FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1441737-000

Total Deleted Page(s) = 140
Page 15 ~ b6; b7C; b7E;
Page 16 ~ b6; b7C; b7E;
Page 17 ~ b6; b7C; b7E;
Page 18 ~ b6; b7C; b7E;
Page 32 ~ b6; b7C; b7E;
Page 33 ~ b6; b7C;
Page 34 ~ b3; b6; b7C; b7D; b7E;
Page 35 ~ b7D; b7E;
Page 41 ~ b3; b6; b7C; b7D; b7E;
Page 42 ~ b6; b7C; b7D; b7E;
Page 43 ~ b6; b7C; b7D; b7E;
Page 44 ~ b6; b7C; b7D; b7E;
Page 45 ~ b6; b7C; b7D; b7E;
Page 46 ~ b6; b7C; b7D; b7E;
Page 47 ~ b6; b7C; b7D; b7E;
Page 48 ~ b6; b7C; b7D; b7E;
Page 49 ~ b6; b7C; b7D; b7E;
Page 50 ~ b6; b7C; b7D; b7E;
Page 51 ~ b6; b7C; b7D; b7E;
Page 52 ~ b6; b7C; b7D; b7E;
Page 53 ~ b6; b7C; b7D; b7E;
Page 54 ~ b6; b7C; b7D; b7E;
Page 55 ~ b6; b7C; b7D; b7E;
Page 56 ~ b6; b7C; b7D; b7E;
Page 57 ~ b6; b7C; b7D; b7E;
Page 58 ~ b6; b7C; b7D; b7E;
Page 59 ~ b6; b7C; b7D; b7E;
Page 60 ~ b6; b7C; b7D; b7E;
Page 61 ~ b7D; b7E;
Page 62 ~ b3; b6; b7C; b7D; b7E;
Page 63 ~ b6; b7C; b7D; b7E;
Page 64 ~ b6; b7C; b7D; b7E;
Page 65 ~ b6; b7C; b7D; b7E;
Page 66 ~ b6; b7C; b7D; b7E;
Page 67 ~ b7D; b7E;
Page 68 ~ b3; b6; b7C; b7D; b7E;
Page 69 ~ b6; b7C; b7D; b7E;
Page 70 ~ b6; b7C; b7D; b7E;
Page 71 ~ b6; b7C; b7D; b7E;
Page 72 ~ b6; b7C; b7D; b7E;
Page 73 ~ b6; b7C; b7D; b7E;
Page 74 ~ b6; b7C; b7D; b7E;
Page 75 ~ b6; b7C; b7D; b7E;
Page 76 ~ b6; b7C; b7D; b7E;
Page 77 ~ b6; b7C; b7D; b7E;
Page 78 ~ b6; b7C; b7D; b7E;
Page 79 ~ b6; b7C; b7D; b7E;
Page 80 ~ b6; b7C; b7D; b7E;
Page 81 ~ b6; b7C; b7D; b7E;
Page 82 ~ b6; b7C; b7D; b7E;
Page 83 ~ b6; b7C; b7D; b7E;
Page 84 ~ b6; b7C; b7D; b7E;
Page 85 ~ b6; b7C; b7D; b7E;
Page 86 ~ b6; b7C; b7D; b7E;
Page 87 ~ b6; b7C; b7D; b7E;
Page 88 ~ b6; b7C; b7D; b7E;
Page 89 ~ b6; b7C; b7D; b7E;
Page 90 ~ b6; b7C; b7D; b7E;
Page 91 ~ b6; b7C; b7D; b7E;
Page 92 ~ b6; b7C; b7D; b7E;
Page 93 ~ b6; b7C; b7D; b7E;
Page 94 ~ b6; b7C; b7D; b7E;
Page 95 ~ b6; b7C; b7D; b7E;
Page 96 ~ b7D; b7E;
Page 97 ~ b3; b6; b7C; b7D; b7E;
Page 98 ~ b6; b7C; b7D; b7E;
Page 99 ~ b6; b7C; b7D; b7E;

Page 100 ~ b6; b7C; b7D; b7E;
Page 101 ~ b6; b7C; b7D; b7E;
Page 102 ~ b6; b7C; b7D; b7E;
Page 103 ~ b6; b7C; b7D; b7E;
Page 104 ~ b6; b7C; b7D; b7E;
Page 105 ~ b6; b7C; b7D; b7E;
Page 106 ~ b6; b7C; b7D; b7E;
Page 107 ~ b6; b7C; b7D; b7E;
Page 108 ~ b6; b7C; b7D; b7E;
Page 109 ~ b6; b7C; b7D; b7E;
Page 110 ~ b6; b7C; b7D; b7E;
Page 111 ~ b7D; b7E;
Page 112 ~ b3; b6; b7C; b7D; b7E;
Page 113 ~ b6; b7C; b7D; b7E;
Page 114 ~ b6; b7C; b7D; b7E;
Page 115 ~ b6; b7C; b7D; b7E;
Page 116 ~ b6; b7C; b7D; b7E;
Page 121 ~ Duplicate;
Page 122 ~ b3; b6; b7C; b7D; b7E;
Page 123 ~ b6; b7C; b7D; b7E;
Page 124 ~ b6; b7C; b7D; b7E;
Page 125 ~ b6; b7C; b7D; b7E;
Page 126 ~ b6; b7C; b7D; b7E;
Page 127 ~ b6; b7C; b7D; b7E;
Page 128 ~ b6; b7C; b7D; b7E;
Page 129 ~ b7D; b7E;
Page 130 ~ b3; b6; b7C; b7D; b7E;
Page 131 ~ b6; b7C; b7D; b7E;
Page 132 ~ b6; b7C; b7D; b7E;
Page 133 ~ b6; b7C; b7D; b7E;
Page 134 ~ b6; b7C; b7D; b7E;
Page 135 ~ b6; b7C; b7D; b7E;
Page 136 ~ b6; b7C; b7D; b7E;
Page 137 ~ b6; b7C; b7D; b7E;
Page 138 ~ b6; b7C; b7D; b7E;
Page 139 ~ b6; b7C; b7D; b7E;
Page 140 ~ b6; b7C; b7D; b7E;
Page 141 ~ b6; b7C; b7D; b7E;
Page 142 ~ b6; b7C; b7D; b7E;
Page 143 ~ b6; b7C; b7D; b7E;
Page 144 ~ b6; b7C; b7D; b7E;
Page 145 ~ b6; b7C; b7D; b7E;
Page 146 ~ b6; b7C; b7D; b7E;
Page 147 ~ b6; b7C; b7D; b7E;
Page 148 ~ b6; b7C; b7D; b7E;
Page 149 ~ b6; b7C; b7D; b7E;
Page 150 ~ b6; b7C; b7D; b7E;
Page 151 ~ b6; b7C; b7D; b7E;
Page 152 ~ b6; b7C; b7D; b7E;
Page 153 ~ b6; b7C; b7D; b7E;
Page 154 ~ b7D; b7E;
Page 155 ~ b3; b6; b7C; b7D; b7E;
Page 156 ~ b6; b7C; b7D; b7E;
Page 157 ~ b3; b6; b7C; b7D; b7E;
Page 158 ~ b6; b7C; b7D; b7E;
Page 159 ~ b3; b6; b7C; b7D; b7E;
Page 160 ~ b7D; b7E;
Page 161 ~ b3; b6; b7C; b7D; b7E;
Page 162 ~ b6; b7C; b7D; b7E;
Page 163 ~ b3; b6; b7C; b7D; b7E;
Page 164 ~ b6; b7C; b7D; b7E;
Page 165 ~ b7D; b7E;
Page 166 ~ b3; b6; b7C; b7D; b7E;
Page 167 ~ b6; b7C; b7D; b7E;
Page 168 ~ b6; b7C; b7D; b7E;
Page 169 ~ b6; b7C; b7D; b7E;
Page 170 ~ b3; b6; b7C; b7D; b7E;
Page 171 ~ b6; b7C; b7D; b7E;
Page 172 ~ b3; b6; b7C; b7D; b7E;
Page 173 ~ b6; b7C; b7D; b7E;
Page 174 ~ b3; b6; b7C; b7D; b7E;
Page 175 ~ b3; b6; b7C; b7D; b7E;
Page 176 ~ b6; b7C; b7D; b7E;

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

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 06/20/2011

To: Cyber   **Attn:** CCS / CCU1
                                         UC   b6
                                         SSA   b7C
                                         SSA
                         Attn: InfraGard Program
                         Attn: CCS / CIRFU
                                         UC
                                         SSA

   New Haven   **Attn:** SA
                                         SA
                                         SA

From: New Haven
      Squad 10
      Contact: SA   b6
                                                                          b7C
Approved By: b7E

Drafted By:
                                                                          b3
Case ID #:   b7E

Title: Unsub(s);
      aka #AntiSec;
      aka Anonymous;
      aka LulzSec;
      General Electric - Victim;
      InfraGard Connecticut - Victim;
      Recol - Victim;
      06/2011
      CIP - Organized Criminal Activities

Synopsis: Open and assign case and investigative sub-files.

Full Investigation Initiated: 06/20/2011

Details: During the week of 06/10/2011, New Haven became aware
of a series of computer network attacks that were carried out by   b3
                                                                          b7E

UNCLASSIFIED

FULL 6/21/11
OPEN (REOPEN) CASE _____ DATE 6-20-2011
SOURCE 9 (1-15) 14
CPI CODE: LEVEL 1 NTP LEVEL 2/3/4 CRINT
PI FULL/ENTERPRISE:
BEGIN: 6-20-2011   DEADLINE: _____
SUPV _____ AGENT _____   b6
      To SA   b7C

170____ b1. WPD

To: Cyber   From: New Haven
Re: [ ]   06/20/2011   /   b3
                                                                              b7E

the group known as Anonymous aka LulzSec aka #AntiSec. A case is
hereby opened to investigate the group and sub-files are hereby
opened to contain information specific to the different group
names that are being used.

Sub-file [ ]

          On 06/19/2011, a file titled "Operation Anti-Security"
was posted at "http://pastebin.com/9KyA0E5v" announcing the
collaboration of the Hacktivist groups known as LulzSec and
Anonymous on Operation Anti-Security aka #AntiSec. The posting
was addressed to "Lulz Lizards" and signed "Lulz Security,
http://LulzSecurity.com/". The posting contained the following
text (in part):

"Welcome to Operation Anti-Security (#AntiSec) - we encourage any
vessel, large or small, to open fire on any government or agency
that crosses their path. We fully endorse the flaunting of the
word "AntiSec" on any government website defacement or physical
graffiti art. We encourage you to spread the word of AntiSec far
and wide, for it will be remembered. To increase efforts, we are
now teaming up with the Anonymous collective and all affiliated
battleships."

"Top priority is to steal and leak any classified government
information, including email spools and documentation. Prime
targets are banks and other high-ranking establishments."

The posting contained several supporting links including
"http://anonyops.com/". The website
"http://anonops.blogspot.com/" contained a link to the Twitter
account "http://twitter.com/#!/anonops", which contained the
following posting:

"http://twitter.com/#!/anonops/status/81794348626345984":
"AnonOps
anonops AnonOps
Attention #Media: about #Lulzsec and #Anonymous, we are not at
war. We are bros of the internetz. Also, /b/ != Anonymous.
17 Jun"

Additionally, the referenced website, "http://lulzsecurity.com/"
contained a link to the Twitter account
"http://twitter.com/#!/LulzSec", which contained the following
posting:

To: Cyber   From: New Haven
Re: [   ]   06/20/2011   b3
                                                              b7E

"http://twitter.com/#!/LulzSec/status/82667686647177216":
"The Lulz Boat
LulzSec The Lulz Boat
#AntiSec begins today: pastebin.com/9KyA0E5v Prepare yourselves.
Join us, join #Anonymous, join the fleet - become a lulz lizard.
15 hours ago"

Sub-file [   ]

   On 06/20/2011, [   ] **(PROTECT IDENTITY)**,   b6
[   ]   b7C
[   ] contacted SSA [   ] via telephone and   b7D
advised GE experienced a distributed denial of service attack
(DDoS) against several Internet web sites owned by GE, to include
"HTTP://WWW.GE.COM". The DDoS attack began on 06/18/2011 and
continued until 06/19/2011. The GE web sites and GE applications
were impacted but not completely shut down as a result of the
attack. [   ] further advised that members of a computer
hacker group called "Anonymous" claimed responsibility for the
DDoS attack and posted several videos to HTTP://www.youtube.com
demonstrating that they utilized a software program called "Low
Orbit Ion Cannon" to conduct the DDoS attack. The members of
Anonymous claimed they conducted the attack because GE
manufactures Nuclear Power plants which are harmful to the
environment. The attack also impacted several customers of the
Internet Service Provider that hosts GE's web sites because the
attack reduced the amount of available Internet bandwidth at the
service provider's facility.

Sub-file [   ]   b3
                                                                          b7E

   On 06/17/2011, a server computer housing member data
for members of InfraGard Connecticut was compromised via an SQL
injection attack and it appears that a copy of the member
database was made. The database included member names, addresses
[   ], telephone numbers, fax
numbers, e-mail addresses, and randomly generated passwords
linked to the e-mail addresses. The attack was conducted from IP
address [   ] between 17:59 EDT and 18:37 EDT. LulzSec   b7E
claimed responsibility for the attack via Twitter posts.

   There is sufficient probable cause that an unauthorized
computer intrusion was conducted against the Connecticut
InfraGard site and a DDoS attack was conducted against GE sites,
therefore, New Haven will imitate a FULL investigation and open
the referenced case and sub-files.

To: Cyber   From: New Haven
Re: [   ] 06/20/2011

b3
b7E

LEAD(s):

Set Lead 1:   (Info)

CYBER

AT CCU1, DC

For your information. Please pass to the InfraGard
Program as well.

Set Lead 2:   (Info)

CYBER

AT CIRFU, DC

For your information.

Set Lead 3:   (Info)

NEW HAVEN

AT NEW HAVEN, CT

For your information.

◆◆

From Case ID :   Documents . : 12   b3
To Case ID . :   Last Serial : 24   b7E

Old Serial New Serial FIF

Old Serial	New Serial	FIF
12	36	
11	35	
10	34	
9	33	
8	32	
7	31	
6	30	
5	29	
4	28	
3	27	
2	26	
1	25	

Total Documents Consolidated :   12

****** Statistical Information from Universal Index *****

       Old Case ID   :   b3

Old Case ID	:		b3
New Case ID	:		b7E
Mains	:	1	
References	:	5	
Total records processed:		6	

b3
b7E

Case ID: [   ]

NH	1	EMAIL FROM NYO SA [ ] TO SA [ ] ON 6/21/11	
NH	2	DATABASE CHECKS, PHOTO OF HOME, NCIC REPORTS	
NH	3	[ ]	

b6
b7C

b7E

FD-340a (Rev. 5-9-05)

(Title)

(File No.)

Item	Date Filed	To be returned			Disposition
		Yes	No		

See attached printout

FD-340 (Rev. 4-11-03)

File Number _____

Field Office Acquiring Evidence _NH_____

Serial # of Originating Document _2_____

Date Received _6/21/2011_____

From _____
(Name of Contributor/Interviewee)

_____
(Address)

_____
(City and State)

By _SA_ [_____]

To Be Returned ☐ Yes   ☑ No
Receipt Given   ☐ Yes   ☑ No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
                 ☐ Yes   ☑ No
Federal Taxpayer Information (FTI)
                 ☐ Yes   ☑ No

Title: UNSUB(s);
          aka # AntiSec
          aks Anonymous
          aka LulzSec
          InfraGard - Victim

Reference: _____
(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of [____]

E-mail from N/O SA [____] to SA [____]

on 6/21/2011

_____

_____ (NH)(FBI)

From: _____(NY) (FBI)
Sent: Tuesday, June 21, 2011 8:26 AM
To: _____(NH) (FBI);_____(CYD) (FBI)
Cc: _____(NH)(FBI);_____(NH) (FBI)
Subject: RE: Anon/Lulzsec --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==

Hey Guys,

We will quiz our CHS more today regarding infragard.

This is what I know from the CHS:

I can explain more over the phone if one of you guys want to give me a call today.

Thx.

From: _____(NH) (FBI)

Sent: Monday, June 20, 2011 5:27 PM
To: _____(NY) (FBI);_____(CYD) (FBI)
Cc: _____(NH)(FBI);_____(NH) (FBI)
Subject: FW: Anon/Lulzsec --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==

[___]I've been informed that your CHS may have information regarding a recent intrusion by LulzSec against the CT InfraGard web site. New Haven is also looking into a DDoS attack against General Electric that was conducted by Anonymous on June 18-19. I would appreciate any information that you are able to provide.

[___]can you please add the following New Haven Agents to the sharepoint site:

SA[_____]
SA[_____]
SA[_____]
SA[_____]
SA[_____]

Thanks!

[_____]
Supervisory Special Agent
FBI New Haven

1

From: [ ] (CYD) (FBI)
Sent: Monday, June 20, 2011 5:17 PM
To: [ ] (NH) (FBI)
Subject: Anon/Lulzsec --- UNCLASSIFIED/~~FOUO~~

Classification: UNCLASSIFIED/~~FOUO~~
==

[ ]

A NY CHS has reporting relevant to your InfraGard intrusion. Contact [ ] for more information on the target and the reporting.

I will add you to [ ]

We have a weekly conference call scheduled for 3pm on Friday for all divisions with a case. I will forward the call information to you.

Let me know if you have any questions.

-[ ]

SSA [ ]
CyD/CCS/CCU-1 PAT-3
[ ] (Office)
[ ] (Mobile)
[ ] (Facsimile)
(U) [ ]

==
Classification: UNCLASSIFIED/~~FOUO~~

==
Classification: UNCLASSIFIED/~~FOUO~~

==
Classification: UNCLASSIFIED/~~FOUO~~

Universal Case File Number _____

Field Office Acquiring Evidence _____ *NH* _____ b3

b7E

Serial # of Originating Document _____

Date Received _____ *1/04/11* _____

From _____ b6

(Name of Contributor) b7C

_____

(Address of Contributor)

_____

(City and State)

By _____ *SA* _____

To Be Returned ☐ Yes ☐ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference: _____

(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

b7E

_____

_____

_____

b3
b7E

File Number

Field Office Acquiring Evidence _BA_

Serial # of Originating Document _10_

Date Received _07/15/2011_

From _____
(Name of Contributor/Interviewee)

_____
(Address)

_____
(City and State)

By _SA_

b6
b7C

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: UNSUB(S);
General Electric - VICTIM;
CIP - Organized Criminal Activities

Reference: _EC dated 07/13/2011_
(Communication Enclosing Material)

_____

Description: ☐ Original notes re interview of

Database checks, Photo of home, NCIC reports.

Reference: 038N000016
Msg Key : RR
Date/Time: 20110701090613581
Source   : NLI1

038N000016.NLI1.RR.20110701090613581.
RR.CTLIC0000.LEBI.
Response To: 11
RR.CTLIC0000
06:06 07/01/2011 13014
06:06 07/01/2011 11415 MDFBIBA00
*MRID51KDU1
TXT

VIN/1J4GW48S21C508975
VYR/01   VMA/JEEP   VMO/GRAND CH   VST/SUV   VCO/BLU
MRI 951202 IN: NLI1 10588 AT 01JUL11 09:06:13
OUT at 01JUL11 09:06:13 LEBI 21

****

b6
b7C

Reference: 038N00001D
Msg Key : RR
Date/Time: 20110701090652310
Source   : NLI1

038N00001D.NLI1.RR.20110701090652310.
RR.NYDMVNY00.LEBI.
Response To: 13
RR.NYDMVNY00
06:06 07/01/2011 88678
06:06 07/01/2011 11434 MDFBIBA00
*MRID51KE46
TXT
*** REGISTRATION DETAILS ***
REGISTRATION ID: [ ]
VEHICLE REGISTRATION EFFECTIVE DATE: 2010-09-30
VEHICLE REGISTRATION EXPIRATION DATE: 2012-10-25
REGISTRATION JURISDICTION CODE (LIS): NY
REGISTRATION STATUS: VALID

REGISTERED TO: [ ]
DATE OF BIRTH: [ ]
GENDER: [ ]
MAILING ADDRESS: [ ]

VEHICLE REGISTRATION PLATE ID: CCR9510
VEHICLE REGISTRATION PLATE TYPE: PASSENGER

*** VEHICLE DETAILS ***
VEHICLE ID: 3VWKB81HXVM030632
VEHICLE VINA: VOLK-GOL
VEHICLE MAKE TEXT: VOLKSWAGEN
VEHICLE MODEL YEAR: 1997
VEHICLE MODEL TEXT: GOLF
VEHICLE STYLE CODE: 4D
VEHICLE PRIMARY COLOR: RED

*** COMMERCIAL VEHICLE DETAILS ***
VEHICLE UNLADEN WEIGHT: 2456

*** INSURANCE DETAILS ***
INSURANCE CARRIER: LIBERTY MUTUAL FIRE INS

```
*** ADDITIONAL INFORMATION ***
FIELD NAME: License Plate Style Code
FIELD VALUE: EMPIRE
FIELD NAME: Same License Plate Indicator
FIELD VALUE: N
FIELD NAME: License Plate On The Road Date
FIELD VALUE: 2002-10-28
FIELD NAME: License Plate Logo
FIELD VALUE: EMPIRE
FIELD NAME: License Plate Legend
FIELD VALUE: PASSENGER

MRI 951424 IN: NLI1 10607 AT 01JUL11 09:06:52
OUT at 01JUL11 09:06:52 LEBI 24

*****************************************************************************
```

Reference: 038N00001K
Msg Key : MRR
Date/Time: 20110701090749603
Source   : MVA1

038N00001K.MVA1.MRR.20110701090749603.
MRR.MD002015V.LEBI.
Response To: 15
TXT
     QUERY FORMAT: LIC/☐   **b6**
                                                                              b7C

LIC.NO. STICKER EXPIRE KEY   TITLE   V.I.N.   YR MAKE ST EXCEPT
☐   12/12 A   42018517 4T1BG12K2TU905762   96 TOYT 4S N/A
GR.WGT: -3700   REG.FEE: $50.50   SUB:NO FR:
GR.COMB.WGT: 00N/A   RUSH: 5 VANITY:
INS.CO: GOVERNMENT EMPLOY INS CO   POLICY#: ☐

PREV.   PREV. *   V E H I C L E   *   I N S P E C T I O N
KEY   LIC. * EXPIRE DATE   STATUS   * DATE   STATUS
              032311   N   032311   K

OWNER OLN
☐   SUS.REV: NO   PRIVACY: YES   **b6**
NAME: ☐   RACE: ☐   WGT: ☐ SEX: ☐   **b7C**
ADDR: HGT: DOB:
CITY: COUNTY: ST: ZIP:

EFFECTIVE DATE   UNIT OF ORIGIN   CONTROL
    05/21/11   INSURANCE INQUIRY   - MVA
    05/21/11   INSURANCE INQUIRY   - MVA
    03/30/11   WARNING MAILED - VEIP   -   VE353
    04/22/11   TAGS SUSPENDED - VEIP   -   VE354
    05/21/11   COMPULSORY INS VIOLATION   - MVA   04825338
    05/21/11   INSURANCE INQUIRY   - MVA   04825338

FLAG:YES   SDX FLAG:YES

SERIAL-FLG/NONE

MRI 951827 IN: MVA1 15669 AT 01JUL11 09:07:49
OUT at 01JUL11 09:07:49 LEBI 27

Reference: 038N00001Q
Msg Key : MRR
Date/Time: 20110701090812130
Source   : MVA1

038N00001Q.MVA1.MRR.20110701090812130.
MRR.MD002015V.LEBI.
Response To: 16
TXT
    QUERY FORMAT: LIC/[   ]   b6
                                                                          b7C

LIC.NO. STICKER EXPIRE KEY   TITLE   V.I.N.   YR MAKE ST EXCEPT
[   ]12/12 M   35152321 2HKYF18563H612234   03 HOND TK N/A
GR.WGT: +3700   REG.FEE: $76.50   SUB:NO FR:
GR.COMB.WGT: 00N/A   RUSH: 5   VANITY: FLAG:NO   SDX FLAG:NO
INS.CO: GEICO GENERAL INS CO   POLICY#: [   ]

PREV. PREV. *   V E H I C L E   *   I N S P E C T I O N
KEY   LIC. * EXPIRE DATE   STATUS   * DATE   STATUS
              051612   N   051612   C01

OWNER OLN
[   ] SUS.REV: NO   PRIVACY: YES   b6
NAME: [   ]   RACE: [   ]   SEX: [   ] b7C
ADDR: [   ]   HGT: [   ]WGT:[ ]   DOB: [   ]
CITY: [   ]   COUNTY: ST:[ ] ZIP: [   ]

TITLE-FLG/NONE

LIEN HOLDER: AMERICAN HONDA FINANCE CORP
ADDR: PO BOX 6034   DATE: 2004-11-18
CITY: NEWARK   STATE: DE   ZIP: 19714

SERIAL-FLG/NONE

MRI 951956 IN: MVA1 15687 AT 01JUL11 09:08:12
OUT at 01JUL11 09:08:12 LEBI 30

****

```
Reference: 038N00001W
Msg Key  : MRR
Date/Time: 20110701090832113
Source   : MVA16


038N00001W.MVA16.MRR.20110701090832113.
MRR.MD002030V.LEBI.
Response To: 17
TXT
     QUERY FORMAT:    LIC[_____]                                          b6
                                                                          b7C
LIC.NO. STICKER EXPIRE KEY   TITLE       V.I.N.          YR  MAKE ST EXCEPT
[_____]04/12  A    40873686  1G1ZT51826F241850   06  CHEV 4S  N/A
GR.WGT: -3700          REG.FEE:   $50.50         SUB:NO  FR:
GR.COMB.WGT: 00N/A     RUSH: 5  VANITY:          FLAG:NO       SDX FLAG:NO
INS.CO:  GEICO GENERAL INS CO      POLICY#: [_____]

PREV.  PREV. *   V E H I C L E    *   I N S P E C T I O N
KEY    LIC.  * EXPIRE DATE      STATUS   *  DATE        STATUS
               103112            N          103112       O70


OWNER OLN
[_____]  SUS.REV: NO   PRIVACY: YES                           b6
  NAME: [_____]          RACE: [_____]     SEX: [_____]       b7C
  ADDR: [               ]          HGT: [      ]WGT:[  ] DOB: [       ]
  CITY: [_____]          COUNTY:       ST:[  ] ZIP: [_____]

TITLE-FLG/NONE

SERIAL-FLG/NONE




MRI 952061 IN: MVA16 02861 AT 01JUL11 09:08:31
OUT at 01JUL11 09:08:32 LEBI 33


****************************************************************************
```

Reference: 038N000022
Msg Key : MRR
Date/Time: 20110701090853380
Source   : MVA1

038N000022.MVA1.MRR.20110701090853380.
MRR.MD002015V.LEBI.
Response To: 18
TXT
       QUERY FORMAT: LIC/[   ]   b6
                                                                                 b7C

LIC.NO. STICKER EXPIRE KEY   TITLE   V.I.N.   YR MAKE ST EXCEPT
[   ] 02/12 A   36736525 WAULT68E93A179044   03 AUDI 4S N/A
GR.WGT: -3700   REG.FEE: $50.50   SUB:NO FR:
GR.COMB.WGT: 00N/A   RUSH: 5 VANITY: FLAG:YES   SDX FLAG:NO
INS.CO: GEICO GENERAL INS CO   POLICY#: [   ]

PREV. PREV. *   V E H I C L E   *   I N S P E C T I O N
KEY   LIC.   * EXPIRE DATE   STATUS   * DATE   STATUS
              071410   N   060910   K

OWNER OLN
[   ] SUS.REV: NO   PRIVACY: YES
NAME: [   ]   RACE: [   ]   SEX: [   ]
ADDR: HGT: [   ] WGT: [ ] DOB: [   ]
CITY: COUNTY: ST: [ ] ZIP: [   ]

CO-OWNER OLN   b6
[   ] SUS.REV: NO   PRIVACY: YES   b7C
NAME: [   ]   RACE: [   ]   SEX: [   ]
ADDR: HGT: [   ] WGT: [ ] DOB: [   ]
CITY: COUNTY: ST: [ ] ZIP: [   ]

EFFECTIVE DATE   UNIT OF ORIGIN   CONTROL
    07/21/10   WARNING MAILED - VEIP   -   VE353
    08/13/10   TAGS SUSPENDED - VEIP   -   VE354
    06/01/11   MONTGOMERY COUNTY POLICE   -SPEED CAMERA   8000
    06/01/11   MONTGOMERY COUNTY POLICE - MVA ADMIN FEE   8000

LIEN HOLDER: JP MORGAN CHASE BANK
ADDR: PO BOX 29214   DATE: 2006-02-11
CITY: PHOENIX   STATE: AZ   ZIP: 85038

SERIAL-FLG/NONE

MRI 952238 IN: MVA1 15737 AT 01JUL11 09:08:53
OUT at 01JUL11 09:08:53 LEBI 36

****

Reference: 038N000028
Msg Key : MRR
Date/Time: 20110701090915360
Source   : MVA1

038N000028.MVA1.MRR.20110701090915360.
MRR.MD002015V.LEBI.
Response To: 19
TXT
    QUERY FORMAT: LIC/☐   b6
                                                                             b7C

LIC.NO. STICKER EXPIRE KEY   TITLE   V.I.N.   YR MAKE ST EXCEPT
☐   M   41518653 5J6YH2H72AL003792   10 HOND SU N/A
GR.WGT: +3700   REG.FEE: $76.50   SUB:NO FR:
GR.COMB.WGT: 00N/A   RUSH: 5 VANITY: FLAG:YES   SDX FLAG:NO
INS.CO: STATE FARM MUTUAL AUTO   POLICY#:☐

PREV.   PREV. *   V E H I C L E   *   I N S P E C T I O N
KEY   LIC. * EXPIRE DATE   STATUS   * DATE   STATUS
            111412   N   111412

OWNER OLN
☐   SUS.REV: NO   PRIVACY: YES
  NAME: ☐   RACE: ☐   SEX: ☐
  ADDR: HGT: ☐   WGT: ☐ DOB:
  CITY: COUNTY: ST: ☐ ZIP:

CO-OWNER OLN   b6
☐   SUS.REV: NO   PRIVACY: YES   b7C
  NAME: ☐   RACE: -NA   SEX: ☐
  ADDR: HGT: ' " WGT:☐ DOB:
  CITY: COUNTY: ST: ☐ ZIP:

EFFECTIVE DATE   UNIT OF ORIGIN   CONTROL
    06/15/11   CITY OF BALTIMORE   - PARKING   1000
    06/29/11   CITY OF BALTIMORE   - MVA ADMIN FEE 1000

LIEN HOLDER: SUNTRUST CNSMR LENDING SVCS
ADDR: PO BOX 305053   DATE: 2010-05-13
CITY: NASHVILLE   STATE: TN   ZIP: 37230

SERIAL-FLG/NONE

MRI 952409 IN: MVA1 15763 AT 01JUL11 09:09:15
OUT at 01JUL11 09:09:15 LEBI 39

****

```
Reference: 038N00002E
Msg Key  : MRR
Date/Time: 20110701090941546
Source   : MVA1


038N00002E.MVA1.MRR.20110701090941546.
MRR.MD002015V.LEBI.
Response To: 20
TXT
    QUERY FORMAT:    LIC/[        ]                                        b6
                                                                          b7C

LIC.NO. STICKER EXPIRE KEY    TITLE       V.I.N.          YR  MAKE ST EXCEPT
[                    ] 10/11  ABY  38820684  JTDKB20U887697549   08  TOYT 4H  N/A
GR.WGT: -3700           REG.FEE:   $60.50         SUB:NO  FR:
GR.COMB.WGT: 00N/A   RUSH: 5  VANITY:             FLAG:NO      SDX FLAG:NO
INS.CO:  GOVERNMENT EMPLOY INS CO   POLICY#:[          ]


PREV.  PREV. *   V  E  H  I  C  L  E     *   I N S P E C T I O N
KEY    LIC.  * EXPIRE DATE       STATUS   *  DATE          STATUS
              041812              N          041812         C01


OWNER OLN
[                    ]   SUS.REV: NO   PRIVACY: YES
 NAME:[            ]              RACE:[       ]        SEX:[        ]
 ADDR:                            HGT:[     ] WGT:[ ]   DOB:[        ]
 CITY:                         COUNTY:        ST:[ ]   ZIP:[        ]

                                                                          b6
                                                                          b7C
CO-OWNER OLN
[                    ]   SUS.REV: NO   PRIVACY: YES
 NAME:[            ]              RACE:[       ]        SEX:[        ]
 ADDR:                            HGT:[     ] WGT:[ ]   DOB:[        ]
 CITY:                         COUNTY:        ST:[ ]   ZIP:[        ]

TITLE-FLG/NONE

SERIAL-FLG/NONE




MRI 952577 IN: MVA1 15789 AT 01JUL11 09:09:41
OUT at 01JUL11 09:09:41 LEBI 41


**************************************************************************
```

Reference: 038N00002W
Msg Key : MRR
Date/Time: 20110701091103361
Source   : MVA1

038N00002W.MVA1.MRR.20110701091103361.
MRR.MD002015V.LEBI.
Response To: 23
TXT
    QUERY FORMAT: LIC/⬜⬜⬜⬜   b6
                                                                  b7C

   VEHICLE TAG RECORD NOT FOUND

MRI 953186 IN: MVA1 15888 AT 01JUL11 09:11:03
OUT at 01JUL11 09:11:03 LEBI 50

****

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 06/21/2011

To: New Haven

From: New Haven
　　　　Squad 10
　　　　Contact: SA ⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚　　　　　　b6
　　　　　　　　　　　　　　　　　　　　　　　　　　　　b7C
Approved By: ⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚　　　　　　　b7E

Drafted By:

Case ID #: ⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚⬚　　　　　　　　b3
　　　　　　　　　　　　　　　　　　　　　　　　　　　　b7E

Title:　Unsub(s);
　　　　aka #AntiSec;
　　　　aka Anonymous;
　　　　aka LulzSec;
　　　　General Electric - Victim;
　　　　InfraGard Connecticut - Victim;
　　　　Recol - Victim;
　　　　06/2011
　　　　CIP - Organized Criminal Activities

Synopsis:　Open grand jury sub-file.

Details:　Open grand jury sub-file to contain information
requiring Rule 6(e) protection.

♦♦

UNCLASSIFIED

　　　　　　　　　　　　　　　　　　　　　　　　　　　　b3
　　　　　　　　　　　　　　　　　　　　　　　　　　　　b7E

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 06/29/2011

To: Baltimore   **Attn:** SSA [   ]
                                     CY-1

      Cyber   **Attn:** SSA [   ]
                                     SSA
                                     CCU-1

b6
b7C
b7E

From: New Haven
          Squad 10 / Cyber Crimes
          Contact: SA [   ]

Approved By:

Drafted By:

Case ID #: [   ]

b3
b7E

Title: UNSUB(S);
        a.k.a. #ANTISEC
        a.k.a. ANONYMOUS
        a.k.a. LULZSEC
        GENERAL ELECTRIC - VICTIM;
        INFRAGARD CONNECTICUT - VICTIM;
        RECOL - VICTIM;
        06/2011
        CIP - ORGANIZED CRIMINAL ACTIVITIES

Synopsis: To request investigative assistance from the Baltimore Division regarding a member of the hacktivist group LulzSec known as [   ].

b6
b7C

Full Investigation Initiated: 06/20/2011

Details: On 06/17/2011, the server housing the Connecticut InfraGard web site and member database was compromised via an SQL injection attack and it appears that a copy of the member database was made during the intrusion. The database included member names, addresses, telephone numbers, fax numbers, e-mail addresses and randomly generated passwords linked to the e-mail addresses. The attack was conducted from IP address [   ] between 17:59 EDT and 18:37 EDT.

b7E

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

b3
b7E

b6
b7C

To: Baltimore From: New Haven
Re: [   ] 06/29/2011

b3
b7E

On 06/19/2011, LulzSec claimed that they gained administrative access to www.reco1.com because the owner reused his password on the LulzSec Twitter page. In addition, LulzSec made several subsequent "tweets" on June 19, 2011 and claimed responsibility for breaking into the www.infragard-ct.org (InfraGard Connecticut) website via a simple SQLi attack and compromised 1000+ FBI affiliated members.

The writer had two conversations with NY Division SA [   ] regarding the Anonymous/LulzSec subject [   ] a.k.a. [   ]. SA [   ] informed the writer his CHS [   ]

b6
b7C
b7D

Based upon the information provided by the NY CHS, along with the LulzSec Twitter posts identifying the Internet Service Provider who hosted the CT InfraGard database and claiming responsibility for the intrusion, New Haven considers LulzSec/Anonymous member [   ] as the primary subject of its investigation of the InfraGard Connecticut computer intrusion.

As per an e-mail message received by the writer from Cyber Division SSA [   ] on 06/28/2011, the Cyber Division has developed profiles on the LulzSec organization's leadership. A person using the nickname [   ], believed to be [   ] [   ] has been identified as a participant in several of the attacks associated with Anonymous/LulzSec. Further research has identified the following two (2) addresses in the Baltimore Area Of Responsibility (AOR) as possibly associated with [   ]:

b6
b7C

Database checks revealed [   ]

b6
b7C
b7E

[   ] Open source database checks indicate that the [   ] are currently listed at that address.

To: Baltimore From: New Haven
Re: [   ] 06/29/2011   b3
                                                                          b7E

Database checks further revealed [   ]   b6
[   ]   b7C
                                                                      b7E
[   ] Open source database
checks indicate that [   ] is
listed at that address.

      New Haven respectfully requests Baltimore Division
to check relevant databases and conduct a spot check on the
aforementioned locations. If a residence is found at either
location, New Haven requests Baltimore to obtain any relevant
license plate data at the locations if possible [   ]   b7E
[   ]

To: Baltimore   From: New Haven
Re: [   ] 06/29/2011   b3
                                                                          b7E

LEAD(s):

Set Lead 1:   (Action)

BALTIMORE

AT BALTIMORE, MD

New Haven respectfully requests Baltimore Division to
check relevant databases and conduct a spot check at the
following locations:

[   ]   b6
                                                                          b7C

If a residence is found at either location, New Haven
requests Baltimore to obtain any relevant license plate data at
the locations if possible [   ]   b7E

[   ]

Set Lead 2:   (Info)

CYBER

AT CCU-1

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   **Date:** 07/15/2011

To: New Haven   **Attn:** SA [ ]
        Squad 10 / Cyber Crimes

        Cyber   **Attn:** SSA [ ]
                                             SSA [ ]
                                             CCU-1

From: Baltimore   b6
          CY-1   b7C
          Contact: [ ]   b7E

Approved By: [ ]

Drafted By: [ ]
                                                                   b3
Case ID #: [ ]   b7E

Title: UNSUB(S);
           a.k.a. #ANTISEC
           a.k.a. ANONYMOUS
           a.k.a. LULZSEC
           GENERAL ELECTRIC - VICTIM;
           INFRAGARD CONNECTICUT - VICTIM;
           RECOL - VICTIM;
           06/2011
           CIP - ORGANIZED CRIMINAL ACTIVITIES

Synopsis: To document lead coverage regarding a member of the
hacktivist group LulzSec known as [ ].

Reference: [ ]   b3
                                                                   b7E

Details: On July 15, 2011, the writer conducted database checks   b6
on the following addresses and reports the following information: b7C

    Address 1: [ ]

       Database checks provided the address to be rectified as
[ ]
This address is described as belonging to [ ]
[ ].

196[ ] 01. EC

b3
b7E

To: New Haven   From: Baltimore
Re: [   ] 07/15/2011

Address 2: [   ]

        Database checks lists ths address as belonging to an
individual named [   ] A Google Map image was obtained
of the residence and it reveals the residence to be a duplex.

        A surveillance was conducted at this address and it
was noted the main entrance of the home has two main entrances, a
door to the left and another door to the right with the house   b6
number appearing in between the two doors. Several registration   b7C
tags were recorded from vehicles parked on the sidewalk in the
vicinity of the residence:

[   ]
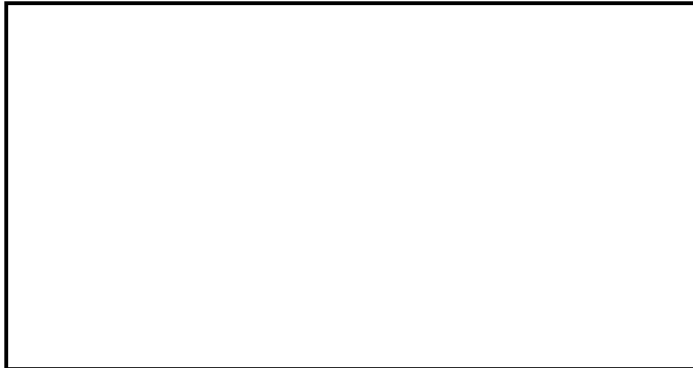
        Subsequent NCIC reports were requested from the tag
numbers listed above. Additionally, a [   ] report and a photo of   b7E
the residence have been obtained and were made part of the file
via 1A envelope.

        Baltimore considers this lead covered.

To: New Haven   From: Baltimore
Re: [   ] 07/15/2011

b3
b7E

Set Lead 1:   (Info)

NEW HAVEN

AT NEW HAVEN, CT

Read and clear.

Set Lead 2:   (Info)

CYBER

AT CCU-1, Washington D.C.

Read and clear.

◆◆

FEDERAL BUREAU OF INVESTIGATION

Date of transcription   07/07/2011

    The following investigative activity was conducted by the writer between July 7, 2011 and July 13, 2011:

Anonymous and Antisec propaganda is distributed by:

b6
b7C

Investigation on   07/07/2011   at   New Haven, Connecticut

File #

by   SA

188   01.302.wpd

Date dictated

b3
b7E

b6
b7C

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE   -   **Date:** 03/24/2011

To: New Haven

From: New Haven
       Cyber Squad 10
         Contact: SA   b6
                                                         b7C

Approved By: b7E

Drafted By:

Case ID #:

Title: COMPUTER INTRUSION - ANONYMOUS   b3
                                                           b7E

Synopsis: Request that a control file be opened as a repository for intelligence regarding the group Anonymous.

Details: A control file is needed for intelligence matters regarding the group Anonymous. Therefore, it is requested that a [ ] control file be opened and assigned.

♦♦

Control File 3/25/11
OPEN (_____)   CASE [ ]
ORIGIN ____11____ DATE 3-24-2011
SUPV [ ] _____ SECT 10 ____
1   2   3   4   5
O&A to SSA [ ] /Squad 10

                                                     b3
                                                     b7E
                                                     b6
                                                     b7C

FREEDOM

FIGHTER

ANONYMOUS

11db1d9e2d38b87ae903d0d9424c1857

Anonymous – The Über-Secret Handbook

Version 2.0
Date 20.02.11

DRAFT VERSION

contains Typos
contains <°-(-(-(-<
contains no (o) (o)
also, no 8====D
also, tl;dr & cocks

ANONYMOUS

Preface

The greatest threats to your safety are:

  I. Social engineering and your behavior - see Social Threats.

  II.Revealing your IP address - see Technical.

Try to follow as many of these suggestions as possible to ensure maximum privacy.

Social Threats

Basic rule: Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember, when in Rome, do as Romans do. Don't try to be a smart ass. Feds are many, Anonymous is Legion, but you are only one. Heroes only exist in comic books keep that in mind! There are no old heroes; there are only young heroes and dead heroes.

Do not give any personal information on the IRC chat as it is public, you mom could read what you write there and so could the Police. And don't mention your involvement with Anonymous in your real life.

DO NOT:

*Include personal information in your screen name.

*Discuss personal information, your address or where you're from.

*Mention your gender, tattoos, scars, piercings, body modifications, your weight or your physical and/or psychological capacities (got the idea?).

*Mention your profession or hobbies or involvement in other activist groups.

*Mention whether you're in a relationship.

*Musical tastes/preferred literature/films are good ways to know someone, don't mention any of those.

*Use special characters, which are existent only in your language, as they would reveal where you are from.

*Give even bogus info. Lot's of no's, make a yes.

*Blend anything from your real life with Anon, don't talk about Anonymous in real life except posting posters anonymously, etc.

*Mention congresses that you have been at, schools or universities, etc.

*Mention your time zone, this can reveal where you live.

*Connect at the same time regularly. Try to alternate.

*Post on the public net while you are in the IRC, and definitely do not mention that you are posting something on Twitter. This is easy to correlate. Stagger your login & log out times on FaceBook, Twitter & IRC. They can be compared for user info.

*Discuss whether you are personally DDoSing or writing How-To's or making graphics etc. or not, just discuss general strategy.

*Post pictures hosted on Facebook. The filename contains your profile ID.

Technical

Basic Rule: Use as many security layers as possible. The question is not whether you are paranoid, but whether you are paranoid enough?

A good start is to use a VPN and run Anonymous related Software from a USB device. A proxy will also do, but it is not as secure as a VPN.

Always use as many security layers as possible. Make sure to use them in the right way. If you don't know how to use them, learn first.

Most Anonymous' use VPN to hide their traces. They use SSL encrypted connections and #vhost when they are on irc.anonops.ru.

Portable Software

Portable software is a software which you can run from an USB drive, so that it leaves almost no traces on your computer.

* http://portableapps.com
* http://portableapps.com/apps/internet/firefox_portable
* http://portable-i2p.blogspot.com

When you join the Anonymous IRC network, do so only via SSL (point you IRC client to port 6697). Port 6697 is an unusual SSL port, just checking the "Always use SSL" box will not work, check for both.

After connection you can register your nickname by using a fake email address, then you join #vhost and AFTER that procedure you join the channels.

Make sure you start by launching I2P with the "I2P Launcher" button in the portable apps tray icon.

You can then use the integrated PChat client; it automatically connects to the I2P IRC server anonymously.
Join #anonops for to keep track of Anonymous activity. Many Operations channels are relayed between I2P and anonops.ru.

VPN

When thinking of a VPN service, think first about the legislation of the country. A USA VPN might provide user data upon warrant issue. In other countries such as Sweden and Iceland, this is unlikely to happen. They have a strong privacy policy, which makes it harder for law enforcement agencies to get access. In addition, some servers do not keep logs of users. Also try to get VPN services that accept anonymous payments (For those that keep user billing information)

More info:

https://secure.wikimedia.org/wikipedia/en/wiki/Vpn

Free VPNs -- **Not recommended.**
If they aren't selling you a service they are selling you.

* http://cyberghostvpn.com
* http://hotspotshield.com -- Occasionally hijacks your traffic to redirect you to advertisers.
* http://proxpn.com
* https://anonymityonline.org

* http://www.bestfreevpn.com
* http://www.your-freedom.net
* http://www.ultravpn.fr
* http://www.itshidden.com
* http://www.thefreevpn.com
* http://www.packetix.net

Commercial VPN providers

* http://www.swissvpn.net
* http://perfect-privacy.com
* https://www.ipredator.se
* http://www.anonine.se
* https://www.vpntunnel.se
* http://www.relakks.com
* http://www.steganos.com
* http://www.bananavpn.net   >   logs IPs
* http://www.strongvpn.com   >   logs IPs
* http://www.secureix.com
* http://www.secretsline.com

* http://www.findnot.com
* http://www.trackbuster.com
* http://www.vpngates.com
* http://www.perfect-privacy.com
* http://www.trilightzone.org
* http://www.vpnaccounts.com
* http://www.securstar.de
* http://www.witopia.net
* http://www.tiggerswelt.net
* http://www.xerobank.com > logs IPs

Extra info about VPNs

List September 2010 - (Korben source)

* http://itshidden.com - PPTP Vpn - 2 offers: Free and Premium ($ 12.99 / month - $ 24.99 / 3 months). Regarding free: there are regular disconnections every 20 minutes, the P2P is legal but inconceivable. The charge: Premium offers including improved speed for downloading, a static IP and port forwarding. The two options both offer direct access to a VPN secure and anonymous. Servers in the Netherlands in particular.

* http://www.bestfreevpn.com
* http://www.cyberghostvpn.com - OpenVPN - Installing a software house - 1 GB / month - off after 6h (reconnection possible) - no guarantee of flow
* http://www.peer2me.com - PPTP - Provides free and unlimited. French company banned = P2P in France. You can create a private community to share your data.
* http://www.hotspotshield.com/ - Software - U.S. servers, adds advertising on web pages. Firefox with adblock and found no ads. Note that you can use it with the public HotSpots New / SFR WiFi.
* http://www.ultravpn.fr/ Openvpn - Vpn free. - Server Lynanda France, the United States. P2P forbidden on this vpn.
* http://www.hideipvpn.com/ Hide - PPTP - VPN offering 100 free accounts beginning of each month. The paid version allows you to connect to openvpn. P2p is not allowed with this vpn.
* http://www.janusvm.com/ - JanusVM VPN Free (open source) and free. - Using VMware virtual machine and based on OpenVPN, Squid, Privoxy and TOR. An old but useful tutorial incompleted is available in French. - A VPN Hardware JanusPA called hardware-based brand Yoggie is also since 2009. P2P forbidden because of the philosophy TOR.

Payable VPNs:

* http://www.vpnfacile.fr - VPN - Site in French, without limits or quotas. The web's cheapest (and en) 5 € / month maximum, minimum flow guaranteed 5mb / s! 2048bits encryption and support very responsive!
* http://proxydaddy.net - OpenVPN / PPTP - quick access without limitations Europe and USA. Site and support in French and English.

* https: / / www.change-my-ip.com - OpenVPN, and PPTP VPN SSTP - From 5 € / month. Servers in the Netherlands, USA and UK. Support and French site. No logs, speed and unlimited tranfer.
* https://www.anti-hadopi.com - OpenVPN / PPTP / Routers - Website in french, no speed limits or transfer. The network is fast (the site a bit slow but certainly housed outside U.S.), IP access with Europe or USA for € 4.99 per month. Just the logo on the page worth visiting. Staff nice.
* http://s6n.org/arethusa/fr.html - OpenVPN Established by an association campaigning for freedom of expression.
* http://xangovpn.com/ - OpenVPN, 4.90 € per month with no speed limit, server in the Netherlands, no logs, SSL key-1024, open enrollment. XangoVPN supports Quadrature du Net qu'FDN well.
* http://fvpn.fr/ - OpenVPN, from € 1.35 per week with no speed limit, server in France, 4 ip changeable 24/24, private VPN creates for French, 2048 and encryption keys with AES- 256.Inscriptions still open.
* http://www.hidemynet.com/ - OpenVPN, L2TP and PPTP VPN using OpenVPN-AS - $ 5 per month is about 3.50 €. Servers in Germany, United Kingdom, Netherlands and USA
* https://www.ananoos.com/ - OpenVPN - from € 4.58 per month, registration reopened!
* http://ipjetable.net/ - PPTP Vpn - 15 € per quarter, closed Beta invitations.
* https://ConnectionVPN.com / en - OpenVPN - Site in French - about 4 € and 5 € per month, unlimited traffic and speed, Key of 2048 bits, a company registered in Greece, servers in Luxembourg, the Netherlands ...
* http://www.psilo.fr/ - OpenVPN - 4.50 € per month, servers outside of France (Europe or USA, your choice), P2P servers allowed on Europe, AES-256 encryption, open enrollment.
* http://www.IdealVPN.com/ - Site in French - PPTP Vpn - 4.90 € per month, unlimited volume and speed, open enrollment. Quality service for a small price. Servers in the Netherlands, Germany ...

* http://www.tonvpn.com - Site in French. SOCKS, PPTP VPN, OpenVPN - 4 to 13 € per month Discount over time. Allopass possible! Speed and unlimited traffic. Free trial of 3 days. Servers in France, Slovenia, Luxembourg, Bulgaria.
* https:// www.ipredator.se/ - PPTP Vpn - 149kr or 14.9 € for 3 months, open enrollment. Uses the network Relakks Sweden.
* https://www.relakks.com/?lang=en - PPTP Vpn - 149 SEK (about 15 €) per quarter, and 449 SEK (about 45 €) per year. Servers in Sweden.
* http://www.anonine.com/ - PPTP VPN, 40Kr or 4 € per month with no log and no speed limit, server in Sweden. Registration open.
* http://www.blackvpn.com/ - Vpn unlimited speed available with openvpn or pptp server choice in europe or the usa for 5 € a month or two for 10 € a month, entries open ..
* http://www.mullvad.net - OpenVPN - 5 € / month with 50 GB of traffic - Free Trial 3h - Company in Sweden, servers in the Netherlands in particular - Redirection of a port.
* http://unblockvpn.com - PPTP Vpn - $ 5 per month but only 2GB per day guaranteed.
* http://www.vpnboy.com - PPTP Vpn - $ 5 per month or about 3.5 € - Reviews free 7d.
* http://www.torrentfreedom.com/ - VPN is the only specially configured for P2P applications - and BitTorrent in particular. OpenVPN on all accounts and subscribers can use both public and private trackers. 2048-bit key that changes automatically every 20 minutes. $ 17 per month
* http://www.perfect-privacy.com - $ 24.95 per month with an additional setup fee of $ 10. The VPN also offers solutions with keys of 4096 bits: PPTP, OpenVPN, 4096 bit SSH-2, 4096-bit SSL / TLS, Squid Proxy, CGI Proxies, Servers and more ... all over the world. In the peak of the servers (usually between 7am and 11am)

subscribers are "encouraged" not to exceed 100GB per month. The rest of the time no limits. Anonymous payments possible (Liberty Reserve, Web Money, Cash ... and PaySafeCard).

* http://vpngates.com - $ 15/month. No setup fees. PPTP, L2TP IPSec VPN services.
* http://www.linkideo.com - PPTP - From 2 € to 10 € / month depending on connection speed and getting or not to open ports. Support friendly and responsive enough. Servers in the U.S., France, the Netherlands.
* http://www.flashvpn.com - Starting from $ 5/month for VPNs, and $ 8 for OpenVPN. Found in the forums of people screaming for the scam that VPN (payment and no account), so caution.
* http://www.purevpn.com - PPTP and L2TP/IPSec VPN. From $ 6 per month. Servers in the U.S., Britain, Germany and Canada. Dedicated IP VPN for $ 15/month. "There are no limits to our VPN service. However, we do not recommend using it for torrents and p2p in violation of copyright. "According to the administrator. Is it to cover themselves or to protect its bandwidth ...
* http://www.securenetics.com - From $ 9.49 per month to $ 39.45. Opportunity also to use the proxy only for $ 5.49 per month. A choice between the Secure Anonymous OpenSSH Proxy, OpenVPN, PPTP VPN, Socks Proxy, or HTTP proxy servers. An industry first to offer this variety of options. Free anonymous email included in all accounts. Servers in the U.S., Britain, Canada, Germany, Netherlands, Malaysia. Anonymous payments by Liberty Reserve, Pecunix, and PaySafeCard.
* http://vpnprivacy.com/ - PPPTP Vpn - $ 15/month, $ 5 for a week. Gladly accepts P2P (the owner says). Servers in the U.S. and Canada.
* http://www.smallvpn.com - From $ 19.95/month to $ 34.95 depending on the OpenVPN server (2048 bits)
* http://www.lamnia.co.uk/ * - From £ 6.5 per month. Servers in the U.S., Britain and Canada.

* http://vpnpronet.com/ - A nice selection of alternatives. Per month, $ 8, there is a good classic. At the time (10h, 20h etc. ..) handy when you will spend the weekend with friends and we do not want "" rot "their IP. Or as the limit of the bandwidth required
* https: / / www.cryptocloud.com/ - $ 17/month. 2048-bit key. Very reliable (a disconnection in six months). About once a week, your server output changes (transparently) so that your IP changes and it is also extra security. It's not always easy to install OpenVPN client type. This provides a vpn setup very simple, just enter the username and password. This vpn is very committed to the freedom of the internet worldwide. He collaborates with the Electronic Frontier Foundation and opened free accounts for militants threatened in their country. If you fear a VPN keeps your logs, this one is one of the safest.
* http://www.banana-vpn.info - PPTP and L2TP/IPSec Vpn - $ 15/month, $ 60 per semester. Servers in the U.S., Britain and Germany. "P2P and Other Illegal use it Not Allowed. Filesharing ports, protocols and sites are blocked. "Says the site in red.
* http://ivacy.com/ * - Price: 10 € / month, 25 € / 3 months, € 0.5 / 1Gb, 100 Mb free for testing - Payments: Paypal, Visa, MasterCard, Ukash - Connection: OpenVPN, PPTP, IPsec - Encryption: MPPE PPTP 128, IPSec ESP 3DES, AES-256 Firefox Extension, OpenVPN 2048bits RSA for authentication and Blowfish 128 for the data - Servers: Great Britain, Russia, United States (down at the moment, seems Is it because of the DMCA notices ...) - P2P: Port forward from 5 random ports, TCP and UDP-Bonus: Firefox Extension, usenet server, internal ivacy sites, utilities ivacy.
* http://www.drakker.com/ * - Price: 25 € / year, 1 week free evaluation - Data encryption via VPN to 1024 bits - certificates exchanged are unique to each user. Changing the IP address: IP address is replaced by that of Drakker servers. Servers in Great Britain, Netherlands, Sweden, Canada. Confidentiality: The network collects and Drakker do not have any data about its users. Portability: it takes is a username / password to use his account Drakker

worldwide. The network Drakker promotes freedom of expression and press freedom worldwide. He is a partner of Amnesty International, Reporters without Borders, and the project 'Enough' for Africa.

* http://www.yourprivatevpn.com - PPTP. Site in French, Price: 6 to 15 € per month free trial. Servers in Great Britain, Netherlands, United States. Changeable servers at each connection. Ideal for sites like hulu.com geo-limits, BBC iPlayer. Very reliable and has great speed.

Proxies

You may use them in conjunction with a VPN.

* http://www.freeproxies.org
* http://www.socks24.org
* http://www.samair.ru/proxy

How to IRC

Basic Rules:

Use SSL Port (in this case 6697). Always.

Use a #vhost. Always.

IRC is public, if don't want an information to be spread in public, don't give this information in the first place.

Ignore trolls. Always.

http://anonnews.org/help/en.html

General:

By connecting to SSL-Port 6697 your IRC-Client may give you a warning because the SSL-Certificate is self-signed. That is OK; you can trust the anonops' certificate.

*Nicknames:
Make sure to pick a good username. For Anonymous related activities it means: don't use a nickname that you already use in general or public online spots. This way you ensure that you won't be tracked down by a common username you use on your gamer profiles or other websites where you might have put real life related info.

*Vhost:
On Anonymous' IRC servers you can ask for a Vhost. Example (by default you will have a host based from you Internet service provider, something like this: `<mynick@theservicefrom.125.comcast.suck.net>` or a hash if you've logged by SSL (recommended): `<mynick@6969E1A1T1COCK152.69.IP>` After setting a desired vhost you could be identified as: `<mynick@myvhostRocks.org>` . Before you can enable your Vhost you first have to register a nickname so you can be identified when logging in on IRC. It's recommend that you take a look at the above link under (HOW TO IRC): `http://anonnews.org/help/en.html`

Requesting a vhost:

Now that you are logged in and have registered your nickname you can activate your Vhost.

Go to the channel #Vhost (`/join #vhost`), after joining the channel.

You can use the command `!vhost` which is used to activate your vhost.
You should use it like this:

```
!vhost [optional@]new.host.here
```

`!vhost` is the command, followed by the host name you want to use just as stated above.
Be aware to use at least 2 dots to separate 3 words. The first parameter optional@ speaks for itself its optional but I suggest you use it!

So a vhost command could look like this:
`!vhost middlefinger@the.corrupt.feds`
If everything is fine you should be kicked out of the channel, this is to prevent spam and other malicious use of the vhost.

Now if you try to look at your host you will still see your original host but this can only be seen by you, so don't panic. If you really want to know if it worked you could ask some one to whois you and get there feedback on what host you use!

Now that you have set your Vhost it will be activated as soon as you login to IRC on your registered nickname.
If you want to change your vhost, you will have to wait 3600 sec.
Also be aware that the vhost only account for the IRC network from anonops
Eventually you can directly ask for the vhost via command without getting in the
specific channel.

*Command:
/hs request vhost@hosthere

Explanation: this will avoid getting into the specific channel. But is not enough to get it
working. The vhost@ part is optional, the important part is the hosthere part.

Considering the previous explanation, use the following:
/hs request hosthere

*Command 2:
/hs on

Explanation: This will effectively activate the vhost.

Vhost Troubleshooting

Q: I have registered my vhost, but once I log in it doesnt activate.
A: Have you identified with your nick? You will only get your regular vhost back once your nick is correctly identified, redo step 2.

Q: I just changed my vhost but it wont apply, why?
A: You need to update your status, in order to make it fully working. Use this:
/msg nickserv update

*Output: HostServ- Your vhost of hosthere is now activated.
*Output: NickServ- Status updated (memos, vhost, chmodes, flags
Once you do that, you normally should have a fully functional vhost.

Basic list of IRC Commands

`/join #channelname`   Joins #channel

`/part`   Parts active #channel

`/query nick`   Opens private conversation with nick

`/msg nick <message>`   Sends <message> to nick

`/whois nick`   Displays info on nick

`/msg nickserv identify <password>`   Identifies your nick

`/ignore <nick>`   Ignore a troll

`/topic`   See the topic of a channel

`/list`   See a listing of available channels

Extended commands:

* http://www.ircbeginner.com/ircinfo/m-commands.html

Where to find current IRC information incase you can't connect:

* http://www.anonnews.org
* http://www.anonops.ru/?id=servers
* Facebook (search Anonymous, Operation Tunisia) http://www.anonnews.org/chat
* (Loads web based IRC client with current server info)

Security:

* Use SSL to connect to the IRC. Server port is 6697.
* Use VPN software, or accounts to hide your IP. IRC servers are pretty secured, but not invulnerable. Tor software is NOT an option (It's banned in the network due to malicious abuse).

IRC-Clients

Mac:

Download Colloquy from one of these:

* http://colloquy.info/downloads/colloquy-latest.zip
* http://files5.majorgeeks.com/files/aaea265a9054b3b8c5df99c64685ec2e/mac/messaging/colloquy-latest.zip

Get a webproxy, one of these. Make sure you connect with SSL. ("ipadress:port")

* 62.112.33.2:80
* 200.125.243.122:8080
* 120.39.24.156:808
* 58.22.151.6:80
* http://www.proxy-list.org/en/index.php?
* pp=any&pt=2&pc=any&ps=y&submit=Filter+Proxy

Usage

* Start Colloquy
* Click on New
* Enter a Nickname (not your real name)
* Enter a Chat Server, for our purpose, irc.anonops.ru.
* Click on Details
* Select the Secure Web proxy and check the SSL option, use port 6697
* Don't put your real name in either User/Real Name. Invent something.
* If you want, click: Remember Connection
* Hit Connect
* Click Join Room and enter the Chat Room #tunisia, for example.
* Or, one of these: #opTunisia #Lobby View Macintosh instructions below.

Linux:

Xchat (Gnome)

* Debian/Ubuntu/Knoppix... :
```
sudo apt-get install xchat
```

* Redhat/Fedora(64bit only):
 http://www.xchat.org/files/binary/rpm

* Gentoo:
```
sudo emerge --sync | sudo emerge  -av xchat
```

Usage
      Start X-Chat
            Click Add button on the network list, and rename to whatever you choose.
            Click the Edit button with new network selected, change the server entry from newserver/6667, to
            irc.anonops.ru/6697 (or use one of the newer domains found from links below).
            Then select the two check boxes that say Use SSL for all servers on this network and Accept invalid SSL
            certificate.
            Click Close, then Connect.

Konversation (KDE) http://konversation.kde.org
* Debian/Ubuntu/Knoppix... :
```
sudo apt-get install konversation  // Usage : similar to X-Chat
```

Windows:

X-Chat2

* Freeware version: http://www.silverex.org/download
* Mirror: http://download.cnet.com/X-Chat-2/3000-2150_4-10972145.html

XChat

* http://xchat.org/download

mIRC

* http://www.mirc.com/get.html

Usage
* Download SSL Library: http://www.mirc.com/download/openssl-0.9.8q-setup.exe

* Install it either in the mIRC folder (typically C:\Program Files\mIRC or C:\Program Files(x86)\mIRC) or in the Windows System folder (typically C:\Windows\System32).
By running mIRC it should find and use the OpenSSL library automatically. To confirm whether mIRC has loaded the OpenSSL library, you open the Options dialog and look in the Connect/Options section to see if the SSL button is enabled.
* Type `/server irc.anonops.ru:6697`

    Webbased
* http://01.chat.mibbit.com
* In the mibbit page, click server, and enter in the box: `webirc.anonops.ru:+6697`
Click Channels.

Q - How do I know if it is working?

A - Just do /whois your_nick and it should inform you that you are using a secure connection.

`http://www.anonops.ru`

General Browsing Safety

Basic Rule: Always browse in "Private Mode" so that fewer traces of your web history remain on your HDD. Opera, Chrome, Firefox, Safari, and Internet Explorer all include a form of Private Browsing.

* Using a free VPN will ensure your privacy in most situations online.
* If possible, use USB drives. You can nuke them if needed and if leaves no traces on your hard drive
* Recycle your online accounts as needed. A virtual name is just that, something people use to refer to you in given situations.
* When creating accounts, use VPN or TOR bundle that will give a bogus origin as well.

*Tip: Use a different VPN for each of your online personas. When checking real email accounts, fb, use a different VPN than from the one you use for Anonymous activities.

Useful (mandatory) plugins/extensions for Firefox:

* BetterPrivacy (Removes persistent cookies from flash stuff >> *.sol)
* NoScript (blocks Javascript)
* AdBlock Plus (blocks Ads) (Subscribe to Easylist and Fanboy's List)
* Element Hider for Adblock Plus
* Ghostery (tracking pixels)
* TACO (More adblocking)
* Redirect Controller
* Refcontrol
* WorldIP (know your country, know your rights)
* Flagfox
* GoogleSharing (GoogleProxy, anonymizes the search) - Scroogle.org is also a very viable (and worthwhile) alternative
* User Agent Switcher: Sends bogus browser identity to servers.
* Optimize Google: Allows to block loads of scum google uses to track searches.
* Outernet explorer (MacOS): Searches for a whole pile of shit on the net every 10 seconds or so, ensures anyone tapping packets will have a hell of a time.
* Https everywhere: automatically loads https on a site if available. <https://www.eff.org/https-everywhere>
* Scroogle SSL search (Google anonymously) url: https://ssl.scroogle.org

Download TOR:

https://www.torproject.org/

- Download Torbutton for Firefox (enable or disable the browser's use of Tor)

  https://www.torproject.org/torbutton

- Make sure your cached data is securely destroyed before re-starting firefox by the following 'debug' procedure - you'll need to go to Start > Run and then open 'cmd' for Command Prompt:

System Safety

Basic rule: Security is a continuing process, not a state. Do audits on a regular and scheduled basis. And do encrypted backups. Backups are important, as there are two types of people, those who have backups and those who have lost their data.

Use the operating system you are familiar with (Linux and Unix are better though)

   *Uninstall everything you not need.

   *Disable all remote tools.

   *Shred or encrypt /temp, /var/temp and all world-readable files.

   *Use Linux for activism purposes. Inside Linux use virtual machines. Use truecrypt + removable devices + hidden volumes if you plan on reusing a virtual machine more than once. - This is just for those who have knowledge of Linux.

*Encrypt your hard disk (Truecrypt : `http://www.truecrypt.org` .

*Debian and other distros offer to encrypt the hard drive during installation. Use it.

*Use a distro that boots from DVD/CD/USB.

*Never ever keep logs.

*Shutdown all unneeded services.

*Use a firewall, (and tail the output do you can see what happens every moment.) NOT FOR NEWBIES - Basic info could be read out of /var/log/auth.log for example but keep in mind that already compromised systems will likely have modified/wiped that.

*If you detect any unwanted activity INSIDE your computer, shut down the Internet, and reinstall everything.

*If you think your router might have been hacked, contact your ISP at once, reset it, and/or reinstall its firmware or buy a new one.

*Public access points are perfect - just about. (Correlating logins with CCTV could prove disastrous so security cameras should be avoided while using such 'free' services. Cybercafés, McDonald's, and many companies offer free internet access, remember though, not to surf those nets without a vpn and/or Tor.

*Keep private keys (pgp gnupgp) in a removable device, and that removable device away from curious eyes. Encrypt the private key before doing this.

*Keep vpn certs away from curious eyes via removable device, or common hidden folders.

*Never use the same users/passwords on reinstall. Take the time to create a new one each time.

*Use random password generators.

*BE paranoid. All rare activity in your computer must be checked and monitored. That will provide 2 things: knowledge once you identify it, and added safety.

Detecting security issues on *Nix:

But be careful, if you don't know how to read Lynis' output, you'll become paranoid.

* http://www.rootkit.nl/projects/lynis.html

Scanner for rootkits, backdoors and local exploits on *Nix:

Again, if you don't know how to read Rootkit Hunters output, you'll get paranoid.

 * http://www.rootkit.nl/projects/rootkit_hunter.html

Destroy data securely in Unix/Linux:

To securely destroy data under Linux you have some possibilities. The command shred -u overwrites single files and deletes them finally; with wipe you overwrite and delete directories. Be careful because shredded/wiped data cannot be recovered.

Open a Terminal and type:

```
shred -u <filename>
wipe -rcf <directory>  (read the manual first: man wipe)
```

If you feel the need to wipe the whole hard drive, the command is as follows for IDE-HDs (/dev/hda is the first HD):
```
wipe -kq /dev/hda
```

For SATA and SCSI HDs you type (/dev/sda ist the first HD):
```
wipe -kq /dev/sda
```

If wipe is not available to you, you can use dd. Use *both* commands, one after the other, if you're paranoid use them multiple times (again the first HD):
```
dd if=/dev/zero of=/dev/hda
dd if=/dev/urandom of=/dev/hda
```

Destroy data securely on Mac:

Anonymous' Privacy Pack for Mac users. It includes a Top Secret (like HBGary's ones) Docs secure Shredder & AES-256 Encryption tool (and some Design as extra stuff) download links:

http://www.megaupload.com/?d=L2VQBEFE

or

http://www.mediafire.com/?1xmu0m8jpy9b2a1

MD5 (Anonymous-MacPackage-Privacy.dmg) = 36e9ea524a86b94a451577ca46d3e15f

Destroy data securely in Windows:

AxCrypt http://www.axantum.com/AxCrypt

i2P - Anonymizing Network

What is I2P?
I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties.

Many applications are available that interface with I2P, including mail, p2p, IRC chat, instant messaging and others.

Enjoy your anonymity and privacy!

There's a version for Windows (also portable), Linux, MacOS.

I2P Tutorial for Windows Video:
https://www.youtube.com/watch?v=5J3nh1DoRMw

I2P Tutorial for Linux - Video:
https://www.youtube.com/watch?v=QeRN2G9VW5E

How to set up your own website on I2P - Video:
https://www.youtube.com/watch?v=2ylW85vc7SA

http://geti2p.net
http://i2p2.de

IRC on i2p:

127.0.0.1:6668
Channels: #operationpayback, #opegypt , #opIran, #opTunisia, #opHBGary, #opitaly
Sites: (currently down) anonops.i2p qr.i2p

For more and active I2P sites visit: http://inr.i2p
The ports I2P is using: http://www.i2p2.de/faq#ports
See also your router's configuration.

I2P installation and running on Linux

I2P on Linux: just download and extract the installation files, no need for separate install (such as apt-get install). Run the router from /i2p folder with 'sudo sh i2prouter start'. In seconds, I2P should open a Konqueror-browser page of I2P-main console. Configure your bandwidth settings. You might also consider opening some ports on your firewall for optimizing the use of your bandwidth.

Portable I2P (windows only)

Windows users can use a portable package; it contains I2P, several plugins (email, torrent client), preconfigured browser, preconfigured IRC client and messenger. Download located at:

 http://portable-i2p.blogspot.com

! Before you can use anything on I2P, you have to start the I2P router from the portable apps tray icon-menu with the button "I2P Launcher".

Anonymous surfing with I2P

To enable I2P to anonymize you in your browser, go to your browser options/preferences (depending on your browser) -> network/connection settings -> select manual proxy configuration and in http insert 127.0.0.1 and 4444 for port, in https 127.0.0.1 and 4445 for port. Make sure that you have 'No proxy for' as 'localhost, 127.0.0.1' so you'll be able to reach your I2P configuration page. To test your anonymity, go as example to: cmyip.com

TroubleShooting.

FAQ (in no particular order)

Q: Can you help us?
A: See http://www.anonops.ru/?id=contact or join irc.anonops.ru, join a channel and contact an operator. Or contact Anonymous on Twitter, Facebook.

Q: Do you guys have a website?
A: http://www.anonops.ru

Q: How do I know what's hot?
A: Lurk in the IRC channels or go to http://www.anonnews.org

Q: Is the news on Anonnews official?
A: Well, in some way, it is official, on the other hand, it is "official" and on the third hand, the more people support an operation, the more official it becomes.

Q: Why not attack that newspaper/TV/Radiostation?
A: Anonynmous does not attack media.

Q: That is no media! It only spreads lies and propaganda!
A: Freedom of speech counts for assholes too.

Q: What is a netsplit?
A: A netsplit is Internet-Darwin doing evolution.

Q: But, but...
A: As Evelyn Beatrice Hall said, "I disapprove of what you say, but I will defend to the death your right to say it." Freedom of speech. Got it?

Q: What are DDoS and defacements good for anyway? It doesn't help the people.
A: DDoS is all about steering media's attention towards the problems of the people. If media takes notice, this will help the people. The fine art of defacing a website is about sending a message to the people and the owner of that website. Besides that Anonymous provides the people with information and guides and software to circumvent censorship, also know as The Care Package"

Q: What's in the Care Package?
A: Software like Tor Onion Router, a Circumventing Censorship Manual, more software, other guides and useful stuff.

Q: Can you give me a How-To about building botnets?
A: Such how-to does not exist.

Q: I have seen some strange download links in the channel, can I trust them?
A: Anonymous recommend to not trust links spread in the chans. The only trustworthy links are those spread by Admins, Operators and those in topic.

Q: Some guy asked me in the IRC where I live and what my name is.
A: Do NOT provide personal information in IRC. Instead contact an operator and tell him what happened. Same goes for other suspicious behavior.

Q: How can I join your club?
A: Anonymous is not a club.

Q: But how does that Anonymous' thing function anyways?
A: Best way to find out is, to join a channel, lurk around and get an impression of it. Anyone who thinks that the freedom of speech is a remunerative goal can fly under the flag of Anonymous.

Q: I am not a hacker, how can I help you?
A: If you:

can collect/spread information
can organize things
can make contacts
can provide insights
can share experiences
can push the IMMA FIRING MA LAZOR button
can write guides
can do artwork
can speak a foreign language and/can translate
... you can be helpful.

Q: Is there a Hive????????????????????
A: 1. Look at the topic by typing /topic
   2. Probably not, but you don't need a hive, you can fire manually, as you wish.

Q: What's the target?????????????????????
A: Look at the topic by typing /topic

Q: What's the target?????????????????????
A: N00b, look at the topic by typing <tt>/topic</tt>

Q: Is the target down????????????
A: Got to www.watchmouse.com and ask there.

Q: Is there a LOIC for Linux/Unix/Mac?????????????
A: Yes, it is called loiq. See http://sourceforge.net/projects/loiq

* Nixfags may use PyLoris http://sourceforge.net/projects/pyloris and Hping3 as well.

Q: Some guy keeps saying, there were Danish girls in #channel.
A: This is obviously a lie; there are not girls on the Internet.

Q: I am a Media-Guy, how can I contact you?
A: See http://www.anonops.ru/?id=contact or send an email to press@anonops.ru

Q: I am a Media-Women, how can I contact you?
A: Please see http://www.anonops.ru/?id=contact or send an email and personal pics to press@anonops.ru

Some useful Links

Throw-away-emails
Use them for registering activism related email-/Facebook-/... accounts.

* http://10minutemail.com
* http://www.sofort-mail.de
* http://www.trash-mail.com
* http://www.guerrillamail.com
* http://www.spam.la

Portable Software
Portable software is software, that you can run from an USB drive, so that it leaves nearly no traces on your computer.

* http://portableapps.com
* http://portableapps.com/apps/internet/firefox_portable
* http://portable-i2p.blogspot.com

Proxies

You may use them in conjunction with a VPN.

* http://www.freeproxies.org
* http://www.socks24.org
* http://www.samair.ru/proxy

VPN

* http://cyberghostvpn.com
* http://hotspotshield.com
* http://proxpn.com
* https://anonymityonline.org
* http://www.swissvpn.net
* http://perfect-privacy.com
* https://www.ipredator.se
* http://www.anonine.se
* https://www.vpntunnel.se

I2P

http://geti2p.net

Chat for more info about I2P
The channels #i2p, #i2p-chat and #irc2p are supported.

https://www.awxcnx.de/i2p-irc-en.htm

Tor Onion Router

http://www.torproject.org

Privacy Box

The PrivacyBox provides non-tracked (and also anonymous) contact forms. It is running primarily for journalists, bloggers and other publishers. But it is open for other people too. Think about an electronic mailbox.

https://privacybox.de/index.en.html

Sending anonymous email

https://www.awxcnx.de/mm-anon-email.htm

Send free faxes

* http://sendfreefax.net (Text only)
* http://www.freefax.com/ff_snd.html (Text only)
* http://www.eztel.com/freefax/ (Text only)
* http://www.popfax.com

Free and uncensored DNS-Servers

87.118.100.175 (Ports: 53, 110)
94.75.228.29 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
62.75.219.7 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
87.118.104.203 (Ports: 53, 110, DNSSEC)
62.141.58.13 (Ports: 53, 110, HTTPS-DNS, DNSSEC)
87.118.109.2 (Ports: 53, 110, DNSSEC)

To see wether you're using them properly, open your browser and type :

`http://welcome.gpf` into the the adressbar. If you're using them you should see a website saying :

« Congratulation You are using a censorship free DNS server! ».

Else, you failed.

If you're a hax0rz you can use a terminal. Open it and type

`nslookup welcome.gpf`

this should result in the following output:

```
Non-authoritative answer:
Name: welcome.gpf
Address: 62.75.217.76
```

Else, you failed. (Else is General Failure's sister. Avoid meeting them at all costs.)
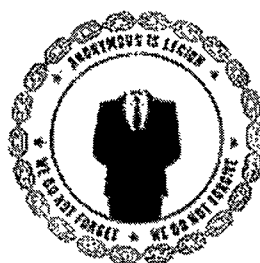
2011. Anonymous.

Protestors Guide to Organize Demonstrations Amidst Repression (Handbook)

DRAFT VERSION

ANONYMOUS

Due to the fact that there are countries starting to face their governments/regimes, a
"Riot Guide" is needed as a how-to guide to demonstrations. So this guide exists to rectify that situation.

Tips:

Teargas (see How to deal with Tear gas chapter)

* Check the wind and move against the wind
* Spread the information to other demonstrators on the streets about where to go
* Never go out without little masks. Cover your mouth and nose.
* Synthetic fibers are better to wear (Ex. Nylon, Acrylic, Polyester). The teargas will not stay on clothing made from these.
* Fabric doused with vinegar will help neutralize teargas.
* If you have some, rinse your eyes with physiological saline or water.

Teams

(If Possible Organize Different Leaders)

BE PEACEFUL! DO NOT ENGAGE IN VIOLENCE IF POSSIBLE! WHEN POSSIBLE, DO NOT ANSWER VIOLEN
CE WITH VIOLENCE IF AT ALL POSSIBLE! TEAMS SHOULD, ACT LIKE PROS!

Different teams, different objectives

Every team needs a person in charge (if possible get Walkie Talkies, referred as WT).
All people that are subject to teams should be wearing cloth with colors, which corresponds with the team.

Important teams:

Runners (White)

Gives information from HQ to other teams and back!
(Need perfect knowing of the neighborhood, with mobile capabilities => bike or so.
If no bike is available, the fastest runner will have to do.)
May also serve as a support team if any other team is in need of backup.
(Used for secret message that can not be send by WT)

Medical Team (Red)

Is in charge of helping people that needs help
Be sure to act nice! THIS TEAM NEEDS RESPECT! In case of an emergency,
you want as many people to help you as possible! It is very important that someone can
take a leader position!
People in this team should carry scissors, Band-Aids, gauze, antiseptic,
painkillers, Physiological Serum, a lot of water, protein bars and a lot of other stuff.
Please check the FirstAidGuide.
Red teams need to very well marked so it is obvious to the people with the
guns what they're doing. Examples: Big patch with red cross/red crescent, reflectors
and red clothing.

Documenting Team (Green)

Very important - People taking pictures, filming and documenting

Using cell phones to create WiFi networks! Upload material as it happens!

Don't necessarily need to be in the riots. Can stay back to organize data
from wireless communications, and other places where data about what is going on can
be accessed. The more that gets out of the riots, the better, as this will draw media
attention.

Protect yourself to upload data: http://pastebin.com/ksw2Xzxd | We do NOT propagate violence.

Use Anonymous contacts to support on editing and spreading the
information; Anonops.ru will help you - leave the editing to people outside the riots, just
keep recording, we'll do the rest.

Real footage and reports are important; cause the media might be not on
side or report in a correct and expected behavior. In some cases your government may
have blacked out all media from reporting. When this happens, ordinary citizens become
reporters, so capturing video/images is very important to get your struggle into the
world and gain international support.

Blur faces of people on pictures! Prevents oppression.

Green Team should be updating Google Maps if possible, letting rioters
know in real time where police are moving. +1(useless in presence of high-tech cops,
with operator cars and videos monitoring (like EU and US zone).

Front Row Team (Black)

These people usually confronts authorities (Be non violent if possible)

The front row demonstrators are what the news and other media will
focus on, they should be well prepared to relay their message effectively. (Signs,
Banners, Megaphones, T-shirts, Effigy's, etc)

Protect yourself: wear cushions, helmets, ski goggles or even a gasmasks.

Observation Team (Gray)

Equipped with Walkie-Talkies, Smartphones, etc.

Posting on Rooftop or someplace high, giving an overview on the streets.
Being stationed up high allows you to see where there is police presence, how many the
demonstrators can expect, which direction they're going, etc.

As much as you may want to show active support with t-shirts, banners

(or possibly throwing some rocks from the rooftop you are looking from), you should refrain from doing so. You do not want any attention that can be avoided. Doing so should allow you to move throughout the city as needed, generally unmolested by the authorities.

Could be using cell phones to create WiFi networks too! Helping to upload material of what happens (as they observe, they're also in open space, what helps for wireless networks!

BASE Team:

Try to set HQs with link to the outside and relay for Crowd teams, (WTStation)

Could coordinate movement through maps, following teams and preventing them from falling in traps

A fast Internet connection is great here, as this team should both provide info to The Running team and fellow Anon's/NewsGroups far and wide.

Groups: Get yourself (and the group(s) you're working with) cheap

mobiles with spare sims (I've known cops nick the sim cards out of phones while searching before) so you can stay in constant touch if you get split up. You can also 'tweet' 'fb' etc info as and when it happens.

Make up group names! Just something short you all remember. This gets useful in unmanageable situations. If you lose the others of your group, you don't need to call their names (which could be written down by police).

Groups should not be bigger than 6 people. Small groups mean more mobility. Big groups are slow, especially in deciding what to do.

Talk about what you want to do before you go to a demonstration. Respect it if someone doesn't want to take risks. Think about getting together with people who want to do the same thing to avoid too much discussion.

Get to know the area before just turning up! It's no good turning up then the cops steam in and you've got nowhere to retreat to. Better to know where you are and where you're going so you retreat around a corner and turn up again behind them from another.

Spread maps of the area with important targets. See the 5-finger-tactic and out-of-control tactic http://de.wikipedia.org/wiki/Fünf-Finger-Taktik (German)

Five Fingers Form a Fist
Concept

The five-finger tactic is used for getting around police lines or blockades.
Protesters allocate on different groups. Every group has one person holding a sing with
a number or color. If you don't want to take a risk, you can disclaim that person and just
wear the color (e.g. wristband, scarf, hat). You start the demonstration together, but if
you see the police the different groups split and stretch. Then you flow through the
police line and bale after it.

"Out of Control" Protest Behavior
Concept

The concept of "Out of Control" is based on a decentralized organization
structure and uncontrolled movements of the crowd as well to circle around police lines
and the suddenly appearance a crowd, similar to a flashmob. The protest participants
try to spread often and reunite at a different place and try to hide the borders between
protests an environment with this behavior.

Target

A close protest can be controlled and steered quite easy by the police. This
concept tries to make the analysis of a protest and its flow difficult for the police.
Black Blocking:(Authorities will be incited to stronger action so this tactic should not be
used in the presence of at risk protest group members.)
The Black Bloc does not need to be affiliated with any group or ideology, it is simply a
tactic, and it WORKS. This is both a defense and offensive tactic.
Similar clothing
Makes it harder to identify individuals
Creates an effect to make mob see larger that it really is
Protects identity ('Guy Fawkes mask popularized by "V for Vendetta")

Masks
Protects identity (If the regime stays in power and your face is found to
be protesting, you can expect jail, beating or even possibly death, keep your identity
hidden when in public!)
Protects against tear gas inhalation/irritation (add water or vinegar to
help with skin irritations caused by tear gas exposure; inject some physiological serum
in the eyes to wash them)

Tactics

Whether advancing or retreating pull debris (trash cans, dumpsters, burning tires/cars, etc.) behind your path. This will slow down APCs, Police, allowing you to maintain mobility.

DONT GET BOXED IN - if you hear some one saying your going to get boxed in (trapped) repeat the message down the line to other protestors.

If the police use violence or tries to arrest people, build chains by linking arms! This prevents arresting and shows power. Turn your backs on police spraying gas and build chains to prevent them doing things you can't see.

Listen to where the observation/basement teams tell you to go and go to exactly where they tell you. And when they tell you to get out, leave the area. They both work to prevent you from entering situations/area's that could land you trapped and subsequently in jail or worse!

Go out with a few friends and watch each others backs at all times. Try not to get separated Use caution when dealing with and speaking to people whom you do not know. Others claiming to support your cause may be infiltrators.

Make sure no one else other than the communications operator of the team is communicating through the radio channel you are utilizing. This could cause a breach of security if undesirables (Police/Other Authorities) are spying on your conversation.

HOW TO DEAL WITH TEAR GAS

HOW TO MAKE A HOMEMADE TEAR-GAS MASK

Cut as follows

8 cms

33 cms

Glue a strip of rubber foam on the inside edge of the bottle

Transparent 2 Litre Soda Bottle
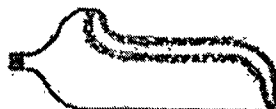
Glue and sew a strip of cloth over the foam rubber

put a clinical mouth-cover in the neck of the bottle and elastic to secure it to your head

cover mouth

Carry a bottle of vinegar to soak the mouth cover before putting on the mask

Breathing in tear gas, or getting it in your eyes, is not fun. This, obviously, is the whole point. But there are things you can do to mitigate the effectiveness of tear gas, and allow you to keep on fighting the good fight.

The first thing to remember about tear gas is that it is primarily a fear weapon. Yes, the gas hurts. But the fear caused by tear gas grenades is a much more effective means of crowd dispersal than the gas itself. So rule number one is to calm down.

Tear gas is most often delivered to its target in the form of grenades. These fit onto the end of gas guns and are fired with blank shotgun cartridges. So, when tear gas is being used you will hear gunshots. Don't worry: you're not being shot at.

After you hear a shot, look up. The grenade will be arcing toward its destination trailing white smoke. If the grenade is not headed directly at you, there is no reason to move. So don't move just yet. Warn people that there is a grenade incoming, and figure out where it will land. If it is headed toward you, you may want to prepare to hold your breath by briefly hyperventilating.

The grenade will explode. This usually happens while it is in the air, but not always. Again, this can be scary until you get used to it. After the explosion, a small gas emitter remains. It is metal and about the size of a hockey puck. It will be hissing and spewing out tear gas.

The wind is your friend. Move upwind of the gas. This will blow the majority of the gas away from you. Do not panic. Do not run. Panic is precisely what the police are trying to create.

If you have gloves and something to protect your face (which I'll talk about soon), you

can pick up the gas emitter and lob it back at the police. This is a considerate thing to do to protect your fellow protesters. The emitter will be hot, so gloves are recommended. Remember, the police are thoroughly protected against gas; throwing it back at them is not a violent act.

WARNING: Picking up the gas emitter will ensure that your clothing is saturated with tear gas. This is extremely unpleasant and will require very thorough laundering with harsh detergent. Prevent contact between gassy clothes and your face, as the chemical agents are active even days later.

WARNING: Do not pick up a grenade which has not exploded. You can be injured if/when it goes off in your hand. Some are, of course, duds. But it is not safe to assume that unexploded grenade at your feet is a dud.

Assuming you don't have a gas mask (which is essential for prolonged operation in a tear-gassy environment), a bandanna or other cloth which has been soaked in vinegar or lemon juice will allow you to breathe long enough to escape the gas. Mask up! Cider vinegar is less harsh-smelling and is recommended. Breathing in vinegar is not pleasant, but compared to tear gas it's like fresh air. Unfortunately, the vinegar's protective effect does not last long (minutes), and your bandanna will be saturated with gas afterward. So bring several. Retying a gassy bandanna around your face is not a good idea. Make sure the bandanna fits tightly around your nose and mouth.

You must wear goggles. Goggles, which are air tight. It is one thing to have severe upper respiratory pain. It is another to have that and also have burning, watering eyes.

Two important notes here First DO NOT wear contact lenses to any event where there is

even a possibility of tear gas usage. The contacts will trap the gas against your eyes, which, aside from being hideously painful, will eventually damage your cornea.

Secondly, many places have, or have recently enacted, laws against wearing masks. In some southern states these laws were implemented to defeat the Ku Klux Klan; these days they're more likely specifically aimed at dissenters who don't wish to have their faces filed away by the FBI. So, be aware that wearing a gas mask or a bandanna may be, in itself, illegal. Yes, protecting yourself from police violence, even passively, can get you thrown in jail.

My description of what tear gas feels like is this: it feels as if the inside of your head is being dissolved by acid. There is a burning pain and a liquefying feeling as mucous; tears and saliva all begin flowing.

Spit, blow your nose, rinse out your mouth, gargle. If necessary, do eyewash by squirting water across your eye from the inside to the outside with your head tilted to the side.

WARNING: You should really get a brief training before you do this. Contact your local activist organization. Also, the eyewash procedure for pepper spray is different.

Different people react differently to the gas. I've seen totally unprotected people go up against cops and gas for hours by sheer force of will. However, don't expect that you will be able to. You may be pleasantly surprised, though.

Finally, diffuse tear gas lingers in the air for a long time. Expect eye, nose and throat irritation for several hours after tear gas has been used in an area, especially if the use of gas was extremely liberal (as in Quebec City).

Update: the following is some information I found regarding the toxicity of both CN and CS tear gas. I, personally, only have direct experience with CS.

I removed the footnotes and references to either appendices or illustrations, but otherwise the following is as written in the original document.

CN has always been associated with potential hazards particularly in regard to its effects on skin and eyes, which provided the impetus to find a standard replacement. It was found to be between 3 and 10 times more toxic than CS in rats, rabbits, mice and guinea pigs. It creates more severe damage to the lung with more edema, patchy acute inflammatory cell infiltration of the trachea, bronchi and bronchioles and more evidence of early bronchopneumonia. Very early on it was noted that CN can induce primary irritant dermatitis. In skin tests it was found CS caused no effects below 20 mg, whereas moist CN caused vesication (blistering) in most subjects. It is also a more potent skin sensitizer than CS with several people developing allergic dermatitis. CN has also been associated with longer lasting burning of the cornea and even permanent eye injuries, particularly if the irritant has been propelled into the eye at short range. In higher doses, it is lethal, particularly in enclosed spaces where even one 128g grenade in a 27-cubic-meter room is sufficient to kill.

CS - There is extensive scientific literature on CS, one recent search claims to have found 115,107 articles. Only some of the most salient aspects can be discussed here. Advocates of CS claim that high levels of exposure to CS are precluded because people are adverse to remaining where this agent is present. (QXZ notes that he's seen totally unprotected people subjecting themselves to CS exposure for hours at a time. CS advocates seem to

ignore this.) More critical authors have noted the lack of epidemiologic inquiry on its use in actual field conditions. However, operational usage sometimes means individuals face additional punishment or even death if they seek to leave a contaminated zone. At higher levels of exposure, inhalation toxicology studies indicate CS can cause chemical pneumonitis and fatal pulmonary edema. (Victims die by drowning in their own lung fluids). CS exposure can also lead to reactive airways dysfunction. Oral toxicological studies note the facility of CS to cause sever gastroenteritis with perforation. CS is a primary skin irritant and some individuals will develop contact dermatitis even after what appears to be an unproblematic initial exposure and severe blistering can emerge several hours later. An exposure to even a low concentration of CS raises blood pressure and there is a particular risk of health damage to anyone over 30, under physical strain or having an undetected aneurysm. At higher levels CS has been associated with heart failure, heptacellular (liver) damage and death. One US based CS manufacturer, Federal Laboratories, has warned that "Firing one Federal No. 230 Flite-Rite (tear gas projectile) in a room (eight-feet by eight-feet by seven-feet) could endanger the life of an average subject if he stayed in the room for seven minutes". CS from canisters has also caused acute mass chemical burns.

Wheat paste   (powerful glue)

Prepare 1 cup (2.4 dl) of very hot water. Make a thin mixture of 3 tablespoons (45 ml) of white flour and cold water (just enough to wet all the flour and make it liquid enough to pour). Pour the cold mixture slowly into the hot water while stirring constantly. Bring to a boil. When it thickens, allow cooling. Smear on like any other glue. For slightly better strength, add 1 tablespoon (15 ml) of sugar after the glue is thickened. After using a portion, reheat the remaining in a covered jar or container to sterilize it for storage or keep refrigerated. If wheat flour is not available, other flours will work.

Rice Paste
Mix one part rice flour and six parts water. Heat while mixing to a smooth consistency.

How to defend against dogs

Steps
1.
Get your bearings straight. Know where you are. If it is your first time to be in the area, familiarize yourself with the best routes that you can take to escape, to avoid further encounters with the aggressive dog, and to avoid being trapped in dead-end streets or alleyways.
2.
Stay calm. One of the first things that you should do is to not let panic take over and cloud your thinking. If you panic, the dog may sense your fear and make you more prone to attack. Look around, and think of possible escape points you can use. Can you get away by climbing, entering or leaving a building or fenced-in area? What objects can you use to ward off the dog if necessary? Make sure the animal does not feel backed into a corner, as its instinct would really be to attack anything that is blocking its path. If the dog does not have space, back up slowly and avoid contact to give the dog more room.
3.
Don't run. This is one of the most important points to keep in mind. Running makes you prey in their mind, and will lead the dog to pursue and chase you. Moreover, you will not be able to outrun the dog -- regardless of what the breed is -- and once the dog catches you, you will be prone to being attacked even more vigorously. The best thing to do is to

stand absolutely still, and avoid making any sudden movements. Make sure that your position is not threatening to the dog.

4.

Avoid making eye contact. Making eye contact signals to the dog that you are provoking it, and want to impose an attack. The dog, in turn, would be aggravated even further. Keep the dog and its actions in your peripheral vision, but never look directly into its eyes.

5.

Yell for help. The owner may just be near by and may be able to get the dog under control, or there may be other people elsewhere who can assist you. If there are no other people who can help you out, shout stern commands at the dog directly, such as "Stop!" or "Down!"

6.

Use any object available to deter the dog from attacking. Bang sticks together, clang steel gates -- make a lot of noise. Throw rocks or get a fistful of dirt or sand to throw in its eyes. If you have a flashlight and it is dark, shine it in the dog's eyes. Take caution, however, in doing this, as this could go either way: it could either momentarily stun the dog, or aggravate it further. An open umbrella is a good object to block a dog from closing the distance. If the dog is coming at you, try and bait it into biting your backpack, purse, briefcase, etc., instead of charging at you directly.

7.

Protect your neck at all times. Most dogs will instinctively attack the neck, which could

quickly lead to death in some cases if attacked. Cover your neck and face with your arms so that if the dog does inflict some wounds, it would be on the less vulnerable areas of your body which would be easier to treat.

8.

If you are trained, stand so that the dog's back is directly underneath you. Extend your hands in around its neck, and lock your arms together quickly in a choke. Kick your feet out, dropping your entire body weight on the dog's neck / back. This will incapacitate the dog long enough just for you to get away. Note: Do NOT attempt this method or try to punch the dog if you are not trained.

9.

Jab your fingers toward its eyes in a quick motion, as if throwing sand. Do this method if the dog is not charging but just trying to bite you, and you cannot do any of the above. This will confuse the dog as to which direction it should charge at, and will prevent the dog from attacking your neck.

10.

If you got away from the dog, stay quiet. Dogs have great hearing, and may sense the direction in which you went. Try to get away as quickly but as quietly as possible.

Tips

* If you find that the dog has inflicted deep cuts and wounds, seek medical help and have the wounds treated.

* Contact the authorities and notify them as soon as possible, providing the owner's address (if you know it) or a description of the dog and where the attack happened.

* Pepper sprays would make a good means of defense, and could buy you time to back away from the attacking dog.

Warnings

* Take note of the warning signs to see if the dog has rabies. If the dog has ropy saliva and has wandering eyes, then it might have rabies. If a rabies-infected dog has inflicted you with wounds, make sure to seek medical attention immediately. Rabies is a serious condition which might be fatal.

How to hop a fence:

run towards the fence

jump at the appropriate time, so that your opposite leg can step onto the fence as high as comfortable

turn your lateral momentum into upward momentum with the foot firmly planted on the fence. grab the top of the fence
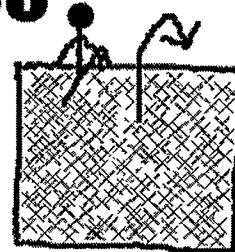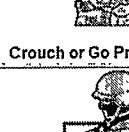
use your momentum and/or arm strength to pull either foot directly on top of the fence
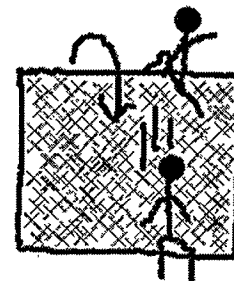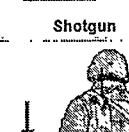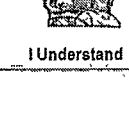
swing your other leg over the fence, and push directly out with your leg on top of the fence to jump off. never put both feet on the top or sit on a fence, as this is a good way to get something caught and fall

quick tip on landing: don't let your heels touch the ground. bend your knees to absorb the impact, and roll if thats what it takes to keep you heels from hitting the ground (if you know how).

if running from authority figures: if you can't hop a fence quickly, avoid fences. if you can, seek fences. cops know how, but they aren't very good at it, and usually hate putting in effort. if they are close enough to grab you, obviously don't as they'll just pull you off.

this all assumes the fence is above your shoulders or so. if it's low enough, you can just vault over the fence by putting both hands on the top and swinging your legs over either side, maintaining your speed.

Standardized Hand Signals For Close Range Engagement (C.R.E.) Operations

One	Two	Three	Four	Five
Six	Seven	Eight	Nine	Ten
You	Me	Come	Listen or I Hear	Watch or I See
Hurry Up	Stop	Freeze	Cover This Area	Go Here or Move Up
Enemy	Hostage	Sniper	Dog	Cell Leader

Column Formation	File Formation	Line Abreast Formation	Wedge Formation	Rally Point
Pistol	Rifle	Shotgun	Ammunition	Vehicle
I Understand	I Don't Understand	Crouch or Go Prone	Breach(er)	Gas
	Door	Window	Point of Entry	

تأكن لم استراتيجيات إلى بحاجة نحن .المظاهرة كيفية للحاجة "القمع مكافحة دليل" وُضِع ، الأنظمة تواجه الأخرى الدول جعلت التي الأحداث بسبب الوضع هذا لتصحيح موجود الدليل هذا و .تونس في لدينا.

* للدموع المسيل الغاز:

- ضدها تحرك و الرياح من تحقق

- الآمن المكان حول الشوارع في للمتظاهرين المعلومات نشر.

- الغاز من تحميك أقنعة بدون تخرج لا.

- هذه من المصنوعة الملابس على يبقى لن للدموع المسيل والغاز (...بوليستر ، أكريليك ، نايلون ، مثلا : اسطناعيّة ألياف من ملابس ارتداء الأفضل المواد.

- للدموع المسيل الغاز إسالة في سيساعد النسيج، على الخل صبّ.

- إذا كان لديك بعض السروم الفسيولوجي في سكبه في العيون ، فإنه سيتم غسلها دون حرق)

* الفرق إن أمكن تنظيم قادة مختلفين)

* كن المسلمي ال طرخنت في ال اعمال عنف اذا عندما يكون ذلك ممكنا ، لا تجب على العنف بالعنف؟!) ال اذا مع يجيبون عريضة؟ هو القانون العدو ال ،
لم يكن هناك استجابة سوى العنف) دون عنف زين بن العابدين علي سيكون لا يزال على مقعده ، ولكن يمكننا الدعوة الى ذلك.

* ينبغي للفرق ان تتصرف بجديّة :

ـ فرق مختلفة وأهداف مختلفة

ـ كل فريق يحتاج الى شخص مسؤول إذا أمكن الحصول على أجهزة اللاسلكي)

* كل أفراد الفرق ينبغي ارتداء الملابس الملونة ، والتي تتوافق مع الفريق.

* فرق هام :

* الهاربون (الابيض)

إلى الفرق الرئيسي المقرر من معلومات يعطي *

(.بذلك القيام عليه سيكون عداء أسرع ، يتوفر لم إذا .ذلك غير أو =< دراجة تواجد قدرات مع ، الحي كامل معرفة ضرورة) *

.الاحتياطي التراجع إلى حاجة في اصبح آخر فريق أي إذا الدعم فريق بمثابة أيضا تكون قد *

(الهاربين طريق عن ترسل أن يمكن لا سرية رسالة تستخدم) *

(الأحمر) الطبي الفريق *

مساعدة إلى حاجة في التي الناس مساعدة عن المسؤول هو *

ما شخصا يتّخذ أن جدا المهم ومن ! لمساعدتك الناس من كثيرا ستريد ، الطوارئ حالة في !الاحترام يحتاج الفريق هذا !بلطف التصرف من تأكد *
!الزعيم موقف

* يجب على الناس في هذا الفريق حمل مقصّات ، وضمادات ، شاش ، مطهّر ، المسكنات ، المياه والقضبان البروتين ، والكثير من الأشياء الأخرى

* فريق وثائقي (الأخضر) (؟ => اقا ما حقا أسهل وضع علامة علييهم ثم استهدافهم) (نعم نقطة جيدة وهذا مجرد مثال على ذلك :)) يعمل في المركز الدان ، ولكن من ناحية، إنهم أخرى ليسوا متميين بضرب الصحفييين :)

* من المهم جدا التقاط الكثير من الصور، و التوثيق و التصوير

* استخدام الهواتف الجوالة لإنشاء شبكات واي واي إفاي تحميل الاخبار كما تحدث إت

* لا تحتاج بالضرورة لتكون في أي أعمال الشغب .يمكن أن تبقى في المؤخرة لتنظم من البيانات من المواصلات اللاسلكية ، وغيرها من الأماكن التي يمكن الوصول إلى البيانات ما حول يجري .وكلما خرجت من أعمال الشغب ، كان ذلك أفضل لأن ذلك سوف يلفت انتباه وسائل الإعلام.

* احمي نفسك لتحميل البيانات : انا نحن لن نشجع العنف

* يساعدكم ؛ المعلومات ونشر تحرير على الاتصالات لدعم المجهولة الهوية استخدم

* معتمدة حكومتكم تكون قد الحالات بعض في. والمتوقع الصحيح السلوك في التقرير أو الإعلام وسائل تكون لا قد و ، ممهمة وتقارير حقيقية لقطات جدا المهم من الصور / الفيديو التقاط حتى ، الصحفيين يصبحون العاديين المواطنين ، ذلك يحدث وعندما. التقارير تقديم من الإعلام وسائل جميع من صوتكم و ، العالم في نضالكم على الحصول.

* الأول الصف (أسود)

* هؤلاء الناس عادة يواجه السلطات تكون غير عنيفة إن أمكن ذلك)

* ومتظاهر الصف الأمامي ما هم ستركز عليهم الأنباء ووسائل الإعلام، الأخرى ينبغي أن تكون مستعدة تماما لنقل رسالتهم على نحو فعال. (لافتات، الصوت مكبرات ، قمصان ، دمى ، الخ)

* فريق المراقبة

* ديزويد بأجهزة اللاسلكي ، الهاتف الذكي ، الخ.

* الشرطة وجود هناك يكون عندما ترى أن لك يسمح ارتفاع في التمركز. الشوارع على عامة لمحة يعطي ما وهو ، مرتفع مكان في أو السطح في الانتشار ،
الخ ، نحوه يسير الذي الاتجاه و ، المتوقع المتظاهرين وعدد.

* أي تريد لا .بذلك القيام عن الامتناع يجب ، (السطح من الحجارة بعض رمي ربما أو) واللافتات بالقمصان النشط الصان اظهار في ترغب قد كنت ما بقدر
عموما السلطات جانب من مضايقة دون ، الحاجة حسب المدينة أنحاء جميع في التحرك لك تسمح بطريقة بذلك القيام وينبغي .تجنبه يمكن اهتمام.

* السفلي الطابق :.

* أول تعيين الرئيسي المقر لتتصل مع الخارج وتتابع المتظاهرين ، محطات اللاسلكي)

* يمكن تنسيق فرق الحوض حركة عن ويويللفبام ومنع الوقوع في خاخالف

* والدانى القاصى أخبار /الهاربين لفريق معلومات تقديم الفريق هذا على يتعين كما ، هنا محبذ سريع إنترنت اتصال.

2011 Anonymous