

**DEVELOPMENT OF AN INTEGRATED DASHBOARD FOR BITCOIN
FORENSIC ANALYSIS USING PUBLICLY AVAILABLE TOOLS.**

By

Zhilan Fadhlurrahman Firdaus
12202001

BACHELOR'S DEGREE
in

INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING & INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

June 2026

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Zhilan Fahdlurrahman Firdaus

Student



Date 13/06/2026

Approved by:



Dipl.-Inf I Eng Kho

19/06/2026

Thesis Advisor

Date



Kalpin Erlangga Silaen, S.Si., M.Kom., CISSP, CEH, ECIH,
ECSA, CHFI

19/06/2026

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium, S.Kom., M.Sc

Dean

Date

Zhilan Fahdlurrahman Firdaus

ABSTRACT

DEVELOPMENT OF AN INTEGRATED DASHBOARD FOR BITCOIN FORENSIC ANALYSIS USING PUBLICLY AVAILABLE TOOLS

By

Zhilan Fadhlurrahman Firdaus

Dipl.-Inf I EngKho, Advisor

Kalpin Erlangga Silaen, S.Si., M.Kom., CISSP, CEH, ECIH, ECSA, CHFI, Co-
Advisor

SWISS GERMAN UNIVERSITY

Bitcoin forensic investigations are increasingly hampered by the use of different tools for a case, high commercial licensing costs, and the absence of standardised investigative procedures, particularly within law enforcement such as in Indonesia. No publicly available tool currently integrates transaction graph visualisation, multi-hop fund tracing, entity attribution, and abuse intelligence into a single open-source interface, forcing investigators to manually reconcile outputs across multiple platforms

and introducing inconsistencies that undermine forensic reproducibility. This study addresses that gap by presenting Cryptrace, a unified open-source Bitcoin forensic dashboard that consolidates five publicly available tools Mempool.space, Blockstream (Esplora), WalletExplorer, Chainabuse, and Bitquery into a single investigative interface incorporating interactive transaction graph visualisation, heuristic-based entity attribution, automated multi-hop fund tracing, three-layer coin mixer detection, and session persistence for evidentiary chain-of-custody compliance. Development followed an Agile Software Development Life Cycle across five iterative phases, and the system was evaluated through four controlled forensic test scenarios alongside a structured user study involving thirteen personnel from Indonesia's PUSLABFOR Digital Forensic Division. Results confirmed full data consistency across all five integrated sources and demonstrated successful identification of peeling chains, CoinJoin activity, and sweeping patterns across three real-world ransomware cases involving the SamSam, LockBit, and Lazarus Group operations. User testing produced a 54% reduction in mean investigation time compared to conventional single-tool methods, and the session persistence feature received approval for its evidentiary value. However, rendering performance degraded on high-volume addresses, open-source methods could not bridge deposit-withdrawal gaps within advanced mixing services, and the absence of a national forensic SOP in Indonesia introduced investigator-dependent variability that the tool alone cannot resolve. Cryptrace demonstrates that publicly available tools, when unified, can satisfy preliminary forensic reproducibility requirements without dependence on proprietary or commercially licensed software.

Keywords: Bitcoin forensics, blockchain analysis, transaction graph visualisation, coin mixer detection, open-source intelligence.

© Copyright 2025

by Zhilan Fadhlurrahman Firdaus

All rights reserved



DEDICATION

I would like to express my deepest gratitude to my parents, Risa Nofiani and Hendri Firdaus, for their unwavering love, sacrifices, and support throughout my academic journey. Their constant encouragement has been my anchor through every challenge I faced over the years.

To my brother Ahmad, thank you for always looking up to me, and for the countless shared moments from childhood toys to our long gaming sessions.

I am also grateful to my long-time friends, Nelson, Clayton, and Kenneth. Thank you for standing by my side for nearly a decade; your enduring friendship means more than words can express.

I would like to thank my new friends I've made on my journey, Fannisa, Esther, Ryan, and Kevin. I am incredibly fortunate to have met you all, and I truly appreciate the time, support, and all the ups and downs we have shared since our paths crossed.

This achievement would not have been the same without all of you.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all the lecturers and staff at SGU who supported me throughout this journey. I am deeply grateful to Pak Kho and Pak Kalpin for their invaluable guidance during the development of this software; their insights challenged my perspectives and helped me address critical elements I had otherwise overlooked.

I also wish to extend my formal thanks to the PUSLABFOR Digital Forensics division for their vital participation and cooperation in the development of Cryptrace. I owe a special debt of gratitude to Commander Pak Panji Zulfikar Sidik, S.I.K., M.T.I., CEH., ECIH., MCFE., for his exceptional support, technical expertise, and for facilitating the resources necessary to bring this project to fruition.

Finally, I am grateful for the thoughtful environment provided by the entire academic program, which equipped me with the essential tools to explore these complex programming concepts with excellence.

TABLE OF CONTENTS

	Page
DEDICATION.....	6
1.1 Background	14
1.2 Problem Statement	15
1.3 Objectives.....	16
1.4 Research Questions	17
1.5 Hypothesis.....	17
1.6 Significance of study.....	18
1.7 Scope and limitations	18
2.1 Theoretical Perspectives	20
2.1.1 Multi-Source Data Fusion	20
2.1.2 Graph Theory and the Bitcoin UTXO Model.....	22
2.1.3 Multi-signal heuristic scoring system	23
2.1.4 Digital Forensic Governance Frameworks	24
2.1.5 Agile Software Development Methodology	25
2.2 Previous Studies.....	26
2.2.1 Evolution of Anti-Forensic Obfuscation Techniques	26
2.2.2 Address Clustering and Entity Attribution	29
3.1 Requirements and Design	30
3.2 System Architecture Design.....	33
3.2.1 System Core Architecture and Artifacts	34
3.2.2 Multi-Source Data Collection and Aggregation Engine	34
3.2.3 Open-Source Intelligence Entity Categorisation	35
3.2.4 Coin Mixer Detection.....	36
3.2.5 Entity Grouping Heuristics	37
3.2.6 Interactive Graph Visualisation	38
3.3 Cryptrace and BACH: A Comparative Overview	39
3.4 Testing and Deployment	40
3.4.1 Scenario 1: Depositing Funds into a Bitcoin Address via Exchange using Onmeta and BEST Wallet.....	41

3.4.2 Scenario 2: Test for validity and consistency of information of the sources	44
3.4.3 Scenario 3: Transferring Bitcoin to another Bitcoin address.....	48
3.4.4 Scenario 4: Coin Mixer Detection.	49
3.5 PUSLABFOR Testing scenario results and feedback	59
3.5.1 Tool limitations observed by users	62
3.5.2 Participants Feedback and Discussion.	67
3.6 Testing Conclusion	69
4.1 Scenario Results	70
4.2 Coin Mixer Detection and Limitations	71
4.3 Coin Mixer Detection and Limitations	75
4.4 Discussion Against Hypothesis.....	76
5.1 Conclusions	77
5.2 Recommendations.....	78
5.3 Future Works.....	78
GLOSSARY	79
REFERENCES	83
APPENDIX.....	87
APPENDIX 1: GitHub Link to Cryptrace.....	87

LIST OF FIGURES

Figures	Page
Figure 1. The framework for cryptocurrency forensic analysis pipeline designed to transform raw blockchain data into structured investigative intelligence.	21
Figure 2. The phases of Agile SDLC (Agile SDLC (Software Development Life Cycle), 2025)	25
Figure 3. A Bitcoin mixer detection framework proposed by Wu et al.	26
Figure 4. A transaction conducted involving a coin mixer visualised using Neo4J (Tippe & Deckers, 2025).	27
Figure 5. The process of Agile Software Development Life Cycle to develop Cryptrace (Agile SDLC (Software Development Life Cycle), 2025).	30
Figure 6. System Architecture design of Cryptrace.	33
Figure 7. The process of buying Bitcoin using BEST Wallet and Onmeta payment gateway.	41
Figure 8. Cryptrace dashboard view of the test address A: bc1qseccp0hj8s63mlh9qlxzruh37mger73842mxra, highlighted in purple. The visualisation shows a cluster of associated addresses attributed to the Onmeta exchange, indicating multiple transactional links converging on the target address.	42
Figure 9. The test address A: bc1qseccp0hj8s63mlh9qlxzruh37mger73842mxra highlighted in purple among the other handful of addresses.	42
Figure 10. Cryptrace displays a set of information for the selected Bitcoin address bc1q4ysrrs8jr9dfcxxpq6gat9etjv88dvfa2z05v5, highlighted in green, and illustrates its connection to the test address A, highlighted in purple.	43
Figure 11. Mempool.space's information showing recent transaction and unspent outputs from bc1q4ysrrs8jr9dfcxxpq6gat9etjv88dvfa2z05v5.	43
Figure 12. Mempool.space showing the test Bitcoin address A: bc1qseccp0hj8s63mlh9qlxzruh37mger73842mxra with a confirmed balance of 0.00005194 BTC and two recorded transactions, used as a baseline reference in Scenario 1.	44
Figure 13. WalletExplorer.com displaying the same test address with two matching transaction entries and balance data consistent with the Mempool.space output, confirming cross-tool data consistency.	45
Figure 14. WalletExplorer.com's list of entities that has their Bitcoin addresses identified and categorised.	45
Figure 15. WalletExplorer.com's list of entities that has their Bitcoin addresses identified and categorised.	46
Figure 16 Chainabuse returning no abuse reports for the test address.	46
Figure 17. Blockstream (Esplora) explorer view of the test address showing UTXO status, input/output addresses, block confirmation count, and fee data consistent with outputs from the other three integrated sources.	47

Figure 18. Bitquery is an API only, so its results are incorporated to Cryptrace. The dashboard is showing the exchange company in this case Onmeta.in networks of Bitcoin addresses.	48
Figure 19. BEST Wallet Home page showing a process of transferring Bitcoin into Wallet 2.	48
Figure 20. Cryptrace showing two Bitcoin address involved in the transaction. Wallet 1 (bc1qseccp0hj8s63mlh9qlxruh37mger73842mxra) which is marked in purple and Wallet 2 (bc1ql752c58uruh8tyrtuwadrtzgytw83vpkegzx5) which is marked in blue.	49
Figure 21. The presence of these three structural features in conjunction pooling clusters, fan-shaped distribution nodes, and a linear peeling chain provides strong indicators that the subject address is interacting with a Bitcoin mixing service (Tippe and Deckers, 2025).	50
Figure 22. The address 1AjZPMsnmpdK2Rv9KQNfMurTXinseVro9V highlighted in green showing multiple transaction hops in a peeling chain pattern.	51
Figure 23. The funds pooling cluster can be identified by seeing the cluster of blue nodes.	51
Figure 24. The funds pooling cluster can be identified below the peeling chain pattern and the cluster of blue nodes.	52
Figure 25. Wallet A is highlighted in red, and Wallet B is highlighted in purple. Cryptrace graph is showing a peeling chain pattern.	52
Figure 26. The pooling of funds cluster can be observed in both analysis.	53
Figure 27. The transaction ID (314cec569296044235344897098e75f59fc402d6dd1f6890fed0d30c9d3a5c6a) is provided by Cryptrace on the left.	53
Figure 28. A snippet of the peeling chain pattern observed in Cryptrace when examining the Bitcoin address 18gaXypKj9M23S2zT9qZfL9iPbLFM372Q5 highlighted in yellow.	54
Figure 29. The large cluster of nodes observed in Cryptrace when examining the Bitcoin address 18gaXypKj9M23S2zT9qZfL9iPbLFM372Q5 highlighted in yellow.	54
Figure 30. Bitcoin Address A analysis in Cryptrace, Address B and C can be seen in one of the peeling chain patterns.	55
Figure 31. The transaction entity 03a7851ea44ed92949138e65a760064308c51171edd8246a8375d13e20475b3d has been marked by Cryptrace as a transaction with CoinJoin mixer characteristics.	56
Figure 32. Cryptrace's confidence reasoning for marking the transaction entity as a CoinJoin mixer.	56
Figure 33. Cryptrace identifying Address B as Huobi.com-2.	57
Figure 34. WalletExplorer.com attributing the Address B as Huobi.com-2.	57
Figure 35. Cryptrace dashboard showing the transaction entity with the ID of 0129046c46734c88558e4f9dd699d2510c2f8f181edbb32d6cb03d0f26e952ff distributing 0.0000101 BTC to multiple addresses.	58
Figure 36. Address C sends 0.0000101 BTC to a transaction entity with the ID cf6090dddacf7dd27af3933458a2cda6e32261dad5f23b2f76dc2f16c90594be which is a funds pooling cluster.	59
Figure 37. A Google form exercise for the test scenario being conducted on the participant.	60

- Figure 38. A graph showing the improvements in time to conclusion compared to the standard tools and Cryptrace. 61
- Figure 39. Mempool.space results failed to display Address B directly. Instead, the search returned a Bitcoin address 3HLAvTRZBcxgEskmsfnvvSMRmVE5FU1RxJ as the first result. 63
- Figure 40. Mempool.space search result of the Bitcoin address 3HLAvTRZBcxgEskmsfnvvSMRmVE5FU1RxJ. Within the list of transaction, address B was found. 63
- Figure 41. WalletExplorer search result of Address A and the list of transaction ID. 64
- Figure 42. WalletExplorer search result of bc1q4ysrrs8jr9dfcxxpq6gat9etjv88dvfa2z05v5 and the list of transaction ID. This address was found by the participants when in search of Address B. 64
- Figure 43. MetaSleuth search result of Address B, it can be observed that MetaSleuth managed to show the participant the timestamp and Bitcoin address connected to it including the Bitcoin address 3HLAvTRZBcxgEskmsfnvvSMRmVE5FU1RxJ. 65
- Figure 44. MetaSleuth search result of Address A and B, participants wasn't able to connect the two address and correlate. 65
- Figure 45. Participants are able to link the target Address B through the Bitcoin address bc1q4ysrrs8jr9dfcxxpq6gat9etjv88dvfa2z05v5. 66
- Figure 46. Participants can link the target Address B which is coloured in red through the graph provided by Cryptrace. 66
- Figure 47. A closer examination of the Address B in Cryptrace. 67
- Figure 48. Google Forms feedback describing the user's challenges. 68
- Figure 49. Google Forms feedback describing the user's approximate time saved during an investigation using Cryptrace. 68
- Figure 50. Google Forms feedback describing the user's feedback when using Cryptrace to identify a transaction has a Coin mixer involved. 69
- Figure 51. A screenshot of Cryptrace search result for 17UVSMegvrzfobKC82dHXpZLtLcqzW9stF Bitcoin address and the transaction history with a sweeping chain pattern. 71
- Figure 52. A screenshot of Mempool search result for 17UVSMegvrzfobKC82dHXpZLtLcqzW9stF Bitcoin address and the transaction history in 2018/08/21 where an exact amount of 6.00000000 Bitcoin is transferred in 10:24:03. 72
- Figure 53. A screenshot of Mempool search result for 17UVSMegvrzfobKC82dHXpZLtLcqzW9stF Bitcoin address and the transaction history in 2018/08/21 where an exact amount of 6.00000000 Bitcoin is transferred in 21:31:28. 72
- Figure 54. A screenshot captured from Mempool.space regarding the Bitcoin address bc1q4ysrrs8jr9dfcxxpq6gat9etjv88dvfa2z05v5 illustrates inconsistent timing patterns and different transaction volumes. 73

LIST OF TABLES

Table	Page
Table 1. A List of studies that has been reviewed and its contribution.	28
Table 2. A table of questionnaire and answers from the interview conducted with personnel from PUSLABFOR Digital forensic division.	31
Table 3. A list of criteria Crytrace has to fulfill in order to complete the requirements from the interview and research objective.	32
Table 4. Feature comparisons between BACH Dashboard and Crytrace.	40
Table 5. Bitcoin addresses selected for the testing scenarios.	55
Table 6. Table of results from the test case.	61
Table 7. Tools and participants notes and observation.	62
Table 8. Comparison of Crytrace coin mixer detection findings with prior literature.	74

LIST OF LISTINGS

Listings	Page
Listing 1. Data Provenance Structure for Evidence Logging..	34
Listing 2. Multi-Source Fallback Routing Mechanism.	35
Listing 3. OSINT profiling and threat classification.	36
Listing 4. Algorithmic patten matching for mixing services.	36
Listing 5. Union-Find Co-Spend Address Clustering Heuristic.	37
Listing 6. Force-Directed Graph Rendering Script for the Interface Layer.	38