

CITATION REPORT

List of articles citing

Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms

DOI: 10.1080/00450618.2015.1066854

Australian Journal of Forensic Sciences, 2016, 48, 469-488.

Source: <https://exaly.com/paper-pdf/65711842/citation-report.pdf>

Version: 2024-04-28

This report has been generated based on the citations recorded by exaly.com for the above article. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

#	Paper	IF	Citations
60	Exploit Kits: The production line of the Cybercrime economy?. 2015 ,		19
59	Scenario-Based Digital Forensics Challenges in Cloud Computing. <i>Symmetry</i> , 2016 , 8, 107	2.7	7
58	An Ensemble Learning Approach for Addressing the Class Imbalance Problem in Twitter Spam Detection. <i>Lecture Notes in Computer Science</i> , 2016 , 215-228	0.9	6
57	Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. <i>Australian Journal of Forensic Sciences</i> , 2016 , 48, 615-642	1.1	27
56	Cloud storage forensics: MEGA as a case study. <i>Australian Journal of Forensic Sciences</i> , 2017 , 49, 344-357	1.1	35
55	Contemporary Digital Forensics Investigations of Cloud and Mobile Applications. 2017 , 1-6		3
54	Forensic Taxonomy of Android Social Apps. <i>Journal of Forensic Sciences</i> , 2017 , 62, 435-456	1.8	14
53	Forensics Analysis of Android Mobile VoIP Apps. 2017 , 7-20		10
52	Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS. 2017 , 41-62		7
51	Astroturfing detection in social media: a binary n-gramBased approach. <i>Concurrency Computation Practice and Experience</i> , 2017 , 29, e4013	1.4	17
50	Mobile Phone Forensics. 2017 , 79-89		6
49	An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes from Windows 8.1. <i>International Journal of Electronic Security and Digital Forensics</i> , 2017 , 9, 326	1	2
48	Investigating Storage as a Service Cloud Platform: pCloud as a Case Study. 2017 , 185-204		8
47	Current and Future Trends in Mobile Device Forensics. <i>ACM Computing Surveys</i> , 2018 , 51, 1-31	13.4	25
46	Forensics study of IMO call and chat app. <i>Digital Investigation</i> , 2018 , 25, 5-23	3.3	6
45	Cyber Threat Intelligence. <i>Advances in Information Security</i> , 2018 ,	0.7	4
44	Profiling of secure chat and calling apps from encrypted traffic. 2018 ,		

43	Electronic crime investigations in a virtualised environment: a forensic process and prototype for evidence collection and analysis. <i>Australian Journal of Forensic Sciences</i> , 2018 , 50, 183-208	1.1	1
42	Detecting crypto-ransomware in IoT networks based on energy consumption footprint. <i>Journal of Ambient Intelligence and Humanized Computing</i> , 2018 , 9, 1141-1152	3.7	123
41	An Evidence-Based Forensic Taxonomy of Windows Phone Communication Apps. <i>Journal of Forensic Sciences</i> , 2018 , 63, 868-881	1.8	2
40	CloudMe forensics: A case of big data forensic investigation. <i>Concurrency Computation Practice and Experience</i> , 2018 , 30, e4277	1.4	24
39	Forensics on Twitter and WeChat Using a Customised Android Emulator. 2018 ,		1
38	Acquisition and Analysis of Forensic Data Artefacts of Some Popular Apps in Android Smartphone. 2018 ,		
37	User Relationship Classification of Facebook Messenger Mobile Data using WEKA. <i>Lecture Notes in Computer Science</i> , 2018 , 337-348	0.9	3
36	Browser Analysis of Residual Facebook Data. 2018 ,		
35	A Cluster-based Approach of Smartphone Camera Fingerprint for User Profiles Resolution within Social Network. 2018 ,		2
34	Mobile Forensics: A Bibliometric Analysis. <i>Advances in Information Security</i> , 2018 , 297-310	0.7	8
33	Machine Learning Aided Static Malware Analysis: A Survey and Tutorial. <i>Advances in Information Security</i> , 2018 , 7-45	0.7	35
32	Spam comments prediction using stacking with ensemble learning. <i>Journal of Physics: Conference Series</i> , 2018 , 933, 012012	0.3	9
31	Social Network Forensics through Smartphones and Shared Images. 2019 ,		1
30	Hybrid Clustering of Shared Images on Social Networks for Digital Forensics. <i>IEEE Access</i> , 2019 , 7, 87288-87302	3.3	3026
29	On approximate nesting of multiple social network graphs. 2019 ,		0
28	Map My Murder. 2019 ,		1
27	Research on Forensic Model of Online Social Network. 2019 ,		2
26	Big Data Forensics: Hadoop Distributed File Systems as a Case Study. 2019 , 179-210		2

25	Evaluation and Application of Two Fuzzing Approaches for Security Testing of IoT Applications. 2019 , 301-327		2
24	Private Cloud Storage Forensics: Seafile as a Case Study. 2019 , 73-127		4
23	An analysis of anti-forensic capabilities of B-tree file system (Btrfs). <i>Australian Journal of Forensic Sciences</i> , 2020 , 52, 371-386	1.1	7
22	Forensic analysis of BiP Messenger on android smartphones. <i>Australian Journal of Forensic Sciences</i> , 2020 , 52, 590-609	1.1	2
21	Data Collection Techniques for Forensic Investigation in Cloud. 2020 ,		5
20	UML-based process model for mobile cloud forensic application framework - a preliminary study. <i>International Journal of Electronic Security and Digital Forensics</i> , 2020 , 12, 262	1	
19	Study of identifying and managing the potential evidence for effective Android forensics. <i>Forensic Science International: Digital Investigation</i> , 2020 , 33, 200897	1	6
18	No Matter What Images You Share, You Can Probably Be Fingerprinted Anyway. <i>Journal of Imaging</i> , 2021 , 7,	3.1	3
17	Forensic analysis of open-source XMPP/Jabber multi-client instant messaging apps on Android smartphones. <i>SN Applied Sciences</i> , 2021 , 3, 1	1.8	1
16	Forensic analysis of open-source XMPP multi-client social networking apps on iOS devices. <i>Forensic Science International: Digital Investigation</i> , 2021 , 36, 301122	1	1
15	NLP-based digital forensic investigation platform for online communications. <i>Computers and Security</i> , 2021 , 104, 102210	4.9	5
14	Forensic analysis of Twitch video streaming activities on Android. <i>Journal of Forensic Sciences</i> , 2021 , 66, 1721-1741	1.8	1
13	Android vs. IOS: a comparative analysis over mobile operator infrastructures based on crowdsourced mobile dataset. <i>Telecommunication Systems</i> , 2021 , 78, 405	2.3	0
12	To sell, or not to sell: social media data-breach in second-hand Android devices. <i>Information and Computer Security</i> , 2021 , ahead-of-print,	1.4	
11	User profiles image clustering for digital investigations. <i>Forensic Science International: Digital Investigation</i> , 2021 , 38, 301171	1	0
10	A Closer Look at Syncany Windows and Ubuntu Clients Residual Artefacts. <i>Lecture Notes in Computer Science</i> , 2016 , 342-357	0.9	5
9	Bibliometric Analysis on the Rise of Cloud Security. 2019 , 329-344		1
8	An Empirical Study on Acquisition of Digital Evidences from Facebook Using Various Tools and Techniques. <i>Lecture Notes in Electrical Engineering</i> , 2020 , 870-883	0.2	

7	Forensic Analysis of Popular Social Media Applications on Android Smartphones. <i>Balkan Journal of Electrical and Computer Engineering</i> ,	0.3	o
6	Shared Images and Camera Fingerprinting May Lead to Privacy Issues. <i>Advanced Sciences and Technologies for Security Applications</i> , 2020 , 3-19	0.6	
5	Forensic investigation of instant messaging services on linux OS: Discord and Slack as case studies. <i>Forensic Science International: Digital Investigation</i> , 2022 , 42, 301401	1	
4	Sickly Apps: A Forensic Analysis of Medical Device Smartphone Applications on Android and iOS Devices.		o
3	Badoo Android and iOS Dating Application Analysis.		o
2	Social Networking Applications: A Comparative Analysis for a Collaborative Learning through Google Classroom and Zoom. 2022 , 210, 61-69		o
1	Network Forensic Analysis of Twitter Application on Android OS. 2022 ,		o