

Integrovaná platforma pro zpracování digitálních dat z bezpečnostních incidentů (TARZAN)

Identifikační kód VI20172020062

Název předkládaného výsledku: *Cryptocurrency Forensics Utilizing a Multi-currency Blockchain Explorer*

Typ výsledku dle UV č. 837/2017	Evidenční číslo (příjemce)	Rok vzniku
A audiovizuální tvorba		2018
ISBN-ISSN	Webový odkaz na výsledek	Kde a kdy publikováno
	https://www.fit.vut.cz/research/publication/11872/	ISS World Europe 2018

Anotace k výsledku:

Seznámí se s aktuálními možnostmi blokovacího řetězce a analýzou provozu pro různé šifrovací sítě (nikoliv pouze Bitcoin, ale také Litecoin, Dash, Monero, Zcash a další). Podrobně vysvětlíme vlastnosti forenzní analýzy včetně clusteringu adres, coinjoining vstupů, mixování transakcí a korelace provozu. Uvedeme existující (ne)komerční nástroje a poskytneme subjektivní seznam vlastností, které by měl mít "dobrý" nástroj. Budeme demonstrovat metody šifrování uživatelů a kriminality v rámci našeho vlastního nástroje.

Řešitelský tým: Petr Matoušek (manažer a hlavní řešitel), Vladimír Veselý (realizační tým)