Excel@FIT 2016

44

Forenzní analýza prohlížeče Google Chrome
Identifikace konkrétního uživatele

Autor: Daniel Dušek, 3BIT

Stručně o práci

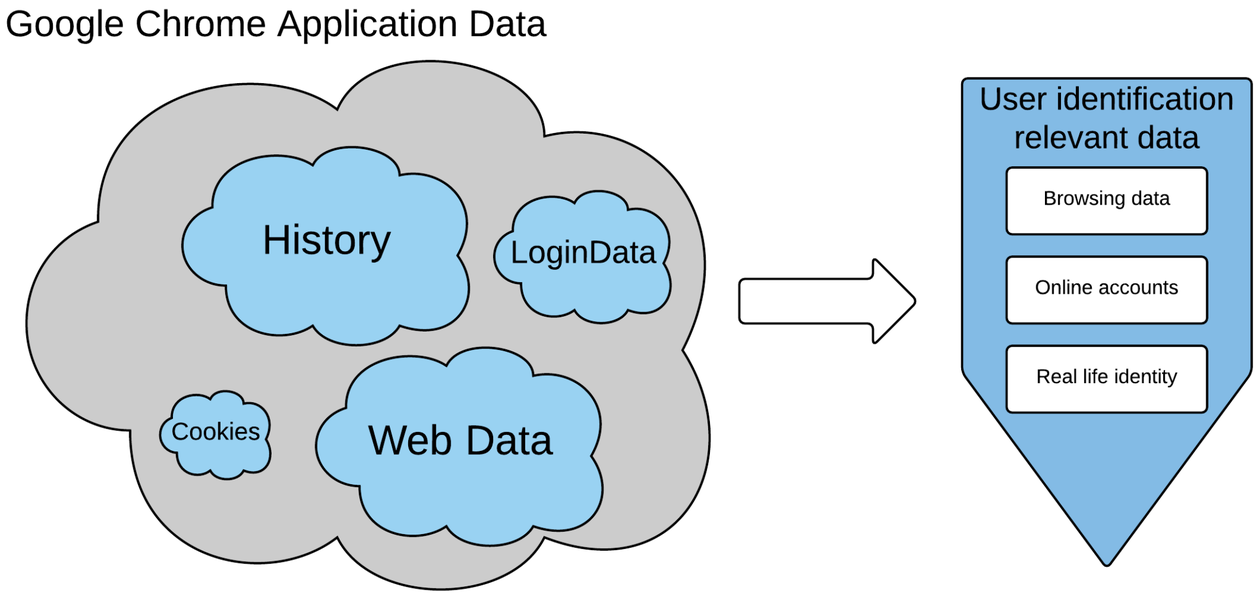
Práce je zacílena na forenzní analýzu dnes velmi rozšířeného prohlížeče Google Chrome s cílem jednoznačné identifikace uživatele, který prohlížeč používal. V rámci procesu extrakce relevantních dat a identifikace konkrétního uživatele bylo třeba extrahovat plný obsah interních databází prohlížeče Google Chrome a určit, které z hodnot jsou relevantní, a které není třeba brát v potaz. Po extrakci a minimalizaci množiny množin hodnot, které je třeba zohledňovat, bylo třeba určit význam hodnot uložených v relevantních množinách hodnot. K určení významu hodnot byla použita kombinace reverzního inženýrství a empirického přístupu. Pro demonstraci efektivity a použitelnosti redukované množiny množin hodnot byla vyvinuta aplikace SD4Gen, která z dostupných dat vytvoří co nejpřesnější otisk konkrétního uživatele, který prohlížeč používal. Čtenář celé této práce pak může těžit z informací a závěrů týkajících se Google Chrome databáze tak, že porozumí způsobu interního ukládání hodnot. Informace a závěry této práce lze využít při implementaci vlastního software pro identifikaci konkrétního uživatele na základě jeho aktivity v prohlížeči Google Chrome, stejně tak jako při implementaci vlastní aplikace pro analýzu databází Google Chrome.

Použití aplikace v praxi

Představme si situaci, kdy se v imaginární firmě nachází zaměstnanec-záškodník, který vynáší, prostřednictvím anonymního Twitter účtu vnitřní záležitosti firmy do světa a firmu tím poškozuje a zesměšňuje. Vedení firmy již pojme podezření o kterého zaměstnance se jedná, ale nemá v ruce žádné pádné důkazy, avšak má plný přístup k zaměstnancově počítači a všichni zaměstnanci musí povinně používat Google Chrome. V takovém případě je možné použít aplikaci SD4Gen k analýze dat, které po sobě uživatel zanechal a následně spojit jeho reálné jméno s účtem na Twitteru skrze který vynášel informace a zaměstnance náležitě potrestat.

Downloads.state column values	
Column value	Description
0	Download in progress
1	Download completed
2	Download cancelled
3	Download interrupted
4	Maximum download state reached

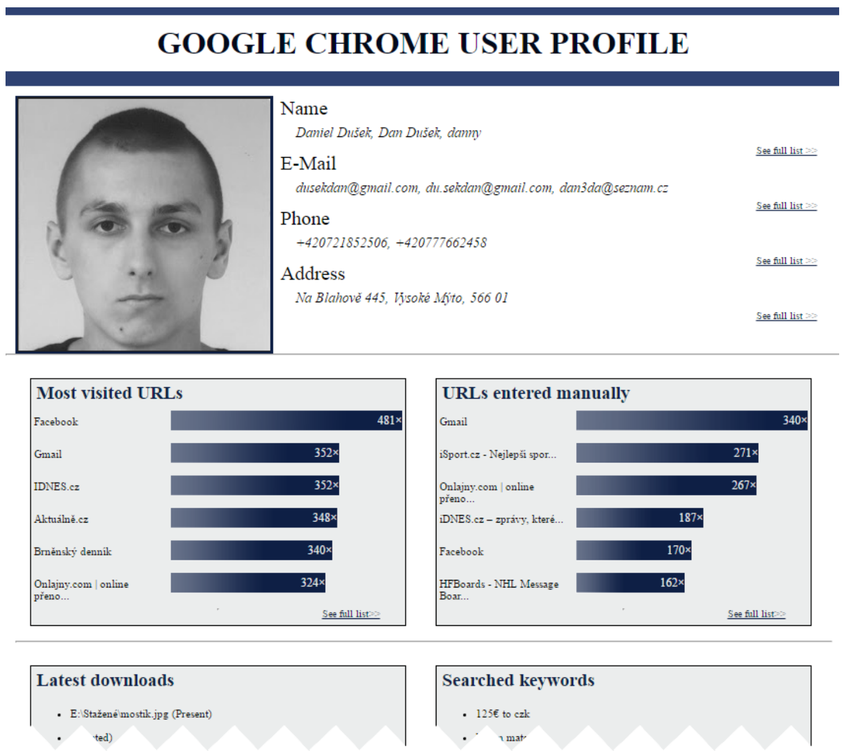
Ukázka zjištěných významů dat pro sloupec ‚state‘ z tabulky Downloads, databáze History



Symbolické vyobrazení z čeho a jak lze identifikovat uživatele na základě jeho aktivity v prohlížeči Google Chrome.

Reverzní inženýrství

Neb k ‚plain‘ konstantám uloženým v analyzovaných databázích neexistuje veřejná dokumentace, bylo třeba se místy dívat do zdrojového kódu aplikace s cílem porozumět významu konstant, které se nachází v databázi. V procesu zjišťování významu hodnot bylo třeba porovnávat možné hodnoty vyskytující se ve zdrojovém kódu s lidmi čitelnými hodnotami nacházejícími se v dokumentaci ke Google Chrome rozšířením. Na základě porovnání byl pak sestaven hrubý seznam možných hodnot a jejich možných významů. Následně bylo třeba nasimulovat situaci, kdy dojde k uložení hodnoty konkrétního typu do databáze a ověřit, zda uložená hodnota odpovídá operaci, která byla provedena a shoduje se s lidsky čitelnou hodnotou v dokumentaci k rozšířením. Tímto způsobem byl vytvořen rozsáhlý seznam hodnot a jejich významů.



Ukázkový screenshot otisku z vyvíjené aplikace SD4Gen