HSPI The Open Access Publisher

J F S R JOURNAL OF FORENSIC SCIENCE AND RESEARCH
ISSN 2575-0186

Short Review

Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions

Nishchal Soni*

Lovely Professional University, India

Abstract

WhatsApp, a widely used instant messaging application, has become a valuable source of digital evidence in forensic investigations. This review article explores the forensic analysis techniques, challenges, and future directions associated with WhatsApp. It covers the extraction and analysis of data from various sources, including mobile devices, cloud backups, and network traffic. The article discusses the challenges faced by forensic examiners, such as encryption, data volatility, and the need for proper validation of tools. It also highlights the importance of keeping up with the latest updates and changes in WhatsApp's features and security measures. The future directions for WhatsApp forensics are explored, focusing on the development of more advanced and efficient analysis techniques, the need for standardization, and the importance of international cooperation in addressing cross-border investigations. This review provides insights for forensic examiners, researchers, and legal professionals involved in cases requiring WhatsApp evidence.

More Information

***Address for correspondence:** Nishchal Soni, Lovely Professional University, India, Email: forensicspedia@gmail.com

Submitted: May 29, 2024
Approved: June 17, 2024
Published: June 18, 2024

How to cite this article: Soni N. Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions. J Forensic Sci Res. 2024; 8: 019-024.

DOI: 10.29328/journal.jfsr.1001059

Keywords: WhatsApp forensics; Data extraction techniques; Encryption challenges; Forensic tool validation; Social media forensics

Check for updates

OPEN ACCESS

Introduction

WhatsApp, a cross-platform instant messaging application owned by Facebook, has over 2 billion users worldwide [1]. Its popularity and widespread use have made it a valuable source of digital evidence in forensic investigations, ranging from personal disputes to criminal cases [2]. The forensic analysis of WhatsApp involves the extraction, examination, and interpretation of data associated with the application [3].

The importance of WhatsApp forensics has grown significantly in recent years, as the application has become increasingly ubiquitous in both personal and professional contexts [4]. WhatsApp's ability to store and transmit a wide range of data, including text messages, images, videos, and audio files, has made it a treasure trove of potential evidence [5]. However, the use of end-to-end encryption in WhatsApp ensures the privacy and security of user communications but also hinders forensic investigations by preventing direct access to message content [6].

Forensic examiners employ a variety of techniques and tools to extract and analyze WhatsApp data from different sources, such as mobile devices, cloud backups, and network traffic [7]. These techniques range from logical and physical extractions to advanced methods like chip-off analysis and network protocol decryption [8]. The choice of technique depends on factors such as the type of device, the availability of backups, and the legal constraints of the investigation [3].

As WhatsApp continues to evolve, with the introduction of new features and updates to its security measures, forensic examiners must stay abreast of these changes to adapt their analysis techniques accordingly [4]. The application's global user base and the transnational nature of many investigations also highlight the need for international cooperation in WhatsApp forensics [5].

This review article aims to provide a comprehensive overview of the techniques, challenges, and future directions in the forensic analysis of WhatsApp. By examining the current state of WhatsApp forensics and the various approaches employed by forensic examiners, this article seeks to contribute to the development of best practices and the advancement of research in this critical field.

Data sources and extraction techniques

Mobile devices: The primary source of WhatsApp data is the mobile device on which the application is installed. Forensic examiners can extract data from the device using various techniques, such as logical extraction, physical extraction, and file system extraction [9]. Logical extraction involves acquiring data through the device's operating system, while physical extraction requires direct access to the device's

storage [10]. File system extraction focuses on specific files and directories related to WhatsApp [11]. Schrittwieser, et al. [12] discuss the challenges and techniques for acquiring data from mobile devices, emphasizing the importance of preserving the integrity of the evidence.

Cloud backups: WhatsApp offers the option to back up chat history and media to cloud storage services like iCloud and Google Drive [13]. Forensic examiners can obtain these backups with the appropriate legal authority and credentials [14]. Cloud backups provide an additional source of data, especially when the physical device is not available or when data has been deleted from the device [15]. Cheng, et al. [16] highlight the significance of cloud backups in mobile forensics and the need for robust acquisition and analysis techniques.

Network traffic: In some cases, forensic examiners may need to analyze network traffic to gather WhatsApp evidence. This can be done by intercepting and decrypting network packets or by using network forensic tools to reconstruct WhatsApp sessions [17]. However, the end-to-end encryption employed by WhatsApp makes it challenging to obtain meaningful data from network traffic [18]. Karpisek, et al. [19] discuss the techniques and limitations of network traffic analysis in the context of WhatsApp forensics.

Data analysis techniques

Database analysis: WhatsApp stores its data in SQLite databases on the mobile device [20]. Forensic examiners can use SQLite viewers and analysis tools to examine the contents of these databases, which include chat messages, contacts, call logs, and other metadata [21]. The analysis of the database structure and content can provide valuable insights into user activities and interactions [22].

One of the primary databases used by WhatsApp is the "msgstore.db" file, which contains the chat history and related information [23]. This database includes tables such as "messages," "chat_list," and "contacts," which store details about individual messages, chat sessions, and contact information, respectively [24]. By examining the data in these tables, forensic examiners can reconstruct conversations, identify participants, and establish timelines of events.

In addition to the main message database, WhatsApp also maintains other databases for storing user preferences, app settings, and media-related information. For example, the "wa.db" database contains information about the user's account, profile picture, and status updates. The "axolotl.db" database is associated with the end-to-end encryption feature and stores cryptographic keys and session information [25].

Forensic examiners can use various tools and techniques to analyze WhatsApp databases. SQLite viewers, such as DB Browser for SQLite or SQLite Expert, provide a graphical interface for browsing and querying the database contents. These tools allow examiners to view tables, execute SQL queries, and export data for further analysis. Command-line tools, such as SQLite command-line shell, can also be used for scripting and automating database analysis tasks.

When analyzing WhatsApp databases, forensic examiners should consider the potential for deleted or overwritten data. SQLite databases do not immediately remove deleted records but instead, mark them as unallocated space. Specialized tools and techniques, such as carving or recovery algorithms, can be used to extract deleted or partially overwritten data from the database files [26].

Media analysis: WhatsApp allows users to share various types of media, such as images, videos, and audio files. Forensic examiners can analyze these media files to extract metadata, such as timestamps, geolocation data, and device information. Media analysis can also involve the use of image and video forensics techniques to detect any manipulations or alterations to the original files [27].

When a user sends or receives media files through WhatsApp, the application automatically downloads and stores these files on the device's storage. The media files are typically stored in dedicated folders, such as "WhatsApp Images," "WhatsApp Videos," and "WhatsApp Audio." Forensic examiners can access these folders and analyze the media files using various forensic tools and techniques.

Metadata analysis is a crucial aspect of media forensics in WhatsApp investigations. Metadata is data that describes other data and can provide valuable information about the origin, creation, and modification of media files. Examiners can use metadata extraction tools, such as ExifTool or MediaInfo, to retrieve metadata from WhatsApp media files. This metadata may include details such as the date and time the file was created, the device model and manufacturer, and GPS coordinates if the media was captured using a camera with geolocation capabilities.

In addition to metadata analysis, forensic examiners may also apply image and video forensics techniques to detect any manipulations or alterations to the original media files. These techniques can help identify if a media file has been edited, cropped, or spliced using image editing software. Some common techniques include Error Level Analysis (ELA), which highlights compression artifacts and inconsistencies in an image, and Photo Response Non-Uniformity (PRNU) analysis, which can identify the unique noise pattern of the camera sensor used to capture the image [28].

Artifact analysis: WhatsApp generates various artifacts on the mobile device, such as log files, configuration files, and cache files. These artifacts can contain valuable information about user activities, settings, and interactions with the application. Forensic examiners can analyze these artifacts to reconstruct timelines, identify patterns, and gather additional evidence [29].

Log files are one of the essential artifacts in WhatsApp forensics. These files record various events and activities within the application, such as user logins, message timestamps, and error messages. WhatsApp stores log files in different locations depending on the operating system. On Android devices, log files are typically stored in the "/data/data/com.whatsapp/files/Logs" directory, while on iOS devices, they can be found in the application's sandbox directory. Forensic examiners can use log analysis tools or manual techniques to examine these log files and extract relevant information.

Configuration files are another important artifact in WhatsApp investigations. These files store user preferences, app settings, and other configuration data. On Android devices, the main configuration file is "com.whatsapp_preferences.xml," which is located in the "/data/data/com.whatsapp/shared_prefs" directory. This file contains information such as the user's registered phone number, last seen settings, and notification preferences. Forensic examiners can parse this XML file using text editors or specialized tools to extract the configuration data.

Cache files are temporary files created by WhatsApp to store frequently accessed data and improve application performance. These files can contain valuable forensic artifacts, such as thumbnails of shared images, profile pictures, and audio or video snippets. On Android devices, WhatsApp cache files are stored in the "/data/data/com.whatsapp/cache" directory. Forensic examiners can analyze these cache files using hex editors, image viewers, or carving tools to recover deleted or partially overwritten data [30].

Artifact analysis in WhatsApp forensics requires a thorough understanding of the application's file structure, data storage mechanisms, and operating system specificities. Forensic examiners should keep abreast of the latest WhatsApp versions and updates, as changes in the application's functionality or storage locations may impact the availability and interpretation of artifacts. Additionally, examiners should follow forensically sound practices, such as creating a forensic image of the device's storage, documenting the analysis process, and ensuring the integrity of the extracted artifacts.

Challenges in whatsapp forensics

Encryption: WhatsApp employs end-to-end encryption, which means that the communication between users is encrypted and can only be decrypted by the intended recipients [31]. This encryption poses a significant challenge for forensic examiners, as they cannot directly access the content of the messages without the encryption keys [32]. While encryption ensures the privacy and security of user communications, it can hinder forensic investigations [33].

WhatsApp uses the Signal Protocol, a highly secure encryption protocol that provides forward secrecy and protects against various types of attacks [34]. The encryption keys are generated and stored on the users' devices, making it difficult for forensic examiners to obtain them without physical access to the devices. Even if the examiner gains access to the encrypted data, decrypting it without the proper keys is computationally infeasible.

To overcome the challenges posed by encryption, forensic examiners may resort to alternative methods, such as analyzing unencrypted metadata, examining the device's memory for encryption keys, or using legal means to compel the disclosure of encryption keys [35]. However, these methods have their own limitations and may not always be feasible or legally permissible.

The use of encryption in WhatsApp has also raised debates about the balance between privacy and security on one hand and the needs of law enforcement and national security on the other. While encryption is essential for protecting user privacy and preventing unauthorized access to sensitive information, it can also be exploited by criminals and terrorists to evade detection and investigation.

Data volatility: WhatsApp data stored on mobile devices is subject to volatility, meaning that it can be easily modified or deleted by users [36]. Forensic examiners must be aware of the potential for data loss and take appropriate measures to preserve the evidence [37]. This may involve using write-blocking techniques, creating forensic images, and documenting the acquisition process [38].

The volatile nature of WhatsApp data can be attributed to several factors. Users can manually delete messages, chats, and media files from within the application, leaving no traces of the deleted data on the device's storage. WhatsApp also has a feature called "disappearing messages," which allows users to set a timer for messages to automatically delete after a specified period.

Moreover, WhatsApp data can be lost due to various reasons, such as device failure, factory reset, or overwriting new data. In such cases, the chances of recovering the lost data depend on factors like the device's storage type, the time elapsed since the deletion, and the amount of new data written to the storage.

To mitigate the risks associated with data volatility, forensic examiners should prioritize the acquisition of WhatsApp data as soon as possible. Live acquisition techniques, such as capturing the device's memory or creating a logical extraction while the device is still powered on, can help preserve volatile data that may be lost during a traditional forensic acquisition.

Tool validation: The forensic analysis of WhatsApp relies on various tools and software to extract and analyze data [39]. It is crucial for forensic examiners to validate these tools to ensure the accuracy and reliability of the results [40]. Validation involves testing the tools against known

datasets, comparing results with other established tools, and documenting any limitations or discrepancies [41]. The lack of proper validation can lead to the inadmissibility of evidence in legal proceedings.

Validating forensic tools is essential to ensure that the retrieved data is accurate, complete, and free from any alterations or artifacts introduced by the tool itself. Validation also helps establish the scientific validity of the forensic process and enhances the credibility of the evidence in court.

However, validating WhatsApp forensic tools can be challenging due to the constant updates and changes in the application's functionality and data storage mechanisms. Forensic tool developers need to keep pace with these changes and regularly update their tools to maintain compatibility and effectiveness.

Forensic examiners should use validated tools whenever possible and document the validation process, including the test cases, results, and any discrepancies observed. If using a non-validated tool is necessary, the examiner should disclose this fact in their report and explain the reasons for using the tool and any potential limitations or uncertainties associated with the results.

Keeping up with updates: WhatsApp continuously evolves, introducing new features, updating its security measures, and modifying its data storage mechanisms [42]. Forensic examiners must stay up-to-date with these changes to adapt their analysis techniques accordingly [43]. Failure to keep up with the latest updates can result in missing or misinterpreting crucial evidence.

WhatsApp regularly releases updates that introduce new features, fix bugs, and improve security. These updates can change the way data is stored, encrypted, or transmitted, rendering existing forensic techniques and tools obsolete. For example, a new encryption algorithm or key management system may require forensic examiners to develop new methods for accessing and decrypting the data.

Additionally, WhatsApp may introduce new features that generate new types of artifacts or metadata that could be relevant to forensic investigations. For instance, the introduction of WhatsApp payments or business accounts may create new sources of financial or transactional data that forensic examiners need to be aware of and know how to acquire and analyze.

To keep up with the latest updates, forensic examiners should regularly monitor official WhatsApp announcements, release notes, and technical documentation. They should also participate in professional forums, attend training and conferences, and collaborate with other experts in the field to share knowledge and best practices.

Forensic tool developers also play a crucial role in keeping up with WhatsApp updates. They should work closely with the forensic community to identify new requirements and challenges and develop timely updates to their tools to address these changes.

Conclusion and future recommendations

The forensic analysis of WhatsApp has become an increasingly important aspect of digital investigations, given the widespread use of the application for communication and the potential for it to contain valuable evidence. This review article has explored the various techniques, challenges, and future directions associated with WhatsApp forensics.

The extraction and analysis of WhatsApp data from mobile devices, cloud backups, and network traffic have been discussed in detail, highlighting the importance of a comprehensive approach to data acquisition. Database analysis, media analysis, and artifact analysis are the key techniques used to examine WhatsApp data and uncover relevant information about user activities, interactions, and timelines.

However, the forensic analysis of WhatsApp is not without its challenges. End-to-end encryption, implemented using the Signal Protocol, is a major hurdle for forensic examiners, as it prevents direct access to the content of user communications. The volatile nature of WhatsApp data stored on mobile devices also poses a risk of data loss, requiring forensic examiners to take prompt and appropriate measures to preserve the evidence. Tool validation is crucial to ensure the accuracy and reliability of the forensic analysis results, but it can be challenging due to the constant updates and changes in WhatsApp's functionality and data storage mechanisms. Keeping up with these updates is essential for forensic examiners to adapt their techniques and avoid missing or misinterpreting crucial evidence. To address these challenges and advance the field of WhatsApp forensics, several future recommendations can be made. First, there is a need for continued research and development of forensic tools and techniques that can effectively deal with the challenges posed by encryption and data volatility. This may involve exploring alternative methods for accessing encrypted data, such as analyzing unencrypted metadata or using legal means to compel the disclosure of encryption keys. Researchers should also focus on developing more robust and efficient data preservation and acquisition techniques to mitigate the risks of data loss.

Second, the forensic community should work towards establishing standard procedures and guidelines for WhatsApp forensics. This would help ensure consistency and reliability in the acquisition, analysis, and reporting of WhatsApp evidence across different jurisdictions and organizations. The development of standardized test datasets and validation methodologies would also facilitate the evaluation and comparison of different forensic tools and techniques.

Third, collaboration and information sharing among forensic examiners, researchers, and tool developers are essential to keep pace with the rapidly evolving landscape of WhatsApp forensics. Regular communication and knowledge exchange through professional forums, conferences, and workshops can help identify new challenges, share best practices, and foster innovation in the field. Fourth, there is a need for enhanced training and education programs for forensic examiners to equip them with the necessary skills and knowledge to handle WhatsApp forensics effectively. This should include training on the latest tools and techniques, as well as an understanding of the legal and ethical considerations surrounding the acquisition and analysis of WhatsApp data.

Finally, the forensic community should engage in ongoing dialogue with policymakers, legal experts, and privacy advocates to address the complex issues surrounding the use of encryption in communication applications like WhatsApp. Balancing the legitimate needs of law enforcement and national security with the fundamental rights to privacy and security is a delicate task that requires careful consideration and informed decision-making.

References

1. WhatsApp. About WhatsApp. 2021. https://www.whatsapp.com/about/
2. Anglano C. Forensic analysis of WhatsApp Messenger on Android smartphones. Dig Investig. 2014; 11(3):201-213.
3. Barmpatsalou K, Cruz T, Monteiro E, Simoes P. Current and future trends in mobile device forensics: A survey. ACM Comput Surv. 2018; 51(3):1-31.
4. Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of Android social-messaging applications. Dig Investig. 2015;14
5. .Satrya GB, Daely PT, Shin SY. Android forensics analysis: Private chat on social messenger. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). 2016; 430-435.
6. Gregorio J, Gardel A, Alarcos B. Forensic analysis of Telegram Messenger for Windows Phone. Dig Investig. 2017; 22:88-106.
7. Zhang X, Baggili I, Breitinger F. Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. Comput Secur. 2017; 70:516-531.
8. Faheem M, Le-Khac NA, Kechadi T. Smartphone forensic analysis: A case study for obtaining root access of an Android Samsung S3 device and analyse the image without an expensive commercial tool. J Inf Secur. 2021; 2014.
9. Chernyshev M, Zeadally S, Baig Z, Woodward A. Mobile forensics: Advances, challenges, and research opportunities. IEEE Secur Priv. 2017; 15(6):42-51.
10. Jiang F, Zhang K. WhatsApp forensics on iPhone. In: Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, Prague, Czech Republic. Proceedings. Springer. 2017; 2016:195.
11. Shortall A, Azhar MAHB. Forensic acquisitions of WhatsApp data on popular mobile platforms. In: 2015 Sixth International Conference on Emerging Security Technologies (EST); 2015; 13-17.
12. Schrittwieser S, Kieseberg P, Weippl E, Holzinger A. Security and privacy in mobile devices and applications. In: Trends and Advances in Information Systems and Technologies. Springer; 2016; 767-777.
13. WhatsApp. About end-to-end encryption. 2021. Available from: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en
14. Yusoff MN, Dehghantanha A, Mahmod R. Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies. In: Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Syngress; 2017; 41-62.
15. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Dig Investig. 2012; 9.
16. .Cheng L, van Dongen BF, van der Aalst WM. Efficient event correlation over distributed systems. In: 2019 IEEE 35th International Conference on Data Engineering (ICDE); 2019; 1690-1693.
17. Sgaras C, Kechadi MT, Le-Khac NA. Forensics acquisition and analysis of instant messaging and VoIP applications. In: Computational Forensics. Springer, Cham; 2015; 188-199.
18. Majeed A, Zia H, Imran R, Saleem S. Forensic analysis of three social media apps in Windows 10. In: 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET); 2015; 1-5.
19. Karpisek F, Baggili I, Breitinger F. WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. Dig Investig. 2015; 15:110-118.
20. Anglano C. Forensic analysis of WhatsApp Messenger on Android smartphones. Dig Investig. 2014; 11(3):201-213.
21. Thakur NS. Forensic analysis of WhatsApp on Android smartphones [dissertation]. 2013.
22. Levendoski M, Datar T, Rogers M. Yahoo! Messenger forensics on Windows Vista and Windows 7. In: IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg; 2014; 317-329.
23. Majeed A, Zia H, Imran R, Saleem S. Forensic analysis of three social media apps in Windows 10. In: 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET); 2015; 1-5.
24. Mehrotra S, Mehtre BM. Forensic analysis of Wickr application on Android devices. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCICR); 2013; 1-6.
25. Satrya GB, Daely PT, Nugroho MA. Digital forensic analysis of Telegram Messenger on Android devices. In: 2016 International Conference on Information & Communication Technology and Systems (ICTS); 2016; 1-7.
26. Jain A, Chhabra GS. Anti-forensics techniques: An analytical review. In: 2014 Seventh International Conference on Contemporary Computing (IC3); IEEE. 2014; 412-418.
27. Meffert C, Baggili I, Breitinger F. Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security; 2016; 1-11.
28. Lukáš J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Trans Inf Forensics Secur. 2006; 1(2):205-214.
29. Chu HC, Deng DJ, Park JH. Live data mining concerning social networking forensics based on a Facebook session through aggregation of social data. IEEE J Sel Areas Commun. 2011; 29(7):1368-1376.
30. Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. Forensic artifacts of Facebook's instant messaging service. In: 2011 International Conference for Internet Technology and Secured Transactions; IEEE. 2011; 771-776.
31. WhatsApp. WhatsApp Encryption Overview. 2021. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
32. Carvey H. Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8. Elsevier; 2014.
33. Casey E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press; 2011.
34. Kobeissi N, Bhargavan K, Blanchet B. Automated verification for secure

messaging protocols and their implementations: A symbolic and computational approach. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE. 2017 Mar; 435-450.

35. Vaziripour E, Wu J, O'Neill M, Metro D, Cockrell J, Moffett T, Seamons K, et al. Action needed! Helping users find and complete the authentication ceremony in signal. In: Proceedings of the Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019); 2019 May.

36. Nguyen TT, Dinh HT, Huynh HA. WhForensics: a forensics tool for WhatsApp. In: 2019 6th NAFOSTED Conference on Information and Computer Science (NICS). IEEE. 2019 Nov; 541-546.

37. Martini B, Do Q, Choo KKR. Mobile cloud forensics: An analysis of seven popular Android apps. arXiv preprint arXiv:1506.05533. 2015.

38. Zhang X, Baggili I, Breitinger F. Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. Comput Secur. 2017; 70:516-531.

39. Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of Android social-messaging applications. Dig Investig. 2015;14

40. Barmpatsalou K, Damopoulos D, Kambourakis G, Katos VA critical review of 7 years of Mobile Device Forensics. Dig Investig. 2013; 10(4):323-349.

41. Ayers R, Brothers S, Jansen W. Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). National Institute of Standards and Technology. 2014.

42. Anglano C. Forensic analysis of WhatsApp Messenger on Android smartphones. Dig Investig. 2014; 11(3):201-213.

43. Gregorio J, Gardel A, Alarcos B. Forensic analysis of Telegram Messenger for Windows Phone. Dig Investig. 2017; 22:88-106.