

Daftar Pustaka

- Agency, N. S. (2014). *MONKEYCALENDAR Operation Schematics*. U.S. Government as the NSA: NSA diverted computers and laptops from shipping facilities to install spyware.
- Barbara, J. (2011). *SIM Forensics*. US: Forensics Megazine.
- Bhadsavle, N., & Wang, J. A. (2009). Validating Tools for Cell Phone Forensics. *Southeast Section Conference*. South Marietta Parkway: ASEE Southern Polytechnic State University.
- Briceno M, G. I. (1998). *An Implementation of The GSM A3 A8 Algorithm*. California.
- DTR-T001-01, D. F. (2001). *A roadmap for digital forensic research*.
- Egners, A., Rey, E., Schmidt, H., Schneider, P., & Wessel, S. (2012). Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals. In P. S. Networks), *Attack analysis and Security concepts for Mobile Network infrastructures*. Germany: ASMONIA consortium.
- Fauzan, M. F. (2013). Program Studi Teknik Informatika, Institut Teknologi Bandung. *Studi dan Perbandingan Keamanan GSM dan CDMA* .
- Goldberg, I., Wagner, D., & Green, L. (1999). Presented at the Rump Session of Crypto. *The (Real-Time) Cryptanalysis* .
- Gubian, F. C. (2011). Forensics and SIM cards. *International Journal of Digital Evidence* , University of Brescia.
- Hayat, C. (2014). *Analisis SIM Card Clone Pada IM3 Smart Serta Penggunaan Ellptic Curve Cryptosystem Untuk Meningkatkan Keamanan Jaringan GSM*. Depok, Indonesia: Jurusan Sistem Informasi, Universitas Gunadarma.
- Howden, W. E. (2005). Software Testing and Validation Techniques. *Computer Society Press*. New York: IEEE Computer Society Press.
- Irhana, N. (2000). Mobile Communications Security. *Introduction to Authentication* , <http://www.elektroindonesia.com/elektro/tel29c.html>.

- Isomäki, M. (November 29, 1999). The relationship between GSM security parameters and functions. *Security in the Traditional Telecommunications Networks and in the Internet*, Figure 5. [7, 8].
- Jansen, W., & Ayers, R. (2005). National Institute of Standards and Technology. *Forensic Software Tools for Cell Phone Subscriber Identity Modul*.
- Jaswo, N. H. (2013). *Desain Penelitian Etnografi*. Kudus: Pasca Sarjana STAIN.
- Montaque, P. (2001). Implementing an Efficient Elliptic Curve Cryptography Over GF(p) on Smart Card. *University of Technology, Australia*.
- Prayudi, Y., & Rifandi, F. (2013). Ekplorasi Bukti Digital pada SIMCard. *Pusat Studi Forensika Digital, SESINDO FTI - Universitas Islam Indonesia*.
- R. Rao, J., Rohatgi, P., & Scherzer, H. (2002). In I. W. Center, *Partitioning Attacks*. Yorktown Heights NewYork: IBM Watson Research Center.
- R. Rao, J., Rohatgi, P., Scherzer, H., & Tingueley, S. (2002). How to Rapidly Clone Some GSM Cards. *Security and Privacy, IEEE Symposium*.
- Tomcs, D. (2013). *The big GSM write-up how to capture, analyze and crack GSM*. domonkos.tomcsanyi.net.
- Tomcsányi, D. P. (2013, October 13). Flowchart Traffic Channel "Call Cloning". *The big GSM write-up, how to capture, analyze and crack GSM*.
- Velazco, C. (2015). *SIM card maker Gemalto investigates spy agencies' hack attack*. US: New York Times.
- Willassen, S. M. (2003). International Journal of Digital Evidence Spring. *Forensics and the GSM mobile telephone system Senior Investigator, Computer Forensics, Ibas AS*.