewer: Ryšavý Ondřej, doc. Ing., Ph.D., DIFS FIT BUT

1. **Assignment complexity** — **more demanding assignment**
   Obtížnost zadání spočívá v množství informací, které je nutné shromáždit a zpracovat.
2. **Completeness of assignment requirements** — **assignment fulfilled**
   Práce splňuje všechny body zadání ve více než dostatečné míře.
3. **Length of technical report** — **exceeds requirements**
   Práce má velký rozsah z důvodů množství uvedených informací. Vzhledem k tomu, že se jednalo o průzkum existujících nástrojů a jejich vyhodnocení, je rozsah akceptovatelný.
4. **Presentation level of technical report** — **90 p. (A)**
   Přestože se jedná o velmi komplexní práci, je text velmi dobře strukturován. K organizaci textu a jeho pochopitelnosti mám pouze několik výhrad/otázek:

   - Proč je text v 3.9.1 uveden v závěru kapitoly a ne mezi ostatními klasifikacemi?
   - Kapitoly 4 a 5 uvádí velmi dlouhé seznamy různých nástrojů a datasetů - je otázkou, zda je nutné mít vše v hlavním text. Příloha práce je pro tyto informace lepší místo.
   - Kapitola 8, která prezentuje novou taxonomii, by mohla poskytovat více informací, zejména co se týká samotného návrhu.
   - V závěru bych očekával výraznější shrnutí poznatků a shromážděných informací. Zejména by se zde mohlo objevit hlubší zhodnocení současného stavu a případné výzvy.
5. **Formal aspects of technical report** — **95 p. (A)**
   Práce má výbornou úpravu a je psána srozumitelně. Jazykem práce je angličtina, která je na velmi dobré úrovni. Autorka používá jednoduchý a dobře srozumitelný styl.
6. **Literature usage** — **100 p. (A)**
   Text se odkazuje na velké množství zdrojů (>200!). Toto číslo je dáno tím, že se jedná o přehledovou práci a je více než dostačující pro pokrytí studijní literatury. Veškeré převzaté informace jsou řádně citovány.
7. **Implementation results** — **90 p. (A)**
   Práce nebyla zaměřena na vytvoření programového řešení. Realizačním výstupem projektu jsou:

   - nové datové sady pro síťovou forenzní analýzu
   - vyřešené demonstrační případy, včetně výsledných reportů
   - on-line stránky, které poskytují katalog nástrojů a datasetů

   Vytvořený realizační výstup je přidanou hodnotou textové části a vhodně jí doplňuje. Zejména nově vytvořené datové sady jsou okamžitě použitelné pro experimenty s metodami analýzy provozu. Zde bych doporučil poskytnout datové sady komunitě, například prostřednictvím vhodné služby jako je IEEE DataAccess.
8. **Utilizability of results**
   Práce je použitelná především jako zdroj informací v oblasti digitální forenzní analýzy a to jak v její aplikaci, tak při dalším výzkumu. Především množství a uspořádaní informací z práce dělá zajímavou publikaci dále využitelnou odbornou komunitou. Podstatné také je, že práce je psána v angličtině a tudíž využitelná v mezinárodním kontextu.
9. **Questions for defence**
   - Co jsou na základě Vašeho přehledu existujících nástrojů největší výzvy pro síťovou forenzní analýzu a proč?
10. **Total assessment** — **95 p. excellent (A)**
    Jedná se o pečlivě zpracovanou práci, která může být použita jako referenční zdroj informací o nástrojích pro síťovou forenzní analýzu. Autorka do svého přehledu zahrnula množství nástrojů a poskytla novou taxonomii pro jejich organizaci. Jak práce samotná, tak její realizační část je výborně zpracována a je dále využitelná odbornou komunitou. Výborné hodnocení odráží především rozsah práce, její kvalitní zpracování a další využitelnost vytvořených výsledků a textu práce.

In Brno 31 May 2021

Ryšavý Ondřej, doc. Ing., Ph.D.
reviewer