Digital Forensics Research Topics

This document contains a collection of research topics in digital forensics domain. This collection forms only a fraction of all possible issues. Each item is accompanied by a list of the main reference that the student should read to identify more specific problems in the particular area.

The covered areas are:

1. Smart Device Forensics
2. Internet-of-Things Forensics
3. VoIP Forensics
4. Cloud Forensics
5. Instant Messaging forensics
6. Web Browser Forensics
7. Social Network Forensics
8. Forensics Data Vizualization
9. Mobile Forensics
10. Network Forensics
11. Anti-forensics

1. Smart Device Forensics

Smart devices have different shape and purpose. Because they are small computers, they have an operating system and thus can contain valuable data for forensics investigators. Digital forensics of electronic devices are now more focusing on the forensics of smart devices because they are increasing in numbers. Devices like smart TVs, watches, navigation tools, and other devices can often be a source of evidence.

REFERENCES:

- Arabo, A., Brown, I., & El-Moussa, F. (2012). Privacy in the age of mobility and smart devices in smart homes. In Proceedings - 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012 (pp. 819–826). http://doi.org/10.1109/SocialCom-PASSAT.2012.108
- Baggili, I., Oduro, J., Anthony, K., Breitinger, F., & McGee, G. (2015). Watch what you wear: Preliminary forensic analysis of smart watches. In Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015 (pp. 303–311). http://doi.org/10.1109/ARES.2015.39
- Berghel, H. (2007). Credit Card Forensics. Communications of the ACM. http://doi.org/10.1145/1323688.1323708
- Bolt, S. (2011). XBOX 360 Forensics. XBOX 360 Forensics. http://doi.org/10.1016/B978-1-59749-623-0.00008-5
- Boztas, A., Riethoven, A. R. J., & Roeloffs, M. (2015). Smart TV forensics: Digital traces on televisions. Digital Investigation, 12(S1), S72–S80. http://doi.org/10.1016/j.diin.2015.01.012
- Burke, P. K., & Craiger, P. (2007). Xbox Forensics. Journal of Digital Forensic Practice, 1(4), 275–282. http://doi.org/10.1080/15567280701417991
- Burke, P., & Craiger, P. (2007). Forensic analysis of Xbox consoles. In IFIP International Federation for Information Processing (Vol. 242, pp. 269–280). http://doi.org/10.1007/978-0-387-73742-3_19
- Calderara, S., Prati, A., & Cucchiara, R. (2009). Video surveillance and multimedia forensics. In Proceedings of the First ACM workshop on Multimedia in forensics - MiFor '09 (p. 13). http://doi.org/10.1145/1631081.1631085
- Cohen, K. (2007). Digital Still Camera Forensics. Small Scale Digital Device Forensics Journal, 1(1), 1–8.
- Elstner, J., & Roeloffs, M. (2016). Forensic analysis of newer TomTom devices. Digital Investigation, 16, 29–37. http://doi.org/10.1016/j.diin.2016.01.016
- Hannay, P. (2011). Kindle Forensics: Acquisition and Analysis. Journal of Digital Forensics, Security and Law, 6(2), 17–24. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/view/138/34
- Hong, G., & Bo, J. (2010). Forensic analysis of skimming devices for credit fraud detection. In Proceedings - 2010 2nd IEEE International Conference on Information and Financial Engineering, ICIFE 2010 (pp. 542–546). http://doi.org/10.1109/ICIFE.2010.5609418
- Khanna, N., Mikkilineni, A. K., Chiang, P.-J., Ortiz, M. V, Shah, V., Suh, S., … Delp, E. J. (2007). Printer and Sensor Forensics. In Signal Processing Applications for Public Security and Forensics, 2007. SAFE '07. IEEE Workshop on (pp. 1–8).

- Khanna, N., Mikkilineni, A. K., Martone, A. F., Ali, G. N., Chiu, G. T. C., Allebach, J. P., & Delp, E. J. (2006). A survey of forensic characterization methods for physical devices. Digital Investigation, 3(SUPPL.), 17–28. http://doi.org/10.1016/j.diin.2006.06.014
- Kiley, M., Shinbara, T., & Rogers, M. (2007). iPod forensics update. International Journal of Digital Evidence, 6, 1–9. Retrieved from http://cryptome.org/isp-spy/ipod-spy.pdf
- Liu, D. (2009). Cisco Router and Switch Forensics. Cisco Router and Switch Forensics, 207–249. http://doi.org/10.1016/B978-1-59749-418-2.00007-7
- Lu, N., Du, P., Guo, X., & Greitzer, F. L. (2012). Smart meter data analysis. Pes T&D 2012, 1–6. http://doi.org/10.1109/TDC.2012.6281612
- Marsico, C. V, & Rogers, M. K. (2005). iPod Forensics. International Journal, 4(2), 267c–267c. http://doi.org/10.1109/HICSS.2007.300
- Mikkilineni, A. K., King-Smith, D., Gelfand, S. B., & Delp, E. J. (2009). Forensic characterization of RF devices. In Proceedings of the 2009 1st IEEE International Workshop on Information Forensics and Security, WIFS 2009 (pp. 26–30). http://doi.org/10.1109/WIFS.2009.5386490
- Souvignet, T., Hatin, J., Maqua, F., Tesniere, D., L??ger, P., & Hormi??re, R. (2014). Payment card forensic analysis: From concepts to desktop and mobile analysis tools. Digital Investigation, 11(3), 143–153. http://doi.org/10.1016/j.diin.2014.06.006
- St??ttgen, J., V??mel, S., & Denzel, M. (2015). Acquisition and analysis of compromised firmware using memory forensics. Digital Investigation, 12(S1), S50–S60. http://doi.org/10.1016/j.diin.2015.01.010
- Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. IEEE Communications Surveys and Tutorials, 16(2), 961–987. http://doi.org/10.1109/SURV.2013.101613.00077
- Sutherland, I., Read, H., & Xynos, K. (2014). Forensic analysis of smart TV: A current issue and call to arms. Digital Investigation, 11(3), 175–178. http://doi.org/10.1016/j.diin.2014.05.019
- Swaminathan, A., Wu, M., & Liu, K. J. R. (2009). Component forensics. IEEE Signal Processing Magazine, 26(2), 38–48. http://doi.org/10.1109/MSP.2008.931076
- van Dongen, W. S. (2008). Case study: Forensic analysis of a Samsung digital video recorder. Digital Investigation, 5(1-2), 19–28. http://doi.org/10.1016/j.diin.2008.04.001
- van Eijk, O., & Roeloffs, M. (2010). Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems. Digital Investigation, 6(3-4), 179–188. http://doi.org/10.1016/j.diin.2010.02.005

2. Internet-of-Things Forensics

While IoT concept was introduced some time ago, the era of Internet of Things seems to start at these days. With the more deployments of IoT systems, the need for digital forensics emerges. Currently, it is not clear how IoT concept will change digital forensics investigation and what methods would be necessary to address the new features of IoT. This topic is quite new, and thus the list of literature available is rather short.

REFERENCES:

- Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (pp. 608–615). http://doi.org/10.4108/icst.collaboratecom.2013.254159
- Perumal, S., Md Norwawi, N., & Raman, V. (2015). Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. In 2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015 (pp. 19–23). http://doi.org/10.1109/ICDIPC.2015.7323000
- Venčkauskas, A., Damaševičius, R., Jusas, V., Toldinas, J., Rudzika, D., & Drėgvaitė, G. (2015). A REVIEW OF CYBER-CRIME IN INTERNET OF THINGS : TECHNOLOGIES , INVESTIGATION METHODS AND DIGITAL FORENSICS. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, (April 2016).

3. VoIP Forensics

VoIP Forensics is a part of application forensics field. It focuses on gathering information from various VoIP systems. The most prominent VoIP system in digital forensics research is Skype. The topics span from identification of VoIP traffic to capturing the content of the communication.

- Castle, D. J. A. (2014). Skype Forensics. Discovery, Invention & Application. Retrieved from http://computing.derby.ac.uk/ojs/index.php/da/article/view/34
- Chu, H. C., Deng, D. J., & Chao, H. C. (2011). The digital forensics of portable electronic communication devices based on a Skype im session of a pocket PC for NGC. Wireless Communications and Mobile Computing, 11(2), 211–225. http://doi.org/10.1002/wcm.954
- Hsu, H. M., Sun, Y. S., & Chen, M. C. (2008). A collaborative forensics framework for VoIP services in multi-network environments. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 5075 LNCS, pp. 260–271). http://doi.org/10.1007/978-3-540-69304-8_26
- Jones, A. (2005). The future implications of computer forensics on VOIP. Digital Investigation, 2(3), 206–208. http://doi.org/10.1016/j.diin.2005.07.007
- Pelaez, J. C., & Fernandez, E. B. (2009). VoIP network forensic patterns. In 4th International Multi-Conference on Computing in the Global Information Technology, ICCGI 2009 (pp. 175–180). http://doi.org/10.1109/ICCGI.2009.53
- Simon, M., & Slay, J. (2010). Recovery of Skype application activity data from physical memory. In ARES 2010 - 5th International Conference on Availability, Reliability, and Security (pp. 283–288). http://doi.org/10.1109/ARES.2010.73
- Slay, J., & Simon, M. (2008). Voice over IP Forensics. ACM International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (E-Forensics). http://doi.org/10.4108/e-forensics.2008.2852

4. Cloud Forensics

Cloud computing is a technology that changes the way the data are processed and stored. Digital forensics of cloud computing environments require new methods to acquire and analyze data. There are various subtopics in this area, namely, analysis of communication in cloud, acquisition and analysis data stored in the cloud, analysis of cloud services, etc.

REFERENCES:

- Almulla, S. A., Iraqi, Y., & Jones, A. (2014). A State-of-the-Art Review of Cloud Forensics. Journal of Digital Forensics, Security and Law. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/view/253
- Almulla, S., Iraqi, Y., & Jones, A. (2013). Cloud forensics: A research perspective. In 2013 9th International Conference on Innovations in Information Technology, IIT 2013 (pp. 66–71). http://doi.org/10.1109/Innovations.2013.6544395
- Damshenas, M., Dehghantanha, A., Mahmoud, R., & Bin Shamsuddin, S. (2012). Forensics investigation challenges in cloud computing environments. In Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012 (pp. 190–194). http://doi.org/10.1109/CyberSec.2012.6246092
- Dykstra, Josiah; Sherman, A. T. (2011). UNDERSTANDING ISSUES IN CLOUD FORENSICS: TWO HYPOTHETICAL CASE STUDIES - ProQuest. Proceedings of the Conference on Digital Forensics, Security and Law, 1–10. Retrieved from http://search.proquest.com/openview/a55aa7a58e5dce50a54632b86eb706b1/1?pq-origsite=gscholar
- Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. In Digital Investigation (Vol. 9). http://doi.org/10.1016/j.diin.2012.05.001
- Fontarensky, E., Martin, I., Picod, M., Bursztein, J., Bursztein, E., Cassidian, I. F., … Picod, J. (2011). Doing forensics in the cloud age - OWADE: beyond files recovery forensic. Black Hat USA 2011, 1–23. Retrieved from http://www.owade.org
- Gebhardt, T., & Reiser, H. P. (2013). Network forensics for cloud computing. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 7891 LNCS, pp. 29–42). http://doi.org/10.1007/978-3-642-38541-4_3
- Holt, L. A., & Hammoudeh, M. (2013). Cloud forensics: A technical approach to virtual machine acquisition. In Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013 (p. 227). http://doi.org/10.1109/EISIC.2013.59
- Kandukuri, B. R., V., R. P., & Rakshit, A. (2009). Cloud Security Issues. In 2009 IEEE International Conference on Services Computing (pp. 517–520). http://doi.org/10.1109/SCC.2009.84
- Keyun, R., Carthy, J., & Kechadi, T. (2011). Cloud Forensics An Overview. 7th IFIP Conference on Digital Forensics, (January), 35–46. http://doi.org/10.1007/978-3-642-24212-0_3
- Marangos, N., Rizomiliotis, P., & Mitrou, L. (2012). Digital forensics in the Cloud Computing Era. In 2012 IEEE Globecom Workshops, GC Wkshps 2012 (pp. 775–780). http://doi.org/10.1109/GLOCOMW.2012.6477673
- Martini, B., & Choo, K. K. R. (2013). Cloud storage forensics: OwnCloud as a case study. Digital Investigation, 10(4), 287–299. http://doi.org/10.1016/j.diin.2013.08.005
- Mehreen, S., & Aslam, B. (2015). Windows 8 cloud storage analysis: Dropbox forensics. In Proceedings of 2015 12th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2015 (pp. 312–317). http://doi.org/10.1109/IBCAST.2015.7058522

- Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation, 13, 38–57. http://doi.org/10.1016/j.diin.2015.03.002
- Quick, D., Martini, B., & Choo, K.-K. R. (2014). Cloud Storage Forensics. Cloud Storage Forensics, (October), 13–21. http://doi.org/10.1016/B978-0-12-419970-5.00002-8
- Ruan, K. (2012). Cybercrime and Cloud Forensics. Cybercrime and Cloud Forensics: Applications for Investigation Processes, 331–344. http://doi.org/10.4018/978-1-4666-2662-1
- Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation, 10(1), 34–43. http://doi.org/10.1016/j.diin.2013.02.004
- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics. Advances in Digital Forensics VII, IFIP Advances in Information and Communication Technology, 361, 35–46. http://doi.org/10.1007/978-3-642-24212-0_3
- Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software, 86, 2263–2268. http://doi.org/10.1016/j.jss.2012.12.025
- Shah, J. J., & Malik, L. G. (2013). Cloud forensics: Issues and challenges. In International Conference on Emerging Trends in Engineering and Technology, ICETET (pp. 138–139). http://doi.org/10.1109/ICETET.2013.44
- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics solutions: A review. In Lecture Notes in Business Information Processing (Vol. 178 LNBIP, pp. 299–309). http://doi.org/10.1007/978-3-319-07869-4
- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics: Identifying the major issues and challenges. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 8484 LNCS, pp. 271–284). http://doi.org/10.1007/978-3-319-07881-6_19
- Simpson, W. R., & Chandersekaran, C. (2014). Cloud forensics issues. In Lecture Notes in Engineering and Computer Science (Vol. 1, pp. 475–480). Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84907396780&partnerID=40&md5=f05e8686486e38f8deff1acb5d45b677
- Thethi, N., & Keane, A. (2014). Digital forensics investigations in the Cloud. 2014 IEEE International Advance Computing Conference (IACC), 1475–1480. http://doi.org/10.1109/IAdCC.2014.6779543
- Zargari, S., & Benford, D. (2012). Cloud forensics: Concepts, issues, and challenges. In Proceedings - 3rd International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2012 (pp. 236–243). http://doi.org/10.1109/EIDWT.2012.44
- Zawoad, S., & Hasan, R. (2013). Digital Forensics in the Cloud. CrossTalk, (October), 17–20. Retrieved from http://www.crosstalkonline.org/storage/issue-archives/2013/201309/201309-Zawoad.pdf
- Zawoad, S., & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. arXiv Preprint arXiv:1302.6312, 1–15. Retrieved from http://arxiv.org/abs/1302.6312

5. Instant Messaging Forensics

Many IM applications are currently available. Some of them have a huge number of users while others are only popular to a rather limited group of people. For forensics investigation, instant messaging applications are extremely attractive as they may provide invaluable information about their users. Research in this area mostly focuses on identification of forensic artifacts that can be acquired from IM applications.

REFERENCES:

- Mark Scanlon and M-Tahar Kechadi. Digital Evidence Bag Selection for P2P Network Investigation. In Proceedings of the 7th International Symposium on Digital Forensics and Information Security (DFIS-2013), pages 307–314. Springer, Gwangju, South Korea, 2014.
- Al Barghuthi, N. B., & Said, H. (2013). Social networks IM forensics: Encryption analysis. Journal of Communications, 8(11), 708–715. http://doi.org/10.12720/jcm.8.11.708-715
- Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. (2011). Forensic artifacts of Facebook's instant messaging service. 6th International Conference on Internet Technology and Secured Transactions, (December), 771 – 776. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=86486166&site=eds-live
- Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 1–13. http://doi.org/10.1016/j.diin.2014.04.003
- Anwar, T., & Abulaish, M. (2014). A social graph based text mining framework for chat log investigation. Digital Investigation, 11(4), 349–362. http://doi.org/10.1016/j.diin.2014.10.001
- Dewes, C., Wichmann, A., & Feldmann, A. (2003). An analysis of Internet chat systems. Proceedings of the 2003 ACM SIGCOMM Conference on Internet Measurement - IMC '03, 51. http://doi.org/10.1145/948205.948214
- Dickson, M. (2006). An examination into AOL Instant Messenger 5.5 contact identification. Digital Investigation, 3(4), 227–237. http://doi.org/10.1016/j.diin.2006.10.004
- Grant, N., & Shaw, J. W. (2014). Unified Communications Forensics. Unified Communications Forensics. http://doi.org/10.1016/B978-1-59749-992-7.00009-3
- Husain, M. I., & Sridhar, R. (2010). iForensics: Forensic analysis of instant messaging on smart phones. In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (Vol. 31 LNICST, pp. 9–18). http://doi.org/10.1007/978-3-642-11534-9_2
- Iqbal, A., Marrington, A., & Baggili, I. (2014). Forensic artifacts of the ChatON Instant Messaging application. In Int. Workshop Syst. Approaches Digit. Forensics Eng., SADFE. http://doi.org/10.1109/SADFE.2013.6911538
- Kalt, C. (2000). RFC 2810: Internet Relay Chat: Architecture. Network Working Group, 1–10.
- Kiley, M., Dankner, S., & Rogers, M. (2008). Forensic Analysis of Volatile Instant Messaging. Advances in Digital Forensics IV. Retrieved from http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?db=pubmed&cmd=Retrieve&dopt=AbstractPlus&list_uids=180795937877977618 1related:tSSB3HkpFxkJ\npapers2://publication/uuid/1A665D02-1B33-43AC-A519-91E1B6F2A96E
- Kiley, M., Dankner, S., & Rogers, M. (2008). Forensic Analysis of Volatile Instant Messaging. Advances in Digital Forensics IV, 285, 129–138. http://doi.org/10.1017/CBO9781107415324.004
- Mahajan, A., Dahiya, M., & Sanghvi, H. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications, 68(8), 38–44. http://doi.org/10.5120/11602-6965

- Peterson, J. (2004). Common Profile for Instant Messaging (CPIM). RFC. Retrieved from http://www.ietf.org/rfc/rfc3860.txt
- Reust, J. (2006). Case study: AOL instant messenger trace evidence. Digital Investigation, 3(4), 238–243. http://doi.org/10.1016/j.diin.2006.10.009
- Simon, M. P., & Slay, J. (2011). Recovery of Pidgin chat communication artefacts from physical memory: A pilot test to determine feasibility. In Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011 (pp. 183–188). http://doi.org/10.1109/ARES.2011.33
- Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. Network Security. http://doi.org/10.1016/S1353-4858(14)70112-6
- Uthus, D. C., & Aha, D. W. (2013). Multiparticipant chat analysis: A survey. Artificial Intelligence, 199-200, 106–121. http://doi.org/10.1016/j.artint.2013.02.004
- van Dongen, W. S. (2007). Forensic artefacts left by Windows Live Messenger 8.0. Digital Investigation, 4(2), 73–87. http://doi.org/10.1016/j.diin.2007.06.019
- van Dongen, W. S. (2007). Forensic artefacts left by Pidgin Messenger 2.0. Digital Investigation, 4(3-4), 138–145. http://doi.org/10.1016/j.diin.2008.01.002
- Zhen, X., Lei, G., & Tracey, J. (2007). Understanding instant messaging traffic characteristics. In Proceedings - International Conference on Distributed Computing Systems. http://doi.org/10.1109/ICDCS.2007.149

6. Web Browser Forensics

Web browser forensics is routinely done in most of the digital forensics investigation. It comprises of finding the location of files related to web browsing, producing timelines and extracting content and searching for keywords or patterns. While this may be seen as a dead research topic, there is still need for new methods able to reconstructing web pages, analysis of private browsing sessions and practical extracting information about user activities from cache content and captured communication.

- Armknecht, F., & Dewald, A. (2015). Privacy-preserving email forensics. Digital Investigation, 14(S1), S127–S136. http://doi.org/10.1016/j.diin.2015.05.003
- Jones, K. J., & Belani, R. (2005). Web Browser Forensics , Part 1. Web Browsers, 2–8.
- Jones, R. (2006). Internet Forensics. Web Browsers. http://doi.org/10.1109/WDFIA.2007.4299368
- Khanikekar, S. K. (2010). Web Forensics. First International Conference, ISDF 2009, London, United Kingdom, September 7-9, 2009, Revised Selected Papers, 183. Retrieved from http://sci.tamucc.edu/~cams/projects/345.pdf\npapers2://publication/uuid/B56BDE60-91C6-48AC-B9E9-76B62F408EA2
- Liu, Y. H., Chen, G. L., & Xie, L. (2013). An Email Forensics Analysis Method Based on Social Network Analysis. 2013 International Conference on Cloud Computing and Big Data, (2009), 563–569. http://doi.org/10.1109/CLOUDCOM-ASIA.2013.38
- Schroader, A. (2007). E-mail Forensics. In Alternate Data Storage Forensics (pp. 147–169). http://doi.org/10.1016/B978-159749163-1/50005-6

7. Social Network Forensics

Social networks represent a significant source of data for intelligence analysis and also a big challenge for forensics investigation. Researchers have identified information value, proposed methods to acquire the data and developed algorithms for their analysis. However, new approaches and techniques can be applied to conduct forensics investigation efficiently.

REFERENCES:

- Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. In Digital Investigation (Vol. 9). http://doi.org/10.1016/j.diin.2012.05.007
- Baca, M., Cosic, J., & Cosic, Z. (2013). Forensic analysis of social networks (case study). Proceedings of the International Conference on Information Technology Interfaces, ITI, 219–223. http://doi.org/10.2498/iti.2013.0526
- Chen, L., Xu, L., Yuan, X., & Shashidhar, N. (2015). Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. In 2015 International Conference on Computing, Networking and Communications, ICNC 2015 (pp. 1132–1136). http://doi.org/10.1109/ICCNC.2015.7069509
- Dezfouli, F. N., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2015). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Australian Journal of Forensic Sciences, 0618(November), 1–20. http://doi.org/10.1080/00450618.2015.1066854
- Halkin, P., Kröger, K., & Creutzburg, R. (2013). Social network forensics: using commercial software in a university forensics lab environment. In Proceedings of the SPIE - The International Society for Optical Engineering (Vol. v 8755, p. 87550Q). http://doi.org/10.1117/12.2017908
- Mulazzani, M., Huber, M., & Weippl, E. (2012). Social Network Forensics : Tapping the Data Pool of Social Networks. Eighth Annual IFIP WG 11.9 International Conference on Digital Forensics.
- Tso, Y.-C., Wang, S.-J., Huang, C.-T., & Wang, W.-J. (2012). iPhone social networking for evidence investigations using iTunes forensics. Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC '12, 1. http://doi.org/10.1145/2184751.2184827
- Wong, K., Researcher, S., Lai, A. C. T., Yeung, J. C. K., & Lee, W. L. (2013). Facebook Forensics Finalized. The Journal of Infectious Diseases, 208, NP. http://doi.org/10.1093/infdis/jis918
- Wu, X. D., Li, Y. D., & Hu, D. H. (2014). Study on social network forensics. Ruan Jian Xue Bao/Journal of Software, 25(12), 2877–2892. http://doi.org/10.13328/j.cnki.jos.004727
- Zhang, S., & Wang, L. (2013). Forensic analysis of social networking application on iOS devices. In Proceedings of SPIE - The International Society for Optical Engineering (Vol. 9067, p. 906715). http://doi.org/10.1117/12.2051375

8. Forensics Data Visualization

Data visualization focuses on efficient data presentation helping users to find relevant information often in high dimensional and the vast amount of data. Visualization for forensics is a relatively subtle research area. However, to cope with a massive amount of data the need for new ways of information presentation is evident.

- Childs, H., Geveci, B., & Schroeder, W. (2013). Research Challenges for Visualization Software. Computer. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6515547
- Erbacher, R. F., & Teelink, S. (2006). Improving the computer forensic analysis process through visualization. Communications of the ACM, 49(2), 71. http://doi.org/10.1145/1113034.1113073
- Forte, D. (2009). Visual Forensics: new or old trend? Computer Fraud and Security, 2009(4), 15–17. http://doi.org/10.1016/S1361-3723(09)70048-X
- Gorg, C., Kang, Y. A., Liu, Z., & Stasko, J. (2013). Visual analytics support for intelligence analysis. Computer, 46(7), 30–38. http://doi.org/10.1109/MC.2013.76
- Isenberg, T., & Saclay, I. (2013). Reimaging the Scientific Visualization Interaction Paradigm. IEEE Computer, (May), 51–57.
- Kosara, R., & Mackinlay, J. (2013). Storytelling: The Next Step for Visualization. IEEE Computer, (May), 44–50. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6412677
- Majumder, A., & Sajadi, B. (2013). Large Area Displays: The Changing Face of Visualization. IEEE Computer, 26–33.
- Osborne, G., & Turnbull, B. (2009). Enhancing computer forensics investigation through visualisation and data exploitation. In Proceedings - International Conference on Availability, Reliability and Security, ARES 2009 (pp. 1012–1017). http://doi.org/10.1109/ARES.2009.120
- Rhyne, T.-M., & Chen, M. (2013). Cutting-Edge Research in Visualization. Computer, 46(5), 22–24. http://doi.org/10.1109/MC.2013.166
- Schreck, T., & Keim, D. (2013). Visual Analysis of Social Media Data. Computer, 46(5), 68–75. http://doi.org/10.1109/MC.2012.430

9. Mobile Forensics

Many research papers were written about mobile forensics, but there is still room for further studies. The research can address techniques in any phase of the investigation, that is, data acquisition methods, data analysis, content extraction, evidence finding. Many papers also present a case study on analysis of the selected mobile applications.

REFERENCES:

- Al Barghouthy, N., & Marrington, A. (2014). A comparison of forensic acquisition techniques for android devices: A case study investigation of orweb browsing sessions. In 2014 6th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2014 Conference and Workshops. http://doi.org/10.1109/NTMS.2014.6813993
- Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. In Digital Investigation (Vol. 9). http://doi.org/10.1016/j.diin.2012.05.007
- AL-Hajri, H., & Sansurooah, K. (2008). iPhone forensics methodology and tools. In Proceedings of the 6th Australian Digital Forensics Conference (pp. 4–18). Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84867730574&partnerID=tZOtx3y1
- Alghafli, K. A., Jones, A., & Martin, T. A. (2012). Forensics Data Acquisition Methods for Mobile Phones. IEEE International Conference for Internet Technology And Secured Transactions, 265–269.
- Andriotis, P., Oikonomou, G., & Tryfonas, T. (2012). Forensic analysis of wireless networking evidence of Android smartphones. In WIFS 2012 - Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (pp. 109–114). http://doi.org/10.1109/WIFS.2012.6412634
- Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 1–13. http://doi.org/10.1016/j.diin.2014.04.003
- Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2011). Novel anti-forensics approaches for smart phones. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 5424–5431). http://doi.org/10.1109/HICSS.2012.452
- Ballagas, R., Borchers, J., Rohs, M., & Sheridan, J. G. (2006). The smart phone: A ubiquitous input device. IEEE Pervasive Computing. http://doi.org/10.1109/MPRV.2006.18
- Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. Digital Investigation, 10(4), 323–349. http://doi.org/10.1016/j.diin.2013.10.003
- Casadei, F. (2006). Forensics and SIM cards : an Overview. International Journal, 5(1), 1–21. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Forensics+and+SIM+cards+:+an+Overview#0
- Casey, E., Bann, M., & Doyle, J. (2010). Introduction to Windows Mobile Forensics. Digital Investigation, 6(3-4), 136–146. http://doi.org/10.1016/j.diin.2010.01.004
- Casey, E., Cheval, A., Lee, J. Y., Oxley, D., & Song, Y. J. (2011). Forensic acquisition and analysis of palm webOS on mobile devices. Digital Investigation, 8(1), 37–47. http://doi.org/10.1016/j.diin.2011.04.003
- Catanese, S., Ferrara, E., & Fiumara, G. (2013). Forensic analysis of phone call networks. Social Network Analysis and Mining, 3(1), 15–33. http://doi.org/10.1007/s13278-012-0060-1

- Chang, C. P., Chen, C. Te, Lu, T. H., Lin, I. L., Huang, P., & Lu, H. S. (2013). Study on constructing forensic procedure of digital evidence on smart handheld device. In ICSSE 2013 - IEEE International Conference on System Science and Engineering, Proceedings (pp. 223–228). http://doi.org/10.1109/ICSSE.2013.6614664
- Chang, Y. H., Yoon, K. B., & Park, D. W. (2013). Technology for forensic analysis of synchronized smartphone backup data. In 2013 International Conference on Information Science and Applications, ICISA 2013. http://doi.org/10.1109/ICISA.2013.6579430
- Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. International Journal, 2, 15–27. http://doi.org/10.4018/jdcf.2010070102
- Dibb, P., & Hammoudeh, M. (2013). Forensic data recovery from android os devices: An open source toolkit. In Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013 (p. 226). http://doi.org/10.1109/EISIC.2013.58
- Do, Q., Martini, B., & Choo, K. K. R. (2015). A forensically sound adversary model for mobile devices. PLoS ONE, 10(9). http://doi.org/10.1371/journal.pone.0138449
- Faheem, M., Le-Khac, N.-A., & Kechadi, T. (2014). 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. Journal of Information Security, 5(3), 83–90. Retrieved from http://search.proquest.com/docview/1553406048?accountid=12118\nhttp://linksource.ebsco.com/linking.aspx?sid=ProQ:abiglobal&fmt=journal&genre=article&issn=21531234&volume=5&issue=3&date=2014-07-01&spage=83&title=Journal+of+Information+Security&atitle=Smart
- Goda, B. S., Bair, J. W., & Costarella, C. E. (2015). Cell Phone Forensics. Proceedings of the 16th Annual Conference on Information Technology Education - SIGITE '15, 39–42. http://doi.org/10.1145/2808006.2808022
- Gomez-Miralles, L., & Arnedo-Moreno, J. (2013). Analysis of the forensic traces left by airprint in apple iOS devices. In Proceedings - 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013 (pp. 703–708). http://doi.org/10.1109/WAINA.2013.40
- Grispos, G., Storer, T., & Glisson, W. B. (2011). A comparison of forensic evidence recovery techniques for a windows mobile smart phone. Digital Investigation, 8(1), 23–36. http://doi.org/10.1016/j.diin.2011.05.016
- Hilgers, C., Macht, H., Muller, T., & Spreitzenbarth, M. (2014). Post-mortem memory analysis of cold-booted android devices. In Proceedings - 8th International Conference on IT Security Incident Management and IT Forensics, IMF 2014 (pp. 62–75). http://doi.org/10.1109/IMF.2014.8
- Hoog, A. (2011). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Security. http://doi.org/10.1016/B978-1-59749-651-3.10001-9
- Irwin, D., & Hunt, R. (2009). Forensic information acquisition in mobile networks. In IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing - Proceedings (pp. 163–168). http://doi.org/10.1109/PACRIM.2009.5291378
- Justice, C., Wu, H., & Walton, E. (2009). Mobile forensics in healthcare. In 2009 8th International Conference on Mobile Business (pp. 255–260). http://doi.org/10.1109/ICMB.2009.51
- Kaart, M., & Laraghy, S. (2014). Android forensics: Interpretation of timestamps. Digital Investigation, 11(3), 234–248. http://doi.org/10.1016/j.diin.2014.05.001
- Lai, Y., Yang, C., Lin, C., & Ahn, T. (2011). Design and implementation of mobile forensic tool for android smart phone through cloud computing. In Communications in Computer and

Information Science (Vol. 206 CCIS, pp. 196–203). http://doi.org/10.1007/978-3-642-24106-2_26
- Lee, S. W., Park, J. S., Lee, H. S., & Kim, M. S. (2011). A study on Smart-phone traffic analysis. In APNOMS 2011 - 13th Asia-Pacific Network Operations and Management Symposium: Managing Clouds, Smart Networks and Services, Final Program. http://doi.org/10.1109/APNOMS.2011.6077033
- Leithner, M., & Weippl, E. (2012). Android forensics. Computers & Security, 31(1), 3. http://doi.org/10.1016/j.cose.2011.10.005
- Lessard, J., & Kessler, G. C. (2010). Android Forensics : Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal, 4(1), 1–12. http://doi.org/10.1.1.185.698
- Mahajan, A., Dahiya, M., & Sanghvi, H. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications, 68(8), 38–44. http://doi.org/10.5120/11602-6965
- Martinez, J. (2007). Mobile Forensics. Technology, 1(1), 40. Retrieved from www.susteen.com
- Marturana, F., Me, G., Bertè, R., & Tacconi, S. (2011). A quantitative approach to triaging in mobile forensics. In Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011 (pp. 582–588). http://doi.org/10.1109/TrustCom.2011.75
- Marzougy, M. Al, Baggili, I., & Marrington, A. (2013). BlackBerry PlayBook Backup Forensic Analysis. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering - Digital Forensics and Cyber Crime, 114, 239–252. http://doi.org/10.1007/978-3-642-39891-9_15
- Miller, C. M. (2014). Mobile Forensics & Human Trafficking. Retrieved from http://www.officer.com/article/11145118/mobile-forensics-human-trafficking
- Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. Digital Investigation, 6(3-4), 112–124. http://doi.org/10.1016/j.diin.2010.03.001
- Moco, N. F. (2014). Mobile forensics: A smartphone-based activity logger. In 2014 21st International Conference on Telecommunications, ICT 2014 (pp. 462–466). http://doi.org/10.1109/ICT.2014.6845159
- Mokhonoana, P. M., & Olivier, M. S. (2007). Acquisition of a Symbian Smart phone ' s Content with an On-Phone Forensic Tool. Southern African Telecommunication Networks and Applications Conference 2007, 1–7.
- Morrissey, S. (2010). iOS Forensic Analysis for iPhone , iPad and iPod touch. Analysis. http://doi.org/10.1007/978-1-4302-3343-5
- Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone forensics: A proactive investigation scheme for evidence acquisition. In IFIP Advances in Information and Communication Technology (Vol. 376 AICT, pp. 249–260). http://doi.org/10.1007/978-3-642-30436-1_21
- Ntantogian, C., Apostolopoulos, D., Marinakis, G., & Xenakis, C. (2014). Evaluating the privacy of Android mobile applications under forensic analysis. Computers and Security, 42, 66–76. http://doi.org/10.1016/j.cose.2014.01.004
- Owen, P., & Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. Digital Investigation, 8(2), 135–140. http://doi.org/10.1016/j.diin.2011.03.002

- Punja, S. S. G., & Mislan, R. R. P. (2008). Mobile Device Analysis. Small Scale Digital Device Forensics …, 2(1), 1–16. Retrieved from http://www.researchgate.net/profile/Rick_Mislan/publication/228374981_Mobile_device_analysis/links/543920e80cf24a6ddb954572.pdf
- Quick, D., & Alzaabi, M. (2011). Forensic analysis of the android file system YAFFS2. Proceedings of the 9th Australian Digital Forensics Conference, (December), 100–109.
- Racioppo, C., & Murthy, N. (2012). Android Forensics : A Case Study of the " HTC Incredible " Phone. Proceedings of Student-Faculty Research Day, 1–8.
- Sack, S., Kröger, K., & Creutzburg, R. (2013). Location tracking forensics on mobile devices. In Proceedings of SPIE - The International Society for Optical Engineering (Vol. 8667, p. 866712). http://doi.org/10.1117/12.2003952
- Sahu, S. (2013). Forensic Analysis of WhatsApp on Android Smartphones. International Journal of Engineering Research, 3(5), 349–350. http://doi.org/10.2307/40130800
- Savoldi, A., & Gubian, P. (2008). Symbian forensics: An overview. In Proceedings - 2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2008 (pp. 529–533). http://doi.org/10.1109/IIH-MSP.2008.239
- Son, N., Lee, Y., Kim, D., James, J. I., Lee, S., & Lee, K. (2013). A study of user data integrity during acquisition of Android devices. In Digital Investigation (Vol. 10). http://doi.org/10.1016/j.diin.2013.06.001
- Yu, X., Jiang, L. H., Shu, H., Yin, Q., & Liu, T. M. (2009). A process model for forensic analysis of Symbian smart phones. In Communications in Computer and Information Science (Vol. 59 CCIS, pp. 86–93). http://doi.org/10.1007/978-3-642-10619-4_11
- Zareen, A., & Baig, S. (2010). Mobile phone forensics challenges, analysis and tools classification. In 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010 (pp. 47–55). http://doi.org/10.1109/SADFE.2010.24
- Zdziarski, J. (2008). iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets. Journal of the Electrochemical Society (Vol. 129). Retrieved from http://books.google.com/books?id=R1XArTHPn9QC
- Zdziarski, J. (2008). iPhone Forensics. Matrix, 129, 120.
- Zhang, S., & Wang, L. (2013). Forensic analysis of social networking application on iOS devices. In Proceedings of SPIE - The International Society for Optical Engineering (Vol. 9067, p. 906715). http://doi.org/10.1117/12.2051375

10. Network Forensics

This field contains an extensive collection of topics related to network communication. For instance, identifying various types of DDoS attacks from capture files requires extracting attack statistics, a list of attacking bots, determining the type of attack (TCP SYN flood, UDP/ICMP flood, HTTP GET/POST flood, HTTP flood with browser emulation, etc.).
The research topics include the usage of machine learning and other methods for automatic analysis of data, content identification and extraction, communication capturing and evidence extraction, etc.

- A, L. B. (2012). IDENTIFYING APPLICATION LEVEL PROTOCOLS BY ANALYZING COMMUNICATION PATTERNS OVER MULTIPLE PORTS.
- Adeyemi, I., Razak, S., & Azhan, N. (2012). Identifying critical features for network forensics investigation perspectives. International Journal of Computer Science & Information Security, Vol. 10(Issue 9), p.108. Retrieved from http://arxiv.org/abs/1210.1645
- Al-Zaidy, R., Fung, B. C. M., Youssef, A. M., & Fortin, F. (2012). Mining criminal networks from unstructured text documents. Digital Investigation, 8(3-4), 147–160. http://doi.org/10.1016/j.diin.2011.12.001
- Aliakbarian, M. S., Fanian, A., Saleh, F. S., & Gulliver, T. A. (2013). Optimal supervised feature extraction in internet traffic classification. In IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing - Proceedings (pp. 102–107). http://doi.org/10.1109/PACRIM.2013.6625457
- Almulhem, A. (2009). Network forensics: Notions and challenges. In IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2009 (pp. 463–466). http://doi.org/10.1109/ISSPIT.2009.5407485
- Ariu, D., Giacinto, G., & Roli, F. (2011). Machine learning in computer forensics (and the lessons learned from machine learning in computer security). … of the 4th ACM Workshop on Security and …, 99–103. Retrieved from http://dl.acm.org/citation.cfm?id=2046700
- Back, G. (2002). DataScript-A specification and scripting language for binary data. Generative Programming and Component Engineering. Retrieved from http://link.springer.com/chapter/10.1007/3-540-45821-2_4
- Ballou, S., & Gilliland, R. G. (2011). Emerging paper standards in computer forensics. Digital Investigation, 8(2), 96–97. http://doi.org/10.1016/j.diin.2011.05.017
- Bangert, J., & Zeldovich, N. (2014). Nail: A Practical Interface Generator for Data Formats. 2014 IEEE Security and Privacy Workshops, 158–166. http://doi.org/10.1109/SPW.2014.31
- Bangert, J., & Zeldovich, N. (2014). Nail: A Practical Tool for Parsing and Generating Data Formats. 11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14), 615–628. Retrieved from https://www.usenix.org/conference/osdi14/technical-sessions/presentation/bangert
- Banks, D. (2013). Custom Full Packet Capture System. SANS Journal.
- Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167. http://doi.org/10.1016/j.diin.2005.04.002
- Beverly, R., Garfinkel, S., & Cardwell, G. (2011). Forensic carving of network packets and associated data structures. In Digital Investigation (Vol. 8). http://doi.org/10.1016/j.diin.2011.05.010

- Beverly, R., Garfinkel, S., & Cardwell, G. (2011). Forensic carving of network packets and associated data structures. Digital Investigation, 8, S78–S89. http://doi.org/10.1016/j.diin.2011.05.010
- Bilge, L., & Kirda, E. (2011). Exposure: Finding malicious domains using passive dns analysis. Proceedings of …. Retrieved from http://gowegian.5gbfree.com/ndss11_exposure.pdf
- Borisov, N., Brumley, D. J., Wang, H. J., Dunagan, J., Joshi, P., & Guo, C. (2007). A Generic Application-Level Protocol Analyzer and its Language. Proceedings of the 14th Annual Network Distributed System Security Symposium NDSS, 15. http://doi.org/10.1.1.70.9780
- Buchanan, W. J. (2010). Introduction to network forensics. Computer Security Journal (Vol. 21). http://doi.org/10.1007/978-1-61779-968-6
- Buchanan, W. J. (2010). Advanced security and network forensics: network forensics. Network, 3–20. Retrieved from http://researchrepository.napier.ac.uk/4148/1/asnf_unit03.html
- Buchholz, F., & Tjaden, B. (2007). A brief study of time. Digital Investigation, 4, 31–42. http://doi.org/10.1016/j.diin.2007.06.004
- Bursztein, E. (2008). Probabilistic Identification for Hard to Classify Protocol. Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, 5019, 49–63.
- Casey, E. (2006). Applications of Research. Digital Investigation, 3(2), 84. http://doi.org/10.1016/j.diin.2006.05.006
- Casey, E. (2011). The increasing need for automation and validation in digital forensics. Digital Investigation, 7(3-4), 103–104. http://doi.org/10.1016/j.diin.2011.02.002
- Casey, E. (2010). Digital investigations, security and privacy. Digital Investigation, 7(1-2), 1–2. http://doi.org/10.1016/j.diin.2010.10.001
- Casey, E. (2005). Case study: Network intrusion investigation – lessons in forensic preparation. Digital Investigation, 2(4), 254–260. http://doi.org/10.1016/j.diin.2005.11.007
- Casey, E. (2011). A unified voice: The need for an international digital forensic convention. Digital Investigation, 8(2), 89–91. http://doi.org/10.1016/j.diin.2011.09.004
- Chen, L. M., Chen, M. C., Liao, W., & Sun, Y. S. (2013). A scalable network forensics mechanism for stealthy self-propagating attacks. Computer Communications, 36(13), 1471–1484. http://doi.org/10.1016/j.comcom.2013.05.005
- Cohen, M. I. (2008). PyFlag – An advanced network forensic framework. Digital Investigation, 5, S112–S120. http://doi.org/10.1016/j.diin.2008.05.016
- Cohen, M. I. (2009). Source attribution for network address translated forensic captures. Digital Investigation, 5(3-4), 138–145. http://doi.org/10.1016/j.diin.2008.12.002
- Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2016). Analyzing Android Encrypted Network Traffic to Identify User Actions. IEEE Transactions on Information Forensics and Security, 11(1), 114–125.
- Corey, V., Peterman, C., Shearin, S., Greenberg, M. S., & Van Bokkelen, J. (2002). Network forensics analysis. IEEE Internet Computing, 6(6), 60–66. http://doi.org/10.1109/MIC.2002.1067738
- Crotti, M., Dusi, M., Gringoli, F., & Salgarelli, L. (2007). Traffic classification through simple statistical fingerprinting. ACM SIGCOMM Computer Communication Review, 37(1), 5. http://doi.org/10.1145/1198255.1198257
- Daniels, T. E. (2004). A functional reference model of passive systems for tracing network traffic. Digital Investigation, 1(1), 69–81. http://doi.org/10.1016/j.diin.2003.12.003
- Donato, W., Pescap??, A., & Dainotti, A. (2014). Traffic identification engine: An open platform for traffic classification. IEEE Network, 28(2), 56–64.

- Eilers, S. M. (2008). IseHarvest: TCP packet data re-assemler framework for network traffic content. Iowa State University.
- Eoghan, & Casey. (2004). Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. Digital Investigation, 1(1), 28 – 43. Retrieved from http://www.sciencedirect.com/science/article/pii/S1742287603000033
- Erman, J., Mahanti, A., & Arlitt, M. (2007). Offline/realtime traffic classification using semi-supervised learning. Performance …, (October), 2–5. Retrieved from http://www.sciencedirect.com/science/article/pii/S0166531607000648
- Fisher, K., & Gruber, R. (2005). PADS: a domain-specific language for processing ad hoc data. ACM Sigplan Notices, 295–304. Retrieved from http://dl.acm.org/citation.cfm?id=1065046
- Foroushani, V. A., & Zincir-Heywood, A. N. (2013). Investigating application behavior in network traffic traces. In Proceedings of the 2013 IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2013 - 2013 IEEE Symposium Series on Computational Intelligence, SSCI 2013 (pp. 72–79).
- Garfinkel, S. (2012). Digital forensics XML and the DFXML toolset. Digital Investigation, 8(3-4), 161–174. http://doi.org/10.1016/j.diin.2011.11.002
- Garfinkel, S. (2002). Network Forensics : Tapping the Internet. Information Security. Retrieved from http://paulohm.com/classes/cc06/files/Week6 Network Forensics.pdf
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64–S73. http://doi.org/10.1016/j.diin.2010.05.009
- Gebrehiwot, A., Sommani, M., & Vita, A. De. (n.d.). 6MON : ROGUE IPV6 ROUTER ADVERTISEMENT DETECTION AND MITIGATION AND IPV6 ADDRESS UTILIZATION NETWORK MONITORING TOOL.
- Geradts, Z. (2011). ENFSI Forensic IT Working group. Digital Investigation, 8(2), 94–95. http://doi.org/10.1016/j.diin.2011.09.003
- Gladyshev, P., & Patel, A. (2004). Finite state machine approach to digital event reconstruction. Digital Investigation, 1(2), 130–149. http://doi.org/10.1016/j.diin.2004.03.001
- Gómez Sena, G., & Belzarena, P. (2009). Early Traffic Classification using Support Vector Machines. Proc. of LANC, 60. http://doi.org/10.1145/1636682.1636693
- Guan, Y. (2013). Network forensics. In Managing Information Security: Second Edition (pp. 313–334). http://doi.org/10.1016/B978-0-12-416688-2.00011-8
- Hajjar, A., Khalife, J., & Díaz-Verdejo, J. (2015). Network traffic application identification based on message size analysis. Journal of Network and Computer Applications, 58, 130–143. Retrieved from http://www.sciencedirect.com/science/article/pii/S1084804515002167
- Hawker, B. M. A. (2008). Writing a Parser from Wire to Window A Beginner ' s Guide to Parser Development.
- Hunt, R. (2012). New developments in network forensics – Tools and techniques. 2012 18th IEEE International Conference on Networks (ICON), 376–381. http://doi.org/10.1109/ICON.2012.6506587
- Hunt, R., & Zeadally, S. (2012). Network forensics: An analysis of techniques, tools, and trends. Computer, 45(12), 36–43. http://doi.org/10.1109/MC.2012.252
- Johnston, A., & Reust, J. (2006). Network intrusion investigation – Preparation and challenges. Digital Investigation, 3(3), 118–126. http://doi.org/10.1016/j.diin.2006.08.001
- Jones, A. (2005). The future implications of computer forensics on VOIP. Digital Investigation, 2(3), 206–208. http://doi.org/10.1016/j.diin.2005.07.007
- Jonnalagedda, M., Coppey, T., Stucki, S., Rompf, T., & Odersky, M. (2014). Staged parser combinators for efficient data processing. Proceedings of the 2014 ACM International

Conference on Object Oriented Programming Systems Languages & Applications - OOPSLA '14, 637–653. http://doi.org/10.1145/2660193.2660241
- K??hnen, C., ??berall, C., Adamsky, F., Rako??evi??, V., Rajarajan, M., & J??ger, R. (2010). Enhancements to Statistical Protocol IDentification (SPID) for self-organised QoS in LANs. Proceedings - International Conference on Computer Communications and Networks, ICCCN. http://doi.org/10.1109/ICCCN.2010.5560139
- Kahvedžić, D., & Kechadi, T. (2009). DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. Digital Investigation, 6, S23–S33. http://doi.org/10.1016/j.diin.2009.06.014
- Karyda, M., & Mitrou, L. (2007). Internet forensics: Legal and technical issues. In Proceedings - 2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA 2007 (pp. 3–12). http://doi.org/10.1109/WDFIA.2007.4299368
- Khalife, J., Hajjar, A., & Diaz-Verdejo, J. (2014). A multilevel taxonomy and requirements for an optimal traffic-classification model. Internation Journal of Network Management, (24), 17–31. http://doi.org/10.1002/nem
- Khater, N. Al, & Overill, R. E. (2015). Forensic Network Traffic Analysis. In Proceedings of The Second International Conference on Digital Security and Forensics (pp. 1–9).
- Kim, H., Claffy, K., & Fomenkov, M. (2008). Internet traffic classification demystified: myths, caveats, and the best practices. Proceedings of the …. Retrieved from http://dl.acm.org/citation.cfm?id=1544023
- Kittler, J., Hater, M., & Duin, R. P. W. (1996). Combining classifiers. In Proceedings - International Conference on Pattern Recognition. http://doi.org/10.1109/ICPR.1996.547205
- Korczyński, M., & Duda, A. (2014). Markov chain fingerprinting to classify encrypted traffic. In Proceedings - IEEE INFOCOM (pp. 781–789). Institute of Electrical and Electronics Engineers Inc.
- Li, Q., Larsen, C., Horst, T. Van Der, & Systems, B. C. (2013). IPv6 : A Catalyst and Evasion Tool for Botnets and Malware Delivery Networks. IEEE Computer, May, 76–82.
- Liao, N., Tian, S., & Wang, T. (2009). Network forensics based on fuzzy logic and expert system. Computer Communications, 32(17), 1881–1892. http://doi.org/10.1016/j.comcom.2009.07.013
- Liberatore, M., Erdely, R., Kerle, T., Levine, B. N., & Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. Digital Investigation, 7, S95–S103. http://doi.org/10.1016/j.diin.2010.05.012
- Lillard, T. V., Garrison, C. P., Schiller, C. a., & Steele, J. (2010). Digital Forensics for Network, Internet, and Cloud Computing. Digital Forensics for Network, Internet, and Cloud Computing. http://doi.org/10.1016/B978-1-59749-537-0.00011-9
- Liu, D. (2009). Cisco Router and Switch Forensics. Cisco Router and Switch Forensics, 207–249. http://doi.org/10.1016/B978-1-59749-418-2.00007-7
- Luo, Y., Xiang, K., & Li, S. (2008). Acceleration of decision tree searching for IP traffic classification. Proceedings of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems - ANCS '08, 40. http://doi.org/10.1145/1477942.1477949
- McCann, P., & Chandra, S. (2000). Packet types: abstract specification of network protocol messages. ACM SIGCOMM Computer Communication …. Retrieved from http://dl.acm.org/citation.cfm?id=347563
- Meghanathan, N., Allam, S. R., & Moore, L. a. (2010). Tools and techniques for Network Forensics. International Journal of Network Security & Its Applications (IJNSA), 1(1), 14–25. Retrieved from http://arxiv.org/abs/1004.0570

- Mikians, J., Dhamdhere, A., Dovrolis, C., Barlet-Ros, P., & Solé-Pareta, J. (2012). Towards a statistical characterization of the interdomain traffic matrix. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7290 LNCS(PART 2), 111–123. http://doi.org/10.1007/978-3-642-30054-7_9
- Miskovic, S., Lee, G. M., Liao, Y., & Baldi, M. (2015). AppPrint: Automatic fingerprinting of mobile applications in network traffic. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 8995, pp. 57–69). Springer Verlag.
- Namdev, N., Agrawal, S., & Silkari, S. (2015). Recent advancement in machine learning based internet traffic classification. Procedia Computer Science, 60(1), 784–791. http://doi.org/10.1016/j.procs.2015.08.238
- Nguyen, T. T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. Communications Surveys & Tutorials, IEEE, 10(4), 56–76. http://doi.org/10.1109/SURV.2008.080406
- Nikkel, B. J. (2004). Domain name forensics: a systematic approach to investigating an internet presence. Digital Investigation, 1(4), 247–255. http://doi.org/10.1016/j.diin.2004.10.001
- Nikkel, B. J. (2004). Domain name forensics: A systematic approach to investigating an internet presence. Digital Investigation, 1(4), 247–255. http://doi.org/10.1016/j.diin.2004.10.001
- Nikkel, B. J. (2006). A portable network forensic evidence collector. Digital Investigation, 3(3), 127–135. http://doi.org/10.1016/j.diin.2006.08.012
- Nikkel, B. J. (2006). Improving evidence acquisition from live network sources. Digital Investigation, 3(2), 89–96. http://doi.org/10.1016/j.diin.2006.05.002
- Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. Digital Investigation, 8, S62–S70. http://doi.org/10.1016/j.diin.2011.05.008
- Olsson, J., & Boldt, M. (2009). Computer forensic timeline visualization tool. Digital Investigation, 6, S78–S87. http://doi.org/10.1016/j.diin.2009.06.008
- Pang, R., Paxson, V., Sommer, R., & Peterson, L. (2006). binpac: A yacc for Writing Application Protocol Parsers. Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, 289–300. Retrieved from http://portal.acm.org/citation.cfm?id=1177119
- Peuhkuri, M. (2001). A method to compress and anonymize packet traces. Proceedings of the First ACM SIGCOMM Workshop on Internet Measurement - IMW '01, 257. http://doi.org/10.1145/505202.505233
- Pilli, E. S., Joshi, R. C., & Niyogi, R. (2011). Data Reduction by Identification and Correlation of TCP / IP Attack Attributes for Network Forensics. In In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (pp. 276–283). http://doi.org/10.1145/1980022.1980085
- Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. Digital Investigation, 7(1-2), 14–27. http://doi.org/10.1016/j.diin.2010.02.003
- Ponec, M., Giura, P., Brönnimann, H., & Wein, J. (2007). Highly efficient techniques for network forensics. CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, 150–160. http://doi.org/10.1145/1315245.1315265
- Reust, J. (2006). Case study: AOL instant messenger trace evidence. Digital Investigation, 3(4), 238–243. http://doi.org/10.1016/j.diin.2006.10.009
- Santcroos, M., Kolkman, O. M., & Labs, N. (2007). DNS Threat Analysis.

- Seifert, C., Steenson, R., Welch, I., Komisarczuk, P., & Endicott-Popovsky, B. (2007). Capture – A behavioral analysis tool for applications and documents. Digital Investigation, 4, 23–30. http://doi.org/10.1016/j.diin.2007.06.003
- Shebaro, B., & Crandall, J. R. (2011). Privacy-preserving network flow recording. Digital Investigation, 8, S90–S100. http://doi.org/10.1016/j.diin.2011.05.011
- Shields, C., Frieder, O., & Maloof, M. (2011). A system for the proactive, continuous, and efficient collection of digital forensic evidence. Digital Investigation, 8, S3–S13. http://doi.org/10.1016/j.diin.2011.05.002
- Shon, T., & Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. Information Sciences, 177(18), 3799–3821. http://doi.org/10.1016/j.ins.2007.03.025
- Tao, H., & Hao, Z. (2010). Periodic sequence in netflow recognizing algorithm. … and Information Security (WCNIS), 2010 IEEE …, 573–576. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5541844
- Thottan, M., Liu, G., & Ji, C. (n.d.). Anomaly Detection Approaches for Communication Networks, 1–19.
- Tulyakov, S., Jaeger, S., Govindaraju, V., & Doermann, D. (2008). Review of classifier combination methods. Studies in Computational Intelligence. http://doi.org/10.1007/978-3-540-76280-5_14
- Velan, P., Cermak, M., Celeda, P., & Drasar, M. (2014). A Survey of Methods for Encrypted Traffic Classification znd Analysis. International Journal of Network Management, 24. http://doi.org/10.1002/nem
- Wang, W. (2010). A graph oriented approach for network forensic analysis by.
- Wei, R., & Hai, J. (2005). Modeling the network forensics behaviors. In Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005 (Vol. 2005, pp. 2–9). http://doi.org/10.1109/SECCMW.2005.1588287
- Wondracek, G., Comparetti, P. M., Kruegel, C., Kirda, E., & Anna, S. S. S. (2008). Automatic Network Protocol Analysis. Network and Distributed System Security Symposium (NDSS), 1–18. http://doi.org/10.1.1.110.7553
- Yen, Y.-S., Lin, I.-L., & Wu, B.-L. (2011). A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence. Digital Investigation, 8(1), 56–67. http://doi.org/10.1016/j.diin.2011.03.003
- Zhen, L., & Qiong, L. (2012). A New Feature Selection Method for Internet Traffic Classification Using ML. Physics Procedia, 33(Ml), 1338–1345. http://doi.org/10.1016/j.phpro.2012.05.220
- Technical Brief : Flow Forensics. (2013).

11. Anti-forensics

Anti-forensics covers methods, techniques, and technologies supposed to affect the existence of evidence and making the digital investigation more difficult or impossible. Anti-forensics field divides into the following subcategories: data hiding, artifact wiping, trail obfuscation and attacks against the computer forensics processes and tools. The role of anti-forensics is not precisely defined. It is accepted that it can serve except to the malicious intent also like the defence against espionage and it also has the role in improving forensics method and tools.

- Azadegan, S., Yu, W., Liu, H., Sistani, M., & Acharya, S. (2011). Novel anti-forensics approaches for smart phones. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 5424–5431). http://doi.org/10.1109/HICSS.2012.452
- B??hme, R., & Kirchner, M. (2013). Counter-forensics: Attacking image forensics. In Digital Image Forensics: There is More to a Picture than Meets the Eye (pp. 327–366). http://doi.org/10.1007/978-1-4614-0757-7_12
- Blunden, B. (2009). Anti-Forensics : The Rootkit Connection. Commentary, 1–44.
- D'Orazio, C., Ariffin, A., & Choo, K. K. R. (2014). IOS anti-forensics: How can we securely conceal, delete and insert data? In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 4838–4847). http://doi.org/10.1109/HICSS.2014.594
- Dahbur, K., & Mohammad, B. (2011). The anti-forensics challenge. Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA '11, 1–7. http://doi.org/10.1145/1980822.1980836
- Distefano, A., Me, G., & Pace, F. (2010). Android anti-forensics through a local paradigm. Digital Investigation, 7(SUPPL.). http://doi.org/10.1016/j.diin.2010.05.011
- Garfinkel, S. (2007). Anti-Forensics : Techniques , Detection and Countermeasures. 2nd International Conference on I-Warfare and Security, 77–84. http://doi.org/10.1.1.109.5063
- Hilley, S. (2007). Anti-forensics – subverting justice with exploitation. Computer Fraud & Security, 2007(2), 16–18. http://doi.org/10.1016/S1361-3723(07)70023-4
- Hilley, S. (2007). Anti-forensics with a small army of exploits. Digital Investigation, 4(1), 13–15. http://doi.org/10.1016/j.diin.2007.01.005
- Jahankhani, H., Anastasios, B., & Revett, K. (2007). Digital anti forensics: Tools and approaches. In ECIW 2007: PROCEEDINGS OF THE 6TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY (pp. 115–120).
- Jain, A., & Chhabra, G. S. (2014). Anti-forensics techniques: An analytical review. In 2014 7th International Conference on Contemporary Computing, IC3 2014 (pp. 412–418). http://doi.org/10.1109/IC3.2014.6897209
- Karlsson, K. J., & Glisson, W. B. (2014). Android anti-forensics: Modifying cyanogenmod. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 4828–4837). http://doi.org/10.1109/HICSS.2014.593
- Kessler, G. C. (2006). Anti-Forensics and the Digital Investigator. Science, 7.
- Kessler, G. C. (2006). Anti-Forensics and the Digital Investigator INTRODUCING ANTI-FORENSICS CATEGORIES OF ANTI-FORENSICS METHODS. Science, 2, 3.
- Mansfield-Devine, S. (2010). Fighting forensics. Computer Fraud and Security, 2010(1), 17–20. http://doi.org/10.1016/S1361-3723(10)70112-3
- Pajek, P., & Pimenidis, E. (2009). Computer anti-forensics methods and their impact on computer forensic investigation. In Communications in Computer and Information Science (Vol. 45, pp. 145–155). http://doi.org/10.1007/978-3-642-04062-7_16

- Stamm, M. C., Lin, W. S., & Liu, K. J. R. (2012). Forensics vs. anti-forensics: A decision and game theoretic framework. In ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings (pp. 1749–1752). http://doi.org/10.1109/ICASSP.2012.6288237
- Stamm, M. C., & Liu, K. J. R. (2011). Anti-forensics of digital image compression. IEEE Transactions on Information Forensics and Security, 6(3 PART 2), 1050–1065. http://doi.org/10.1109/TIFS.2011.2119314
- Stamm, M. C., Tjoa, S. K., Lin, W. S., & Liu, K. J. R. (2010). Anti-forensics of JPEG compression. In ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings (pp. 1694–1697). http://doi.org/10.1109/ICASSP.2010.5495491
- Sun, H. M., Weng, C. Y., Lee, C. F., & Yang, C. H. (2011). Anti-forensics with steganographic data embedding in digital images. IEEE Journal on Selected Areas in Communications, 29(7), 1392–1403. http://doi.org/10.1109/JSAC.2011.110806
- Van Belle, J.-P. (2015). Anti-Forensics: A Practitioner Perspective. International Journal of Cyber-Security and Digital Forensics, 4(2), 390–403. http://doi.org/10.17781/P001593
- Wu, Z. H., Stamm, M. C., & Liu, K. J. R. (2013). Anti-forensics of median filtering. In ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings (pp. 3043–3047). http://doi.org/10.1109/ICASSP.2013.6638217
- Wundram, M., Freiling, F. C., & Moch, C. (2013). Anti-forensics: The next step in digital forensics tool testing. In Proceedings - 7th International Conference on IT Security Incident Management and IT Forensics, IMF 2013 (pp. 83–97). http://doi.org/10.1109/IMF.2013.17