Daftar Pusataka

Adelstein, F., 2006. Diagnosing your system without killing it first. *Communications of the ACM*, 49(2), pp.63–66.

Anmulwar, S. et al., 2014. Rogue access point detection methods: A review. *International Conference on Information Communication and Embedded Systems (ICICES2014)*, (978), pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7034106.

Cai, M., Wu, Z. & Zhang, J., 2014. Research and Prevention of Rogue AP Based *MITM* in Wireless Network. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, (2013), pp.538–542. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7024642.

Chandavarkar, B.R. et al., 2015. Detecting Rogue Access Points using Kismet., pp.172–175.

Client P. Garrison, 2010. *Digital Forensic for Network, Internet, and Clud Computing*,

Dong, Z. et al., 2015. Detecting and Locating Man-in-the-Middle *Attack*s in Fixed Wireless Networks., pp.283–293.

Lanze, F. et al., 2015. Hacker's toolbox: Detecting software-based 802.11 *Evil Twin* access points. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CC{Bibliography}NC 2015*, pp.225–232.

Mangut, H.A. et al., 2015. ARP Cache Poisoning Mitigation and Forensics Investigation. *2015 IEEE Trustcom/BigDataSE/ISPA*, pp.1392–1397. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7345444.

Mustafa, H. & Xu, W., 2014. CETAD: Detecting *Evil Twin* access point *attack*s in wireless *hotspot*s. *2014 IEEE Conference on Communications and Network Security, CNS 2014*, pp.238–246.

Nakhila, O. et al., 2015. User-side Wi-Fi *Evil Twin Attack* detection using SSL/TCP protocols. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.239–244.

Nanavare, V. V, 2016. Robust and Effective *Evil Twin* Access Point., pp.9074–9084.

Pilli, E.S., Joshi, R.C. & Niyogi, R., 2010. A Generic Framework for Network Forensics. *International Journal of Computer Applications*, 1(11), pp.1–6.

Rahman, S. & Khan, M.N.A., 2015. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, 8(2), pp.379–388. Available at: http://www.sersc.org/journals/IJHIT/.

Utami Putri, R. & Istiyanto, J.E., 2012. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *International Journal of Computer Science and Security*, 6(2). Available at: http://journal.ugm.ac.id/index.php/ijccs/article/view/2157.

Yang, C., Song, Y.M. & Gu, G.F., 2012. Active User-Side *Evil Twin* Access Point Detection Using Statistical Techniques. *Ieee Transactions on Information Forensics and Security*, 7(5), pp.1638–1651.

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), pp.17–31.

Adelstein, F., 2006. Diagnosing your system without killing it first. *Communications of the ACM*, 49(2), pp.63–66.

Anmulwar, S. et al., 2014. Rogue access point detection methods: A review. *International Conference on Information Communication and Embedded Systems (ICICES2014)*, (978), pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7034106.

Cai, M., Wu, Z. & Zhang, J., 2014. Research and Prevention of Rogue AP Based *MITM* in Wireless Network. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, (2013), pp.538–542. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7024642.

Chandavarkar, B.R. et al., 2015. Detecting Rogue Access Points using Kismet., pp.172–175.

Client P. Garrison, 2010. *Digital Forensic for Network, Internet, and Clud Computing*,

Dong, Z. et al., 2015. Detecting and Locating Man-in-the-Middle *Attack*s in Fixed Wireless Networks., pp.283–293.

Lanze, F. et al., 2015. Hacker's toolbox: Detecting software-based 802.11 *Evil Twin* access points. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.225–232.

Mangut, H.A. et al., 2015. ARP Cache Poisoning Mitigation and Forensics Investigation. *2015 IEEE Trustcom/BigDataSE/ISPA*, pp.1392–1397. Available at:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7345444.

Mustafa, H. & Xu, W., 2014. CETAD: Detecting *Evil Twin* access point *attack*s in wireless *hotspot*s. *2014 IEEE Conference on Communications and Network Security, CNS 2014*, pp.238–246.

Nakhila, O. et al., 2015. User-side Wi-Fi *Evil Twin Attack* detection using SSL/TCP protocols. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp.239–244.

Nanavare, V. V, 2016. Robust and Effective *Evil Twin* Access Point., pp.9074–9084.

Pilli, E.S., Joshi, R.C. & Niyogi, R., 2010. A Generic Framework for Network Forensics. *International Journal of Computer Applications*, 1(11), pp.1–6.

Rahman, S. & Khan, M.N.A., 2015. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, 8(2), pp.379–388. Available at: http://www.sersc.org/journals/IJHIT/.

Utami Putri, R. & Istiyanto, J.E., 2012. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *International Journal of Computer Science and Security*, 6(2). Available at: http://journal.ugm.ac.id/index.php/ijccs/article/view/2157.

Yang, C., Song, Y.M. & Gu, G.F., 2012. Active User-Side *Evil Twin* Access Point Detection Using Statistical Techniques. *Ieee Transactions on Information Forensics and Security*, 7(5), pp.1638–1651.

Yusoff, Y., Ismail, R. & Hassan, Z., 2011. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), pp.17–31.

Singh, O., 2009. *Network* Forensik. Indian Computer *Response Team (CERT-In). Department of Information Technology*, New Delhi, India.

Sulianta, F., 2008, *Komputer* Forensik. Jakarta : PT. Elex Media Komputindo.

Volonino, L. and Reynaldo A., 2008, *Computer* Forensik *For Dummies*. Indianapolis, Indiana : Wiley Publishing, Inc.

Ruchandani, B., Kumar, M., Kumar, A., Kumari, K., Sinha., A.,K., 2006, Ekperimentation In *Network* Forensik Analysis. *Proceedings of the Term Paper Series under CDACCNIE Bangalore*, India, December 2006.

Dhinda. maydhita dcp 2014. Implementasi Teknik Mitigasi *ARP Cache Poisoning* Dengan Kendali Penulisan *Arp Cache Table*. Tugas Akhir, Program Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya, Malang.

Marcella, Albert J., and Robert S. Greenfiled, "*Cyber* Forensik *a field manual for collecting, examining, and preserving evidence of computer crimes*", by CRC Press LLC, United States of America

Casey. "*Digital Evidence and Computer Crime*", 2nd ed., hal. 20

Arbough, William A, Narendar Shankar and Y.C Justine Wan, 2001. Your 802.11 *Wireless Network* Has No Clothes. Departemen of Computer *Science* University of Mary*LAN*d. 22 September 2004.

Eoghan Casey. *Digital Evidence and Computer Crime - 2nd Edition. Academic* Press, 2004.

Purbo, O., Tanuhandaru, P., Noertam, P., & Djajadikara, M. (2007) Jaringan *Wireless* Di Dunia Berkembang. Andi Yogyakarta, 425. http://doi.org/004.68 PUR j

Naskah akademik RUU tindak pidana di bidang Teknologi Informasi disusun oleh Mas Wigantoro Roes Setiyadi, Op.Cit, hal.25-26

Barda Nawawi Arief., Antisipasi Penanggulangan "*Cybercrime*" dengan hukum Pidana.,makalah pada seminar Nasional mengenai "*Cyberlaw*"., di STHB, Bandung, Hotel Grand *Aquila*, 9 April 2001.

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarto, Cybercrime-Motif dan Penindakan, Pensil 324, Jakarta, hal.13-14

T. Sukardi, "Forensik Komputer Prinsip Prinsip Dasar," pp. 1– 21, 2012.

Diakses dari http://vistumbler.id.uptodown.com/ di acsses pada tanggal 24 April 2016.21.00 WIB

Diakses dari http://file.scirp.org/Html/3-7800083_21340.htm di accsess tanggal 24 April 2016 21.00 WIB

Diakses dari http://etutorials.org/*Network*ing/ di accsess tanggal 24 April 2016 21.00 WIB

Diakses dari http://syworks.blogspot.co.id/2014/01/wireless-ids-intrusion-detection system.html di akses pada tanggal 24 April 2016. 21.00 WIB.