

## PREFACE

I would want to give gratitude to God who grants me life, wisdom and blessings and giving the opportunity to finish this work. This thesis is written as the final requirement to attain a degree at the Study Program of Electrical Engineering, Faculty of Science and Technology, Universitas Pelita Harapan, Karawaci, Tangerang.

I also want to thank the help and guidance of many people, including :

1. Prof. Dr. Manlian Ronald A. Simanjuntak, ST., MT., D. Min., as the Dean of Faculty of Science and Technology, Universitas Pelita Harapan.
2. Dr. Henri P. Uranus, as the Head of Electrical Engineering Department, Universitas Pelita Harapan. Also as the co-supervisor who guided and advised me in doing this thesis.
3. Dr.-Ing. Ihan Martoyo ST, M.Sc., MTS as the supervisor who inspired, enlightened, advised and guided me in doing the experiment and finishing the thesis.
4. All lecturers and staffs who helped the author in the whole four years of study at the Department of Electrical Engineering, Universitas Pelita Harapan.
5. My mother and my late father who guided and taught me most of the things that I know in this life and for my mother's support in doing this thesis.
6. My siblings, Ezra and Kharis who were always there to help and support me.
7. All my friends who helped and guided the author in finishing this thesis especially the ones in Electrical Engineering batch of 2012, Andy Tjee, Billy Tirta, Jason Thenneil and William Suryawirawan.

8. Many people who helped me, whose name could not be written one by one

I humbly realize that there is a lot of room for improvements and I am hoping for critiques and suggestions from the readers of this thesis.

Karawaci, 12<sup>th</sup> August 2016

Paul Elijah Setiasabda



## TABLE OF CONTENTS

	Page
<b>COVER PAGE</b> .....	i
<b>STATEMENT OF THESIS AUTHENTICITY</b> .....	ii
<b>APPROVAL FROM THESIS SUPERVISORS</b> .....	iii
<b>APPROVAL BY THESIS EXAMINATION COMMITTEE</b> .....	iv
<b>ABSTRACT</b> .....	v
<b>PREFACE</b> .....	vii
<b>TABLE OF CONTENTS</b> .....	ix
<b>LIST OF FIGURES</b> .....	xii
<b>LIST OF TABLES</b> .....	xvi
<b>CHAPTER I. INTRODUCTION</b>	
1.1 Background .....	1
1.2 Aims and Objectives .....	2
1.3 Scope of Problem .....	2
1.4 Research Method .....	3
1.5 Thesis Structure .....	3
<b>CHAPTER II. BASIC THEORY</b>	
2.1 Software Defined Radio .....	4
2.2 HackRF One .....	5
2.3 GNU Radio Companion .....	9
2.4 Antenna .....	10

2.5 Frequency Modulation .....	10
2.6 Global System for Mobile Communication (GSM).....	12
2.7 Wireless Fidelity (WiFi) .....	16
<b>CHAPTER III. HACKRF ONE SETUP AND PROGRAMMING</b>	
3.1 FM Receiver .....	18
3.2 Dual Channel FM Receiver.....	21
3.3 FM Transmitter .....	22
3.4 GSM Receiver.....	24
3.5 Jammer .....	26
3.6 Antennas.....	27
<b>CHAPTER IV. DATA ANALYSIS</b>	
4.1 FM Receive Configuration.....	30
4.2 FM Transmit Configuration .....	33
4.3 Jamming FM 100.6 MHz .....	41
4.4 GSM Receiver (Base Station Identity).....	43
4.5 GSM Receiver (SMS) .....	49
4.6 GSM Receiver (Phone Call).....	56
4.7 GSM Jamming .....	59
4.8 WiFi Jamming.....	63
<b>CHAPTER V. CONCLUSION AND FUTURE OUTLOOKS</b>	
5.1 Conclusions .....	65
5.2 Future Outlooks.....	66
<b>BIBLIOGRAPHY .....</b>	<b>67</b>

**APPENDIX**

A. Transmission Results.....A-1 – A-8

B. Required Programs Installation.....B1



## LIST OF FIGURES

	Page
Figure 2.1 HackRF One .....	6
Figure 2.2 HackRF One Front-End Diagram.....	8
Figure 2.3 HackRF One Front-End Block Diagram .....	8
Figure 2.4 HackRF One Digital Stage Block Diagram.....	8
Figure 2.5 An Example of GNU Radio Companion Flowchart .....	9
Figure 2.6 ANT500, A Monopole Antenna .....	10
Figure 2.7 Frequency modulation at time domain .....	11
Figure 2.8 Frequency modulation at frequency domain carrying a music..	11
Figure 2.9 Block Diagram of FM Receiver .....	12
Figure 2.10 Channels of FDMA Systems .....	13
Figure 2.11 Multicarrier TDMA channels .....	14
Figure 3.1 HackRF One Experimental Set-Up .....	17
Figure 3.2 Implementation of HackRF One Set-Up .....	17
Figure 3.3 FM Receiver Block Diagram.....	20
Figure 3.4 Dual Channel FM Receiver Block Diagram.....	21
Figure 3.5 FM Transmitter Block Diagram .....	23
Figure 3.6 GSM Receiver Block Diagram.....	25
Figure 3.7 Jammer Block Diagram .....	26
Figure 3.8 ANRD82421703-SMA Antenna .....	27
Figure 3.9 ANRD245X05-SMA Antenna .....	28
Figure 4.1 Spectrum Analyzer GSP-827.....	29

Figure 4.2	Setup of HackRF One and Spectrum Analyzer .....	30
Figure 4.3	Distance between UPH to Heartline Center from Google Maps.....	31
Figure 4.4	FM Signal Received in HackRF One with Telescopic Antenna ANT500 .....	32
Figure 4.5	FM Signal Received in Spectrum Analyzer .....	32
Figure 4.6	Background around 84 MHz before audio signal was sent .....	33
Figure 4.7	Signals around 84 MHz while audio signal with IF gain of 30 dB using Telescopic Antenna ANT500 .....	34
Figure 4.8	Signals around 84 MHz when audio signal with IF gain of 60 dB using Telescopic Antenna ANT500 .....	34
Figure 4.9	Signals around 850 MHz while audio signal with IF gain of 30 dB using Telescopic Antenna ANT500 .....	35
Figure 4.10	Signals around 850 MHz while audio signal with IF gain of 60 dB using Telescopic Antenna ANT500.....	35
Figure 4.11	Signals around 1.9 GHz while audio signal with IF gain of 30 dB using Telescopic Antenna ANT500.....	36
Figure 4.12	Signals around 1.9 GHz while audio signal with IF gain of 60 dB using Telescopic Antenna ANT500.....	36
Figure 4.13	Signals around 2.5 GHz while audio signal with IF gain of 30 dB using Telescopic Antenna ANT500 .....	37
Figure 4.14	Signals around 2.5 GHz while audio signal with IF gain of 60 dB using Telescopic Antenna ANT500 .....	37

Figure 4.15	WBFM 84 MHz was transmitted when a song was played.....	40
Figure 4.16	100.6 MHz when a song was played .....	40
Figure 4.17	The signal when a single tone is played .....	41
Figure 4.18	100.6 MHz vs 101.2 MHz Transmitted by HackRF One at 60 dB IF .....	42
Figure 4.19	100.6 MHz with Cosine Wave Transmitted from HackRF One with IF 30 dB .....	42
Figure 4.20	100.6 MHz with Cosine Wave Transmitted from HackRF One with IF 60 dB .....	43
Figure 4.21	Kalibrate-HackRF scanned at GSM-900.....	44
Figure 4.22	Kalibrate-HackRF scanned at DCS-1800.....	44
Figure 4.23	Gr-gsm Block Diagram run at 957.6 MHz.....	45
Figure 4.24	Wireshark Run at 957.6 MHz.....	45
Figure 4.25	Spectrum Analyzer with 958 MHz as the Center .....	46
Figure 4.26	Gr-gsm with 958 MHz as the Center.....	47
Figure 4.27	Spectrum Analyzer with 954 MHz as the Center .....	47
Figure 4.28	Gr-gsm with 954 MHz as the Center.....	48
Figure 4.29	Gr-gsm with 947.2 MHz as the Center.....	49
Figure 4.30	Wireshark Result at 947.2 MHz .....	50
Figure 4.31	Base Stations that were connected to the phone.....	51
Figure 4.32	The phone was connected only to 17413.....	52
Figure 4.33	Capturing The Traffic at 947.2 MHz for a Minute.....	52
Figure 4.34	SMS were Sent and Received by 082261343263.....	53



Figure 4.35	Decode and Replay the Captured Traffic .....	53
Figure 4.36	TMSI Number from Captured Traffic .....	53
Figure 4.37	Immediate Assignment and SDCCH Information.....	54
Figure 4.38	Decode and Replay The Captured Traffic with SDCCH and Kc Information .....	54
Figure 4.39	A SMS Text Captured .....	55
Figure 4.40	Another SMS Text Captured .....	55
Figure 4.41	Capturing Voice with ARFCN instead of Frequency.....	56
Figure 4.42	TMSI of the Phone Call Process.....	57
Figure 4.43	SDCCH Channel and Timeslot.....	57
Figure 4.44	Decode and Replay The Captured Traffic with SDCCH and Kc Information .....	57
Figure 4.45	Phone Call Setup Information .....	58
Figure 4.46	The Timeslot Used for the Phone Call .....	59
Figure 4.47	The Voice in the Phone Call was Extracted .....	59
Figure 4.48	947.2 MHz Before Jammed.....	60
Figure 4.49	947.2 MHz After Jammed .....	60
Figure 4.50	The Base Stations that were Connected to Both Phones .....	61
Figure 4.51	The Signals of Both Phones before Jamming.....	62
Figure 4.52	The Signal Reception After Jamming .....	62
Figure 4.53	Tjung's Territory router connected to the laptop.....	63
Figure 4.54	Checking the frequency of the connection .....	64
Figure 4.55	The laptop is disconnected to from the router .....	64

## LIST OF TABLES

	Page
Table 2.1      2.4 GHz WiFi Operating Frequencies .....	16
Table 4.1      Signal peak in FM transmission experiments.....	38
Table 4.2      SNR in FM transmission experiments.....	38

