Supervisor assessment of Bachelor's Thesis

Student: Manoilov Ivan
Title: Visualization System of Network Forensic Data (id 23888)
Supervisor: Hynek Jiří, Ing., Ph.D., DIFS FIT BUT

1. **Assignment comments**
   Smyslem práce bylo implementovat informační systém, který by umožnil zpracovávat data reprezentující záznamy síťové komunikace a poskytl nástroje pro jejich forenzní analýzu (např. analýza konverzací nebo DNS záznamů). Student konkrétně navrhl a implementoval systém skládající se ze serverové části a webové aplikace. Serverová část slouží pro zpracování a ukládání forenzních dat (konkrétně PCAP souborů) a dále pak pro jejich poskytování přes REST API. Webový klient slouží jako rozhraní pro uživatele, kteří prostřednictvím něho mohou dodat zmíněné datové soubory a následně zobrazit tyto data formou uživatelsky přívětivých diagramů zdůrazňující podstatné informace. Pro tyto účely student prostudoval pojmy a principy síťové forenzní analýzy, analyzoval existující řešení a využil moderní technologie (např. Kotlin, Spring Boot, libpcap, jnetpcap, Timescale, React, Nivo, Docker a další). Student se měl primárně soustředit na prezentační část systému, nicméně nakonec své úsilí soustředil zejména na problematiku zpracování dat a prezentační část spíše upozadil. I tak hodnotím výsledek kladně. Student vytvořil celou infrastrukturu pro zpracování a vizualizaci dat, včetně optimalizací umožňující agregace dat. Systém lze využít jako dobrý základ pro tvorbu systémů řešící úzce specifické případy užití síťové forenzní analýzy.
2. **Literature usage**
   Student si aktivně dohledával literaturu s využitím dostupných nástrojů pro vyhledávání odborné literatury, dále pak zejména dokumentace použitých technologií.
3. **Assignment activity, consultation, communication**
   Student komunikoval během celého akademického roku. Konzultace probíhaly online přibližně každé dva týdny. Student plnil zadané úkoly a práce postupovala dobrým tempem. V některých případech se nicméně soustředil více na věci, které hrály menší roli v celé práci.
4. **Assignment finalisation**
   Praktická část byla dokončená s předstihem, technická zpráva byla dokončována na poslední chvíli, a zbývalo tak méně času na její vylepšování.
5. **Publications, awards**
   Student publikoval své výsledky na konferenci Excel@FIT 2021.
6. **Total assessment** **very good (B)**
   Student ke své práci až na problémy s dokončováním technické práce přistupoval svědomitě. Prostudoval celou řadu pokročilých technologií, s jejichž využitím vypracoval použitelný systém. Výsledky byly publikovány na studentské konferenci. Oceňuji rovněž, že psal práci v anglické jazyce. Navrhuji hodnocení **stupněm B**.

In Brno 2 June 2021

Hynek Jiří, Ing., Ph.D.
supervisor