REFERENCES

Abdi, H., 2010. Coefficient of variation. *Encyclopedia of research design*. Available at: http://www.utdallas.edu/~herve/abdi-cv2010-pretty.pdf [Accessed June 30, 2016].

Albitz, P. & Liu, C., 2006. *DNS And BIND 5th Ed*, Available at: http://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=9780596100575.

Barford, P. et al., 2002. A signal analysis of network traffic anomalies. *Proceedings of the 2nd ACM …*. Available at: http://dl.acm.org/citation.cfm?id=637210 [Accessed April 17, 2016].

Bellis, R., 2010. RFC 5966 - DNS Transport over TCP - Implementation Requirements. Available at: https://tools.ietf.org/html/rfc5966 [Accessed May 29, 2016].

Biermann, E., Cloete, E. & Venter, L., 2001. A comparison of intrusion detection systems. *Computers & Security*. Available at: http://www.sciencedirect.com/science/article/pii/S0167404801008069 [Accessed April 12, 2016].

Bilge, L., 2011. E XPOSURE : a Passive DNS Analysis Service to Detect and Report Malicious Domains. , V.

Bilge, L. et al., 2011. EXPOSURE : Finding Malicious Domains Using Passive DNS Analysis. *Ndss*, pp.1–17. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:EXPOSURE+:+Finding+Malicious+Domains+Using+Passive+DNS+Analysis#0.

Bilge, L. et al., 2014. EXPOSURE: a passive DNS analysis service to detect and report malicious domains. *ACM Transactions on Information and System Security (TISSEC)*, 16(4), p.14.

Bramer, M., 2007. *Principles of data mining*, Springer.

Buitinck, L. et al., 2013. {API} design for machine learning software: experiences from the scikit-learn project. In *ECML PKDD Workshop: Languages for Data Mining and Machine Learning*. pp. 108–122.

Cannady, J. & Harrell, J., 1996. A Comparative Analysis of Current Intrusion Detection Technologies. *Pattern Recognition*, 96, pp.212–218. Available at: http://iw.gtri.gatech.edu/Papers/ids_rev.html.

Chandola, V., Banerjee, A. & Kumar, V., 2009. Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, 41(September), pp.1–58. Available at: http://portal.acm.org/citation.cfm?id=1541882\nhttp://dl.acm.org/citation.cfm?id=1541882\nhttp://portal.acm.org/citation.cfm?doid=1541880.1541882 [Accessed February 3, 2016].

Chatfield, C., 1989. *The analysis of time series. An introduction*, Available at: https://www.google.com/books?hl=en&lr=&id=qKzyAbdaDFAC&oi=fnd&pg=PP1&dq=The+Analysis+Of+Time+Series+-+An+Introduction&ots=sxA086SyNm&sig=mnGpt2DI2gUlLBoPaxDdJCgGxAY [Accessed June 30, 2016].

Cheung, S., 2006. Denial of service against the domain name system. *IEEE Security and Privacy*, 4(1), pp.40–45. Available at: https://www.computer.org/csdl/mags/sp/2006/01/j1040.pdf [Accessed February

3, 2016].

Cotton, M. et al., 2011. *Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry*, [[Internet Engineering Task Force|IETF]]. Available at: https://tools.ietf.org/html/rfc6335 [Accessed June 18, 2016].

Debar, H., Dacier, M. & Wespi, A., 1999. Towards a taxonomy of intrusion-detection systems. *Computer Networks*. Available at: http://www.sciencedirect.com/science/article/pii/S1389128698000176 [Accessed April 12, 2016].

Denning, D.E., 2012. An intrusion-detection model. In *Proceedings - IEEE Symposium on Security and Privacy*. pp. 118–131.

Eastlake, D.I.I.I. & Laufman, C., 1997. RFC 2065 - Domain Name System Security Extensions. , 2009(November 5). Available at: http://www.ietf.org/rfc/rfc2065.txt [Accessed May 29, 2016].

Elich, M., 2013. Flow-based Network Anomaly Detection in the Context of IPv6. Available at: http://is.muni.cz/th/72577/fi_r/thesis.pdf [Accessed April 21, 2016].

Ellens, W. et al., 2013. Flow-based detection of DNS tunnels. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*. pp. 124–135.

Evron, R.V. and G., 2006. DNS Amplification Attacks. *Network Security*, 2006, pp.1–2. Available at: https://www.us-cert.gov/ncas/alerts/TA13-088A [Accessed May 29, 2016].

Fachkha, C., Bou-Harb, E. & Debbabi, M., 2014. Fingerprinting internet DNS amplification DDoS Activities. In *2014 6th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2014 Conference and Workshops*.

Farnham, G., 2013. *Detecting DNS Tunneling*.

Fawcett, T., 2006. An introduction to ROC analysis. *Pattern recognition letters*. Available at: http://www.sciencedirect.com/science/article/pii/S016786550500303X [Accessed February 3, 2016].

Gudmundsson, O., 2001. RFC 3226 - DNSSEC and IPv6 A6 aware server/resolver message size requirements. Available at: https://tools.ietf.org/html/rfc3226 [Accessed April 18, 2016].

Hamilton, J., 1994. *Time series analysis*, Available at: https://sisis.rz.htw-berlin.de/inh2007/12357004.pdf [Accessed June 18, 2016].

Heide, H. van der & Barendregt, N., 2011. DNS anomaly detection. *... , staff. science. uva. nl/~ delaat/sne- ...*. Available at: https://caldav.os3.nl/_media/2010-2011/courses/rp1/p17_report.pdf [Accessed April 8, 2016].

Hesselman, C. et al., 2014. A Privacy Framework for “DNS Big Data ” Applications. *Privacy en Informatie*, 6(September). Available at: https://www.sidnlabs.nl/uploads/tx_sidnpublications/SIDN_Labs_Privacyraamwerk_Position_Paper_V1.4_ENG.pdf.

IANA.Org, 2016. Domain Name System (DNS) Parameters. Available at: http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml [Accessed July 21, 2016].

IANA, O., IANA — Root Zone Database. Available at: http://www.iana.org/domains/root/db [Accessed May 3, 2016].

IANA, O., 2016. IANA TLD Alpha by Domain. Available at:

http://data.iana.org/TLD/tlds-alpha-by-domain.txt [Accessed May 29, 2016].

ICANN, 2014. *ICANN Bylaws*, Available at: https://www.icann.org/resources/pages/governance/bylaws-en [Accessed June 19, 2016].

Internetlivestats.com, 2016. Number of Internet Users (2016) - Internet Live Stats - Indonesia. Available at: http://www.internetlivestats.com/internet-users/indonesia/.

Jonathan Strickland, Who Owns Internet.

Jung, J., Krishnamurthy, B. & Rabinovich, M., 2002. Flash crowds and denial of service attacks. In *Proceedings of the eleventh international conference on World Wide Web - WWW '02*. New York, New York, USA: ACM Press, p. 293. Available at: http://dl.acm.org/citation.cfm?id=511446.511485 [Accessed April 4, 2016].

Kind, A., Stoecklin, M. & Dimitropoulos, X., 2009. Histogram-based traffic anomaly detection. *IEEE Transactions on Network and Service Management*, 6(2), pp.110–121. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5374831 [Accessed April 12, 2016].

Kothari, C.R., 2004. *Research Methodology: Methods & Techniques*,

Kumar, V., 2005. Parallel and distributed computing for cybersecurity. *IEEE Distributed Systems Online*, 6(10), pp.1–9.

Liaw, A. & Wiener, M., 2002. Classification and regression by randomForest. *R news*, 2(3), pp.18–22.

Lunt, T. & Jagannathan, R., 1988. A prototype real-time intrusion-detection expert system. *null*. Available at: http://www.computer.org/csdl/proceedings/sp/1988/0850/00/08500059.pdf [Accessed April 12, 2016].

Lynch, S., 2015. Attacks over DNS - InfoSec Resources. Available at: http://resources.infosecinstitute.com/attacks-over-dns/ [Accessed May 29, 2016].

Microsoft, T., 2010. DNS: The forwarding timeout value should be 2 to 10 seconds. Available at: https://technet.microsoft.com/en-us/library/ff807396(v=ws.10).aspx [Accessed April 27, 2016].

Mikle, O., Slaný, K. & Veselý, J., 2011. Detecting hidden anomalies in DNS communication. *Casalicchio E. DNS …*. Available at: https://labs.nic.cz/files/labs/Detecting_Hidden_Anomalies_in_DNS_Communication-2011.pdf [Accessed May 2, 2016].

Mills, D.L., 1981. RFC 799 - Internet name domains. , (799). Available at: ftp://ftp.isi.edu/in-notes/rfc799.txt [Accessed April 16, 2016].

Mockapetris, P.V., 1987a. RFC 1034 - Domain names: Concepts and Facilities. *Network Working Group*, p.55. Available at: http://tools.ietf.org/html/rfc1034.

Mockapetris, P.V., 1987b. RFC 1035 - Domain names: Implementation and Specification. *Network Working Group*, p.55. Available at: http://tools.ietf.org/html/rfc1035.

Mockapetris, P.V., 1983a. RFC 882 - Domain names: Concepts and Facilities. *Rfc 882*. Available at: https://tools.ietf.org/html/rfc882 [Accessed April 16, 2016].

Mockapetris, P.V., 1983b. RFC 883 - Domain names: Implementation and Specification. Available at: https://tools.ietf.org/html/rfc883 [Accessed April 16, 2016].

Mook, R., 2009. RFC 5452 - Measures for Making DNS More Resilient against Forged Answers. Available at: https://tools.ietf.org/html/rfc5452 [Accessed May

29, 2016].

Nainggolan, F., 2016. SFCNPcapDNS.

Narayana, M. & Prasad, B., 2011. Data Mining Machine Learning Techniques–A Study on Abnormal Anomaly Detection System. *International Journal of …*. Available at: http://www.ijcst.org/Volume2/Issue6/p3_2_6.pdf [Accessed April 12, 2016].

P. Maindi, W., 2014. Research Paper on Basic of Artificial Neural Network. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2(1), pp.96–100.

Patcha, A. & Park, J., 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*. Available at: http://www.sciencedirect.com/science/article/pii/S138912860700062X [Accessed April 12, 2016].

Pedregosa, F. et al., 2011. Scikit-learn: Machine Learning in {P}ython. *Journal of Machine Learning Research*, 12, pp.2825–2830.

Pei, J. et al., 2004. Data mining for intrusion detection: techniques, applications and systems. *null*. Available at: http://www.computer.org/csdl/proceedings/icde/2004/2065/00/20650877.pdf [Accessed April 12, 2016].

Perdisci, R. et al., 2009. Detecting malicious flux service networks through passive analysis of recursive DNS traces. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, pp.311–320. Available at: http://libra.msra.cn/Publication/6431504/detecting-malicious-flux-service-networks-through-passive-analysis-of-recursive-dns-traces [Accessed November 21, 2015].

Pete, C. et al., 2000. CRISP-DM 1.0: Step-by-step data minning guide. *CRISP-DM Consortium*, p.76.

Plonka, D. & Barford, P., 2009. Network anomaly confirmation, diagnosis and remediation. , pp.128–135. Available at: http://dl.acm.org/citation.cfm?id=1793974.1793996 [Accessed April 29, 2016].

Postel, J., 1994. RFC 1591 - Domain Name System Structure and Delegation. Available at: https://tools.ietf.org/html/rfc1591 [Accessed May 29, 2016].

Qayyum, A., Islam, M.H. & Jamil, M., 2005. Taxonomy of statistical based anomaly detection techniques for intrusion detection. In *Proceedings - IEEE 2005 International Conference on Emerging Technologies, ICET 2005*. pp. 270–276.

Ruan, W., Liu, Y. & Zhao, R., 2013. Pattern discovery in DNS query traffic. *Procedia Computer Science*. Available at: http://www.sciencedirect.com/science/article/pii/S1877050913001452 [Accessed April 12, 2016].

Satam, P. et al., 2015. Anomaly Behavior Analysis of DNS Protocol. *Journal of Internet Services …*. Available at: http://isyou.info/jisis/vol5/no4/jisis-2015-vol5-no4-05.pdf [Accessed April 18, 2016].

Schuba, C., 1993. Addressing weaknesses in the domain name system protocol. *Analysis*, (August). Available at: http://forum.ouah.org/schuba-DNS-msthesis.pdf [Accessed February 2, 2016].

Seifert, C., Welch, I. & Komisarczuk, P., 2008. Identification of malicious web pages through analysis of underlying DNS and web server relationships. *LCN*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.139.9691&rep=rep1&type=pdf [Accessed October 22, 2015].

Stalmans, E. & Irwin, B., A Framework for DNS Based Detection of Botnets at the ISP Level.

Steinwart, I., Hush, D. & Scovel, C., 2005. A Classification Framework for Anomaly Detection. *Journal of Machine Learning Research*, 6, pp.211–232.

Thomson, S. et al., 2003. RFC 1886 - DNS Extensions to Support IP Version 6. *RFC Editor United States*, (3596), p.8. Available at: http://www.ietf.org/rfc/rfc3596.txt [Accessed May 29, 2016].

Villamarin-Salomon, R. & Brustoloni, J.C., 2008. Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic. In *2008 5th IEEE Consumer Communications and Networking Conference*. IEEE, pp. 476–481. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=4446410 [Accessed April 29, 2016].

Villamarín-Salomón, R. & Brustoloni, J.C., 2009. Bayesian bot detection based on DNS traffic similarity. *Proceedings Of The Acm Symposium On Applied Computing*, (1), pp.2035–2041. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-72949095419&partnerID=40&md5=450769b4fc6be3ba67a0c6dbe3ef3d97.

Wang, Y. et al., 2006. Tracking anomalous behaviors of name servers by mining DNS traffic. In *Frontiers of High Performance Computing and …*. ISPA'06. Berlin, Heidelberg: Springer-Verlag, pp. 351–357. Available at: http://dx.doi.org/10.1007/11942634_37 [Accessed April 18, 2016].

Weimer, F., 2005. Passive DNS replication. *FIRST Conference on Computer Security Incident*. Available at: http://static.enyo.de/fw/volatile/pdr-draft-11.pdf [Accessed April 18, 2016].

Wireshark.narkive.com, 2010. Wireshark fails opening large-file on windows vista 32-bit. Available at: http://wireshark-users.wireshark.narkive.com/iBqM3R3C/wireshark-1-4-0-fails-opening-large-file-on-windows-vista-32-bit.

Wireshark.org, 2013. KnownBugs - OutOfMemory. Available at: https://wiki.wireshark.org/KnownBugs/OutOfMemory.

Wright, N.F., 2012. DNS in Computer Forensics. *Journal of Digital Forensics Security and Law*, 7(2), pp.11–42. Available at: http://ojs.jdfsl.org/index.php/jdfsl/article/view/117.

Wu, X. et al., 2008. Top 10 algorithms in data mining. *Knowledge and Information Systems*, 14(1), pp.1–37. Available at: http://link.springer.com/10.1007/s10115-007-0114-2 [Accessed July 11, 2016].

Xiao Hu, X. et al., 2008. Multivariate anomaly detection in real-world industrial systems. In *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*. IEEE, pp. 2766–2771. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4634187 [Accessed June 18, 2016].

Yarochkin, F. et al., 2013. Investigating DNS traffic anomalies for malicious activities. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*. IEEE, pp. 1–7. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6615506 [Accessed April 29, 2016].

Yarochkin, F. & Kropotov, V., 2013. Investigating DNS traffic anomalies for malicious activities. *… Workshop (DSN-W), …*. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6615506 [Accessed April

23, 2016].

Yuchi, X. et al., 2010. A new statistical approach to DNS traffic anomaly detection. , pp.302–313. Available at: http://dl.acm.org/citation.cfm?id=1948448.1948480 [Accessed April 12, 2016].

Zdrnja, B., Brownlee, N. & Wessels, D., 2007. Passive monitoring of dns anomalies. *Detection of Intrusions and Malware, and Vulnerability Assessment. Springer*, pp.129–139. Available at: http://www.springerlink.com/index/f6183017061l22xq.pdf.