FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-CV-290

Total Deleted Page(s) = 244
Page 1 ~ b3 - 1; b7E - 1,-2;
Page 2 ~ b3 - 1; b7E - 1,-2;
Page 3 ~ b3 - 1; b7E - 1,-2;
Page 4 ~ b3 - 1; b7E - 1,-2,-4;
Page 5 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 6 ~ b3 - 1; b7E - 1;
Page 7 ~ b3 - 1; b7E - 1,-2,-4;
Page 8 ~ b3 - 1; b7E - 1;
Page 9 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 10 ~ b3 - 1; b7E - 1;
Page 11 ~ b3 - 1; b7E - 1,-2,-4;
Page 12 ~ b3 - 1; b7E - 1;
Page 13 ~ b3 - 1; b7E - 1,-2,-4;
Page 14 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 15 ~ b3 - 1; b7E - 1,-2,-4;
Page 16 ~ b3 - 1; b7E - 1,-2,-4;
Page 17 ~ b3 - 1; b7E - 1,2,3;
Page 18 ~ b3 - 1; b7E - 1,-2;
Page 19 ~ b3 - 1; b7E - 1,-2;
Page 20 ~ b3 - 1; b7E - 1,-2,-4;
Page 21 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 22 ~ b3 - 1; b7D - 1,-2,-4;
Page 24 ~ b3 - 1; b7E - 1,-2,-4;
Page 27 ~ b3 - 1; b7E - 1,-2,-4;
Page 29 ~ b3 - 2; b7E - 1,-2,-3;
Page 30 ~ Duplicate;
Page 31 ~ Duplicate;
Page 32 ~ Duplicate;
Page 33 ~ Duplicate;
Page 34 ~ Duplicate;
Page 35 ~ Duplicate;
Page 36 ~ Duplicate;
Page 37 ~ Duplicate;
Page 38 ~ Duplicate;
Page 39 ~ Duplicate;
Page 40 ~ Duplicate;
Page 41 ~ Duplicate;
Page 42 ~ Duplicate;
Page 43 ~ Duplicate;
Page 44 ~ Duplicate;
Page 45 ~ Duplicate;
Page 46 ~ Duplicate;
Page 47 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-6;
Page 48 ~ b3 - 1; b7E - 1,-2;
Page 50 ~ b3 - 1; b7E - 1,-2;
Page 51 ~ b3 - 1; b7E - 1;
Page 52 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 53 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;

Page 54 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 55 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,;
Page 56 ~ b3 - 1; b7E - 1;
Page 57 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 59 ~ b3 - 1; b7E - 1,-2,-6;
Page 60 ~ b3 - 1; b7E - 1,-2;
Page 61 ~ b3 - 1; b7E - 1,-2;
Page 62 ~ b3 - 1; b7E - 1,-2;
Page 63 ~ b3 - 1; b7E - 1,-2;
Page 64 ~ b3 - 1; b7E - 1,-2;
Page 65 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-3;
Page 66 ~ b3 - 1; b7E - 1,-2;
Page 67 ~ b3 - 1; b7E - 1,-2;
Page 68 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 69 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 70 ~ b3 - 1; b7E - 1,-2;
Page 71 ~ b3 - 1; b7E - 1,-2;
Page 72 ~ b3 - 1; b7E - 1,-2;
Page 73 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 74 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 75 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 76 ~ b3 - 1; b7E - 1,-2;
Page 77 ~ b3 - 1; b7E - 1,-2;
Page 78 ~ b3 - 1; b7E - 1,-2;
Page 79 ~ b3 - 1; b7E - 1,-2;
Page 80 ~ Duplicate;
Page 81 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 82 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 83 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 84 ~ b3 - 1; b7E - 1,-2;
Page 85 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 86 ~ b3 - 1; b7E - 1,-2;
Page 87 ~ b3 - 1; b7E - 1,-2,-6;
Page 88 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 89 ~ Duplicate;
Page 91 ~ b3 - 1; b7E - 1,-2,-3,-4;
Page 92 ~ b3 - 1; b7E - 1,-2,-4;
Page 94 ~ Duplicate;
Page 95 ~ Duplicate;
Page 96 ~ Duplicate;
Page 97 ~ Duplicate;
Page 98 ~ Duplicate;
Page 99 ~ b3 - 1; b7E - 1,-2,-6;
Page 100 ~ b3 - 1; b7E - 1,-6;
Page 101 ~ b3 - 1; b7E - 1,-2;
Page 102 ~ b3 - 1; b7E - 1,-2;
Page 103 ~ b3 - 1; b7E - 1,-2,-4;
Page 104 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 105 ~ b3 - 1; b7E - 1,-2,-4;
Page 106 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 107 ~ b3 - 1; b7E - 1,-2;
Page 108 ~ b3 - 1; b7E - 1,-2;
Page 109 ~ b3 - 1; b7E - 1,-2;
Page 110 ~ Duplicate;

Page 111 ~ Duplicate;
Page 112 ~ Duplicate;
Page 113 ~ Duplicate;
Page 114 ~ Duplicate;
Page 115 ~ Duplicate;
Page 116 ~ Duplicate;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 119 ~ Duplicate;
Page 120 ~ Duplicate;
Page 121 ~ Duplicate;
Page 122 ~ Duplicate;
Page 123 ~ Duplicate;
Page 124 ~ Duplicate;
Page 125 ~ Duplicate;
Page 126 ~ Duplicate;
Page 127 ~ Duplicate;
Page 128 ~ Duplicate;
Page 129 ~ b3 - 1; b5 - 3; b7E - 1,-2;
Page 130 ~ b3 - 1; b5 - 3; b7E - 1,-2;
Page 131 ~ b3 - 1; b5 - 3; b7E - 1,-2;
Page 132 ~ b3 - 1; b5 - 3; b7E - 1,-2;
Page 134 ~ b3 - 1; b7E - 1;
Page 135 ~ b3 - 1; b7E - 1;
Page 136 ~ b3 - 1; b7E - 1,-2;
Page 137 ~ b3 - 1; b7E - 1,-2;
Page 138 ~ b3 - 1; b7E - 1,-2,-3;
Page 139 ~ b3 - 1; b7E - 1,-2;
Page 140 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 141 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 142 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 143 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 144 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 145 ~ b3 - 1; b7E - 1,-2;
Page 146 ~ b3 - 1; b7E - 1,-2;
Page 147 ~ b3 - 1; b7E - 1,-2;
Page 148 ~ b3 - 1; b7E - 1,-2;
Page 149 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 150 ~ b3 - 1; b7E - 1,-2,-4;
Page 151 ~ b3 - 1; b7E - 1,-2,-4;
Page 152 ~ b3 - 1; b7E - 1,-2,-4;
Page 153 ~ b3 - 1; b7E - 1,-2,-4;
Page 154 ~ b3 - 1; b7E - 1,-2,-4;
Page 155 ~ b3 - 1; b7E - 1,-2,-4;
Page 156 ~ b3 - 1; b7E - 1,-2,-4;
Page 157 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 158 ~ b3 - 1; b7E - 1,-2;
Page 159 ~ b3 - 1; b7E - 1,-2,-3;
Page 161 ~ b3 - 1; b7E - 1;
Page 163 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 164 ~ b3 - 1; b7E - 1,-2;
Page 165 ~ b3 - 1; b7E - 1,-2;
Page 166 ~ b3 - 1; b7E - 1,-2,-4;
Page 167 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;

```
Page 168 ~ b3 - 1; b7E - 1,-2;
Page 169 ~ b3 - 1; b7E - 1,-2;
Page 170 ~ b3 - 1; b7E - 1,-2;
Page 171 ~ b3 - 1; b7E - 1,-2;
Page 172 ~ b3 - 1; b7E - 1,-2;
Page 173 ~ b3 - 1; b7E - 1,-2;
Page 174 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 175 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 176 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 177 ~ Duplicate;
Page 178 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 179 ~ Duplicate;
Page 180 ~ b3 - 1; b7E - 1,-2;
Page 181 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 182 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 183 ~ b3 - 1; b7E - 1,-2;
Page 184 ~ b3 - 1; b7E - 1,-2;
Page 185 ~ b3 - 1; b7E - 1,-2;
Page 186 ~ b3 - 1; b7E - 1,-2;
Page 187 ~ b3 - 1; b7E - 1,-2;
Page 188 ~ b3 - 1; b7E - 1,-2;
Page 189 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 190 ~ b3 - 1; b7E - 1,-2,-6;
Page 191 ~ b3 - 1; b7E - 1,-2,-6;
Page 192 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 193 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 194 ~ b3 - 1; b7E - 1,-2,-6;
Page 195 ~ b3 - 1; b7E - 1,-2,-6;
Page 196 ~ Duplicate;
Page 197 ~ Duplicate;
Page 198 ~ Duplicate;
Page 199 ~ Duplicate;
Page 200 ~ Duplicate;
Page 201 ~ Duplicate;
Page 202 ~ Duplicate;
Page 203 ~ Duplicate;
Page 204 ~ Duplicate;
Page 205 ~ Duplicate;
Page 206 ~ Duplicate;
Page 207 ~ Duplicate;
Page 208 ~ Duplicate;
Page 209 ~ Duplicate;
Page 210 ~ Duplicate;
Page 211 ~ Duplicate;
Page 212 ~ Duplicate;
Page 213 ~ Duplicate;
Page 214 ~ Duplicate;
Page 215 ~ Duplicate;
Page 216 ~ Duplicate;
Page 217 ~ Duplicate;
Page 218 ~ Duplicate;
Page 219 ~ Duplicate;
Page 220 ~ Duplicate;
Page 221 ~ Duplicate;
Page 222 ~ Duplicate;
Page 223 ~ Duplicate;
Page 224 ~ b3 - 1; b7E - 1,-2;
Page 225 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 226 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 227 ~ b3 - 1; b7E - 1,-2,-3,-6;
Page 228 ~ Duplicate;
Page 229 ~ Duplicate;
Page 230 ~ Duplicate;
Page 231 ~ Duplicate;
Page 232 ~ Duplicate;
Page 233 ~ Duplicate;
Page 234 ~ Duplicate;
Page 235 ~ Duplicate;
Page 236 ~ Duplicate;
Page 237 ~ Duplicate;
Page 238 ~ Duplicate;
Page 239 ~ Duplicate;
Page 240 ~ Duplicate;
Page 241 ~ Duplicate;
Page 242 ~ Duplicate;
Page 243 ~ Duplicate;
Page 244 ~ Duplicate;
Page 245 ~ Duplicate;
Page 246 ~ Duplicate;
Page 247 ~ Duplicate;
Page 248 ~ Duplicate;
Page 249 ~ Duplicate;
Page 250 ~ Duplicate;
Page 251 ~ Duplicate;
Page 252 ~ Duplicate;
Page 253 ~ Duplicate;
Page 254 ~ Duplicate;
Page 255 ~ Duplicate;

                                            XXXXXXXXXXXXXXXXXXXXXXXX
                                            X   Deleted Page(s)    X
                                            X   No Duplication Fee X
                                            X   For this Page      X
                                            XXXXXXXXXXXXXXXXXXXXXXXX
```

Usernames

What is a username? A username is the name given or created for a user on a computer or for an application that can be alternatively referred to as an account name or login ID. While emails and phone numbers are typically unique to a person, a *username is typically only unique to a specific application.*

[redacted]

b3 -1
b7E -1,-2

Appendix

Appendix

[redacted]

b3 -1
b7E -1,-2

OSAG Weekly Meeting

September 25, 2017

Questions/Comments

[redacted]

b3 -1
b7E -1

[redacted]

b3 -1
b7E -1,-2

[redacted]

SOS [redacted]

CS-FO [redacted]

b6 -1
b7C -1

Cincinnati Division

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
Civil Action# 19-CV-290

Total Deleted Page(s) = 221
Page 1 ~ b1 - 1; b3 - 1; b6 - 1; b7C - 1; b7E - 1,-6;
Page 2 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-6,-8;
Page 3 ~ b1 - 1; b3 - 1; b7E - 1,-2,-6,-8;
Page 4 ~ b1 - 1; b3 - 1; b7E - 1,-2,-8;
Page 5 ~ b3 - 1; b7E - 1,-8;
Page 6 ~ b3 - 1; b7E - 1,-2,-3,-8;
Page 7 ~ b3 - 1; b7E - 1,-2,-6,-8,-9;
Page 8 ~ b3 - 1; b7E - 1,-2,-3,-8;
Page 9 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-3,-8;
Page 10 ~ b3 - 1; b7E - 1,-3,-8;
Page 11 ~ b3 - 1; b7E - 1,-3,-8;
Page 12 ~ b3 - 1; b7E - 1,-2,-8;
Page 13 ~ b3 - 1; b7E - 1,-2,-3,-8;
Page 14 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-8;
Page 15 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-8;
Page 16 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-8;
Page 17 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-8;
Page 18 ~ b3 - 1; b7E - 1,-2,-8;
Page 19 ~ b3 - 1; b7E - 1,-2,-8;
Page 20 ~ b3 - 1; b7E - 1,-2,-8;
Page 21 ~ b1 - 1; b3 - 1; b7E - 1,-2,-3,-8;
Page 22 ~ b3 - 1; b7E - 1,-2,-3,-8;
Page 23 ~ b3 - 1; b7E - 1,-2,-8;
Page 24 ~ b3 - 1; b7E - 1,-2,-8;
Page 25 ~ b3 - 1; b7E - 1,-2,-8;
Page 26 ~ b3 - 1; b7E - 1,-2,-3,-8;
Page 27 ~ b3 - 1; b7E - 1,-2,-8;
Page 28 ~ b3 - 1; b7E - 1,-2,-8;
Page 29 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-6,-8;
Page 30 ~ b3 - 1; b7E - 1,-8;
Page 31 ~ b3 - 1; b7E - 1,-8;
Page 32 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-3;
Page 33 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-3;
Page 68 ~ b3 - 1; b6 - 1,-3; b7C - 1,-3; b7E - 1,-2;
Page 69 ~ b3 - 1; b6 - 1,-3; b7C - 1,-3; b7E - 1,-2;
Page 70 ~ b3 - 1; b7E - 1,-2;
Page 71 ~ b3 - 1; b7E - 1,-2;
Page 72 ~ b3 - 1; b6 - 1,-3; b7C - 1,-3; b7E - 1,-2;
Page 73 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2;
Page 74 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 75 ~ b3 - 1; b6 - 1,-3; b7C - 1,-3; b7E - 1,-2;
Page 76 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 77 ~ b3 - 1; b7E - 1,-2,-8;
Page 78 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 79 ~ b3 - 1; b7E - 1,-2,-8;
Page 80 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 81 ~ b3 - 1; b7E - 1,-2,-8;
Page 82 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;

```
Page 83 ~ b3 - 1; b7E - 1,-2,-8;
Page 84 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 85 ~ b3 - 1; b7E - 1,-2,-8;
Page 86 ~ b3 - 1; b7E - 1,-2,-8;
Page 87 ~ b3 - 1; b7E - 1,-2,-8;
Page 88 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 89 ~ b3 - 1; b7E - 1,-2,-3;
Page 90 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2,-8;
Page 91 ~ b3 - 1; b7E - 1,-2,-8;
Page 92 ~ b3 - 1; b7E - 1,-2,-8;
Page 93 ~ b3 - 1; b7E - 1,-2,-8;
Page 94 ~ b3 - 1; b7E - 1,-2,-8;
Page 95 ~ b3 - 1; b7E - 1,-2,-8;
Page 96 ~ b3 - 1; b7E - 1,-2,-8;
Page 97 ~ b3 - 1; b7E - 1,-2,-8;
Page 98 ~ b3 - 1; b7E - 1,-2,-8;
Page 99 ~ b3 - 1; b7E - 1,-2,-8;
Page 100 ~ b3 - 1; b7E - 1,-2,-8;
Page 101 ~ b3 - 1; b7E - 1,-2,-8;
Page 102 ~ b3 - 1; b7E - 1,-2,-8;
Page 103 ~ b3 - 1; b7E - 1,-2,-8;
Page 104 ~ b3 - 1; b7E - 1,-2,-8;
Page 105 ~ b3 - 1; b7E - 1,-2,-8;
Page 106 ~ b3 - 1; b7E - 1,-2,-8;
Page 107 ~ b3 - 1; b7E - 1,-2,-8;
Page 108 ~ b3 - 1; b7E - 1,-2,-8;
Page 109 ~ b3 - 1; b7E - 1,-2,-8;
Page 110 ~ b3 - 1; b7E - 1,-2,-8;
Page 111 ~ b3 - 1; b7E - 1,-2,-8;
Page 112 ~ b3 - 1; b7E - 1,-2,-8;
Page 113 ~ b3 - 1; b7E - 1,-2,-8;
Page 114 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 115 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 116 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 117 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 118 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 119 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 120 ~ b3 - 1; b7E - 1,-2,-8;
Page 121 ~ b3 - 1; b7E - 1,-2,-8;
Page 122 ~ b3 - 1; b7E - 1,-2,-8;
Page 123 ~ b3 - 1; b7E - 1,-2,-8;
Page 124 ~ b3 - 1; b7E - 1,-2,-8;
Page 125 ~ b3 - 1; b7E - 1,-2,-8;
Page 126 ~ b3 - 1; b7E - 1,-2,-8;
Page 127 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 128 ~ b3 - 1; b7E - 1,-2,-8;
Page 129 ~ b3 - 1; b7E - 1,-2,-8;
Page 130 ~ b3 - 1; b7E - 1,-2,-8;
Page 131 ~ b3 - 1; b7E - 1,-2,-8;
Page 132 ~ b3 - 1; b7E - 1,-2,-8;
Page 133 ~ b3 - 1; b7E - 1,-2,-8;
Page 134 ~ b3 - 1; b7E - 1,-2,-8;
Page 135 ~ b3 - 1; b7E - 1,-2,-8;
Page 136 ~ b3 - 1; b7E - 1,-2,-8;
Page 137 ~ b3 - 1; b7E - 1,-2,-8;
Page 138 ~ b3 - 1; b7E - 1,-2,-8;
Page 139 ~ b3 - 1; b7E - 1,-2,-8;
Page 140 ~ b3 - 1; b7E - 1,-2,-8;
Page 141 ~ b3 - 1; b7E - 1,-2,-8;
Page 142 ~ b3 - 1; b7E - 1,-2,-8;
Page 143 ~ b3 - 1; b7E - 1,-2,-8;
Page 144 ~ b3 - 1; b7E - 1,-2,-8;
Page 145 ~ b3 - 1; b7E - 1,-2,-8;
Page 146 ~ b3 - 1; b7E - 1,-2,-8;
Page 147 ~ b3 - 1; b7E - 1,-2,-8;
Page 148 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 149 ~ b3 - 1; b7E - 1,-2,-8;
Page 150 ~ b3 - 1; b7E - 1,-2,-8;
Page 151 ~ b3 - 1; b7E - 1,-2,-8;
Page 152 ~ b3 - 1; b7E - 1,-2,-8;
Page 153 ~ b3 - 1; b7E - 1,-2,-8;
Page 154 ~ b3 - 1; b7E - 1,-2,-8;
Page 155 ~ b3 - 1; b7E - 1,-2,-8;
Page 156 ~ b3 - 1; b7E - 1,-2,-8;
Page 157 ~ b3 - 1; b7E - 1,-2,-8;
Page 158 ~ b3 - 1; b7E - 1,-2,-8;
Page 159 ~ b3 - 1; b7E - 1,-2,-8;
Page 160 ~ b3 - 1; b7E - 1,-2,-8;
Page 161 ~ b3 - 1; b7E - 1,-2,-8;
Page 162 ~ b3 - 1; b7E - 1,-2,-8;
Page 163 ~ b3 - 1; b7E - 1,-2,-8;
Page 164 ~ b3 - 1; b7E - 1,-2,-8;
Page 165 ~ b3 - 1; b7E - 1,-2,-8;
Page 166 ~ b3 - 1; b7E - 1,-2,-8;
Page 167 ~ b3 - 1; b7E - 1,-2,-8;
Page 168 ~ b3 - 1; b7E - 1,-2,-8;
Page 169 ~ b3 - 1; b7E - 1,-2,-8;
Page 170 ~ b3 - 1; b7E - 1,-2,-8;
Page 171 ~ b3 - 1; b7E - 1,-2,-8;
Page 172 ~ b3 - 1; b7E - 1,-2,-8;
Page 173 ~ b3 - 1; b7E - 1,-2,-8;
Page 174 ~ b3 - 1; b7E - 1,-2,-8;
Page 175 ~ b3 - 1; b7E - 1,-2,-8;
Page 176 ~ b3 - 1; b7E - 1,-2,-8;
Page 177 ~ b3 - 1; b7E - 1,-2,-8;
Page 178 ~ b3 - 1; b7E - 1,-2,-8;
Page 179 ~ b3 - 1; b7E - 1,-2,-8;
Page 180 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-3;
Page 181 ~ b3 - 1; b7E - 1,-2,-8;
Page 182 ~ b3 - 1; b7E - 1,-2,-8;
Page 183 ~ b3 - 1; b7E - 1,-2,-8;
Page 184 ~ b3 - 1; b7E - 1,-2,-8;
Page 185 ~ b3 - 1; b7E - 1,-2,-8;
Page 186 ~ b3 - 1; b7E - 1,-2,-8;
Page 187 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 188 ~ b3 - 1; b7E - 1,-2,-8;
Page 189 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 190 ~ b3 - 1; b7E - 1,-2,-8;
Page 191 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 192 ~ b3 - 1; b7E - 1,-2,-8;
Page 193 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 194 ~ b3 - 1; b7E - 1,-2,-8;
Page 195 ~ b3 - 1; b7E - 1,-2,-8;
Page 196 ~ b3 - 1; b7E - 1,-2,-8;
Page 197 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 198 ~ b3 - 1; b7E - 1,-2,-8;
Page 199 ~ b3 - 1; b7E - 1,-2,-8;
Page 200 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 201 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 202 ~ b3 - 1; b7E - 1,-2,-8;
Page 203 ~ b3 - 1; b7E - 1,-2,-8;
Page 204 ~ b3 - 1; b7E - 1,-2,-8;
Page 205 ~ b3 - 1; b7E - 1,-2,-8;
Page 206 ~ b3 - 1; b7E - 1,-2,-8;
Page 207 ~ b3 - 1; b7E - 1,-2,-8;
Page 208 ~ b3 - 1; b7E - 1,-2,-8;
Page 209 ~ b3 - 1; b7E - 1,-2,-8;
Page 210 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 211 ~ b3 - 1; b7E - 1,-2,-8;
Page 212 ~ b3 - 1; b7E - 1,-2,-8;
Page 213 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1;
Page 214 ~ b3 - 1; b7E - 1,-2,-8;
Page 215 ~ b3 - 1; b7E - 1,-2,-8;
Page 216 ~ b3 - 1; b7E - 1,-2,-8;
Page 217 ~ b3 - 1; b7E - 1,-2,-8;
Page 218 ~ b3 - 1; b7E - 1,-2,-8;
Page 219 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 220 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 221 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 222 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 223 ~ b3 - 1; b7E - 1,-2,-8;
Page 224 ~ b3 - 1; b7E - 1,-2,-8;
Page 225 ~ b3 - 1; b7E - 1,-2,-8;
Page 226 ~ b3 - 1; b7E - 1,-2,-8;
Page 227 ~ b3 - 1; b6 - 2; b7C - 2; b7E - 1,-2,-8;
Page 228 ~ b3 - 1; b7E - 1,-2,-8;
Page 229 ~ b3 - 1; b7E - 1,-2,-8;
Page 230 ~ b3 - 1; b7E - 1,-2,-8;
Page 231 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 232 ~ b3 - 1; b7E - 1,-2,-8;
Page 233 ~ b3 - 1; b7E - 1,-2,-8;
Page 234 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-8;
Page 235 ~ b3 - 1; b7E - 1,-2,-8;
Page 236 ~ b3 - 1; b7E - 1,-2,-8;
Page 237 ~ b3 - 1; b7E - 1,-2,-8;
Page 238 ~ b3 - 1; b7E - 1,-2,-8;
Page 239 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2;
Page 240 ~ b3 - 1; b7E - 1,-2,-4;
Page 241 ~ b3 - 1; b7E - 1,-2,-4;
Page 242 ~ b3 - 1; b7E - 1,-2,-4;
Page 243 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;
Page 244 ~ b3 - 1; b7E - 1,-2,-4;
```

Page 245 ~ b3 - 1; b7E - 1,-2,-4;
Page 246 ~ b3 - 1; b6 - 1; b7C - 1; b7E - 1,-2;
Page 247 ~ b3 - 1; b7E - 1,-2;
Page 248 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 249 ~ b3 - 1; b7E - 1,-2,-4;
Page 250 ~ b3 - 1; b7E - 1,-2,-4;
Page 251 ~ b3 - 1; b7E - 1,-2;
Page 252 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2;
Page 253 ~ b3 - 1; b7E - 1,-2;
Page 254 ~ b3 - 1; b7E - 1,-2;
Page 255 ~ b3 - 1; b6 - 3; b7C - 3; b7E - 1,-2,-4;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-15-2019 BY V6[redacted]G

b6 -1
b7C -1

twitter

blah, blah, blah, blah
at 140 character speed.

facebook

myspace.com
a place for friends

PerfSpot

friendster

flickr

Google+

Exploiting Social Web Sites: A Guide for the Open Source Intelligence (OSINT) Analyst

bebo

NETLOG

BlackPlanet.com

MiGente.com

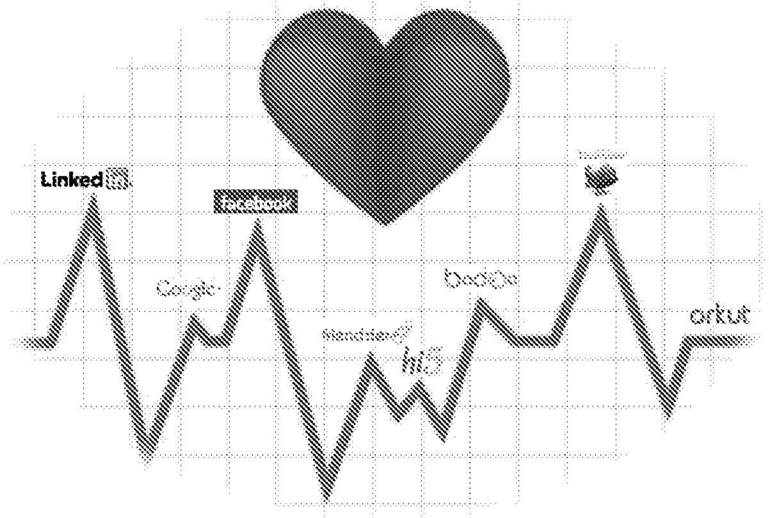
hi5

LinkedIn

badoo

orkut

The Heart of Analysis: Bringing it all Together to Monitor the Beat



Authors Note:

This is a living document and is relentlessly updated as new sources of information are discovered. Nevertheless, for the benefit of all recipients I would be grateful for any input you may have to keep this handbook up to date and available to the user. Please forward new sources of information to ben.benavides@gmail.com Heaps of social thanks in advance.

OSINT Analysts do it Overtly

Social networking sites can be especially useful to the open source analyst for intelligence gathering and the results will in many instances come very close to and/or equal the analysis derived from classified sources. The intelligence garnered from these sites very often consist of dates and times, and very frequently are accompanied with photos that may also expand on the individual targeted and the subject at hand. The one problem you may run into though is that of individuals with the same name causing you to work extra hard to track down the target, however, it can be done if you have the patience. Careful analysis of these open source worlds will yield intelligence you never knew existed if you are patient, relentless, and investigative. Taking advantage of several sites and gathering bits and pieces of information from each will narrow the focus. It is like a jigsaw puzzle, each location will reveal only a small piece of the larger picture. The criminal element will not post everything at one location but rather spread it out thus the reason for exploiting multiple sites.

But this should be exhilarating for the open source analyst because no one can do it like we can. We are HUMINT (*intelligence derived from information collected and provided by human sources)*, SIGINT (*Intelligence derived from interception of signals between people and/or machines*), IMINT (*Intelligence derived from satellite and/or aerial photography)*, GEOINT (*a combination of disciplines*), and MASINT (e*lectronic version of all-source intelligence*) all rolled into one and it is called OSINT (*intelligence produced from publicly available information*).

We talk, listen and rub shoulders with humans; we listen to the radio and watch television; we examine and study photographs; we do open source analysis of the natural features and characteristics of the topography (includes internet); and when combined we touch on MASINT. OSINT is more than information, it represents a careful sifting, selecting, analyzing and presenting of open source material on a timely basis, and the keyword is timely. OSINT is a valuable contributor to "all source" intelligence, supports the classical "INTs", helps drive the collection effort, and tells the "INTs" where to look, but most important where not to look and as a consequence saving precious resources and time.

Overtly Covert or Covertly Overt

The one thing to remember is that of covering your own tracks when conducting research. What if the person you're following has his/her own website and control their own server? Their IT person would very easily identify your IP address and be able to follow you back to a location even through an in between referrer link. Using software like Tor (The Onion Router) a free open-source Web surfing program that runs in the background and hides your surfing habits and location will help in covering your tracks; it accomplishes this by routing the user's data through a series of computers each one of which encrypts the data passing through it. According to a project overview the Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations. The drawback is that it slows down page views because of the numerous hops to hide your IP address. Another way to maintain anonymity is by way of a virtual private network (VPN). To prevent traces you can use a VPN to hide your IP address. It's the same sort of connection used by many corporations to prevent security breaches using encrypted tunneling, but you can use it to route your connections through a remote server, often in a different country, and thus thwart trackers. Download Tor manual at http://www.makeuseof.com/pages/really-private-browsing-an-unofficial-users-guide-to-tor

Free and popular commercial VPN services include Tunnelbear (http://www.tunnelbear.com), Strong (http://strongvpn.com/), Private WiFi and proXPN. I have to add one more pointer and that is that even when utilizing privacy software, make certain to clear your browser's history at the end of each research session.

Other Privacy Tools

Our easy-to-use software lets you change your IP address anytime by routing your Internet traffic through private and secure servers worldwide. A small dropdown box will appear on your web browser toolbar (e.g. Internet Explorer / Firefox) with a list of several countries. Select one and your IP address will change so that you appear to be located in that country.

Hotspot Shield VPN is the ultimate Internet security solution that secures your browsing session, detects and blocks malware, protects your privacy and allows you to **access blocked sites**. Hotspot Shield is available both as a **free VPN** and a paid Hotspot Shield Elite subscription.

Hide your IP: Nobody will know where you are from; Encrypt internet data: Protect your Internet data with strong 256-bit encryption; Remove limits: Use any site you need without any limitations.

Your online activities can reveal intimate details about you and the websites you visit. Anonymizer Universal ensures your identity remains anonymous and your personal information is protected and secure every time you're online.

Proxify is an anonymous proxy service which allows anyone to surf the Web privately and securely. Through Proxify, you can use websites but they cannot uniquely identify or track you. Proxify hides your IP address and our encrypted connection prevents monitoring of your network traffic. Once using Proxify, you can surf normally and forget that it is there, protecting you.

Use our free proxy to surf anonymously online, hide your IP address, secure your internet connection, hide your internet history, and protect your online identity.

Want to still use your favorite search engine without worrying about your IT department, or government, spying on you? Disconnect search is designed to do just that. Developed by an ex-NSA engineer and three former Googlers, Disconnect allows users to query their favorite search engine in complete privacy. Disconnect currently supports the three top US search engines: Google, Yahoo, and Bing.

Many mice surf the web under the illusion that their actions are private and anonymous. Unfortunately, this is not the way it is. Every time you visit a site for a piece of cheese, you leave a calling card that reveals where you are coming from, what kind of computer you use, and other details. And many cats keep logs of all your visits, so that they can catch you! This service allows you to surf the web without revealing any personal information. It is fast, it is easy, and it is free!

Many web sites are harmful and attempt to log your IP address for improper use. Some spyware applications and web sites with harmful code sometimes need your personal IP address in order to do their dirty work. An anonymous proxy hides this information from the web sites you visit. Just type an address in the form above this paragraph and click browse and you will see the page load. Any links you click from there will also be secure. There will also be a new form located at the top of the page. Use that form to continue to surf the web anonymously.

Online Anonymizer is a free online tool that helps any Internet user to surf the Internet being protected. However, if you tend to forget to enter the URL there is always Offline Anonymizer. Just download, install anonymizer and push the button "Make me invisible" and all your information and real IP address will be unavailable for any webmaster or hacker.

CyberGhost VPN lets you surf anonymously by hiding your IP address and replacing it with that of the server you choose to connect to, making it impossible for hackers, third parties or other organizations to track you or meddle in your business. Every time you connect through CyberGhost VPN a protective tunnel is formed around your information and all your data becomes encrypted. You don’t have to worry anymore about passwords, financial transactions or private conversations.

How does OkayFreedom VPN work? Upset when you can't view a video online? With our VPN-service OkayFreedom this problem is now history. But OkayFreedom VPN is also the right choice when you just want to prevent someone from following your traces on the internet. OkayFreedom VPN recognizes whether content, videos and entire websites are restricted in your country and automatically directs you over a server which enables you to view the content.

Go to http://www.makeuseof.com/pages/best-vpn-service-providers for further information on VPNs.

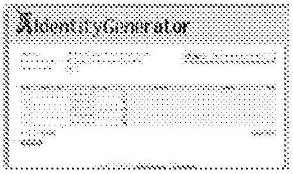
Criminals and Social Media

Criminals also are very much aware of the electronic footprints they can leave behind and will attempt to hide their own activities. Don't assume they operate out in the open for you to nab 'em. I call this the battle of 0s and 1s. (I use the word "criminal" as an umbrella term for anything punishable as a crime under the law, including terrorists, gangs, drug cartels, human traffickers, etc.)

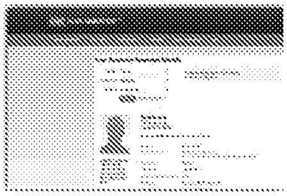
There is always something happening and up and running 24/7/365. Open up Twitter or any other social media application and you will be seeing the latest events. People are so tuned in to local and global events that a newspaper, I believe, is read solely for the purpose of feeling something in one's hands while having breakfast, and besides, a newspaper can only print so much information that could already be obsolete by the time you finish your morning cup of coffee. Events and updates travel at the speed of (light) the enter key; a crisis at the opposite side of the globe can reach you in 2 seconds once the enter key is depressed.

If you are a person that posts information on a regular basis, or run a blog, you can have a great following if you take pride in what you post. By doing this there will always be someone feeding you complementary information to add to your posts and make you look even better. On the flip side of the coin, follow only those that you trust and are sure are posting accurate information. However, always verify, verify, verify. If your source reporting an event is not the original source, can the original source be identified and authenticated? Even if the original source is found, does the time and date of the original report make sense? Our world is so tightly connected that every world event, big or small, is felt in real time. Internet, smart phones and social media have taken down the walls that used to separate individuals.

Social media has a tendency to be self-correcting. There will always be someone with inside knowledge and rectify posts that are not valid. Those that post without verifying their sources and simply wanting to scoop their competition to be first will not last long. So what if you are not the first to post something. Later and accurate is better than first, wrong, and humiliated. We see that constantly on the news. Networks are always trying to outdo each other.



If you don't have an account (yeah, right) you should go ahead and establish one. It can be for facebook, twitter or whatever you want. Make it a fake one if you so desire. I would venture to say that many who do investigative research have fake accounts. These are two sites that can assist you in establishing a fake identity: http://www.identitygenerator.com/ and http://www.fakenamegenerator.com/ . However, to avoid leaving electronic footprints I recommend using the tor software then printing a copy of what you filled out via the print screen button on your keyboard. Don't forget to clear the browser's history. Now you can modify the printed hardcopy to your liking without doing it online. Be sure to retain a copy for your records; you may have to remember who you are at a later date because of some account verification. There is definitely no criminal intent by doing this unless you ARE a criminal.



Let's put it all in perspective and admit it is no secret these sites are being used by gang members, drug cartels, terrorists, in other words criminals. The Zetas, a violent group and former muscle for the Gulf Cartel, has made its presence known on Youtube and are there to recruit and send out instructions. They have produced their own videos and glamorized their business, if beheadings can be characterized as a business. They have posted videos of their violence to send a message to other cartels that they mean business and are not about to be driven from their turf. They have been successful in recruiting teenagers who have gone on to become assassins for the cartel. Laredo, Texas, is a good case in point. A teenager and a hired gun (hitman) for the cartel by the name of Rosalio "Bart" Reta confessed to 30 hits in Mexico and several in the US between the age of ***13 and 17***. Fancy cars, women and money are a strong lure for these school dropouts with nothing better to do, and at the same time the drug lords benefit. They benefit in the sense they are totally divorced from the crime and there is always someone in line ready to fill the vacancy.

Terrorists are no strangers to the web sites. They have created their own cyber turf or else join those that are already in operation, and with key words are able to start their exchange.

According to Intelligence Bureau officials, terrorists use the Internet not only to learn how to build bombs but also to plan and coordinate specific attacks. Al Qaeda operatives for instance relied heavily on the Internet in planning and coordinating the Sep 11 attacks on the twin towers in New York. To preserve their anonymity, terrorists use the Internet in public places. Some of the 9/11 hijackers communicated using free web-based e-mail accounts. Gabriel Weimann, a senior fellow at the US Institute of Peace who has written widely on modern terrorism, says Hamas activists use chat rooms to plan operations against Israel. Its operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon and Israel. Instructions in the form of maps, photographs, directions and technical details of how to use explosives are often disguised by means of steganography.

Steganography is the practice of concealing data within a carrier—may be used to obscure malicious or criminal information and activity from law enforcement. While steganography dates to the fifth century BC, it has long been regarded as, and remains, one of the most advanced forms of clandestine communication. In modern usage, the Internet allows accessibility to, and broad dissemination of, steganography tools, and its application continues to evolve with technology. Understanding steganography in its current state is essential to its identification and detection, which involves hiding messages inside graphic files. Sometimes, however, instructions concealed in only the simplest of codes are delivered.

Mohammed Atta's final message to the other 18 terrorists who carried out 9/11 reportedly read: The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." (The reference to the faculties was apparently the code for the buildings targeted in the attacks.) All the terrorists had already been versed to the keywords that would start the operation.

Then there are the gangs, like MS-13, Hell's Angels, Florencia 13, Mexican Mafia, and on and on. The gang members, either individually or as a group, have their own accounts and brag about their exploits. They are proud of their affiliation and use these services to advertise their association. Gang investigators (law enforcement), I am certain, are conducting surveillance on these sites in order to gain an understanding of the gang networks operating within their jurisdiction, and how they connect to other jurisdictions. With the revelations by Edward Snowden of NSA snooping I am sure the nets are teeming with law enforcement agencies and the military to monitor how the criminals are modifying their presence on the internet. Intelligence Oversight Be Gone!

As mentioned above the criminals operate with keyword strategy, and don't think they stick to one particular social web site; they use several to mask their activities and use diverse monikers for each site. Think about them in the same sense the military uses frequency hopping radios to avoid interception on one channel. Keywords alert the users to examine several sites to retrieve numerous pieces of information that are then put together to receive the intended message. This is akin to a kite smuggled out of prison with a secret message.
http://blogs.kqed.org/newsfix/2013/09/17/111570/secret-letter-from-mexican-mafia-gang-leader-to-la-street-gangs

Keywords can be anything that the members are familiar with and known only inside the tightly knit group. Leaders of The Mexican Mafia, even though imprisoned, retain extreme control not only of their own members outside prison walls but that of other gangs as well. They do this through keywords that are disseminated through visitors, either relatives, friends or attorneys, that come to visit them and the guests are not even aware they are carrying a message.

Most everyone knows how the NSA data mines by use of a watch list or dictionary of key words, individual names, IP addresses, or telephone numbers. I often wonder how many more were added from the interrogations at the Guantanamo facility, and it is anyone's guess as to how many keywords are in the database. Law Enforcement Agencies (LEA) can do basically the same thing at the tactical level. NSA and the other security agencies supposedly share their watch list with the LEAs but I take this lightly. LEAs may not know it but they already have access to keywords in their files. How many interrogations have taken place at the police station and how many conversations have you heard between groups and individuals. Keywords were used and they are there just waiting to be exploited.

Think of the last supposedly innocent conversations that took place between gang members. Did they make sense? “My mother has decided to go ahead and *cook* the next batch of *chili rellenos* for delivery to the first *communion* of my cousin”. Her communion is the second Sunday of next month. Is there really a communion that is going to take place with all the fanfare normally attached to one? There most definitely is and the coded message is being piggy-backed on a real and live upcoming event. Aren’t they clever?

Rob D'Ovidio, a Drexel University criminologist, says gang members use code to boast about their deeds. For example, he says, they use "biscuit" or "clickety" for a gun, "food," "sea shells" or "gas" for bullets and "rock to sleep early" for murder. Source: http://www.usatoday.com/story/news/nation/2013/09/29/twitter-crime-dark-side/2875745/

There also are strong indications al-Shabaab gunmen who attacked the Westgate Mall in Nairobi, Kenya may have used certain cryptic keywords to marshal the attackers into place and signal the beginning of the attack. “Wedding begins at noon, all groomsmen in place.”

Everyone is familiar with the Navajo Code Talkers and how the Japanese were never able to break their code. Following are a few examples of words the Navajo communicated and their meanings. These should give you an idea of what I’m referring to.

Names Of Airplanes	
Planes	Air Force
Dive Bomber	Chicken Hawk
Torpedo Plane	Swallow
Observer	Owl
Fighter Plane	Humming Bird
Bomber Plane	Buzzard
Patrol Plane	Crow
Transport	Eagle

Names Of Ships	
Ships	Sea Force
Battleship	Whale
Aircraft	Bird Carrier
Submarine	Iron Fish
Mine Sweeper	Beaver
Destroyer	Shark
Transport	Man Carrier
Cruiser	Small Whale

MiningThe Internet For Intelligence

Internet 2012 in numbers. Source: http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

There is so much happening on the Internet during a year that it’s impossible to capture it all in a blog post, but we’re going to give it a shot anyway. How many emails were sent during 2012? How many domains are there? What’s the most popular web browser? How many Internet users are there? These are some of the questions we’ll answer for you.

To bring you these answers, we’ve gone to the ends of the web – wherever that is – and back again, and compiled a list of truly fascinating facts about the year that was. Some of the numbers are snapshots taken during the year, others cover the entire period. Either way, they all contribute to giving us a better understanding of Internet in 2012. Enjoy!

Email

- **2.2 billion** – Number of email users worldwide.
- **144 billion** – Total email traffic per day worldwide.
- **61%** – Share of emails that were considered non-essential.
- **4.3 billion** – Number of email clients worldwide in 2012.
- **35.6%** – Usage share of the most popular email client, which was Mail for iOS.
- **425 million** – Number of active Gmail users globally, making it the leading email provider worldwide.
- **68.8%** – Percentage of all email traffic that was spam.
- **50.76%** – Percentage of all spam that was about pharmaceuticals, the top category of all spam.
- **0.22%** – Share of worldwide emails that comprised some form of phishing attack.

Web pages, Websites, and Web hosting

- 634 million – **Number of websites (December).**
- 51 million – **Number of websites added during the year.**
- 43% – **Share of the top 1 million websites that are hosted in the U.S.**
- 48% – **Share of the the top 100 blogs that run WordPress.**
- 75% – **Share of the top 10,000 websites that are served by open source software.**
- 87.8 million – **Number of Tumblr blogs.**
- 17.8 billion – **Number of page views for Tumblr.**
- 59.4 million – **Number of WordPress sites around the world.**
- 3.5 billion – **Number of webpages run by WordPress viewed each month.**
- 37 billion – **Number of pageviews for Reddit.com in 2012.**
- 35% – **The average web page became this much larger during 2012.**
- 4% – **The average web page became this much slower to load during 2012.**
- **191 million –** Number of visitors to Google Sites, the number 1 web property in the U.S. in November.

Web Servers

- **-6.7%** – Decline in the number of Apache websites in 2012.
- **32.4%** – Growth in the number of IIS websites in 2012.
- **36.4%** – Growth in the number of NGINX websites in 2012.
- **15.9%** – Growth in the number of Google websites in 2012.

Domain Names

- 246 million – **Number of domain name registrations across all top-level domains.**
- 104.9 million – **Number of country code top-level domain name registrations.**
- 329 – **Number of top level domains.**
- 100 million – **Number of .com domain names at the end of 2012.**
- 14.1 million – **Number of .net domain names at the end of 2012.**
- 9.7 million – **Number of .org domain names at the end of 2012.**
- 6.7 million – **Number of .info domain names at the end of 2012.**
- 2.2 million – **Number of .biz domain names at the end of 2012.**
- 32.44% – **Market share for GoDaddy.com, the biggest domain name registrar in the world.**
- $2.45 million – **The price for Investing.com, the most expensive domain name sold in 2012.**

Internet Users

- 2.4 billion – **Number of Internet users worldwide.**
- 1.1 billion – **Number of Internet users in Asia.**
- 519 million – **Number of Internet users in Europe.**
- 274 million – **Number of Internet users in North America.**
- 255 million – **Number of Internet users in Latin America / Caribbean.**
- 167 million – **Number of Internet users in Africa.**
- 90 million – **Number of Internet users in the Middle East.**
- 24.3 million – **Number of Internet users in Oceania / Australia.**
- 565 million – **Number of Internet users in China, more than any other country in the world.**
- 42.1% – **Internet penetration in China.**

Social Media

- **85,962 –** Number of monthly posts by Facebook Pages in Brazil, making it the most active country on Facebook.
- **1 billion –** Number of monthly active users on Facebook, passed in October.
- **47% –** Percentage of Facebook users that are female.

- **40.5 years** – Average age of a Facebook user.
- **2.7 billion** – Number of likes on Facebook every day.
- **24.3%** – Share of the top 10,000 websites that have Facebook integration.
- **200 million** – Monthly active users on Twitter, passed in December.
- **819,000+** – Number of retweets of Barack Obama's tweet "Four more years", the most retweets ever.
- **327,452** – Number of tweets per minute when Barack Obama was re-elected, the most ever.
- **729,571** – Number of messages per minute when the Chinese microblogging service Sina Weibo saw 2012 finish and 2013 start.
- **9.66 million** – Number of tweets during the opening ceremony of the London 2012 olympics.
- **175 million** – Average number of tweets sent every day throughout 2012.
- **37.3 years** – Average age of a Twitter user.
- **307** – Number of tweets by the average Twitter user.
- **51** – Average number of followers per Twitter user.
- **163 billion** – the number of tweets since Twitter started, passed in July.
- **123** – Number of heads of state that have a Twitter account.
- **187 million** – Number of members on LinkedIn (September).
- **44.2 years** – Average age of a Linkedin user.
- **135 million** – Number of monthly active users on Google+.
- **5 billion** – How many times per day the +1 button on Google+ is used.
- **20.8%** – Usage share of HootSuite as a social media management tool among the world's top 100 brands.

Web Browsers (see http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/)

Search

- 1.2 trillion – **Number of searches on Google in 2012.**
- 67% – **Google's market-leading share of the U.S. search market (December).**
- 1 – **The top trending question of the year on Ask.com: "Will Rob and Kristen get back together?"**

Mobile

- **1.1 billion** – Number of global smartphone subscribers.
- **6.7 billion** – Number of mobile subscriptions.
- **5 billion** – Number of mobile phone users.
- **5.3 billion** – Number of mobile handsets.
- **1.3 billion** – Number of smartphones in use worldwide by end of 2012.
- **465 million** – Number of Android smartphones sold in 2012, a 66% market share.
- **31%** – Percentage of the U.S. Internet population that used a tablet or e-reader.
- **13%** – Mobile share of global Internet traffic.
- **5 billion** – Number of mobile broadband subscriptions.
- **1.3 exabytes** – Estimated global mobile data traffic per month in 2012.
- **59%** – Share of global mobile data traffic that was video.
- **500 megabytes** – Amount of monthly data traffic consumed by the average smartphone.
- **504 kbps** – The average mobile network connection speed globally (all handsets).
- **1,820 kbps** – The average mobile network connection speed globally (smartphones).

Video

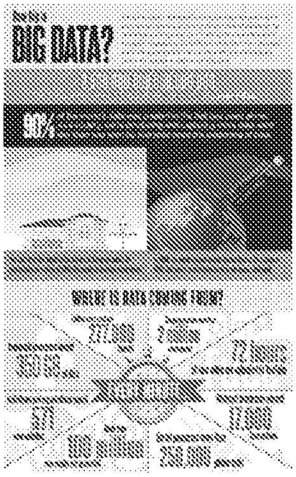
- **14 million** – Number of Vimeo users.
- **200 petabytes** – Amount of video played on Vimeo during 2012.
- **150,648,303** – Number of unique visitors for video to Google Sites, the number one video property (September).

- **1 billion** – PSY's Gangnam Style video became the first online video to reach 1 billion views (currently just over 1.1 billion) and it achieved it in just 5 months.
- **2.7 billion** – Number of views of videos uploaded to YouTube tagged Obama or Romney during the 2012 U.S. election cycle
- **2.5 million** – Number of hours of news-related video that was uploaded to YouTube.
- **8 million** – The number of concurrent viewers of the lifestream of Felix Baumgartner's jump from the edge of space, the most ever on YouTube.
- **4 billion** – Number of hours of video we watched on YouTube per month.
- **60 million** – Number of global viewers monthly on Ustream.
- **16.8 million** – Number of total viewers in a 24 hour period for a video on Ustream, the most ever.
- **181.7 million** – Number of total unique viewers of online video in the U.S. during December.

Images

- 7 petabytes – **How much photo content Facebook added every month.**
- 300 million – **Number of new photos added every day to Facebook.**
- 5 billion – **The total number of photos uploaded to Instagram since its start, reached in September 2012.**
- 58 – **Number of photos uploaded every second to Instagram.**
- 1 – **Apple iPhone 4S was the most popular camera on Flickr.**

What about the internet in 2013?
Just a couple of weeks into 2013 we don't yet know much about what the year ahead has in store for us. However, we can perhaps make a few predictions: we will be accessing the Internet more with mobile devices, social media will play an increasingly important role in our lives, and we'll rely even more on the Internet both privately as well as professionally.



How Much Data is on the Internet and Generated Online Every Minute?
Source: http://removeandreplace.com/2013/03/13/how-much-data-is-on-the-internet-and-generated-online-every-minute/

Have you ever wondered how many bytes of data are created everyday online?
In the last twenty years, internet access has increased across the globe causing a boom in the amount of data being produced and collected.
Here are some facts about data on the internet.
There are 277,000 Tweets every minute, Google processes over 2 million search queries every minute, 72 hours of new video are uploaded to YouTube every minute, More than 100 million emails are sent every minute, Facebook processes 350 GB of data every minute and 571 new websites are created every minute.

Megabytes, Gigabytes, Terabytes... What Are They?

These terms are usually used in the world of computing to describe disk space, or data storage space, and system memory. For instance, just a few years ago we were describing hard drive space using the term Megabytes. Today, Gigabytes is the most common term being used to describe the size of a hard drive. In the not so distant future, Terabyte will be a common term. But what are they? This is where it gets quite confusing because there are at least three accepted definitions of each term.

According to the IBM Dictionary of computing, when used to describe disk storage capacity, a megabyte is 1,000,000 bytes in decimal notation. But when the term megabyte is used for real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes is the appropriate notation. According to the Microsoft Press Computer Dictionary, a megabyte means either 1,000,000 bytes or 1,048,576 bytes. According to Eric S. Raymond in The New Hacker's Dictionary, a megabyte is always 1,048,576 bytes on the argument that bytes should naturally be computed in powers of two. So which definition do most people conform to?

When referring to a megabyte for disk storage, the hard drive manufacturers use the standard that a megabyte is 1,000,000 bytes. This means that when you buy an 80 Gigabyte Hard drive you will get a total of 80,000,000,000 bytes of available storage. This is where it gets confusing because Windows uses the 1,048,576 byte rule so when you look at the Windows drive properties an 80 Gigabyte drive will report a capacity of 74.56 Gigabytes and a 250 Gigabyte drive will only yield 232 Gigabytes of available storage space. Anybody confused yet? With three accepted definitions, there will always be some confusion so I will try to simplify the definitions a little.

The 1000 can be replaced with 1024 and still be correct using the other acceptable standards. Both of these standards are correct depending on what type of storage you are referring.

Processor or Virtual Storage	**Disk Storage**
· 1 Bit = Binary Digit	· 1 Bit = Binary Digit
· 8 Bits = 1 Byte	· 8 Bits = 1 Byte
· 1024 Bytes = 1 Kilobyte	· 1000 Bytes = 1 Kilobyte
· 1024 Kilobytes = 1 Megabyte	· 1000 Kilobytes = 1 Megabyte
· 1024 Megabytes = 1 Gigabyte	· 1000 Megabytes = 1 Gigabyte
· 1024 Gigabytes = 1 Terabyte	· 1000 Gigabytes = 1 Terabyte
· 1024 Terabytes = 1 Petabyte	· 1000 Terabytes = 1 Petabyte
· 1024 Petabytes = 1 Exabyte	· 1000 Petabytes = 1 Exabyte
· 1024 Exabytes = 1 Zettabyte	· 1000 Exabytes = 1 Zettabyte
· 1024 Zettabytes = 1 Yottabyte	· 1000 Zettabytes = 1 Yottabyte
· 1024 Yottabytes = 1 Brontobyte	· 1000 Yottabytes = 1 Brontobyte
· 1024 Brontobytes = 1 Geopbyte	· 1000 Brontobytes = 1 Geopbyte

This is based on the IBM Dictionary of computing method to describe disk storage - the simplest.
Source: http://www.whatsabyte.com/

Now let's go into a little more detail.

Bit: A Bit is the smallest unit of data that a computer uses. It can be used to represent two states of information, such as Yes or No.
Byte: A Byte is equal to 8 Bits. A Byte can represent 256 states of information, for example, numbers or a combination of numbers and letters. 1 Byte could be equal to one character. 10 Bytes could be equal to a word. 100 Bytes would equal an average sentence.

Kilobyte: A Kilobyte is approximately 1,000 Bytes, actually 1,024 Bytes depending on which definition is used. 1 Kilobyte would be equal to this paragraph you are reading, whereas 100 Kilobytes would equal an entire page.

Megabyte: A Megabyte is approximately 1,000 Kilobytes. In the early days of computing, a Megabyte was considered to be a large amount of data. These days with a 500 Gigabyte hard drive on a computer being common, a Megabyte doesn't seem like much anymore. One of those old 3-1/2 inch floppy disks can hold 1.44 Megabytes or the equivalent of a small book. 100 Megabytes might hold a couple volumes of Encyclopedias. 600 Megabytes is about the amount of data that will fit on a CD-ROM disk.

Gigabyte: A Gigabyte is approximately 1,000 Megabytes. A Gigabyte is still a very common term used these days when referring to disk space or drive storage. 1 Gigabyte of data is almost twice the amount of data that a CD-ROM can hold. But it's about one thousand times the capacity of a 3-1/2 floppy disk. 1 Gigabyte could hold the contents of about 10 yards of books on a shelf. 100 Gigabytes could hold the entire library floor of academic journals.

Terabyte: A Terabyte is approximately one trillion bytes, or 1,000 Gigabytes. There was a time that I never thought I would see a 1 Terabyte hard drive, now one and two terabyte drives are the normal specs for many new computers. To put it in some perspective, a Terabyte could hold about 3.6 million 300 Kilobyte images or maybe about 300 hours of good quality video. A Terabyte could hold 1,000 copies of the Encyclopedia Britannica. Ten Terabytes could hold the printed collection of the Library of Congress. That's a lot of data.

Petabyte: A Petabyte is approximately 1,000 Terabytes or one million Gigabytes. It's hard to visualize what a Petabyte could hold. 1 Petabyte could hold approximately 20 million 4-door filing cabinets full of text. It could hold 500 billion pages of standard printed text. It would take about 500 million floppy disks to store the same amount of data.

Exabyte: An Exabyte is approximately 1,000 Petabytes. Another way to look at it is that an Exabyte is approximately one quintillion bytes or one billion Gigabytes. There is not much to compare an Exabyte to. It has been said that 5 Exabytes would be equal to all of the words ever spoken by mankind.

Zettabyte: A Zettabyte is approximately 1,000 Exabytes. There is nothing to compare a Zettabyte to but to say that it would take a whole lot of ones and zeroes to fill it up.

Yottabyte: A Yottabyte is approximately 1,000 Zettabytes. It would take approximately 11 trillion years to download a Yottabyte file from the Internet using high-power broadband. You can compare it to the World Wide Web as the entire Internet almost takes up about a Yottabyte.

Brontobyte: A Brontobyte is (you guessed it) approximately 1,000 Yottabytes. The only thing there is to say about a Brontobyte is that it is a 1 followed by 27 zeroes!

Geopbyte: A Geopbyte is about 1000 Brontobytes! Not sure why this term was created. I'm doubting that anyone alive today will ever see a Geopbyte hard drive. One way of looking at a geopbyte is 15267 6504600 2283229 4012496 7031205 376 bytes!

Now you should have a good understanding of megabytes, gigabytes, terabytes and everything in between. Now if we can just figure out what a WhatsAByte is......:)

The byte converter http://www.whatsabyte.com/P1/byteconverter.htm

DATA IS ABUNDANT, INFORMATION IS USEFUL, KNOWLEDGE IS PRECIOUS.

Data. – Data is raw and it’s abundant. It simply exists and has no significance beyond its existence . It can exist in any form, usable or not. It does not have meaning of itself. Collecting users activity log will produces data.

Information. – Information is data that has been given meaning by way of relational connection.

Knowledge. - Knowledge is the appropriate collection of information, such that its intent is to be useful.

Internet users are generating petabytes of data every day. Millions of users access billions of web pages every millisecond, creating hundreds of server logs with every keystroke and mouse click. Having only user log data is not useful. To give better service to user and generate money for business it is required to process raw data and collect information which can be used for providing knowledge to users and advertisers. **Source:** http://www.whatsabyte.com/

Based on these figures, I opine that intelligence exists out there just waiting to be tapped. Lots of data but guess what, even Google which is considered currently the best search engine, has only indexed about 170 terabytes. Now you know why I recommend using more than one search engine with good keywords to assist.

Facebook represents a huge potential market for your social media efforts, but it is becoming increasingly difficult to stand out from the crowd. The following statistics highlight some relevant Facebook facts and can ultimately help you to navigate it better, increasing your return on investment (ROI) and leading to greater marketing success

Worldwide, there are over 1.11 billion active Facebook users. (Source: Facebook) This is a 23 percent increase from March 2012. What this means for you: In case you had any lingering doubts, statistically, Facebook is too big to ignore.

4.5 billion likes generated daily as of May 2013 which is a 67 percent increase from August 2012 (Source: Facebook)

665 million people log onto Facebook daily, which represents a 26% increase from 2012 (Source: Facebook) The Implication: A huge and vastly growing number of Facebook users are active and consistent in their visits to the site, making them a promising audience for your marketing efforts.

There are 751 million mobile active users which is a 54 percent increase from 2012. (Source: Facebook)
In Europe, over 223 million people are on Facebook.(Source: Search Engine Journal) The Takeaway: This isn't just a U.S. phenomenon – a worldwide market is available via Facebook.

Age 25 to 34, at 29.7% of users, is the most common age demographic. (Source:Emarketer 2012) What this means for you: This is the prime target demographic for many businesses' marketing efforts, and you have the change to engage these key consumers on Facebook.

Five new profiles are created every second. (Source: ALLFacebook 2012) The Implication: Your potential audience on Facebook is growing exponentially.

Facebook users are 53% female and 47% male. (Source: Emarketer) The Takeaway: Since this isn't a large statistical difference, you should be able to effectively reach both genders on Facebook.

Highest traffic occurs mid-week between 1 to 3 pm. (Source: Bit.ly blog) How this can help you: Since you have the potential to reach more consumers and drive higher traffic to your site during peak usage times, consider this statistic in determining when todo more frequent or important status updates, offers and other posts.

On Thursdays and Fridays, engagement is 18% higher. (Source: Bit.ly blog) The Implication: Again, use this information to determine when to post in order to optimize your social media marketing efforts.

There are 83 million fake profiles. (Source: CNN) The Takeaway: Nothing is perfect, so always remain thoughtful and strategic in your efforts. Also, fake or not, these are still potential consumers. There are various reasons for fake profiles, including professionals doing testing and research, and people who want to segment their Facebook use more than is possible with one account.

Photo uploads total 300 million per day. (Source: Gizmodo) The Implication: Again, this is an indication of engaged users; also, it is an indication that there are a lot of photos, as well as other information, competing for users' attention, so target your efforts strategically.

Average time spent per Facebook visit is 20 minutes. (Source: Infodocket) What this means for you: You could have a short time period to make your impression, so use it wisely with relevant, interesting and unique posts and offers in order to get the most return on your efforts.

Every 60 seconds on Facebook: 510 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded. (Source: The Social Skinny) The Implication: Again, there are a lot of engaged and active users, but also a huge amount of information competing for their attention, so quality and strategy on your part matter.

4.75 billion pieces of content shared daily as of May 2013 which is a 94 percent increase from August 2012. (Source: Facebook)

50% of 18-24 year-olds go on Facebook when they wake up. (Source: The Social Skinny) What this means for you: Facebook is important to these users, and potentially, if done correctly, so is the content you post on it.

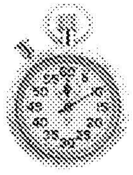
One in five page views in the United States occurs on Facebook. (Source: Infodocket 2012) How this helps you: This is a huge market on the web; if you use social media marketing efforts on Facebook well, you could have huge returns to show for it.

42% of marketers report that Facebook is critical or important to their business. (Source: State of Inbound Marketing 2012 The Takeaway: This is a crowded marketplace, but you can't afford to sit it out, because odds are fairly high that your competition is there. The key is to use Facebook marketing correctly and make sure that your efforts stand out from the crowd.

16 Million local business pages have been created as of May 2013 which is a 100 percent increase from 8 million in June 2012. (Source: Facebook)

7.5 million promoted posts have been made from June 2012 to May 2013. (Source: Facebook)

Every 60 Seconds (tick, tick, tick, tick)



- 72 hours of video are uploaded to YouTube.
- 700,000 pieces of content are shared on Facebook.
- 4,000 images are uploaded to Flickr.
- 500 new websites are created.
- In one second on the Internet there are... http://onesecond.designly.com/

The following sites for exploring facebook can deliver results with just the right tweaking. It's amazing just how much information is out there even after users are warned over and over to secure their sites and be careful about posting very personal information. I especially take advantage of the photos that are posted. I don't study the subject; I study the backgrounds. You may recall how law enforcement was able to take down a pornographer simply by studying objects that were in a photo that identified not only the individual but also the year it took place. Of course in my opinion law enforcement went too far in the information that was released. They basically told the criminals how to cover their tracks in the future. http://www.dailynews.com/crime/ci_22310291/child-pornography-suspect-sought-by-federal-agents-arrested

People Search

ZABA SEARCH	www.zabasearch.com	Performs great in conjunction with Pipl
123people	www.123people.com	
pipl	www.pipl.com	Use alongside ZabaSearch
peekyou	www.peekyou.com	Use with Spokeo
spokeo	www.spokeo.com	
wink People Search	http://wink.com/	
peepDB	http://peepdb.com/	

As I have already admitted I do have a fake account to do research, and I do mean research. However for some of the sites you don't even need a fake account to be able to view the results. My favorites, in order are: Topsy, Booshaka, Open Facebook Search, Graph Search and Tagboard. Bing does have utility but does not deliver like the others.

TOPSY Search and analyze the social web. I like this site because of the basic analytics when comparing 3 queries. Even the basic site has utility. My only warning is be careful with keywords you may use. The photos returned may not be what you want to look at. The search syntax is similar to what you may use in the google search.

booshaka! See what's trending on Facebook — right now.

Search Facebook, Myspace, Twitter, Google+, and Linkedin without logging in. This one is awesome. With the results from 5 separate sites, keyword harvesting becomes quite simple.

Graph Search Graph Search is a social-network search engine that ingests natural language queries on people, places, and things and spits out results previously hidden inside Facebook's world. This one actually requires a login but do you really have to use a real account? Amazing what you are able to dig up

TouchGraph Facebook visualization. http://www.touchgraph.com/seo

#tagboard With tagboards you see the whole conversation, across networks, making them the perfect hub for social media.

bing When you search for people you know on Bing, you will be able to see public Facebook timelines of people close to you (ex. your Friends or Friends of Friends). This can happen when you go to Bing while logged in to Facebook or if you connect to Facebook while on Bing.

Twitter Gumshoe

Want to find out if there is an associated account for an email address or mobile number within Twitter for a person you're tracking? Here are some instructions on how to go about it. The downside is that it will only tell you if the number or email address is linked to an active account but it should still prove to be useful.

Go to the Twitter homepage. Navigate to the upper right hand corner where it says sign in. Click on the down arrow and click again on the "forgot password" link. This will take you to another page titled "forgot password"? Here you have a choice of entering an email address or a phone number, or a username in a separate box. As in facebook below, do not press return or click submit as this will alert the account holder. After a few moments a message will appear letting you know if what you entered is associated with an active account with the terms "looks good" or "invalid."

While this may seem somewhat trivial it is enough information to keep an investigator on the right track.

What is Twitter: A rapid and short (140-character or less) message on Twitter (and viral) sharing of information in a real time communication platform. Twitter happens in real time, 24 hours a day. Expect to miss stuff if it's not sent direct to you. Be succinct – you only have 140 characters (including spaces in between text) to say anything. https://twitter.com/

Twitter Search is the Google of Twitter. Allows searches for tweets with specific keywords where the results come up in real time. Even after the search has ended the screen refreshes if more tweets are posted. https://twitter.com/search-home

You may also be interested in monitoring tweets from a specific location that perhaps just experienced a shooting, robbery, assault, or something that law enforcement may want to be on the lookout. Let's say I want to monitor Huntington Park just south of Los Angeles, California. Open Google Maps and zoom into the particular area where the event took or is taking place. Right click the location and a menu will pop up. Click on the "what's here"? tab. The geo location will appear in the search box of google maps. For example "33.979453,-118.231271" comes up. Copy the geo coordinates and paste it in the search box of twitter search (https://twitter.com/search-home) and add a distance from the location you want to monitor. Perhaps you want to know what is being tweeted within a 10 mile radius of the location. In that case the correct search would be "geocode:33.979453,-118.231271,10mi." Notice that there aren't any spaces in the search arrangement. Note: If you use Google Earth the geo coordinates appear at the bottom right.

Monitoring Twitter (and others)

This one is amazing and you'll see why after you take it for a spin. I've tried it quite a bit and am just stunned at what I can do with it when used in combination with other monitors. Think of the possibilities. EchoSec harvests location data from posts on popular social media sites like Facebook, Twitter, Instagram and Foursquare and displays it on a map – making it easy to see exactly who is posting what, and where they are located. It's a new way to search. Instead of searching for text, now you search an area. The company's prospective clients include government and law enforcement organizations (duh). Though it may seem creepy, because the tool utilizes data people have shared publicly, albeit potentially unwittingly, it is completely legal. Imagine locating a supposedly stealth/hidden submarine because someone aboard it twitted a message.

A similar functionality as echosec, but run them side by side and you have power.

GeoSocial Footprint: A geosocial footprint is the combined bits of location information that a user divulges through social media, which ultimately forms the users location "footprint". For Twitter.com users, this footprint is created from GPS enabled tweets, social check-ins, natural language location searching (geocoding), and profile harvesting.

This website provides twitter users with an oppurunity to view their geosocial footprint. In additional it informs users of some potential areas of concern with their current sharing habits. To begin, enter you Twitter.com username in the input box below and press "Retrieve Tweets".

I really like this one and always have a lot of fun just experimenting. I could not think of any user names to input so I just took a shot at what I thought people would use and bingo! I was amazed at the results. I was able to download the tweets into notepad and from there work my way into facebook and instagram, just to name two sites, and really dig into these individuals.

This one is awesome when used in conjunction with Ready Or Not below.

Enter a hash tag like #losangeles policebrutality and see the results. You can also modify it to #losangeles brutality or #losangeles police and the results will be different. It is a matter of resourcefulness and playing with the hash tag words to get the best results. You can also modify the URL for results.

This app shows how people could use your social-media posts to find you in the physical world. It uses GPS data attached to Twitter and Instagram posts to create a map of where someone's been posting from recently.

Try to find yourself, your friends, or your favorite celebrity! Where are you most likely to be at 2:00 on a Tuesday?

Then follow the links and find out how to keep your social-media posts from giving your location away.

TweetDeck gives the Twitter experience more flexibility and allows advanced users to gain valuable insight to what's happening at this very moment on Twitter. TweetDeck is currently available as a desktop app, a web app, or a Chrome app, and can be downloaded at tweetdeck.com

TweetDeck makes it easier for publishers, marketers and power users to track the real-time conversations they care about. It brings more flexibility and insight to power users through a customizable layout that lets you keep up with the people and topics that matter most to you. And, you can join the conversation by tweeting, sharing photos and links to news stories, and more. *Note:* Twitter will soon kill this app.

Twitterfall is a Twitter client specialising in real-time tweet searches. New tweets fall into the page. Twitterfall does not store any identifying information on the server about any users.

TweetTabs Is An Awesome Way To Search Twitter In Near Real-Time.

Trendsmap is a real-time mapping of Twitter trends across the world. See what the global, collective mass of humanity are discussing right now.

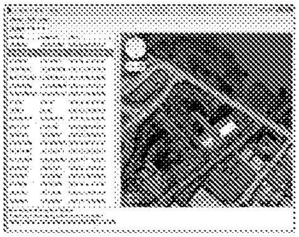
GeoChirp helps you search for people Twittering for specific things in a specific area. For example, if you want to search for people Tweeting about 'Golf' in Richmond, Virginia, you can just select the area in the map, set the radius within 1-50 miles of that area, enter the keyword "Golf" or any other related keyword and BOOM you have all the people Twittering about 'Golf' in Richmond, Virginia.

Tracking Users

Simply enter the twitter user on the map page and click the Show on Map button to show that user's tweets on the map. Clicking on one of the markers on the maps will show the details of that tweet.

Twtrland is a pretty cool snapshot of someone's Twitter account. Go to twtrland.com, put in any username and they will show you the last 1400-2000 tweets depending on the account.

You can see how often they get retweeted, how many tweets per day, the break down on a pie chart of their activity and much more. What's nice is that you see how conversational they are or how many links they send out. CNNbrk, Mashable, and SocMedHotbed are mainly links but if that is what you are looking for then you have it. Looking at a user's twitter stream will give you one side of them that you can't get from them. Twtrland does a great breakdown and it can be addictive.



Creepy is an application that allows you to gather geolocation related information about users from social networking platforms and image hosting services. The information is presented in a map inside the application where all the retrieved data is shown accompanied with relevant information (i.e. what was posted from that specific location) to provide context to the presentation.

If you feel like you need to know where the friends, family, and acquaintances in your online social networks are, or have been, there's a free tool that can help you pinpoint their locations, and most info just requires a user ID. Sound Creepy? It is. Not only in its purpose but also because that's the name of this free online sleuthing program.

Dataminr's analytics engine transforms social media streams into actionable signals, providing enterprise clients with one of the earliest warning systems for market-relevant information, noteworthy events, and emerging trends.

Search Twitter for People

Twitter is a fairly boring place if there's nobody interesting you are following - but it's always been an issue to find interesting people. That's where tweepz comes in! Think of us as the whitepages for twitter. Search for twitter accounts based on names, locations and keywords.

Same as above.

Same as above.

Same as above.

Alternatives

Tweet Tunnel leads you to special features that you wouldn't find on Twitter.

Real-time social media search and analysis.

Search by location first to find data that's missed by traditional keyword and hashtag monitoring tools. Uncover the hidden 70% of social media content that is missed by keyword-based discovery tools. Complement traditional keyword based social listening tools with a highly contextual dataset that was inaccessible…until now.

Digsby is a social networking tool that alerts you of events like new messages and gives you a live Newsfeed of what your friends are up to.

Mapping Social Networks. We provide unique tools to visually map, search and record social networks. Uses range from criminal investigations to marketing. Please note our products only ever access publicly available information on the web, and do not do any "hacking".

Searches social media Blogs, Twitter, FaceBook or all. I have favorite keywords to input like jihad, jihadist and jihadists to test the returns. Police brutality in different cities (ie "police brutality" Chicago or "los angeles") also work wonders. The idea is to see what other keywords may pop up to help an investigation. These works for all sites. You just have to be resourceful with keywords. Take pen to paper and brainstorm keywords that may help in your research and investigations. It's not that difficult. Five minutes with pen and paper may save you five hours of work.

Data-mining of blogs

Real-time tweet posts between subscribers

Social media monitoring and real-time analytics.

Searches blogs and twitter.

Addictomatic searches the best live sites on the web for the latest news, blog posts, videos and images. It's the perfect tool to keep up with the hottest topics, perform ego searches and feed your addiction for what's up, what's now or what other people are feeding on.

The leading blog search engine and directory, Technorati.com indexes more than a million blogs. The site has become the definitive source for the top stories, opinions, photos and videos emerging across news, entertainment, technology, lifestyle, sports, politics and business. Technorati.com tracks not only the authority and influence of blogs, but also the most comprehensive and current index of who and what is most popular in the Blogosphere.

Samepoint, LLC is a social media API aggregation and monitoring company. Headquartered in New York, NY, it provides data from thousands of social media websites via one API. These social media sources includes, but are not limited to Facebook, Twitter, Blogs and Internet forum. The API also includes sentiment, analyzing whether a comment is positive or negative based on natural language processing.

A social media search tool that allows users to search for conversations surrounding the topics that they care about most. Whether it be your favorite sport, favorite food, celebrity, or your company's brand name; Whostalkin.com can help you join in on the conversations that you care about most. Our search and sorting algorithms combine data taken from over 60 of the internet's most popular social media gateways.

Type your keywords with a space between them. Keywords can be associated with a plus (+) between words, e.g. steve+jobs. I like this one as it takes advantage of several blogs nd goes back quite a bit into the past. Type in drug cartels and see the results.

As the name implies, this one searches twitter and google.

Facebook Detective

Want to find an associated account for an email address or mobile number within Facebook or Twitter for a criminal you're tracking? Here are some step by step instructions on how to go about it. (The Twitter instructions are in Twitter Gumshoe above.) However, you may not have much luck if your target has made good use of their security settings. Don't give up, they always stumble somewhere.

Open facebook, go to the upper right and click on the "forgot your password." This will bring up a new window with a "find your account" heading. I am sure that if you're up to this level you already have your target's email, phone number, user name or full name. So go ahead and input whatever you have into the search box. If whatever you input is in fact associated with an account you will get a new window with a "reset your password" heading and instructions on how to go about it. Maybe you'll luck out and a photo will appear identifying the profile name. Wouldn't that be nice!

In this window I found out that one of my friends has 2 other email accounts (I was experimenting, really, I was). Although some of the letters had been replaced with asterisks (*) to keep them safe, I quickly figured out the letters by comparing the number of asterisks to the email I already had on him. To test my theory I emailed him on one of the newly discovered emails and sure enough I had a reply. "How did you get this address"? I bet your target will be dumb enough to reply also!

If you don't get a hit then your input probably does not have an account or profile associated with it. On the other hand even if the profile name is not uncovered you may still get hits on email addresses, as I did above, or phone numbers. Note that part of the phone numbers will also be replaced with asterisks as were the email addresses.

One more thing, do not, I repeat do not click on continue after you get your results. This will only alert the account holder that someone is toying with them.

Belkasoft Facebook Profile Saver captures information publicly available in Facebook profiles. This small utility is designed for computer forensic and security specialists who need to automate the downloading of Facebook pages to their local computers. A local copy of public Facebook pages may be required for performing investigations and/or presented as court evidence. Performing this task manually may be a time-consuming operation. Many Belkasoft customers asked for a tool automating this routine.

Facebook has always been an easy way to expose criminal behavior and with the new Facebook Graph Search it's quite possible to identify the individuals. Criminals may think they have effectively locked their accounts but all it takes is for someone to come up with the right search term and their secrets will come spilling out. Read on:

Two rival gangs battled in the streets of Brooklyn during a three year period leaving several dead and scores of others wounded. They may have kept on like this if cops didn't get savvy to their activities and whereabouts on Facebook. Based on that knowledge 49 alleged gangsters are locked up facing murder charges. "Detectives used social media as well as good old fashioned police work to track the killers."

The war started when a member of the "Rockstarz" gang murdered a member of the "Very Crispy Gangsters" (VCG) named Taquan "Tay Weez" Crandell in 2009. As the two gangs fought over turf, they increasingly brought their threats, taunting, and grandstanding to Facebook.

BrightPlanet Deep Web Intelligence Software

Deep Web Harvester™
This is the only tool that can harvest Deep Web content at Big Data scale and prepare it for mission critical analytics. Whether you want to access your harvested content through a thin client delivery, or you want to license and create or augment an enterprise solution behind the security of your firewall, the Deep Web Harvester can be customized for your specific environment. This is the best Deep Web Intelligence option for those who want total control over their Deep Web harvests.

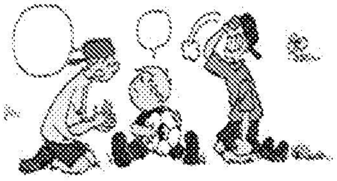
Deep Web Silo Services™
If you want help finding, harvesting, enriching and storing harvested data, look no further than our Deep Web Silo Services. We can build a custom solution that combines the power of our Deep Web Harvester with the skills of BrightPlanet's Deep Web Investigators – experts at finding, harvesting and storing content in Deep Web Silos.

Deep Web Monitor™
This lightweight, thin-client solution allows a single user to set up your own harvests through any Web browser. With the Monitor, you can identify, track, monitor and alert directly from sources YOU target with keywords YOU create. Automated email alerts let you know whenever new or modified content is added.

BlueJay for Law Enforcement
BlueJay captures tweets from the entire Twitter firehose unlike all other products on the market. BlueJay is invisible and covert, and all you need is a web browser to access the tool. BlueJay provides real-time intelligence following only those users, keywords and locations YOU want to track and monitor. Tweets are geographically tagged and can be exported to support more detailed analysis and investigation.

Photos & Videos

Another subject is that of photos and videos on social media. Everyone has heard the term "a picture is worth a thousand words", however, in the open source world a picture is worth a thousand leads. Not that one photo has a thousand leads but rather that one lead in a photo can lead to another lead that leads to another and so on. I think you get the picture (no pun intended). How many pictures are posted on social websites is anyone's guess but I would venture to say with 100% accuracy there are more than a thousand. Pictures tell a story if you study them. There is always something in the background.



How many times have you walked or driven by the same place over the years either to work or just out for a casual stroll? Then one day as you are sitting at a traffic light you start noticing your surroundings. You notice things that you never did before and start seeing more detail than usual; perhaps a new building went up and you never really paid attention until today. Welcome to the world of open source! What about family photographs from years past? Look at some family photos from previous years and really study them. You will find details that you had not noticed before. Is there any information in the photos that you can use to your advantage? Perhaps there's a silverware set sitting on the kitchen table. You never paid attention to it until now. You start wondering where it is and you always had your eye on it. Now is the time to start buttering up to your grandmother or aunt. What have you just accomplished? You have taken simple information from a photo and are now plotting to use it to your advantage. You now have intelligence rather than just information to support a planned operation of perhaps making sure that you are the one to inherit the silverware setting, or maybe just getting it as a gift.

(Source: http://en.wikipedia.org/wiki/A_picture_is_worth_a_thousand_words) The adage "A picture is worth a thousand words" refers to the idea that complex stories can be described with just a single still image, or that an image may be more influential than a substantial amount of text. It also aptly characterizes the goals of visualization where large amounts of data must be absorbed quickly.

Try this experiment the next time you have time to kill. Take a photograph of the street or apartment complex you live in, or whatever suits you. A camera with good telephoto and pixel capability will do the trick. Now look at the photos you just took either on your computer or camera screen. Zoom in to different areas. Maybe when you took the photo you were concentrating on a car but now as you zoom in you notice a person or persons in the background that you had completely missed. Look at other backgrounds. What else is there? It's amazing what a simple photo can reveal.

Photo Tools

twipho

TwiPho searches the twitter timeline for images shared by twitter users on sites such as img.ly, TwitPic and YFrog. You just need to enter your search term (and you do not even have to press any buttons!) and the site searches all tweets from the twitter timeline to search for images matching your keywords.

Every now and again Tweeters post links to photos they have taken out and about and post them on some popular image hosting sites such as TwitPic, img.ly and yfrog. All we do is take your search query, look through the whole twitter website and give you images Tweeters have posted! Simple!
https://twitter.com/twipho https://www.facebook.com/twipho http://topsy.com/twitter/twipho

twitpic

Twitpic is a website that allows users to easily post pictures to the Twitter microblogging and social media service. Twitpic is often used by citizen journalists to upload and distribute pictures in near real-time as an event is taking place.

thudit

Thudit is a real-time image search presenting users with a mosaic of pictures on any topic of their choosing. From breaking news stories and current affairs thudit pulls pictures from Twitter, Flickr and Instagram to create a comprehensive visual story.
https://twitter.com/Thud_it

twicsy

The service, launched by the social search engine Searchles, features a main page that is filled with image thumbnails. All of them are images shared over Twitter on either TwitPic or yFrog (two of the most popular Twitter picture sites, currently). The default is to show images from the past hour, but you can set different time intervals to change what images are shown. Hovering over any of them shows a larger version of the image, along with some details about it, like its link and tags. https://twitter.com/Twicsy

www.photo-freeware.net - there are a number of different Image Meta EXIF Data tools located here, find the one that shows the type of data you want to see
www.photome.de - PhotoME is a powerful tool to show and edit the metadata of image files
www.tawbaware.com - basic exif viewer
www.geosetter.de - free but powerful exif viewer with nice geo-locator display & IPTC data
www.sourceforge.net - hide a file in a picture with hip2.1
www.bartdart.com - BartMark Bitmap Encoder allows you to encode text messages into bitmap images

Metadata (Data about Data)

Metadata is simply data about other data and if properly exploited can lead to many concealed surprises about various records. Metadata can reveal information about a certain document's content. Imagery contains loads of hidden information that can reveal such things as the size of a photo, resolution, date of photo, type of camera used, location of imagery, and other data that is useful to the OSINT analyst. On the other hand, a Microsoft office document or .pdf file contain information about the particular document like who created it and the initials of the creator, when, the number of revisions, company name, names of previous authors, personal views along with comments, size, and whether an original document for something totally different was modified to create something entirely new (this alone is a surprise in itself).

Photo Surprises (discovering out of sight information)

http://www.tineye.com/ (reverse image search engine)
It finds out where an image came from, how it is being used, if modified versions of the image exist, or if there is a higher resolution version

ImgOps

http://imgops.com/ Image operations meta-tool.
You can also insert http://imgops.com/ in front of any image URL.

Google

https://encrypted.google.com/imghp?hl=en

Submit a JPEG or PNG picture for Forensic Analysis. Process a URL image or upload a picture. http://fotoforensics.com/

CamStudio OPEN SOURCE

This piece of software could come in handy to keep you from visiting the same site over and over and leaving footprints. Simply record what you need and save to a file for later viewing. CamStudio is able to record all screen and audio activity on your computer and create industry-standard AVI video files and using its built-in SWF Producer can turn those AVIs into lean, mean, bandwidth-friendly Streaming Flash videos (SWFs).

Screenpresso

Screenpresso captures your desktop (screenshots and HD videos) for your training documents, collaborative design work, IT bug reports, and more...
Light-weight Windows screen grab tool with built-in image editor, user guide generator and sharing options.

AutoScreenRecorder Same as above.

How to Stalk with RSS

…and for those of us that are lazy or just plain don't have the time to sit down and monitor sites by inputting keywords there is always RSS (really simple syndication). This link provides a good introduction to RSS and does not take long to read. https://s3.amazonaws.com/manuals.makeuseof.com/for-mobile/Newspaper_2.0_RSS_-_MakeUseOf.com.pdf

I personally like RSS Bandit. I did not say prefer. I have been using it for several years and have gotten very used to it and just know how to tweak it to answer my requirements. When it comes to handling information overload RSS is simply the answer.

The following is a list of several aggregators that you may find useful. Some are dated but are still functional.

Top RSS feeds by date

Active Web Reader - Free aggregator. Supports RSS feed formats 0.9x, 1.x and 2.x. Requires Internet Explorer 6 or higher.
Aggie - A .NET based open source application for reading RSS feeds. Supports RSS versions 0.91, 0.92, 0.93, 0.94, 1.0, and 2.0.
Awasu - Free RSS client, allowing monitoring of a variety of news sites and weblogs. Using plugin architecture, can also be customized to monitor databases, email accounts, and other resources.
CITA RSS Aggregator - Free full function aggregator that can also deliver bittorrents. Can access feeds secured by user ID and password. Includes tool to remove adverts from feeds. Requires .NET Framework.
Chaos Wallpaper - A utility that rotates desktop wallpaper while displaying RSS or Atom feeds on the desktop.
Composite - A free desktop RSS/RDF aggregator application for .NET.
CyberBuddy - CyberBuddy is a freeware application that delivers a variety of content to your desktop, including RSS News Feeds, via talking agent characters.
EffNews RSS Reader - The EffNews RSS Reader is a minimalist RSS reader (not aggregator) for Windows. The reader is shipped as part of the effbot.exe application framework - a freely available Python library that includes a tolerant RSS parser and an asynchronous HTTP client module.
Feed Notifier - Feed Notifier is an application for Windows and Mac OS X that resides in the system tray or status bar and displays pop-up notifications on your desktop when new items arrive in your subscribed RSS or Atom feeds.
FeedReader - Open-source aggregator that supports RSS and Atom formats. Runs under Windows 95 and later versions.
FeedThing - Syndicated news reader which supports all flavours of RSS as well as Atom.
Fuzzy Duck RSS Reader - Reads RDF, RSS and Atom formatted XML news feeds.
GreatNews - Supports all major RSS feed formats; integrates with Bloglines. Doesn't need .NET or Java runtime. [Windows 2000/XP/2003].
Headline Viewer - Shareware newsreader client for Windows.
News Interceptor - Aggregator reads both RSS feeds and non-RSS based news sources.
NewsPiper - A freeware RSS feed and web news reader that can speak headlines.
Newz Crawler - Provides access to news content from several sources, including XML, RSS, Usenet, and the Web.
NewzSpider - NewzSpider is a news aggregator that runs on your computer and downloads headers from your favorite news sites and blogs. It is flexible and

very easy to use. NewzSpider supports ALL RSS standards (0.9x, 1.0 and 2.0) as well as the new ATOM format.

Novobot - A heavily featured desktop newsreader, that can also scrape non-RSS sites.

Omea Reader - RSS/Atom feed reader, newsgroup reader and Web bookmark manager. Features include searches, categorization, flagging, annotations, clippings and notifications. Requires .NET Framework. [Windows 2000/XP/2003].

QM nooze - Very simple RSS/RDF reader with simple interface and small memory footprint. [Win 95/98/Me/NT/2000/XP]

RSS Aggregator - An RSS reader that as well as reading feeds it can form a new feed from several existing feeds.

RSS Bandit - A free desktop news aggregator for Windows built on the .NET Framework.

RSS Captor - A configurable RSS feed reader. Supports all versions of RSS and has an audible alert for new messages.

RSS Popper - A free news aggregator for Outlook. Allows reading of RSS/RDF/Atom feeds in Outlook.

RSS Toolbar - An RSS Toolbar for Internet Explorer that monitors RSS feeds and displays the feed through the web browser.

RssReader - Free RSS reader is able to display any RSS news feed. Requires Microsoft .NET Framework 1.1.

SharpReader - Three-pane RSS Aggregator for the .NET framework.

Vienna - Vienna is an RSS/Atom reader for Mac OS X, packed with powerful features that help you make sense of the flood of information that is distributed via these formats today.

Vox Lite - Allows visitors to keep up-to-date with sources of information that support the RSS protocol. Requires .NET Framework 1.1.

Web Reader - You can follow your favorite sites, online newspapers, blog, forums, comments, video channels, photo albums, deal-of-the-day websites and more.

Wildgrape NewsDesk - Wildgrape NewsDesk is a fast, convenient, and easy to use RSS headline reader for Windows. Requires Microsoft .NET Framework.

blogbot for Outlook - Blogbot for Outlook is an RSS/Atom/weblog aggregator that plugs into Microsoft Outlook 2000/XP/2003. It monitors subscriptions to Internet news feeds and delivers new posts to folders within Outlook.

blogbot lite - RSS/Atom news and weblog application integrated with Internet Explorer in a sidebar.

Facebook is among the most popular websites offering RSS integration. You can get RSS for almost any Facebook page that offers notifications, which will greatly cut down on the number of Facebook notifications spamming your email inbox. Source: https://s3.amazonaws.com/manuals.makeuseof.com/for-mobile/Newspaper_2.0_RSS_-_MakeUseOf.com.pdf

Flickr includes an RSS feed for any individual account, based on the URL: http://api.flickr.com/services/feeds/activity/all?user_id=USERID&secret=6PC5p7ygo3VWGAlaTVUHeKMagSo%3D&lang=en-us&
Source: https://s3.amazonaws.com/manuals.makeuseof.com/for-mobile/Newspaper_2.0_RSS_-_MakeUseOf.com.pdf

Twitter can also let you track individual users using the following URL: http://search.twitter.com/search.atom?q=@USERNAME
Simply replace “USERNAME” with the user ID of anyone you would like to follow via RSS.

Here’s another way to configure an RSS feed with Bing based on your interests. Let’s say you are interested in Mexican Drug Cartels. In the Bing search window type in “Mexican drug cartels” with quotation and enter. You will of course get the results but the URL also displays the following: http://www.bing.com/search?q=%22mexican+drug+cartels%22&go=&qs=bs&form=QBRE, or maybe http://www.bing.com/search?q=%22mexican+drug+cartels%22&go=&qs=bs&form=QBLH. Either way simply add “&format=rss” at the end of the url and you now have a feed you can add to your favorite feed reader like RSS Bandit.

Google also offers customized searches, although not on the same level as Bing. Essentially, to generate an RSS for Google, you must use Google Alerts. Simply navigate to Google Alerts, input your search criteria, and output as an RSS.

A social news and entertainment website. Every possible Reddit page also includes an RSS feed. Simply by adding “.RSS” to the end of any URL on Reddit will allow you to insert it into a reader, such as Feedly. However, many readers actually support directly inserting Reddit links without the .RSS appendage. This is similar to Bing by taking advantage of the URL.

A Firefox extension that allows you to monitor any webpage for updates. This is particularly useful for older sites that haven’t caught onto RSS feed technology. To use the extension, simply install it and when you find a site that requires monitoring, right-click on it and select “scan for updates”. Monitors web pages for updates. Useful for websites that don't provide Atom or RSS feeds.

Allows the user to automatically monitor a website for any changes made. The service actually makes a distinction between changed and unchanged text, displaying both together for comparison. For keeping track of website changes when RSS is unavailable, ChangeDetection is an excellent service.

Page2RSS is web app that will convert any website into an RSS feed. Has functionality with Twitter, as well as a Google Chrome extension. To use Page2RSS, simply cut and paste the URL of the webpage that you would like to monitor. Page2RSS will output an RSS feed, which you can plug into your reader.

Do criminals use facebook? (Source: http://247wallst.com/special-report/2012/05/16/nine-major-ways-criminals-use-facebook/2/

1. Hacking Accounts
When criminals hack a Facebook account, they typically use one of several available “brute force” tools, Grayson Milbourne, Webroot’s Manager of Threat Research for North America, told 24/7 Wall St. in an interview. These tools cycle through a common password dictionary, and try commonly used names and dates, opposite hundreds of thousands of different email IDs. Once hacked, an account can be commandeered and used as a platform to deliver spam, or — more commonly — sold. Clandestine hacker forums are crawling with ads offering Facebook account IDs and passwords in exchange for money. In the cyber world, information is a valuable thing.

2. Commandeering Accounts
A more direct form of identity theft, commandeering occurs when the criminal logs on to an existing user account using an illegally obtained ID and password. Once they are online, they have the victim’s entire friend list at their disposal and a trusted cyber-identity. The impostor can use this identity for a variety of confidence schemes, including the popular, London scam in which the fraudster claims to be stranded overseas and in need of money to make it home. The London scam has a far-higher success rate on Facebook — and specifically on commandeered accounts — because there is a baseline of trust between the users and those on their friends list.

3. Profile Cloning
Profile cloning is the act of using unprotected images and information to create a Facebook account with the same name and details of an existing user. The cloner will then send friend requests to all of the victim’s contacts. These contacts will likely accept the cloner as a friend since the request appears to be from someone they’re familiar with. Once accepted, the crook has access to the target’s personal information, which they can use to clone other profiles or to commit fraud. As Grayson Milbourne puts it, “Exploiting a person’s account and posturing as that person is just another clever mechanism to use to extract information.” Perhaps what’s scariest about this kind of crime is its simplicity. Hacking acumen is unnecessary to clone a profile; the criminal simply needs a registered account.

4. Cross-Platform Profile Cloning
Cross-platform profile cloning is when the cyber criminal obtains information and images from Facebook and uses them to create false profiles on another social-networking site, or vice versa. The principle is similar to profile cloning, but this kind of fraud can give Facebook users a false sense of security because their profile is often cloned to a social platform that they might not use. The result is that this kind of fraud may also take longer to notice and remedy.

5. Phishing
Phishing on Facebook involves a hacker posing as a respected individual or organization and asking for personal data, usually via a wall post or direct message. Once clicked, the link infects the users’ computers with malware or directs them to a website that offers a compelling reason to divulge sensitive information. A classic example would be a site that congratulates the victims for having won $1,000 and prompts them to fill out a form that asks for a credit card and Social Security number. Such information can be used to perpetrate monetary and identity fraud. Grayson Milbourne of Webroot, also explained that spearphishing is becoming increasingly common, a practice that uses the same basic idea but targets users through their individual interests.

6. Fake Facebook
A common form of phishing is the fake Facebook scam. The scammers direct users via some sort of clickable enticement, to a spurious Facebook log-in page designed to look like the real thing. When the victims enter their usernames and passwords, they are collected in a database, which the scammer often will sell. Once scammers have purchased a user’s information, they can take advantage of their assumed identity through apps like Facebook Marketplace and buy and sell a

laundry list of goods and services. Posing as a reputable user lets the scammer capitalize on the trust that person has earned by selling fake goods and services or promoting brands they have been paid to advertise.

7. Affinity Fraud
In cases of affinity fraud, con artists assume the identity of individuals in order to earn the trust of those close to them. The criminal then exploits this trust by stealing money or information. Facebook facilitates this type of fraud because people on the site often end up having a number of “friends” they actually do not know personally and yet implicitly trust by dint of their Facebook connection. Criminals can infiltrate a person’s group of friends and then offer someone deals or investments that are part of a scheme. People can also assume an identity by infiltrating a person’s account and asking friends for money or sensitive information like a Social Security or credit card number.

8. Mining Unprotected Info
Few sites provide an easier source of basic personal information than Facebook. While it is possible to keep all personal information on Facebook private, users frequently reveal their emails, phone numbers, addresses, birth dates and other pieces of private data. As security experts and hackers know, this kind of information is often used as passwords or as answers to secret security questions. While the majority of unprotected information is mined for targeted advertising, it can be a means to more pernicious ends such as profile cloning and, ultimately, identity theft.

9. Spam
Not all spam — the mass sending of advertisements to users’ personal accounts — is against the law. However, the existence of Facebook and other social sites has allowed for a new kind of spam called clickjacking. The process of clickjacking, which is illegal, involves the hacking of a personal account using an advertisement for a viral video or article. Once the user clicks on this, the program sends an advertisement to the person’s friends through their account without their knowledge. This has become such an issue for the social media giant that earlier this year that the company has teamed up with the U.S. Attorney General to try to combat the issue.

While police have for some time used social networking sites to identify and investigate suspected criminals, now criminals are using such sites to identify and investigate law enforcement officers, including undercover police. In addition, hostage-takers and suspects who barricade themselves in buildings are monitoring social media to track police movements in real time, and gang members are launching their own surveillance operations targeting police. Source http://www.foxnews.com/tech/2011/05/10/officials-warn-facebook-twitter-increase-police-vulnerability/

SENIOR police have warned officers that criminals are using Facebook and other social media to befriend them and tap into secret information. Officers have been told that cavalier use of social media puts members in danger of being tracked by criminals using "geo-tagging" technology.

In an address to members Supt Steve Gleeson said there was a risk of online networking among officers being used to "assess your vulnerabilities".

"Criminals have been known to use information gleaned from social media to engineer relationships with police for the purpose of securing access to law enforcement information or to compromise a member's integrity," he said. "Reckless social networking can literally put someone's life in danger. It could be yours, a relative's or another member's." http://www.heraldsun.com.au/news/law-order/criminalss-use-social-media-to-track-police/story-fni0fee2-1226675624831

Searching for Saddam: A five-part series on how the U.S. military used social networking to capture the Iraqi dictator.

By Chris WilsonUpdated Monday, Feb. 22, 2010, at 8:06 AM ET

Traffic had slowed to a crawl in Baghdad's Azamiyah district as drivers stopped to ogle the president. It was April 2003, and Saddam Hussein cheerily greeted his subjects as a few bodyguards tried to keep the crowd at bay. Someone handed Saddam a bewildered baby, which he hoisted up in the air a few times and handed back. When he reached a white sedan, Saddam climbed onto the hood to survey the sea of loyalists.

Not long after—possibly that same day, just a few miles away from where Saddam went on his celebratory walk—U.S. Marines in Baghdad tore down a 40-foot-tall bronze statue of the Iraqi dictator. At the time, American intelligence officers didn't know whether Saddam had survived a hailstorm of 2,000-pound bombs and Tomahawk missiles fired at the beginning of the war. When grainy footage of the Butcher of Baghdad's last promenade surfaced 10 days later, most analysts were preoccupied with determining whether it was authentic. Nobody was particularly worried about the guy next to the dictator, a heavyset man in a brown striped shirt and sunglasses. He wasn't anyone on the deck of playing cards depicting the regime's 55 most-wanted members, and the coalition troops had much bigger priorities than hunting down bodyguards.

It would be months before anyone realized that this man was the key to capturing Saddam Hussein. His identity was classified, but those on his trail would take to calling him "Fat Man."

The war in Iraq will always be remembered for the failures of intelligence that preceded it and the insurgency that bedeviled coalition forces long after President George W. Bush declared an end to major combat operations. Amid all that disaster, the capture of Saddam Hussein has become a forgotten success story. It's an accomplishment that wasn't inevitable. In a five-part series that begins today, I'll explain how a handful of innovative American soldiers used the same theories that underpin Facebook to hunt down Saddam Hussein. I'll also look at how this hunt was a departure in strategy for the military, why its techniques aren't deployed more often, and why social-networking theory hasn't helped us nab Osama Bin Laden.

In the war's early days, coalition forces raced through the deck of the cards. By May 1, 2003, when President George W. Bush stood beneath that infamous "Mission Accomplished" banner, 15 of the men on the cards had surrendered or been captured. Coalition troops bagged another 12 top targets in May, including one of Saddam's sons-in-law. But despite snagging all those high-profile detainees, the trail to Saddam—if he was alive—was not getting any warmer. And when the military did catch someone important, he usually wasn't much help.

Consider the case of Abid Hamid Mahmoud al-Khatab, Saddam's trusted personal secretary and the Ace of Diamonds. Abid, a ubiquitous presence behind the dictator in pre-war photos, had controlled access to Saddam during his years in power. Newspapers trumpeted his mid-June capture as the war's biggest feat. "Captured Iraqi May Know Fate of Saddam," the Associated Press declared. But hopes that Abid could lead the United States to Saddam were quickly dashed. The trusted aide, who some called "Saddam's Shadow," told interrogators he and Saddam's two sons had parted ways with the dictator a while back, after Saddam became convinced they could survive longer if they separated. This was bad news for the war effort for two reasons. First, if Abid was to be believed, Saddam Hussein was alive. Second, Saddam appeared not to be seeking protection from the men on the deck of cards. If the military was going to locate him, it would have to start from scratch. In searching for Saddam, the military was targeting the wrong people.

Saddam's personal secretaryThe deck of cards didn't help in the hunt of Saddam, very simply, because the cards had many of the wrong people on them. Virtually every single person in the deck, which was produced by the Defense Intelligence Agency, was a member of Saddam's regime. Many of the men on the lower-numbered cards were essentially middle managers, like the deputy head of the tribal affairs office

(Nine of Clubs) and the trade minister (Six of Hearts). While it was reasonable for these men, as government officials and members of the Baath party, to be on a wanted list, capturing them was neither going to cripple the budding insurgency or lead the American-led coalition to their former boss. Their power vanished the moment the regime collapsed and Iraq was once again governed by tribal networks. An extended catalog of hundreds more targets, known as the Black List, had similar inadequacies. While there were some valuable targets near the bottom of the list—men like the "Fat Man" who would prove central to the post-invasion insurgency—they were mixed in with people who were misidentified, completely innocent, or both.

So, why weren't Saddam's post-war cronies in the deck of cards? The war's architects had failed to account for the fact that Iraqi society functions completely differently than our own. Saddam's regime had been built on top of the country's ancient tribal traditions—a heritage that he either suppressed or tried to co-opt, depending on how much he needed the backing of the sheikhs at the moment. (As the *New York Times* wrote in a cautionary note two months before the invasion, tribes are the "ultimate swing voters in the brutal politics of the Middle East.") When Baghdad fell, the institutions of Saddam's regime fell along with it. Suddenly, the Baath Party regional chairmen—the guys that populated the bottom of the deck—lost any connection they once had to Saddam (unless they happened to be related to him).

Who should the coalition have been going after? A careful study of Iraq's tribal structure, particularly around the Tikrit region where most of Saddam's top men were from, would have uncovered an entirely different cast of troublemakers. Most were high-ranking bodyguards, many of them related to Saddam, who lived in opulent houses and farms outside Tikrit. Some had served in Saddam's alphabet soup of security forces, but their influence with the president derived from their personal connections, not the contents of their résumés.

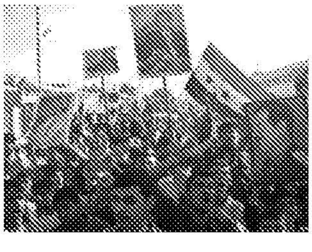
Information about Iraq's social fabric was easy to find before the war. In 1997, Iraq expert Amatzia Baram, now a professor at the University of Haifa, published perhaps the most influential paper on Saddam's tribal policies. The study described how, by the mid-1990s, Saddam had incorporated powerful tribal leaders into his government and granted them a certain autonomy, leading some of these sheikhs to overstep their authority. The paper got the attention of weapons inspectors as well as then-Iraqi U.N. representative Nizar Hamdun, who sent it to Baghdad. (Baram believes Saddam read it himself; about five weeks after the paper came out, Saddam issued a decree reasserting that the government's laws superseded tribal ones.)

Nor was there a scarcity of information on Saddam's peculiar personality. Jerrold M. Post, who formerly headed the CIA's Center for the Analysis of Personality and Political Behavior, published a long analysis of the dictator in 1991. From his youngest days, Post notes, Saddam was a consummate survivor who made sure to keep himself protected at all costs. When the war began, Saddam knew coalition forces were going after his top lieutenants; Post guesses that Saddam figured his odds of surviving were better if he ditched his government allies and went on the lam.

But to whom would he turn instead? Twenty-four years of murderous rule, punctuated by repeated coup attempts, had made Saddam understandably paranoid. "His conspiratorial mindset had wheels within wheels," Post says. Now that Saddam lacked the muscle to bully his associates into submission, he had to turn to those he felt he could trust most. As anyone familiar with *The Godfather* knows—and, as Post notes, Saddam was a huge fan of that film—in times of crisis one turns to family for trust and support.

If the deck of cards had been drawn up based on this understanding of how Saddam operated, it would have included the families in Tikrit who had strong ties to the regime. It's possible that even the fat man in the brown-striped shirt—the bodyguard tailing Saddam through the streets of Baghdad—would have made the cut. Even if Saddam and his sons had perished on the first day of the war, these were the kind of people who could carry on an insurgency in his stead.

On one point, however, the Americans guessed right. After Baghdad fell, Saddam went where he always did when he was in trouble. He went home.



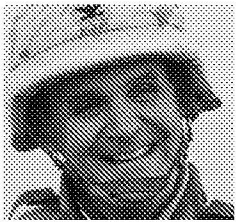
TikritThe nine months Saddam spent in the womb were devastating for his mother Sabha. First, her husband—a member of Tikrit's Majid family in the

Abu Nasir tribe—died, most likely of cancer. (Some accounts say he just disappeared.) A month before Saddam was born in 1937, her elder son died of cancer as well. According to one scholarly account, Saddam's mother went so far as to try to abort him before a Jewish family took her in and nurtured her to health. As soon as he was born, Saddam was sent to live with his mother's brother, Khayrallah Talfah Msallat, a radical Iraqi nationalist and the author of the charming pamphlet *Three Whom God Should Not Have Created: Persians, Jews, and Flies.*

Sabha would remarry a man named Ibrahim Hasan, with whom she would have three sons, Saddam's half-brothers. Saddam lived with them for several years before returning to his uncle, who would become his political mentor. Six decades after his unstable upbringing, Saddam would again bounce from house to house. The families that surrounded his childhood—Msallat, Hasan, Majid—would be the same ones he returned to as a man on the run.

There were two American units set up in Tikrit by the time Saddam reached his hometown. A small, secretive special operations team working out of one of Saddam's palaces focused on hunting down major fugitives. The much larger 1st Brigade Combat Team of the 4th Infantry Division was in charge of maintaining peace and stability in the entire Tikrit region. Catching Saddam would be a large step in that direction, but it was never explicitly part of the 1st BCT's mission.

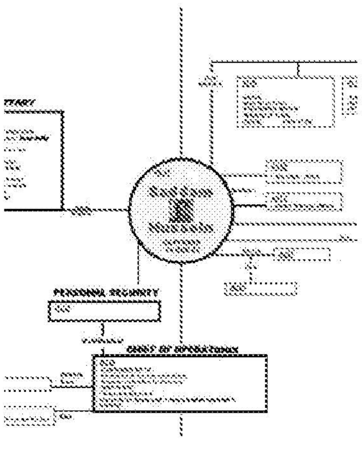
By June, insurgent attacks began to pick up speed and ferocity. Bradley Fighting Vehicles were struck by RPGs and a brazen attack on a military building left 19-year-old military police officer Pfc. Jesse Halling dead. The worst seemed yet to come. The Republican Guard in the area had not engaged with coalition troops during the first phase of the war, leaving abundant supplies of weapons and people willing to use them.



In mid-June, Col. James Hickey took command of the 1st BCT and prepared for a major series of raids, known as Operation Desert Scorpion. Hickey's goal was not simply to kill or capture as many insurgents as possible. The archetypal warrior-scholar, Hickey holds advanced degrees in diplomacy, public policy, and Russian. "War is a thinking man's game," he told me in his office at the Pentagon. This war effort, Hickey emphasized to his troops, was foremost about reconnaissance: Who were all these insurgents, and where were they coming from?

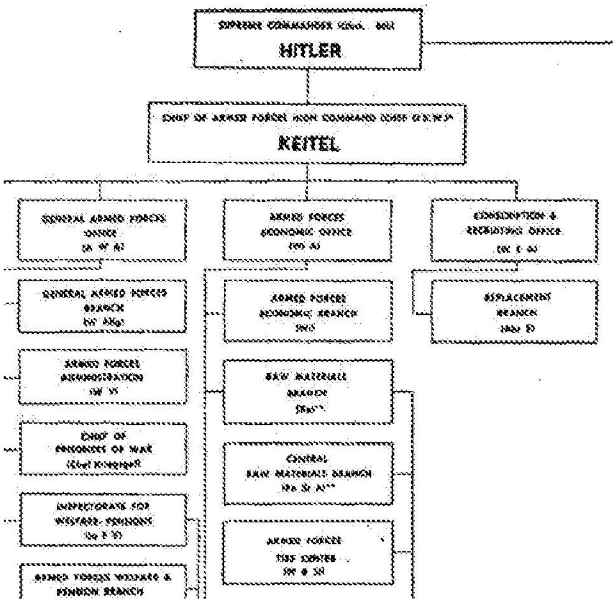
Diagnosing the insurgency in these early stages proved close to impossible. While the 1st BCT's intelligence shop had gathered a great deal of information about individual bad guys, nobody had put it together into a coherent picture. Hickey wasn't pleased. What he needed, the colonel told his intelligence officer, Maj. Stan Murphy, was a chart that showed the personal relationships of everyone they captured or wanted to capture.

This chart would become a social network diagram of the bad guys in Tikrit. The lines connecting their faces delineated who belonged to which of several influential families, how those families were intertwined by marriage, and who among them connected directly to Saddam Hussein. As Desert Scorpion continued over the next several months, the diagrams ballooned into sprawling networks. They showed no explicit hierarchy since none existed. Unlike in a traditional organizational chart, The Butcher of Baghdad was not at the top of this diagram. He was at the center, a yellow dot labeled "Saddam Hussein."



This shift in thinking about how the enemy organized itself was a long time coming in the Army. Through World War II, the U.S. military was accustomed to fighting an enemy structured like we are, making combat a clash of egos between generals. Prof. David Segal, an expert on military sociology at the University of Maryland, recalls the scene in *Patton* when the general, having beaten back a Panzer division, reacts angrily when he is informed that his archrival Erwin Rommel was not present due to "severe nasal diphtheria." While that brand of warfare might be 65 years old, Segal maintains that the American military perpetually refights "the last war we liked." In that model, the enemy is always organized in a hierarchy, like in this 1945 organizational chart of the Nazi military from a contemporary U.S. handbook.

Modes of warfare have evolved since 1945, of course, but the vertical image of the enemy has persisted. Part of the trouble is that, until very recently, soldiers received very little exposure to sociology—a subject that views a group of people more like a blob or a network than a totem pole. As *Joint Forces Quarterly* laid out in a 2005 article (PDF), the military had almost none of this in its curriculum at the time of the Iraq invasion. Most of the soldiers I spoke with said they had little or no formal training in network theory—they built their social networks by instinct, moving around the faces when intelligence revealed an unknown connection. (It didn't hurt, though, that one influential officer—Maj. Brian Reed, who we'll meet in the second part of the series tomorrow—had a masters degree in sociology.)



The Fat ManSocial networks have two fundamental units, *nodes* and *edges*. In a visualization of one's Facebook friends, for example, every node would be a person and every edge would indicate a friendship. (Incidentally, Saddam was captured about three months before Facebook was founded.) In a network of your friends, you'd be at the center—everyone would be connected to you. Of course, everyone would not be connected to everyone else. Your friends from school would exist in one highly connected clique, your friends from work in another. There would also be some unexpected connections; perhaps a co-worker went to high school with a friend from college. (You can see a visualization of your Facebook friends here.)

What Hickey was looking for were those unexpected connections—surprising bonds that might eventually lead to Saddam Hussein. As the Saddam social network came together, it started looking a lot like the New York Mafia. There were five families in Tikrit with close ties to Saddam's operation: the Hasans, Majids, Musslits, Hadooshis, and Heremoses. It was this network, as well as a similar one maintained by the special operations forces in the area, that would eventually lead them to the "Fat Man," and from there to Saddam. To get there, they were going to have to start banging down doors. The remaining four parts can be read at t http://www.slate.com/articles/news_and_politics/searching_for_saddam/2010/02/searching_for_saddam_5.single.html

Top 15 Most Popular Social Networking Sites | September 2013
http://www.ebizmba.com/articles/social-networking-websites

Here are the 15 Most Popular Social Networking Sites as derived from our *eBizMBA Rank* which is a constantly updated average of each website's Alexa Global Traffic Rank, and U.S. Traffic Rank from both Compete and Quantcast. *"*#*" Denotes an estimate for sites with limited Compete or Quantcast data.*

1 | Facebook
2 - eBizMBA Rank | **750,000,000** - Estimated Unique Monthly Visitors | 2 - Compete Rank | 2 - Quantcast Rank | 2 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

2 | Twitter
13 - eBizMBA Rank | **250,000,000** - Estimated Unique Monthly Visitors | 24 - Compete Rank | 5 - Quantcast Rank | 9 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

3 | LinkedIn
27 - eBizMBA Rank | **110,000,000** - Estimated Unique Monthly Visitors | 44 - Compete Rank | 23 - Quantcast Rank | 14 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

4 | Pinterest
31 - eBizMBA Rank | **85,500,000** - Estimated Unique Monthly Visitors | 42 - Compete Rank | 16 - Quantcast Rank | 36 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

5 | MySpace
84 - eBizMBA Rank | **70,500,000** - Estimated Unique Monthly Visitors | 51 - Compete Rank | 62 - Quantcast Rank | 138 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

6 | Google Plus+
95 - eBizMBA Rank | **65,000,000** - Estimated Unique Monthly Visitors | *NA* - Compete Rank | *NA* - Quantcast Rank | *NA* - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

7 | DeviantArt
183 - eBizMBA Rank | **25,500,000** - Estimated Unique Monthly Visitors | 346 - Compete Rank | 74 - Quantcast Rank | 130 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

8 | LiveJournal
303 - eBizMBA Rank | **20,500,000** - Estimated Unique Monthly Visitors | 605 - Compete Rank | 203 - Quantcast Rank | 102 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

9 | Tagged
315 - eBizMBA Rank | **19,500,000** - Estimated Unique Monthly Visitors | 447 -

Compete Rank | 217 - Quantcast Rank | 282 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

10 | Orkut
350 - eBizMBA Rank | **17,500,000** - Estimated Unique Monthly Visitors | *NA* - Compete Rank | *NA* - Quantcast Rank | 156 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

11 | CafeMom
451 - eBizMBA Rank | **12,500,000** - Estimated Unique Monthly Visitors | 127 - Compete Rank | 82 - Quantcast Rank | 1,144 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

12 | Ning
456 - eBizMBA Rank | **12,000,000** - Estimated Unique Monthly Visitors | 617 - Compete Rank | 411 - Quantcast Rank | 339 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

13 | Meetup
621 - eBizMBA Rank | **7,500,000** - Estimated Unique Monthly Visitors | 838 - Compete Rank | 516 - Quantcast Rank | 509 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

14 | myLife
728 - eBizMBA Rank | **5,400,000** - Estimated Unique Monthly Visitors | 122 - Compete Rank | 391 - Quantcast Rank | 1,670 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA

15 | Ask.fm
957 - eBizMBA Rank | **4,300,000** - Estimated Unique Monthly Visitors | 1,769 - Compete Rank | NA - Quantcast Rank | 144 - Alexa Rank.
Most Popular Social Networking Websites | **Updated 9/3/2013** | eBizMBA
Related eBizMBA Articles