VIZUALIZÁCIA ČASOVEJ OSI FORENZNÝCH ARTEFAKTOV OPERAČNÉHO SYSTÉMU WINDOWS

Autor: Bc. Kristína Kováčová
Vedúci práce: RNDr. JUDr. Pavol Sokol, PhD.
Konzultant: Ing. Miroslav Sidor, CSIRT.SK

MOTIVÁCIA

- Neustále zvyšujúce sa množstvo dát používateľov.
- Rôzne formáty, štruktúry a metadáta forenzných artefaktov.
- Po zaistení dôkazov je potrebné vytvorenie si prvotného obrazu o prípade a určenie artefaktov dôležitých pre ďalšiu analýzu.

ČASOVÁ OS

“Timeline analysis is great to determine when something has occurred at a certain time on a system.” Harrel(2011)

- Jedna z kľúčových úloh forenzného analytika.
- Pozostáva zo zachytávania systémových a sieťových udalostí, ktoré sú následne časovo zoradené.
- Udalosťou môže byť všetko od vytvorenia súboru, cez jeho úpravy a odstránenie, história webového prehliadača, prenosy súborov, prihlásenia do rôznych účtov, a mnoho ďalších.
- Na základe časového obdobia, ktoré zachytávajú sa delia na super, mikro a nano časové osi.

EXISTUJÚCE NÁSTROJE

Log2Timeline & plaso

- Prvýkrát predstavené v roku **2009** Gudjonssonom.
- **Open-source analytický nástroj,** ktorý spája dokopy ďalšie forenzné nástroje na vytváranie **super časových osí.**
- **L2T** je považovaný za **frontend, plaso** za **backend.**
- Po spustení Log2Timeline sa vytvorí **plaso súbor** (kontajner pre udalosti/protokoly/časové pečiatky), ktoré sú ďalej **paralelne** spracovávané.
- Plaso súbor je možné prekonvertovať do **csv súboru.**
- Zložité použitie, preto vymysleli Timeline2GUI.
- Môže byť použitý na **MAC OS, Windowse,** aj **Linuxe.**

EXISTUJÚCE NÁSTROJE

Timesketch

- Timesketch je **open-source** nástroj na **vizualizáciu** časových osí.
- Navrhnutý bol s cieľom **spolupráce** a **zdieľania**.
- Umožňuje **rýchle vyhľadávanie** a rýchlu **koreláciu** rôznorodých udalostí
- Vyvíjaný je od roku **2018 Berggrenom a kol.**
- Negatívom je **zložitá inštalácia** a miestami **nedostatočná dokumentácia.**

CIELE

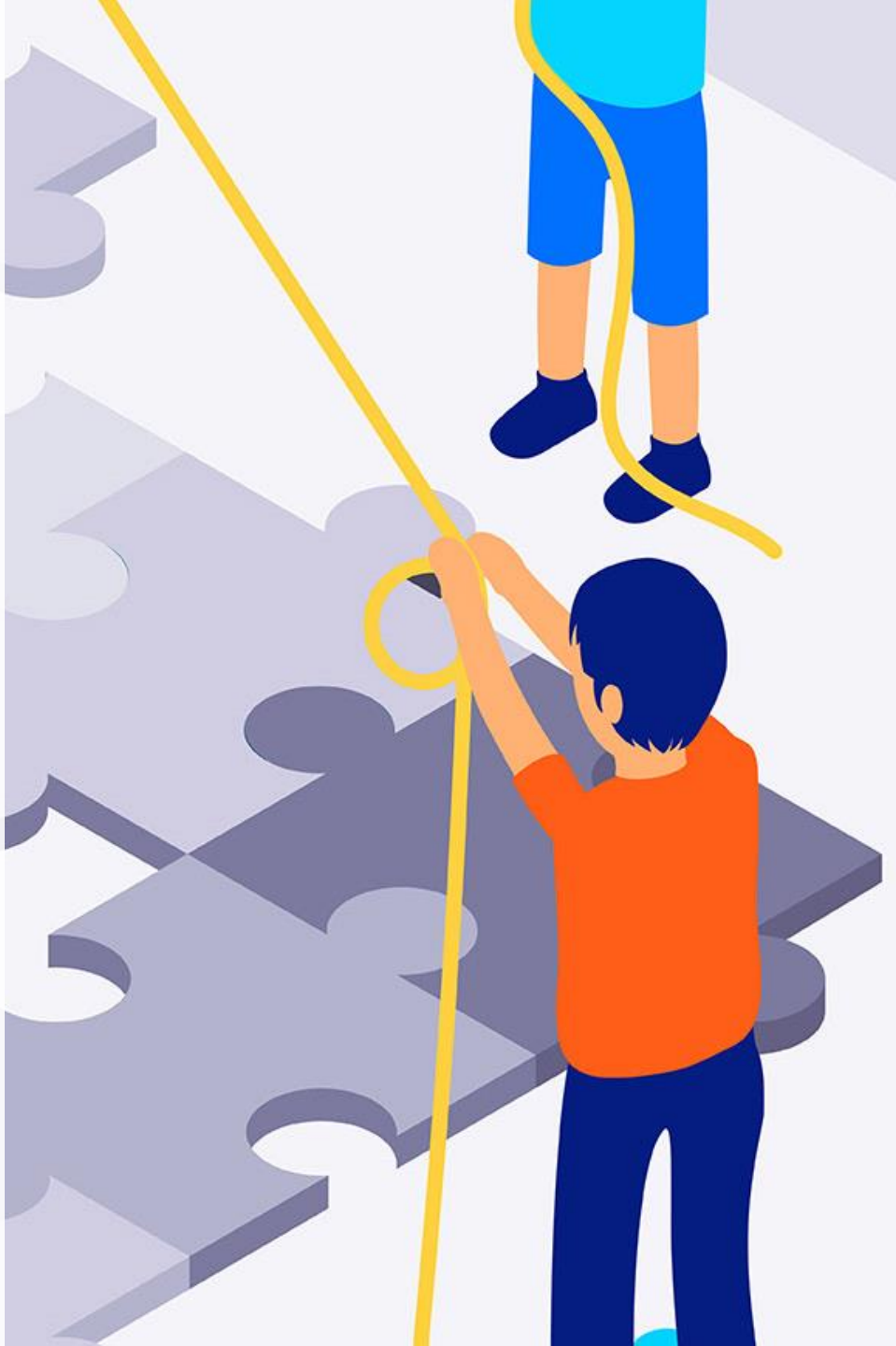
1. Aktuálne prístupy k spracúvaniu časových osí forenzných artefaktov operačného systému Windows.

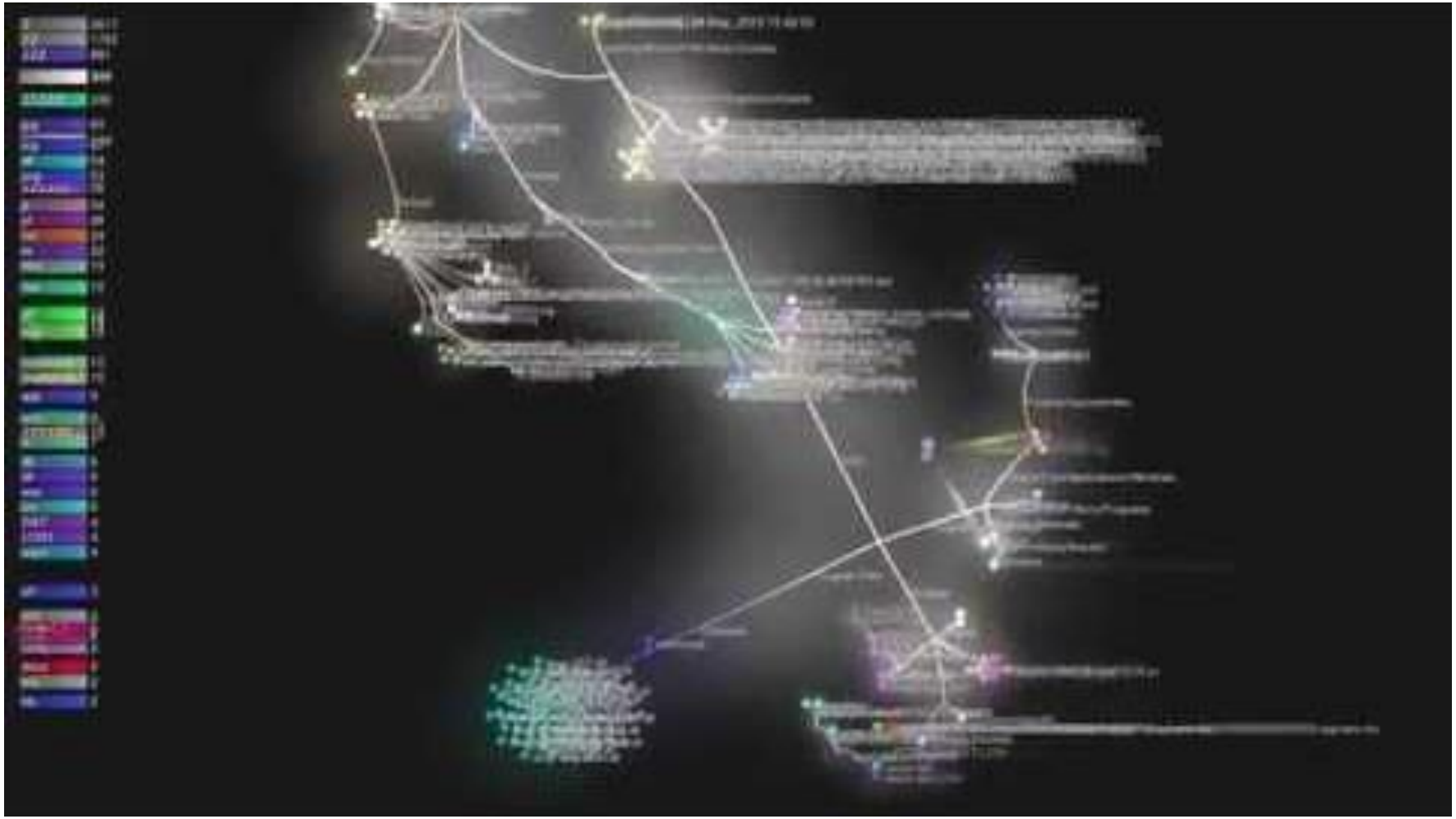
2. Analýza spôsobu vizualizácie atribútov forenzných artefaktov a vzťahov medzi nimi.

3. Návrh, implementácia a vyhodnotenie vizualizácie časovej osi forenzných artefaktov operačného systému Windows.

POŽIADAVKY NA VÝSLEDNÝ PRODUKT

1. Dynamická vizualizácia
2. Paralelné spracovanie
3. Kolaboračný a zdieľaný prístup





VISUALIZATION OF USN JOURNAL ENTRIES WHEN CCLEANER RUNS

ZOZNAM LITERATÚRY

- Osborne G., Thinyane H., Slay J. (2012) Visualizing Information in Digital Forensics. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics VIII. DigitalForensics 2012. IFIP Advances in Information and Communication Technology, vol 383. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33962-2_3
- Mark Debinski, Frank Breitinger, Parvathy Mohan (2019), Timeline2GUI: A Log2Timeline CSV parser and training scenarios, Digital Investigation, Volume 28, Pages 34-43, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2018.12.004.

ĎAKUJEM ZA POZORNOSŤ!