Telegram Investigator

Studiengang: MAS Digital Forensics & Cyber Investigation

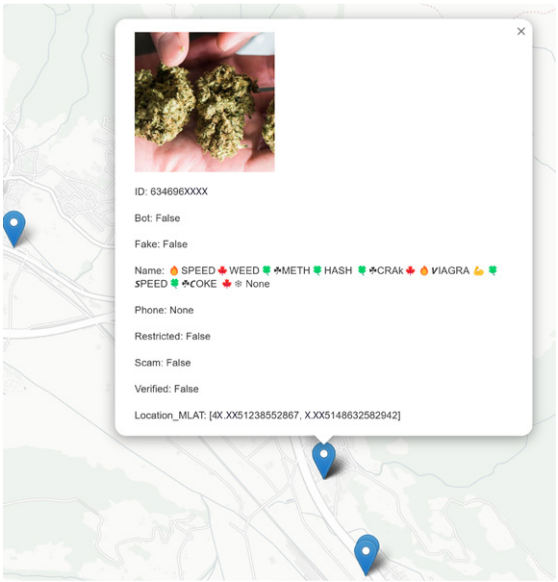
«Coke Seller Wil» oder «Rapperswil-Jona Weed» sind Chat-Bezeichnungen, die im Instant-Messaging-Dienst Telegram gefunden werden können, wenn nach öffentlich einsehbaren Kontakten in der eigenen Umgebung gesucht wird. Diese Arbeit stellt ein Verfahren vor, um diese und andere Chats mit potentiellem Bezug zu Betäubungsmitteldelikten zu identifizieren und geolokalisieren.

Ausgangslage

Bis dato gab es keine Möglichkeit, eine Übersicht über Telegram-Chats mit potentiellem Bezug zu Betäubungsmitteldelikten in einem spezifischen geografischen Gebiet zu erhalten. Dementsprechend fehlten Entscheidungsträgern von Strafverfolgungsbehörden bislang die grundlegenden Informationen, um präventive Massnahmen oder proaktive Ermittlungen mit Bezug zu Telegram anordnen zu können.
Im Rahmen einer Machbarkeitsstudie wurde ein Verfahren, für die automatisierte Erfassung von Chats mit potentiellem Bezug zu Betäubungsmitteldelikten in einer spezifizierbaren Region, entwickelt. Dieses Verfahren besteht aus Komponenten zur Erfassung und Klassifizierung der Chat-Metadaten sowie zur Geolokalisation der Chat-Positionen.

Methodik und Umsetzung

Die Datenerfassung erfolgt über die Programmierschnittstelle von Telegram. Dabei werden ausgehend von verschiedenen Standorten, die Distanzen zu Chats in der näheren Umgebung erfasst.



Beispiel-Visualisierung der Metadaten eines Chats, an einer durch Multilateration näherungsweise bestimmten Position

Mittels Multilateration werden daraus die Positionen dieser Chats näherungsweise ermittelt. Ausgehend von den so identifizierten Kanälen, werden weitere öffentlich zugängliche Kanäle mittels Crawling-Techniken ermittelt, indem innerhalb der Kanäle nach Verlinkungen zu weiteren Kanälen gesucht wird. Die gefundenen Chats werden anhand ihrer Metadaten mit einer Keyword-Liste sowie einem nachtrainierten Machine-Learning-Modell, als relevant oder irrelevant hinsichtlich des potentiellen Bezugs zu Betäubungsmitteldelikten klassifiziert. Die Kombination der beiden Methoden erwies sich als besonders wirkungsvoll, da so sämtliche verdächtigen Chats gefunden werden konnten. Die Chats können mit ihren errechneten Positionen und Metadaten in einer Karte visualisiert werden. Dies ermöglicht auch technisch nicht versierten Entscheidungstragenden, einen strukturierten Überblick über die Daten.
Das entwickelte Verfahren hat sich als effektiv erwiesen, um Chats mit einem potentiellen Bezug zu Betäubungsmitteldelikten in einer definierbaren Region zu identifizieren. Die verwendeten Methoden sind auf öffentlich verfügbare Informationen beschränkt.

Resultate

Im Zuge dieser Thesis wurde erfolgreich ein Verfahren entwickelt, welches die Identifikation, Geolokalisierung und Klassifizierung von Telegram Chats ermöglicht. Durch die Anwendung dieses Verfahrens, wurden diverse Chats mit potentiellem Bezug zu Betäubungsmitteldelikten identifiziert und einem geografischen Gebiet zugeordnet. Es konnte jedoch nicht verifiziert werden, ob die gemachten Angaben in diesen Chats authentisch sind. Es wird empfohlen Massnahmen zu treffen, um die Echtheit der Angebote in den Chats zu überprüfen. Um die Umsetzung dieser Empfehlung zu erleichtern, zeigt der Bericht Methoden auf, wie Chat-Teilnehmende kontaktiert und identifiziert werden können.

Mathias Kluser