NextGen Scientific Review - Annual Perspectives on Next Generation Science – Vol. 1
ISSN 2940-0929

MoNA

Eine Analyseplattform für mobile Kommunikation

Michael Spranger*, Lukas Jaeckel und Dirk Labudde

Zusammenfassung

Mobile Kommunikationsgeräte sind ein beliebtes Mittel zur Planung, Beauftragung und Durchführung von Straftaten. Insbesondere Daten von Messengern, wie WhatsApp oder Telegram, enthalten oft beweiskräftige Informationen. In Fällen organisierter Kriminalität sind zudem meist viele Geräte involviert, von denen jedoch nicht alle den vollständigen Kommunikationsverlauf beinhalten. Dieser ist vielmehr durch individuelle Löschungen von Nachrichten oder unterschiedliche Beitrittszeiten zu Gruppen stark fragmentiert. Somit ist eine singuläre Auswertung einzelner Geräte oft nicht zielführend, da wichtige Zusammenhänge nicht erkannt werden können. Die Verknüpfung zusammengehöriger Kommunikation ermöglicht hingegen eine nahezu vollständige Rekonstruktion der Kommunikation bei gleichzeitiger Reduktion des Leseaufwands durch Verschmelzung identischer Nachrichten. Das Gruppieren kohärenter Nachrichten zu Gesprächen ermöglicht den effizienten Abgleich mit einem Wissensmodell. In dieser Arbeit wird mit MoNA eine Plattform zur interaktiven Analyse und Verknüpfung mobiler Kommunikationsdaten vorgestellt, die durch Implementierung dieser Konzepte eine effektive u nd effiziente Filterung verfahrensrelevanter Kommunikation bei gleichzeitigem Kontexterhalt erlaubt.

Keywords: forensics, communication analysis, software.

1 Einleitung

Mobile Kommunikationsgeräte sind zu einem integralen und unverzichtbaren Bestandteil der täglichen Kommunikation geworden. So stieg beispielsweise die Anzahl der Smartphone-Nutzer:innen seit dessen Erfindung a uf aktuell über 62 Millionen, allein in Deutschland (Tenzer, 2022). Das entspricht rund 72 Prozent der deutschen Bevölkerung. Damit einhergehend nimmt auch die Nutzung dieser Geräte zur Planung, Beauftragung und Durchführung von Straftaten und damit die Anzahl zu analysierender Geräte im Zuge von polizeilichen Ermittlungsverfahren stetig zu. Die Herausforderung dabei ist, die riesige Menge an Kommunikationsdaten auf einem Gerät nach den oft wenigen fallrelevanten Informationen zu durchsuchen. Im Falle organisierter Kriminalität müssen meist sogar ganze Netzwerke von mobilen Kommunikationsgeräten untersucht werden.

Die forensische Untersuchung mobiler Kommunikationsgeräte umfasst einerseits die physikalische und logische Sicherung und Rekonstruktion von Daten auf mobilen Endgeräten, wie Smartphones oder Tablets, andererseits die inhaltliche Analyse von Text-, Bild-, Audio- und Videodaten. Gemeinsam mit verfügbaren Metadaten, wie Zeitstempeln, Log-Dateien, Geo- und Kontaktdaten, genutzten Apps etc., kann eine Vielzahl an forensischen Fragestellungen beantwortet und eine Art digitales Nutzer:innen-Profil erzeugt werden.

Während sich viele Arbeiten mit der Bereit- und Wiederherstellung von Daten auf mobilen Endgeräten (Jeon et al., 2012; Liu et al., 2017; Pawlaszczyk & Hummert, 2021) oder der Aufklärung von Datenbankstrukturen befassen (Anglano, 2014; Anglano et al., 2017; Chang & Yen, 2020; Thebaity et al., 2020), existieren kaum dedizierte Arbeiten zu deren inhaltlicher Analyse.

Bei textbasierter Kommunikation, wie etwa bei SMS oder diversen Messengerdiensten, hängt das Verständnis des Gesprächsinhaltes stark vom Vorhandensein eines möglichst lückenlosen Chatverlaufs ab. Genau das ist aber oftmals nicht der Fall. Stattdessen findet man häufig stark fragmentierte Chatverläufe vor. Die Gründe hierfür sind vielfältig, aber wohl vor allem im Löschen vereinzelter Nachrichten auf einem Gerät oder partiellen Zugehörigkeitszeiten eines Mitglieds zu einem Gruppenchat sowie in Hardwareveränderungen zu finden. Eine Rekonstruktion ist jedoch, vor allem bei Gruppenchats, durch Verknüpfen unterschiedlicher Geräte möglich. Ein positiver Nebeneffekt besteht in der drastischen Reduktion des Analyseaufwandes, da es nun ausreichend ist, den Chatverlauf eines einzigen Beteiligten zu analysieren. Die anschließende Detektion von kohärenten Konversationen ermöglicht eine fehlertolerantere Suche, bei gleichzeitigem Kontexterhalt. Dies ist insbesondere für die spätere Beurteilung der Bedeutung durch eine Ermittlungsperson notwendig.

Die Suche in diesen Konversationen mit einzelnen Suchanfragen ist ebenso zeitaufwändig wie fehleranfällig. Klassische maschinelle Lernmodelle scheitern an der fehlenden Verfügbarkeit annotierter Trainingsdaten und an der speziellen Charakteristik mobiler Kommunikation im forensischen Kontext. Ein Wissensmodell, das Erfahrungs- und Fallwissen der Ermittlungsperson einbezieht, schafft hier Abhilfe.

In dieser Arbeit wird mit MoNA (Mobile Network Analyzer) die Implementierung einer Plattform zur Analyse mobiler Kommunikation vorgestellt, welche alle genannten Ansätze implementiert und in der Erprobungsphase mit Anwender:innen aus der Praxis gezeigt hat, dass sie die wesentlichen Anforderungen an eine zeitgemäße Analyse mobiler Kommunikationsdaten erfüllt.

In Abschnitt 2 werden die Konzepte der Rekonstruktion und Analyse von textueller Kommunikation sowie der Aufbau eines Wissensmodells zum Filtern verfahrensrelevanter Kommunikation ausführlich erläutert. Die Arbeit schließt mit einer kurzen Zusammenfassung und einem Ausblick auf künftige Entwicklungsschritte im Abschnitt 3.

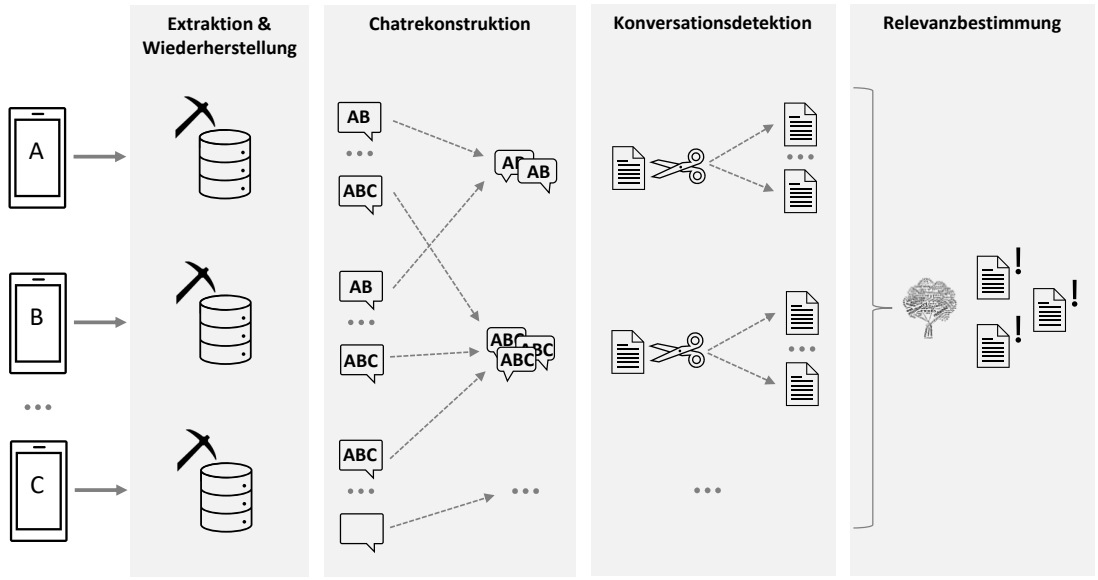

Abbildung 1: Interaktiver Prozess zur intelligenten Analyse von Kommunikationsdaten.

2 Analyseprozess in MoNA

Der Fokus des in MoNA integrierten Analyseprozesses liegt auf der Verknüpfung von Kommunikationsdaten, sowie deren Reduktion auf verfahrensrelevante Daten. Dadurch wird die Vollständigkeit der Daten erhöht und gleichzeitig die Menge der zu beurteilenden Nachrichten deutlich reduziert, wodurch Zeit und Ressourcen eingespart werden können. Wie in Abbildung 1 zu erkennen, kann der gesamte Prozess dabei in mehrere Schritte unterteilt werden. Diese erfolgen zum größten Teil automatisch, binden mitunter aber auch aktiv die Nutzer:innen mit ein.

Zu Beginn werden die Chatverläufe aus den von den Nutzer:innen angegeben Kommunikationsdaten extrahiert und gelöschte Inhalte wiederhergestellt und zur Vervollständigung der Chats genutzt. Im Anschluss werden gleiche Chats von verschiedenen Endgeräten jeweils zu einem gemeinsamen Chat ohne jegliche Informationsverluste zusammengeführt. Dadurch erhöht sich einerseits die Vollständigkeit der rekonstruierten Chatverläufe. Andererseits verringert die Zusammenführung den Analyseaufwand, da gleiche Chats nicht mehrfach betrachtet werden müssen.

Daraufhin folgt die Konversationsdetektion, welche jeweils einen Chat in mehrere, kohärente Konversationen aufteilt. Dabei besteht eine Konversation aus einer Menge von zusammenhängenden Nachrichten eines Chats, die in einem gemeinsamen zeitlichen Kontext stehen. Genau diese Konversationen und nicht die einzelnen Nachrichten, werden letztlich für die Bestimmung der Relevanz verwendet. (Spranger et al., 2016; Spranger & Labudde, 2014, 2017)

Um Konversationen korrekt als verfahrensrelevant klassifizieren zu können, ist ein Wissensmodell notwendig, welches beliebig komplexe Suchanfragen, die über die klassische Textsuche weit hinausgehen, ermöglicht. In MoNA wird dieses Modell als Begriffsbaum bezeichnet. Bei der Erstellung des Begriffsbaum kann dabei das Wissen der Ermittlungsperson, z.B. spezifisches Fallwissen, mit einbezogen werden. Nach Anwendung des Begriffsbaums gibt das System automatisch alle Konversationen zurück, die mindestens eine als verfahrensrelevant klassifizierte Nachricht beinhalten. Wie bereits anfänglich erwähnt, muss die Ermittlungsperson im Vergleich zur gesamten Datenmenge nur eine in der Regel deutlich reduzierte Anzahl von Konversationen beurteilen.

2.1 Wiederherstellung gelöschter Chatinhalte

Wie in Abschnitt 2 kurz beschrieben, folgt auf die Identifikation und Extraktion der Daten die Wiederherstellung gelöschter Chatinhalte. Dafür existieren mehrere Methoden, die in MoNA kombiniert werden.

Eine Vielzahl der Anwendungen auf mobilen Kommunikationsgeräten nutzt SQLite-Datenbanken zur Speicherung lokaler Daten (Epifani & Stirparo, 2016; Skulkin et al., 2018). Dazu gehören auch insbesondere aktuelle Messengerdienste, wie z.B. WhatsApp (Anglano, 2014), Telegram (Anglano et al., 2017) und der Facebook Messenger (Chang & Yen, 2020).

Eine Besonderheit von SQLite-Datenbank ist, dass gelöschte Einträge in nicht zugewiesenen sowie in freien Blöcken verbleiben, bis die Blöcke überschrieben werden. Somit lassen sich in bestimmten Fällen gelöschte Daten aus diesen Bereichen einer SQLite-Datenbank wiederherstellen. (Jeon et al., 2012)

Darüber hinaus legt SQLite ab der Version 3.7.0 eine spezielle Datei an, falls als optionaler Modus das Write-Ahead Logging (WAL) aktiviert ist (SQLite Consortium, 2018). Dabei werden Datenbank-Transaktionen nicht direkt in die Hauptdatenbank geschrieben, sondern zuerst in einer WAL-Datei zwischengespeichert. Erst nachdem diese Datei eine bei der Initialisierung festgelegte Anzahl an Einträgen überschreitet, führt die Datenbank einen Checkpoint durch. Dadurch werden alle Einträge aus der WAL-Datei in die Hauptdatenbank geschrieben. Demzufolge können vor einem Checkpoint die Datenbank und WAL-Datei jeweils einen unterschiedlichen Stand besitzen, was von wesentlicher forensischer Relevanz sein kann. Beispielsweise könnten sich die neusten Einträge nur in der WAL-Datei befin-

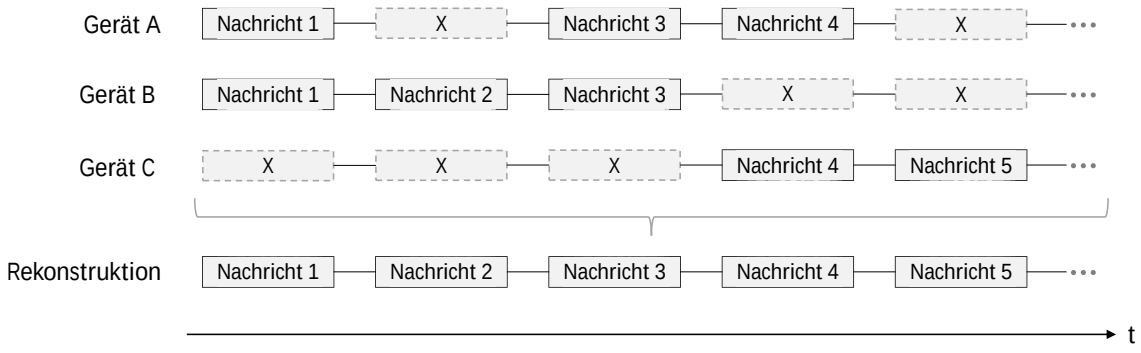

Abbildung 2: Vollständige Rekonstruktion eines Gruppenchats anhand von drei Geräten. Die Geräte A, B und C enthalten jeweils eigene Versionen des gemeinsamen Gruppenchats, welche zu unterschiedlichen Zeitpunkten Lücken aufweisen. Eine Lücke, die als gestrichelt und mit „X“ gekennzeichnet ist, stellt hierbei eine gelöschte oder nicht erhaltene Nachricht dar. Die Zusammenführung der verschiedenen Versionen führt zur Rekonstruktion des vollständigen Chatverlaufs.

den. Andererseits könnte die Datei bereits aus der Hauptdatenbank gelöschte Einträge enthalten, die sich wiederherstellen lassen, wie bereits Liu et al. (2017) zeigten.

Als Alternative zum Write-Ahead Logging kann SQLite bereits in Versionen vor 3.7.0 ein Rollback-Journal erstellen. Dabei wird vor einer Transaktion der gesamte Inhalt der betroffenen Datenbank-Seiten in das Journal kopiert, um im Falle eines Fehlers zum letzten validen Stand zurück springen zu können. In der Praxis verbleiben nach einer erfolgreichen Transaktion die kopierten Daten im Journal. Nur der Header des Journals wird mit Nullen überschrieben. Weitere Kopiervorgängen von Datenbank-Seiten überschreiben den aktuellen Inhalt des Journals. Da die Größe der Datenbank-Seiten stark variieren kann, ist es allerdings möglich, dass Daten aus vorherigen Transaktionen zum Teil im Journal verbleiben. Deshalb lassen sich gelöschte Inhalte womöglich aus einer Rollback-Journal-Datei wiederherstellen. (Sanderson, 2018)

Um die beschriebenen Möglichkeiten zur Wiederherstellung gelöschter Datenbankinhalte zu realisieren, verwendet MoNA das Forensic SQLite Data Recovery Tool (Pawlaszczyk, 2021).

Zusätzlich werden lokal gespeicherte Backups einbezogen. Beispielsweise sichert WhatsApp unter Android nach einem von den Gerätenutzer:innen zu definierenden Zeitraum die Datenbank, welche die Chatverläufe enthält, als neue Kopie (Anglano, 2014). Durch das Vergleichen aller Einträge der Backups mit der aktuellen Hauptdatenbank können gelöschte Nachrichten oder gesamte Chatverläufe erkannt und wiederhergestellt werden. Sofern jedes Backup einen Zeitstempel besitzt, lässt sich zusätzlich der Zeitraum bestimmen, in dem die jeweiligen Daten gelöscht wurden.

2.2 Rekonstruktion von Chatverläufen

Trotz der in Unterabschnitt 2.1 beschriebenen Methoden ist es auch möglich, dass bestimmte Daten auf einem mobilen Endgerät nicht wiederhergestellt werden können. Dennoch lassen sich unvollständige oder gelöschte Chats rekonstruieren, unter der Voraussetzung, dass im Rahmen der forensischen Untersuchung mehrere zu einem Netzwerk gehörige Geräte sichergestellt worden sind. Dazu sucht MoNA auf den verschiedenen Geräten nach identischen Chats. Diese sind beispielsweise anhand einer eindeutigen Chat-ID oder gleicher Chatmitglieder erkennbar. Im Anschluss werden alle Nachrichten der jeweils gleichen Chats gegenübergestellt. Die Grundidee besteht darin, dass Nachrichten, welche auf einem mobilen Endgerät gelöscht wurden, im gleichen Chat auf anderen Geräten weiterhin vorhanden sein können. Wenn demzufolge ein Chat auf zwei Geräten existiert, aber sich bestimmte Nachrichten des Chats nur auf einem Gerät befinden, wurden diese Nachrichten auf dem anderen Gerät mit Sicherheit gelöscht oder nicht empfangen.

Zur Überprüfung, ob zwei Nachrichten identisch sind, eignen sich je nach Gegebenheit ein Vergleich der Nachrichten-ID oder des Nachrichteninhalts in Kombination mit der Sendezeit. Sofern gelöschte oder nicht empfangene Nachrichten gefunden wurden, fügt MoNA diese automatisch in die jeweils lückenhaften Chats ein. Dabei ist die Chance, möglichst viele Chats vollständig rekonstruieren zu können umso höher, je mehr Geräte in den Analyseprozess einbezogen werden. Da am Ende des Prozessschrittes der Inhalt identischer Chats garantiert gleich ist, müssen sowohl die Ermittlungspersonen als auch MoNA diese Chats nur in einer einzigen, vollständigen Version analysieren. Demzufolge entfällt die mehrfache Betrachtung gleicher Chats pro Gerät, was Zeit und Ressourcen spart. Zur Demonstration zeigt Abbildung 2 beispielhaft die Rekonstruktion eines Gruppenchats mithilfe von drei Geräten, welche jeweils Teile des gesamten Chatverlaufs enthalten.

2.3 Konversationsdetektion und Termbaum

Nach der in den letzten Abschnitten beschriebenen Wiederherstellung und Rekonstruktion einzelner Chatnachrichten $m \in M$ erfolgt deren Gruppierung in einzelne Konversationen, wie in Gleichung 1 dargestellt.

$$c = (m_1, ...m_n | t_i^m - t_{i+1}^m <= \epsilon, \forall i = 1...n) \qquad (1)$$

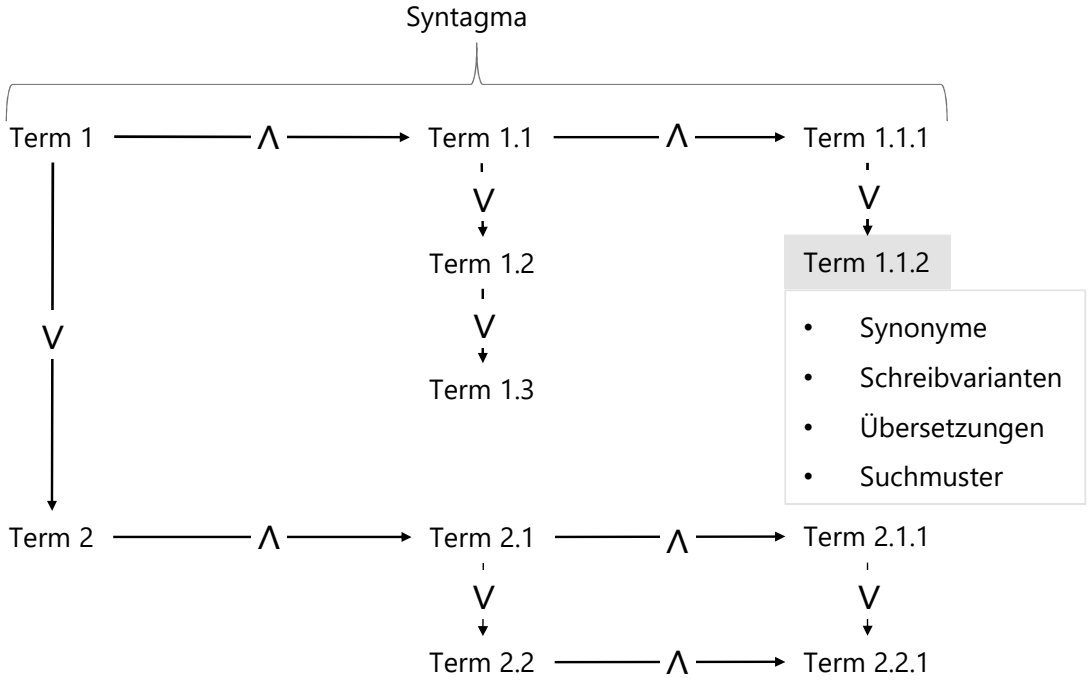

Abbildung 3: Termbaum als zentrales Klassifikationselement zur Entscheidung über Relevanz einzelner Konversationen.

Jede Konversation setzt sich demnach aus der Menge an Nachrichten zusammen, die aufeinanderfolgend zu den Zeitpunkten t_i und t_{i+1}, ohne Überschreitung einer individuell bestimmten maximalen Antwortzeit ϵ, ausgetauscht wurden. Diese Gruppierung macht den Einsatz konservativer Wort-Matching-Algorithmen erfolgversprechender, da sich die Wahrscheinlichkeit eines Suchtreffers durch die größere Anzahl an Wörtern in einer Konversation gegenüber einzelner Nachrichten natürlicherweise erhöht. Ein weiterer Vorteil dieser Methode besteht im daraus resultierenden Kontexterhalt. Jeder Suchtreffer muss von einer Ermittlungsperson überprüft und bestätigt werden. Dieser Vorgang ist einfacher und weniger fehleranfällig, wenn der Kontext der Nachricht erhalten bleibt, wie das bei der Betrachtung von Konversationen der Fall ist. (Spranger et al., 2016)

Nach Bestimmung der Konversationen $C = c_1, ..., c_n$, besteht der nächste Schritt darin, herauszufinden, welche dieser Konversationen deliktbezogen relevante Nachrichten hinsichtlich des Untersuchungsauftrages beinhalten. Die Bestimmung relevanter Konversationen bzgl. eines spezifischen Falles erfordert aus verschiedenen Gründen die Einbeziehung von Ermittlerwissen, wie ausführlich in Spranger et al. (2016) dargelegt. So können insbesondere fallspezifische Informationen, beispielsweise zum Kreis der Tatverdächtigen oder Opfer, oder Erfahrungen über millieuspezifische sprachliche Besonderheiten wichtige Indikatoren für die Relevanzeinstufung liefern.

Unter Berücksichtigung der Erkenntnis, dass eine Relevanzentscheidung zu einem nicht unwesentlichen Teil auf Erfahrungswissen beruht, wurde in MoNA ein regelbasierter Ansatz zugrunde gelegt, der es erlaubt, komplexe Systeme von Syntagmen in einer Baumstruktur zu beschreiben. Diese als Termbaum bezeichnete Wissensstruktur ist in Abbildung 3 dargestellt. Als Syntagma bezeichnet man dabei in einem lokalen Kontext (hier Nachricht) miteinander vorkommende sprachliche Elemente (hier Terme). Ein Term wird dabei nicht nur durch ein Wort repräsentiert, sondern durch einen Vektor $\vec{t} = (w_0, ..., w_n, p_0, ..., p_k)$, wobei w_i eine Menge an sprachlichen Variationen (Wortvarianten, Synonyme, gruppenspezifische Ausdrücke etc.) und p_i eine Menge an Musterdefinitionen (hier reguläre Ausdrücke) bezeichnet.

Ein Syntagma syn ist dann die verpflichtende Kombination verschiedener Terme t_i in einer Nachricht m_j im Sinne einer Konjunktion, also $syn = t_0 \wedge t_1 \wedge ....$ Ein Termbaum $\xi = syn_0 \vee syn_1 \vee ...$ ist dann die disjunktive Verknüpfung verschiedener Syntagmen. Natürlich lässt sich dieses Prinzip rekursiv anwenden, d.h. $\xi_{gesamt} = \xi_0 \vee \xi_1 \vee ...$, wodurch die Wiederverwendung von so kodiertem fallübergreifendem oder -unabhängigem Wissen ermöglicht wird, was den Erzeugungsaufwand sukzessive auf Termbäume für spezifisches Fallwissen beschränkt.

Erzielt mindestens ein Syntagma einen Treffer in einer Konversation, wird diese als verfahrensrelevant eingestuft und entsprechend farblich hervorgehoben.

3 Zusammenfassung und Ausblick

Die Analyse von Kommunikationsdaten mobiler Endgeräte ist eine zeitaufwendige und fehleranfällige Aufgabe. Aktuelle Analyseanwendungen können bisher diesen Prozess zwar unterstützen, tragen aber nur wenig zur Reduktion des Aufwandes bei. In dieser Arbeit wurde deshalb eine Prozesskette vorgestellt, welche den Analyseaufwand nach der Extraktion und Wiederherstellung der Kommunikationsdaten in drei Schritten erheblich verringert.

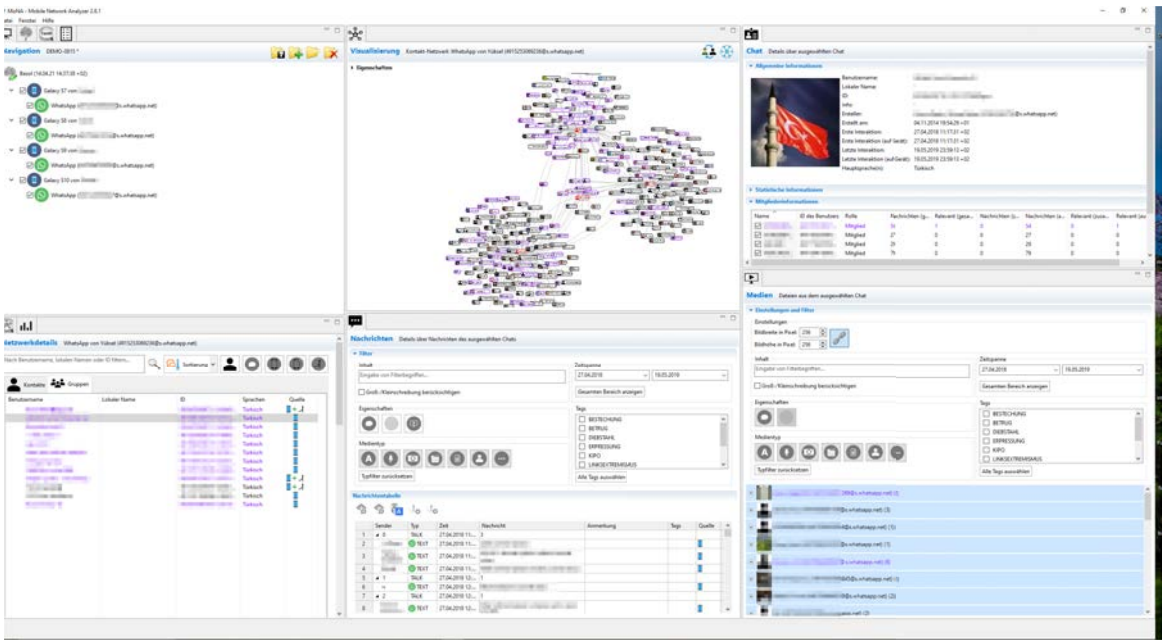

Abbildung 4: Screenshot der aktuellen MoNA-Version, in welcher die vorgestellten Konzepte implementiert sind.

In einem ersten Schritt werden dabei die Messengerdaten unterschiedlicher Geräte miteinander verknüpft, wodurch die Kommunikationshistorie nahezu vollständig rekonstruiert werden kann. Als positiver Nebeneffekt verringert sich der Leseaufwand durch die Deduplizierung erheblich. Im nächsten Schritt werden Nachrichten der Historie in Gespräche eingeteilt, wodurch größere Mengen zusammengehöriger Text zur Analyse bereitstehen, was die Trefferwahrscheinlichkeit erhöht. Gleichzeitig wird durch den damit verbundenen Kontexterhalt die Interpretation der Ergebnisse durch Ermittlungspersonen vereinfacht. In einem letzten Schritt werden mithilfe einer regelbasierten Wissensbasis, dem sogenannten Termbaum, verfahrensrelevante Gespräche gefiltert, was den Suchaufwand nochmals drastisch reduziert.

Die Prozesskette wurde in einer prototypischen Anwendung, dem Mobile Network Analyzer (MoNA) implementiert und wird aktuell durch verschiedene Ermittlungsbehörden evaluiert (siehe Abbildung 4).

Die größte Herausforderung liegt jetzt noch in der Entwicklung und Ausgestaltung der Inhalte des Termbaums. Hier müssen zukünftig Vorschlagssysteme für Begriffe auf Basis maschineller Lernverfahren entwickelt werden.

Literatur

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android Smartphones. *Digital Investigation*, *11*(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. *Digital Investigation*, *23*, 31–49. https://doi.org/10.1016/j.diin.2017.09.002

Chang, M.-S., & Yen, C. P. (2020). Evidence Gathering of Facebook Messenger on Android. *International Journal of Network Security*, *22*(5), 828–837. https://doi.org/10.6633/IJNS.202009_22(5).13

Epifani, M., & Stirparo, P. (2016). *Learning IOS Forensics* (2. Aufl.). Packt Publishing.

Jeon, S., Bang, J., Byun, K., & Lee, S. (2012). A recovery method of deleted record for SQLite database. *Personal and Ubiquitous Computing - PUC*, *16*, 1–9. https://doi.org/10.1007/s00779-011-0428-7

Liu, Y., Xu, M., Xu, J., Zheng, N., & Lin, X. (2017). SQLite Forensic Analysis Based on WAL. In R. Deng, J. Weng, K. Ren & V. Yegneswaran (Hrsg.), *Security and Privacy in Communication Networks* (S. 557–574). Springer International Publishing.

Pawlaszczyk, D. (2021). *Forensic SQLite Data Recovery Tool*. Verfügbar 25. Oktober 2022 unter https://www.staff.hs-mittweida.de/~pawlaszc/fqlite/

Pawlaszczyk, D., & Hummert, C. (2021). Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records. *International Journal of Cyber Forensics and Advanced Threat Investigations*, *1*(1–3), 27–41. https://doi.org/10.46386/ijcfati.v1i1-3.17

Sanderson, P. (2018). *SQLite Forensics*. Independently published.

Skulkin, O., Tindall, D., & Tamma, R. (2018). *Learning Android Forensics: Analyze Android Devices with the Latest Forensic Tools and Techniques* (2nd). Packt Publishing.

Spranger, M., Heinke, F., Appelt, L., Puder, M., & Labudde, D. (2016). MoNA: Automated Identification of Evidence in Forensic Short Messages. *International Journal On Advances in Security*, *9*(1&2), 14–24.

Spranger, M., & Labudde, D. (2014). Semantic Tools for Forensics: Towards Finding Evidence in Short Messages. In A. Schmidt & A. Yarali (Hrsg.), *Proc. 4th. International Conference on Advances in Information Mining and Management (IMMM)* (S. 1–4). IARIA.

Spranger, M., & Labudde, D. (2017). Textforensik. In D. Labudde & M. Spranger (Hrsg.), *Forensik in der digitalen Welt* (S. 167–198). Springer Spektrum Akademischer Verlag. https://doi.org/10.1007/978-3-662-53801-2_6

SQLite Consortium. (2018). *Write-Ahead Logging*. Verfügbar 25. Oktober 2022 unter https://www.sqlite.org/wal.html

Tenzer, F. (2022). *Anzahl der Smartphone-Nutzer in Deutschland bis 2021*. Verfügbar 25. Oktober 2022 unter https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Thebaity, M. A., Mishra, S., & Shukla, M. K. (2020). Forensic Analysis of Third-party Mobile Application. *HELIX*, *10*, 32–38. https://doi.org/10.29042/2020-10-4-32-38