

## DAFTAR GAMBAR

<b>Gambar II.1</b> Tiga Aspek Keamanan Sistem Informasi .....	46
<b>Gambar II.2</b> Pendekatan & Metodologi ISSAF (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	50
<b>Gambar II.3</b> Logo Kali Linux .....	55
<b>Gambar II.4</b> Tampilan <i>Tools</i> OWASP ZAP .....	56
<b>Gambar II.5</b> Tampilan <i>Tools</i> Nessus Vuulnerability Scanner .....	57
<b>Gambar II.6</b> Tampilan <i>Tools</i> Nmap – Zenmap GUI.....	57
<b>Gambar II.7</b> Tampilan <i>Tools</i> Nmap – Kali Linux.....	58
<b>Gambar II.8</b> Tampilan <i>Tools</i> PuTTY .....	58
<b>Gambar II.9</b> Tampilan <i>SSL Security Test</i> (Qualys <i>SSL Labs</i> ).....	59
<b>Gambar II.10</b> Tampilan <i>Tools WhoIS</i> Kali Linux.....	59
<b>Gambar II.11</b> Tampilan <i>Tools SpiderFoot</i> .....	60
<b>Gambar II.12</b> Tampilan <i>Tools BurpSuite</i> .....	60
<b>Gambar II.13</b> Tampilan <i>Tools DirSearch</i> .....	61
<b>Gambar II.14</b> Tampilan <i>Tools ParamSpider</i> .....	61
<b>Gambar II.15</b> Tampilan <i>Tools DalFox</i> .....	61
<b>Gambar II.16</b> Tampilan <i>Tools Hydra</i> .....	62
<b>Gambar II.17</b> Tampilan <i>Tools WireShark</i> .....	62
<b>Gambar II.18</b> Tampilan <i>Tools SQLMap</i> .....	63
<b>Gambar II.19</b> Tampilan <i>Tools SlowHttpTest</i> .....	63
<b>Gambar II.20</b> Tampilan <i>Tools SlowHttpTest</i> .....	64
<b>Gambar II.21</b> Tampilan <i>Tools SlowHttpTest</i> .....	64
<b>Gambar II.22</b> Tampilan <i>Tools SlowHttpTest</i> .....	65
<b>Gambar II.23</b> Tampilan <i>Tools BleachBit</i> .....	65
<b>Gambar II.24</b> Tampilan <i>Tools Tor Browser</i> .....	66
<b>Gambar II.25</b> Tampilan <i>Tools ProxyChain (Dynamic)</i> .....	66
<b>Gambar III.1</b> Alur Penelitian Berdasarkan <i>Framework</i> ISSAF (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	67
<b>Gambar III.2</b> Alur Tahapan <i>Information Gathering</i> .....	70
<b>Gambar III.3</b> Alur Tahapan <i>Network Mapping</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	71

<b>Gambar III.4</b> Alur Tahapan <i>Vulnerabilities Identification</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005).....	71
<b>Gambar III.5</b> Alur Tahapan <i>Penetration</i> .....	72
<b>Gambar III.6</b> Alur Tahapan <i>Gaining Access and Privilege Escalation</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	73
<b>Gambar III.7</b> Alur Tahapan <i>Enumerating Further</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005).....	73
<b>Gambar III.8</b> Alur Tahapan <i>Maintaining Access</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	74
<b>Gambar III.9</b> Alur Tahapan <i>Covering Tracks</i> (Information Systems Security Assessment Framework (ISSAF) Draft 0.2, 2005) .....	74
<b>Gambar V.1</b> Situs Utama Yayasan Dana Sosial Al Falah.....	84
<b>Gambar V.2</b> Hasil Dari <i>Tools Wappalyzer</i> .....	84
<b>Gambar V.3</b> Hasil <i>Scan Ping Test</i> (Terminal Kali Linux) .....	85
<b>Gambar V.4</b> Hasil <i>Scan Ping Test</i> Menggunakan CMD ( <i>Command Prompt Windows</i> ).....	85
<b>Gambar V.5</b> Hasil <i>Scan Nslookup (Domain)</i> .....	86
<b>Gambar V.6</b> Hasil <i>Scan Nslookup Reverse DNS (IP Address)</i> .....	86
<b>Gambar V.7</b> Hasil <i>Scan Nslookup Pencarian Data DNS</i> .....	86
<b>Gambar V.8</b> Hasil <i>Scan Nslookup Pencarian Data SOA (Start of Authority)</i> ...	87
<b>Gambar V.9</b> Hasil <i>Scan Nslookup Mapping Domain Address ke Daftar Server DNS</i> .....	87
<b>Gambar V.10</b> Hasil <i>Scan Nslookup Data DNS</i> .....	87
<b>Gambar V.11</b> Hasil <i>Scan Nslookup Mail Exchange (Mencari Data MX)</i> .....	88
<b>Gambar V.12</b> Hasil <i>Scan Nslookup TXT (Mencari Data TXT)</i> .....	88
<b>Gambar V.13</b> Hasil <i>Scanning WhoIS (Domain) Ke-1</i> .....	88
<b>Gambar V.14</b> Hasil <i>Scanning WhoIS (Domain) Ke-2</i> .....	89
<b>Gambar V.15</b> Hasil <i>Scanning WhoIS (Domain) Ke-3</i> .....	89
<b>Gambar V.16</b> Hasil <i>Scanning WhoIS (IP Address) Ke-1</i> .....	90
<b>Gambar V.17</b> Hasil <i>Scanning WhoIS (IP Address) Ke-2</i> .....	91
<b>Gambar V.18</b> Hasil <i>Scanning WhoIS (IP Address) Ke-3</i> .....	91

<b>Gambar V.19</b> Hasil <i>Scanning WhoIS (IP Address) Ke-4</i> .....	92
<b>Gambar V.20</b> Hasil <i>Scanning WhoIS (IP Address) Ke-5</i> .....	92
<b>Gambar V.21</b> Hasil <i>Scanning SpiderFoot Ke-1</i> .....	94
<b>Gambar V.22</b> Hasil <i>Scanning SpiderFoot Ke-2</i> .....	94
<b>Gambar V.23</b> Hasil <i>Scanning SpiderFoot (Affilliate Domain)</i> .....	95
<b>Gambar V.24</b> Hasil <i>Scanning SpiderFoot (IP Address V4)</i> .....	95
<b>Gambar V.25</b> Hasil <i>Scanning SpiderFoot (IP Address V6)</i> .....	96
<b>Gambar V.26</b> Hasil <i>Scanning SpiderFoot (Country Name)</i> .....	96
<b>Gambar V.27</b> Hasil <i>Scanning SpiderFoot (Domain Name)</i> .....	96
<b>Gambar V.28</b> Hasil <i>Scanning SpiderFoot (Domain Name Parent)</i> .....	97
<b>Gambar V.29</b> Hasil <i>Scanning SpiderFoot (Email Gateway (DNS MX Record))</i> .....	97
<b>Gambar V.30</b> Hasil <i>Scanning SpiderFoot (Internet Name)</i> .....	97
<b>Gambar V.31</b> Hasil <i>Scanning SpiderFoot (Open TCP Port)</i> .....	98
<b>Gambar V.32</b> Hasil <i>Scanning SpiderFoot (Summary, Scan Status, Cerelations, Data Types)</i> .....	98
<b>Gambar V.33</b> Hasil <i>Scanning SpiderFoot (Correlation)</i> .....	99
<b>Gambar V.34</b> Tampilan <i>SpiderFoot New Scan (By Use Case All)</i> .....	99
<b>Gambar V.35</b> <i>SpiderFoot Command Running</i> .....	100
<b>Gambar V.36</b> Hasil <i>Regular Nmap Scan (Kali Linux)</i> .....	102
<b>Gambar V.37</b> Hasil <i>Regular Nmap Scan (Windows)</i> .....	102
<b>Gambar V.38</b> Hasil <i>Nmap Identify Live Hosts (Kali Linux)</i> .....	103
<b>Gambar V.39</b> Hasil <i>Zenmap Intense Scans All TCP Port (Windows)</i> .....	103
<b>Gambar V.40</b> Hasil <i>Nmap Regular TCP Port Scanning (Kali Linux)</i> .....	104
<b>Gambar V.41</b> Hasil <i>Nmap Regular UDP Port Scanning (Kali Linux)</i> .....	105
<b>Gambar V.42</b> Hasil <i>Nmap Service Version and OS Detection (Kali Linux)</i> ..	106
<b>Gambar V.43</b> Hasil <i>SSL Security Test (ImmuniWeb)</i> .....	106
<b>Gambar V.44</b> Hasil <i>SSL Security Test (SSL Labs)</i> .....	107
<b>Gambar V.45</b> Tampilan Hasil <i>Scanning Nessus Basic Network Scan (1)</i> .....	109
<b>Gambar V.46</b> Tampilan Hasil <i>Scanning Nessus Basic Network Scan (2)</i> .....	109
<b>Gambar V.47</b> Hasil <i>Nessus Basic Network Scan (3)</i> .....	109

<b>Gambar V.48</b> Hasil Nessus <i>Basic Network Scan Folder ISC Bind (Multiple Issues)</i> .....	110
<b>Gambar V.49</b> Kerentanan DNS <i>Server Spoofed Request Amplification DDoS</i> .....	110
<b>Gambar V.50</b> Kerentanan DNS <i>Server Recursice Query Cache Poisoning Weakness</i> .....	111
<b>Gambar V.51</b> Hasil Nessus <i>Basic Network Scan Folder HTTP (Multiple Issue)</i> .....	111
<b>Gambar V.52</b> Kerentanan HSTS <i>Missing From HTTPS Server (RFC 6797)</i> . 112	
<b>Gambar V.53</b> Hasil Nessus <i>Basic Network Scan Folder DNS (Multiple Issue)</i> .....	112
<b>Gambar V.54</b> Kerentanan DNS <i>Server Cache Snooping Remote Information Disclosure</i> .....	113
<b>Gambar V.55</b> Tampilan Hasil <i>Scanning Nessus Web Application Tests (1)</i> ... 115	
<b>Gambar V.56</b> Tampilan Hasil <i>Scanning Web Application Tests (2)</i> .....	115
<b>Gambar V.57</b> Tampilan Kerentanan <i>Web Application Potentially Vulnerable to Clickjacking</i> .....	115
<b>Gambar V.58</b> Hasil Nessus <i>Web Application Tests Folder HTTP (Multiple Issue)</i> .....	116
<b>Gambar V.59</b> Tampilan Kerentanan HSTS <i>Missing From HTTPS Server (RFC 6797)</i> .....	116
<b>Gambar V.60</b> Hasil Nessus <i>Web Application Tests Folder Web Server (Muliple Issue)</i> .....	117
<b>Gambar V.61</b> Tampilan Kerentanan <i>Web Server Allows Password Auto-Completion</i> .....	117
<b>Gambar V.62</b> Tampilan OWASP ZAP <i>Using Automated Scan Use Traditional and Ajax Spider</i> .....	119
<b>Gambar V.63</b> Hasil <i>Scanning OWASP ZAP Automated Scan Use Traditional and Ajax Spider</i> .....	120
<b>Gambar V.64</b> Tampilan Kerentanan <i>Hash Disclosure - Mac OSX salted SHA-1 (High)</i> .....	120

<b>Gambar V.65</b> Tampilan Kerentanan <i>Absence of Anti-CSRF Tokens (Medium)</i> .....	121
<b>Gambar V.66</b> Tampilan Kerentanan <i>Content Security Policy (CSP) Header Not Set (Medium)</i> .....	121
<b>Gambar V.67</b> Tampilan Kerentanan <i>Cross-Domain Misconfiguration (Medium)</i> .....	121
<b>Gambar V.68</b> Tampilan Kerentanan <i>Hidden File Found (Medium)</i> .....	122
<b>Gambar V.69</b> Tampilan Kerentanan <i>Missing Anti-clickjacking Header (Medium)</i> .....	122
<b>Gambar V.70</b> Tampilan Kerentanan <i>Vulnerable JS Library (Medium)</i> .....	123
<b>Gambar V.71</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Beranda) .	127
<b>Gambar V.72</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Laporan Kurban) .....	127
<b>Gambar V.73</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Hitung Zakat) .....	128
<b>Gambar V.74</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Layanan Donatur) .....	128
<b>Gambar V.75</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu ( <i>Event</i> Donasi Ramadhan) .....	129
<b>Gambar V.76</b> <i>SQLInjection</i> Menampilkan <i>Database</i> Pada Menu (Program Donasi).....	129
<b>Gambar V.77</b> <i>SQLInjection</i> Pada ( <i>Login Page</i> ) Dengan <i>Risk Level 3 Ke-1</i> ...	130
<b>Gambar V.78</b> <i>SQLInjection</i> Pada ( <i>Login Page</i> ) Dengan <i>Risk Level 3 Ke-2</i> ...	131
<b>Gambar V.79</b> <i>SQLInjection</i> Pada ( <i>Login Page</i> ) Dengan <i>Risk Level 3 Ke-3</i> ...	131
<b>Gambar V.80</b> <i>SQLInjection</i> Pada ( <i>Login Page</i> ) Dengan <i>Risk Level 3 Ke-4</i> ...	131
<b>Gambar V.81</b> <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi.....	132
<b>Gambar V.82</b> Hasil <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi (1) .....	133
<b>Gambar V.83</b> Hasil <i>Input XSS Payload</i> Pada <i>Form</i> Registrasi (2) .....	133
<b>Gambar V.84</b> Tampilan <i>Instalasi Golang-Go</i> .....	134
<b>Gambar V.85</b> Tampilan <i>Instalasi Tools Dalfox</i> .....	134
<b>Gambar V.86</b> Tampilan <i>Change Directory</i> Untuk <i>Tools Dalfox</i> .....	135
<b>Gambar V.87</b> Tampilan <i>Instalasi Tools ParamSpider</i> .....	135

<b>Gambar V.88</b> Tampilan <i>Scanning</i> URL Parameter <i>Website</i> YDSF.....	135
<b>Gambar V.89</b> Tampilan <i>Result</i> atau <i>Output</i> dari <i>Tools</i> ParamSpider.....	136
<b>Gambar V.90</b> Tampilan Hasil <i>Scanning Tools</i> Dalfox (14 URL Parameter)..	136
<b>Gambar V.91</b> Melakukan Instalasi <i>Tools</i> Slowhttptest .....	137
<b>Gambar V.92</b> Melakukan Serangan DDoS Menggunakan <i>Tools</i> Slowhttptest .....	137
<b>Gambar V.93</b> Tampilan <i>Website</i> YDSF Sebelum Dilakukan Serangan DDoS .....	137
<b>Gambar V.94</b> Tampilan <i>Website</i> YDSF Setelah Dilakukan Serangan DDoS.	138
<b>Gambar V.95</b> Tampilan <i>Website</i> YDSF Setelah Proses Serangan DDoS Selesai Dilakukan .....	138
<b>Gambar V.96</b> Tampilan Hasil Dari Serangan DDoS Menggunakan <i>Slowhttptest</i> .....	139
<b>Gambar V.97</b> Tampilan Hasil <i>Regular Nmap Scan</i> ( <i>Port</i> 21 FTP) .....	140
<b>Gambar V.98</b> Mengakses <i>Port</i> FTP 21 menggunakan <i>Quick Access File Explorer</i> .....	141
<b>Gambar V.99</b> Tampilan <i>Log On As</i> Saat Mengakses <i>Port</i> FTP 21 Menggunakan <i>Quick Access</i> .....	141
<b>Gambar V.100</b> Tampilan <i>Tools</i> PuTTY <i>Configuration</i> Untuk Akses <i>Port</i> 22 <i>Service</i> SSH.....	141
<b>Gambar V.101</b> Tampilan PuTTY Saat Mengakses <i>Port</i> 22 Dengan Layanan SSH .....	142
<b>Gambar V.102</b> Tampilan IP <i>Subneting</i> Untuk Mencari IP <i>Network</i> dari IP <i>Website</i> YDSF.....	145
<b>Gambar V.103</b> Tampilan Nmap Untuk Mencari IP Dari <i>Port</i> FTP (21) Yang Terbuka .....	145
<b>Gambar V.104</b> Tampilan Nmap Untuk Mencari IP Dari <i>Port</i> SSH (22) Yang Terbuka .....	146
<b>Gambar V.105</b> <i>Passwordlist</i> Yang Digunakan Untuk Melakukan <i>Bruteforce Attack</i> .....	147
<b>Gambar V.106</b> <i>UsernameList</i> Yang Digunakan Untuk Melakukan <i>Bruteforce Attack</i> .....	147

<b>Gambar V.107</b> <i>Hydra</i> Penyerangan SSH Login (Tidak Menggunakan <i>usernamelist.txt</i> ) .....	148
<b>Gambar V.108</b> <i>Hydra</i> Penyerangan SSH Login (Menggunakan <i>usernamelist.txt</i> ) .....	149
<b>Gambar V.109</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (1) .....	151
<b>Gambar V.110</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (2) .....	151
<b>Gambar V.111</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (3) .....	152
<b>Gambar V.112</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (4) .....	152
<b>Gambar V.113</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (5) .....	153
<b>Gambar V.114</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (6) .....	153
<b>Gambar V.115</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (7) .....	154
<b>Gambar V.116</b> Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (1) .....	156
<b>Gambar V.117</b> Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (2) .....	156
<b>Gambar V.118</b> Tampilan <i>BurpSuite Maintaining an Autenticated Session</i> (3) .....	157
<b>Gambar V.119</b> Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (3) .....	157
<b>Gambar V.120</b> Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (4) .....	158
<b>Gambar V.121</b> Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (5) .....	158
<b>Gambar V.122</b> Tampilan <i>Tools BurpSuite Maintaining an Autenticated Session</i> (6) .....	159

<b>Gambar V.123</b> Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (1).....	160
<b>Gambar V.124</b> Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (2).....	160
<b>Gambar V.125</b> Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (3).....	160
<b>Gambar V.126</b> Tampilan <i>Tools</i> WireShark <i>Sniffing Traffic</i> (4).....	161
<b>Gambar V.127</b> Tampilan <i>Tools</i> WireShark (Contoh Percobaan <i>Sniffing Traffic</i> Yang Berhasil) .....	162
<b>Gambar V.128</b> Tampilan <i>Tools</i> WireShark (Contoh Percobaan <i>Sniffing Traffic</i> Yang Berhasil) .....	162
<b>Gambar V.129</b> Tampilan <i>tools</i> Nmap Untuk Mencari <i>Open Port</i> FTP (21)...	165
<b>Gambar V.130</b> Tampilan <i>tools</i> Nmap Untuk Mencari <i>Open Port</i> SSH (22) ..	165
<b>Gambar V.131</b> Tampilan <i>Tools</i> Nmap SSH <i>Brute</i> Pada <i>Port</i> SSH (1) .....	166
<b>Gambar V.132</b> Tampilan <i>Tools</i> Nmap SSH <i>Brute</i> Pada <i>Port</i> SSH (2) .....	167
<b>Gambar V.133</b> Hydra Penyerangan <i>Port</i> SSH 22 (Tidak Menggunakan <i>usernamelist.txt</i> ) .....	167
<b>Gambar V.134</b> Hydra Penyerangan <i>Port</i> SSH 22 (Menggunakan <i>usernamelist.txt</i> ) .....	168
<b>Gambar V.135</b> Hydra Penyerangan <i>Port</i> FTP / <i>Port</i> 21 .....	170
<b>Gambar V.136</b> Hydra Penyerangan <i>Port</i> HTTP 80 (1).....	171
<b>Gambar V.137</b> Hydra Penyerangan <i>Port</i> HTTP 80 (2).....	171
<b>Gambar V.138</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (1) .....	172
<b>Gambar V.139</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (2) .....	172
<b>Gambar V.140</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (3) .....	173
<b>Gambar V.141</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (4) .....	173
<b>Gambar V.142</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (5) .....	174
<b>Gambar V.143</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (6) .....	174



<b>Gambar V.144</b> Tampilan <i>BurpSuite</i> Dalam Melakukan <i>Brute Force Attack</i> (7)	175
<b>Gambar V.145</b> Tampilan <i>BurpSuite</i> ClickJacking (1)	175
<b>Gambar V.146</b> Tampilan <i>BurpSuite</i> ClickJacking (2)	176
<b>Gambar V.147</b> Tampilan <i>BurpSuite</i> ClickJacking (3)	176
<b>Gambar V.148</b> Tampilan <i>BurpSuite</i> ClickJacking (4)	177
<b>Gambar V.149</b> Tampilan <i>BurpSuite</i> ClickJacking (5)	177
<b>Gambar V.150</b> Tampilan <i>BurpSuite</i> ClickJacking (6)	177
<b>Gambar V.151</b> Tampilan <i>BurpSuite</i> ClickJacking (7)	178
<b>Gambar V.152</b> Tampilan <i>BurpSuite</i> ClickJacking (8)	178
<b>Gambar V.153</b> Tampilan <i>BurpSuite</i> ClickJacking (9)	179
<b>Gambar V.154</b> Tampilan <i>BurpSuite</i> ClickJacking (9)	179
<b>Gambar V.155</b> <i>Command</i> Untuk <i>Setting ProxyChains4 (Dynamic)</i>	183
<b>Gambar V.156</b> Aktifkan <i>Dynamic Chain</i> dan Non Aktifkan <i>Strict Chain</i>	184
<b>Gambar V.157</b> Ilustrasi Cara Kerja <i>Proxy Chain</i>	184
<b>Gambar V.158</b> <i>Scanning WhoIs</i> Menggunakan <i>Dynamic ProxyChains</i>	185
<b>Gambar V.159</b> Instalasi <i>Tor Browser</i>	186
<b>Gambar V.160</b> Akses <i>Tor Browser</i> (CLI or GUI)	186
<b>Gambar V.161</b> Tampilan <i>Tor Browser</i> (IP Address Otomatis Disamarkan)	186
<b>Gambar V.162</b> Tampilan <i>Log File</i> Yang Ada Pada <i>File System</i>	187
<b>Gambar V.163</b> Tampilan <i>Log File</i> Yang Ada Pada Direktori <i>File System</i> (CLI/Terminal)	187
<b>Gambar V.164</b> Tampilan Isi Dari <i>Log File</i> <i>macchanger.log</i>	187
<b>Gambar V.165</b> <i>Command</i> Untuk Menghapus <i>File Log</i>	188
<b>Gambar V.166</b> Tampilan <i>Tools BleachBit</i>	188