OPSEC for hackers: because jail is for wuftpd

the.grugq@gmail.com

OPSEC for hackers

FREEDOM FIGHTERS

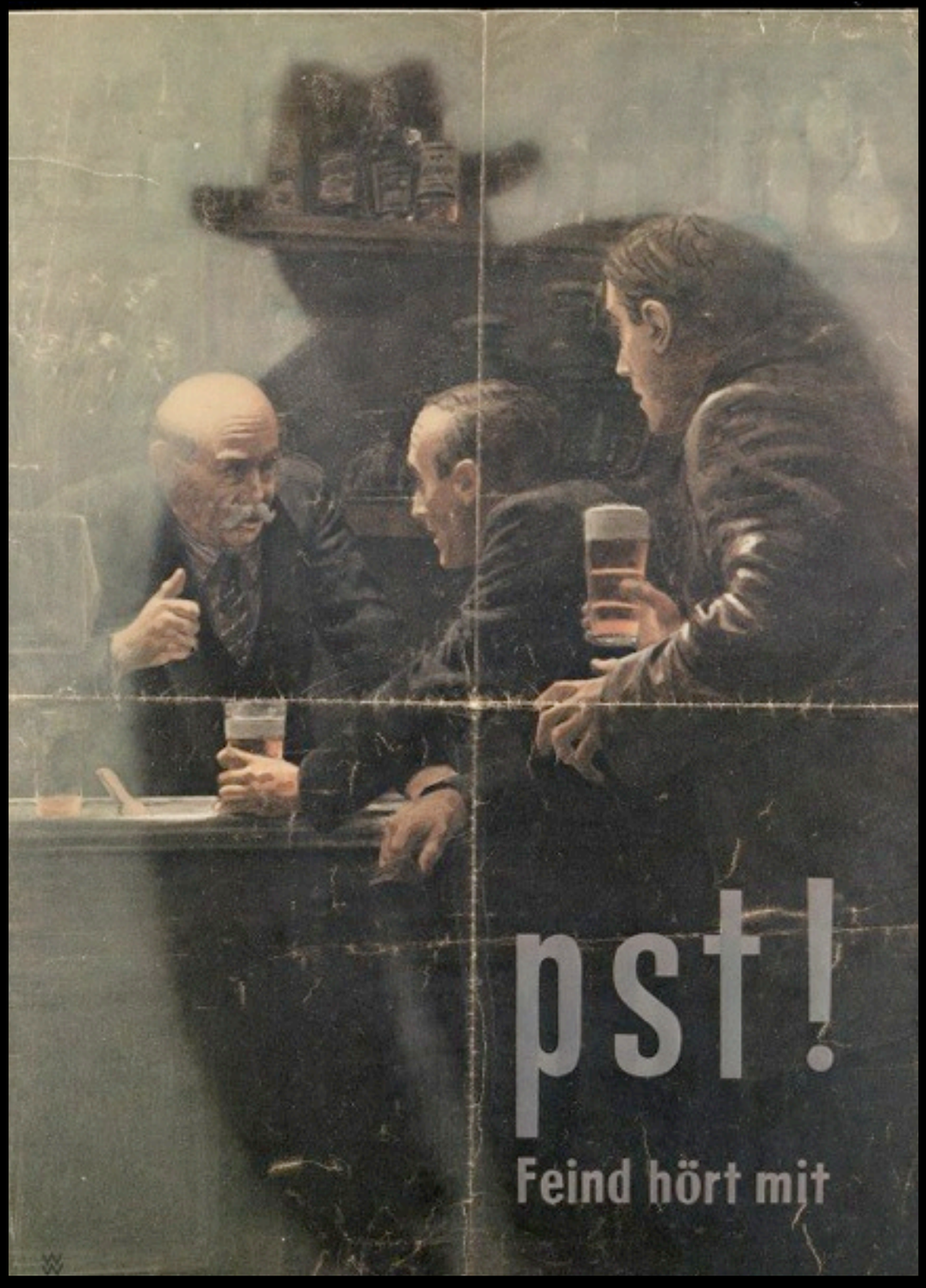
because jail is for wuftpd

the.grugq@gmail.com

Overview

- Intro to OPSEC
  - Methodology
  - lulzsec: lessons learned
  - Techniques
  - Technology
- Conclusion

Avon: You only got to fuck up once… Be a little slow, be a little late, just once. How you ain't gonna never be slow? Never be late? You can't plan for that. Thats life.



Intro to OPSEC

WTF is it?

OPSEC in a nutshell

- Keep your mouth shut
- Guard secrets
  - Need to know
- Never let anyone get into position to blackmail you

STFU

MILLIONS OF AMERICANS ARE VICTIMS OF DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER.
BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

FOR 33 YEARS, SEATTLE LAWYER **JEFF STEINBORN** HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)

Be careful. Be cool.

...and keep your fucking mouth shut!

HERE'S JEFF'S ADVICE---

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE.

PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR YOUR POCKET) S/HE'LL FIND A HARD OBJECT & CAN PULL IT OUT.

Sloppy joint-roller? Cigarette-rolling machines are cheap!

IN YOUR CAR:

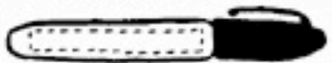
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

❼ Again- be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑hollowed-out Sharpie

BAGGIES IN THE GLOVEBOX WHEN YOU GO FOR YOUR REGISTRATION? JOINT IN YOUR WALLET WHEN YOU'RE PULLING OUT YOUR I.D.? Tsk!!

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE, & WEAR YOUR SEAT BELT.

AND DON'T HAVE ANY OUTSTANDING WARRANTS!

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

By ellen forney © 2001
www.ellenforney.com

MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER. BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

FOR 33 YEARS, SEATTLE LAWYER **JEFF STEINBORN** HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)

Be careful. Be cool.

...and keep your fucking mouth shut!

HERE'S JEFF'S ADVICE---

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

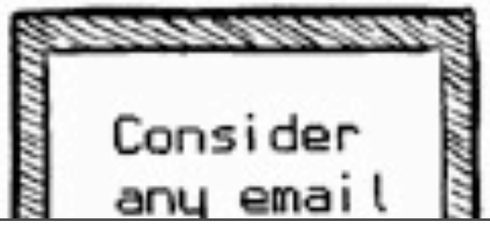
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. *BUT*, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.



By ellen forney © 2001
www.ellenforney.com

MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER.
BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

Be careful. Be cool.

...and keep your fucking mouth shut!

FOR 33 YEARS, SEATTLE LAWYER **JEFF STEINBORN** HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)

HERE'S JEFF'S ADVICE---

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

Hello, sir! A lost cat- HEY!

shit!

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. *BUT*, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

Can I come over?

YES!

I'd like 2 green sweaters.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

Consider any email

By ellen forney © 2001
www.ellenforney.com

MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER. BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

Be careful. Be cool.

...and keep your fucking mouth shut!

FOR 33 YEARS, SEATTLE LAWYER JEFF STEINBORN HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)

HERE'S JEFF'S ADVICE---

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

Hello, sir! A lost cat- HEY!

shit!

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

Can I come over?

YES!

I'd like 2 green sweaters.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

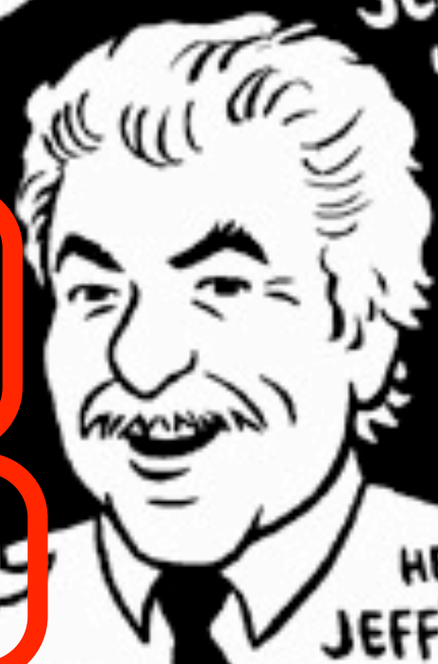
Consider any email

By ellen forney © 2001
www.ellenforney.com

MILLIONS OF AMERICANS SMOKE MARIJUANA, DESPITE THE SPECTER OF FANATICAL DRUG LAWS THAT HAVE SENT MANY GENTLE POT SMOKERS UP THE RIVER. BUT-- WHAT'S A RESPONSIBLE STONER TO DO?

HOW D'YA SMOKE POT AND STAY OUT OF JAIL??

FOR 33 YEARS, SEATTLE LAWYER **JEFF STEINBORN** HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)



HERE'S JEFF'S ADVICE---

Be careful. Be cool.

...and keep your fucking mouth shut!

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

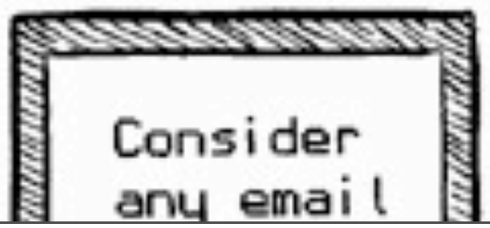
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. *BUT*, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.



FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. *BUT*, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE. PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR

IN YOUR CAR:

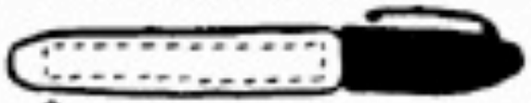
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

❼ Again-be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑hollowed-out Sharpie

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE.

& WEAR

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. *BUT*, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE. **PIPES** CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR

IN YOUR CAR:

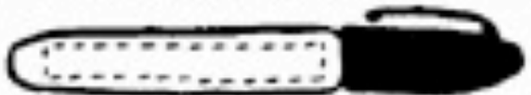
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE **PARKED**.

❼ Again-be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑hollowed-out Sharpie

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE.

& WEAR

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

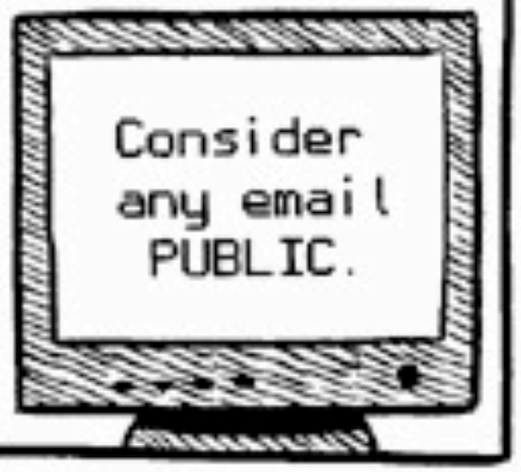
NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, [illegible] DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.



IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE. PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR

IN YOUR CAR:

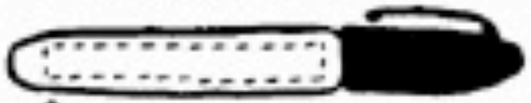
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

❼ Again-be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑ hollowed-out Sharpie

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE, & WEAR

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

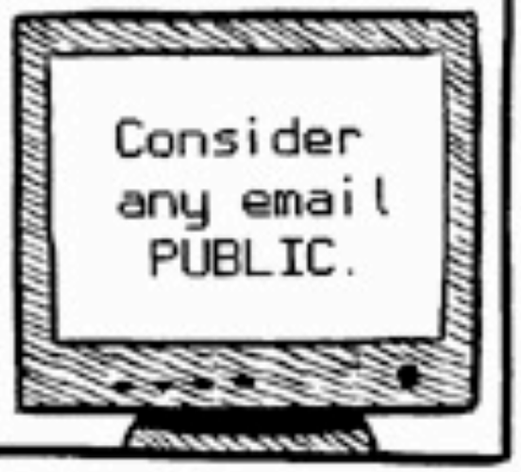
NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, [illegible] DON'T BE EXPLICIT, AND DON'T USE CODE.

❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.



IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE. PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR

IN YOUR CAR:

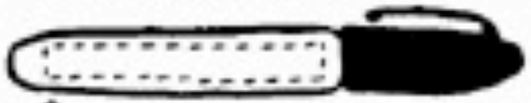
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

❼ Again-be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑hollowed-out Sharpie

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE. & WEAR

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)

AT HOME: (the safest place to smoke)

❶ Smoke out back.

KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.

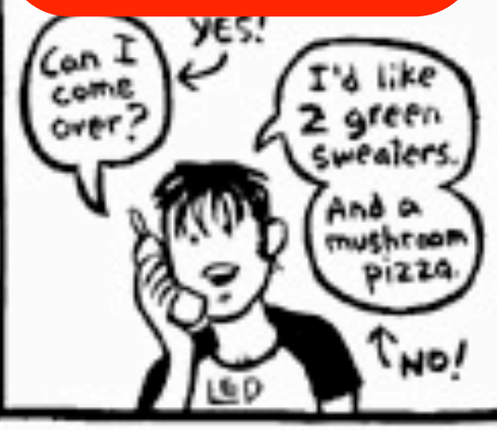
❷ Be tidy.

MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.

NOTE! YOUR HOUSE MAY BE ENTERED WITHOUT A WARRANT IN CASE OF A FIRE, OR IN AN INVESTIGATION OF A DOMESTIC VIOLENCE COMPLAINT.

❸ The phone.

NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, [illegible] DON'T BE EXPLICIT, AND DON'T USE CODE.



❹ Email.

KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.

IN PUBLIC:

❺ Smoke joints.

ROLL YOUR JOINT TO LOOK LIKE A CIGARETTE, & SMOKE IT LIKE A CIGARETTE. PIPES CAN'T BE SWALLOWED IN AN EMERGENCY, & IF A COP HAS GROUNDS TO PAT YOU DOWN FOR A WEAPON (E.G. IF YOU MAKE A SUDDEN REACH FOR

IN YOUR CAR:

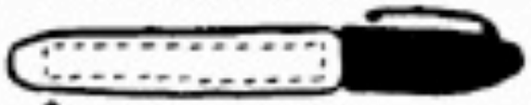
❻ Be a moving target.

PASSENGERS: WHILE THE CAR'S IN MOTION, TAKE A FEW DRAGS OF YOUR CIGARETTE-LOOKING JOINT, AND THEN STASH IT.

YOU'RE MUCH EASIER TO SPOT IF YOU'RE PARKED.

❼ Again-be tidy.

KEEP YOUR ROAD STASH IN A SMELL-PROOF CONTAINER.



↑hollowed-out Sharpie

❽ One law at a time.

IF YOU'VE GOT DOPE IN YOUR CAR, DON'T SPEED, HAVE CURRENT TABS & LICENSE. & WEAR

IN GENERAL:

❾ Camouflage is good.

DON'T LOOK LIKE A POTHEAD.

A SQUARE IS LESS OF A TARGET THAN A FREAK.

SAD AND UNFAIR, BUT TRUE.

Methodology

- put the plumbing in first
  - create a cover (new persona)
  - work on the legend (history, background, supporting evidence for the persona)
  - Create sub-aliases
  - NEVER CONTAMINATE

The 10 Hack Commandments

The 10 FREEDOM FIGHTING Commandments

- Rule 1: Never reveal your operational details

- Rule 1: Never reveal your operational details
- Rule 2: Never reveal your plans

- Rule 1: Never reveal your operational details
- Rule 2: Never reveal your plans
- Rule 3: Never trust anyone

- Rule 1: Never reveal your operational details
- Rule 2: Never reveal your plans
- Rule 3: Never trust anyone
- Rule 4: Never confuse recreation and

FREEDOM FIGHTING

- Rule 1: Never reveal your operational details
- Rule 2: Never reveal your plans
- Rule 3: Never trust anyone
- Rule 4: Never confuse recreation and [illegible] FREEDOM FIGHTING
- Rule 5: Never operate from your own house

- Rule 6: Be proactively paranoid, it doesn't work retroactively

- Rule 6: Be proactively paranoid, it doesn't work retroactively
- Rule 7: Keep personal life and [redacted] separated

FREEDOM FIGHTING

- Rule 6: Be proactively paranoid, it doesn't work retroactively
- Rule 7: Keep personal life and [redacted] separated

FREEDOM FIGHTING

- Rule 8: Keep your personal environment contraband free

- Rule 6: Be proactively paranoid, it doesn't work retroactively
- Rule 7: Keep personal life and [redacted] separated

FREEDOM FIGHTING

- Rule 8: Keep your personal environment contraband free
- Rule 9: Don't talk to the police

- Rule 6: Be proactively paranoid, it doesn't work retroactively
- Rule 7: Keep personal life and [redacted] separated

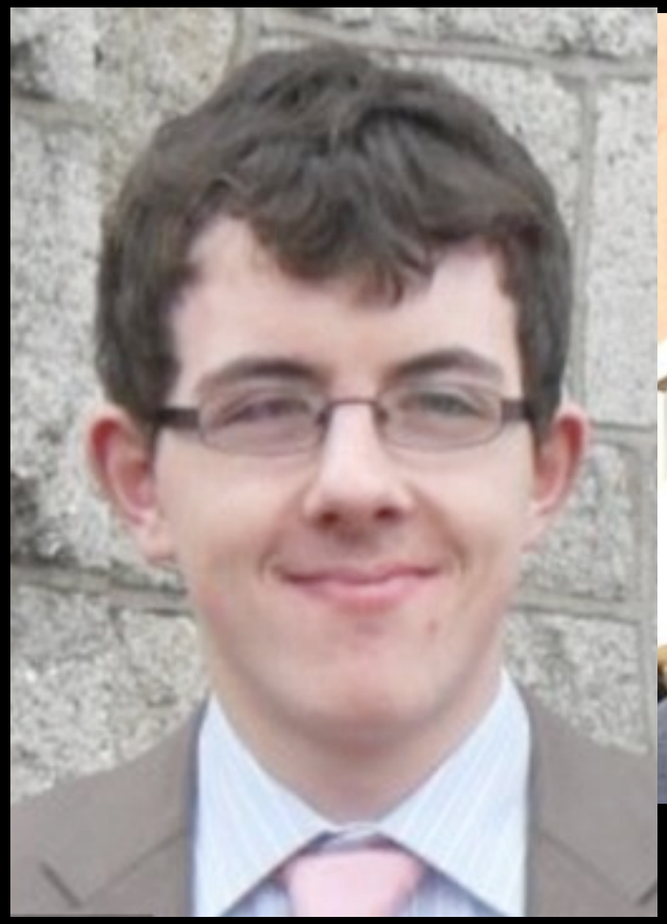
FREEDOM FIGHTING

- Rule 8: Keep your personal environment contraband free
- Rule 9: Don't talk to the police
- Rule 10: Don't give anyone power over you

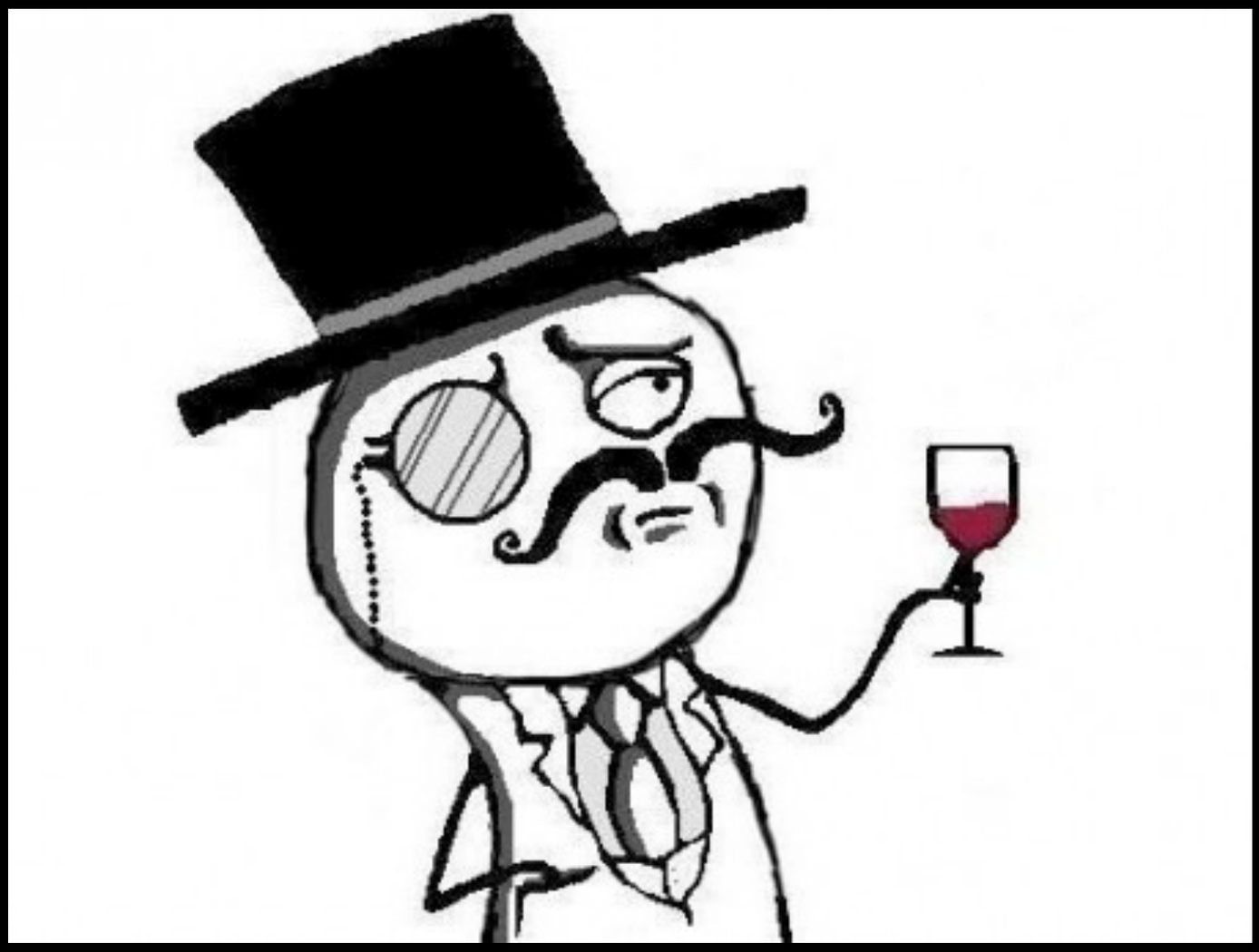
Why do you need OPSEC?

It hurts to get fucked

No one is going to go to jail for you.



Your friends will betray you.



#lulzsec: lessons learned

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool." In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool." In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool." In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool." In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

never ever ever do this

Violation

Never trust anyone

the website of Fine Gael, an Irish political party, was hacked and Fine Gael's website was defaced with an Anonymous-related symbol and, among other things, the words "<owned [hacked] by Raepsauce and Palladium>." I have spoken with another agent who has reviewed the contents, obtained pursuant to a search warrant obtained in the Southern District of New York, of a Facebook account held by a co-conspirator not named as a defendant herein. Based on my conversation with that agent, I have learned that on or about January 9, 2011 (around the time the Fine Gael website was defaced), the user of the Facebook account received an electronic message from another Facebook user with the name "Donncha Carroll" ["Carroll" is an English equivalent of the Gaelic "O'Cearrbhail"]. The message from "Donncha Carroll" contained computer code which produces the same defacement as appeared on the Fine Gael website when it was defaced.

the website of Fine Gael, an Irish political party, was hacked and Fine Gael's website was defaced with an Anonymous-related symbol and, among other things, the words "<owned [hacked] by Raepsauce and Palladium>." I have spoken with another agent who has reviewed the contents, obtained pursuant to a search warrant obtained in the Southern District of New York, of a Facebook account held by a co-conspirator not named as a defendant herein. Based on my conversation with that agent, I have learned that on or about January 9, 2011 (around the time the Fine Gael website was defaced), the user of the Facebook account received an electronic message from another Facebook user with the name "Donncha Carroll" ["Carroll" is an English equivalent of the Gaelic "O'Cearrbhail"]. The message from "Donncha Carroll" contained computer code which produces the same defacement as appeared on the Fine Gael website when it was defaced.

the website of Fine Gael, an Irish political party, was hacked and Fine Gael's website was defaced with an Anonymous-related symbol and, among other things, the words "<owned [hacked] by Raepsauce and Palladium>." I have spoken with another agent who has reviewed the contents, obtained pursuant to a search warrant obtained in the Southern District of New York, of a Facebook account held by a co-conspirator not named as a defendant herein. Based on my conversation with that agent, I have learned that on or about January 9, 2011 (around the time the Fine Gael website was defaced), the user of the Facebook account received an electronic message from another Facebook user with the name "Donncha Carroll" ["Carroll" is an English equivalent of the Gaelic "O'Cearrbhail"]. The message from "Donncha Carroll" contained computer code which produces the same defacement as appeared on the Fine Gael website when it was defaced.

the website of Fine Gael, an Irish political party, was hacked and Fine Gael's website was defaced with an Anonymous-related symbol and, among other things, the words "<owned [hacked] by Raepsauce and Palladium>." I have spoken with another agent who has reviewed the contents, obtained pursuant to a search warrant obtained in the Southern District of New York, of a Facebook account held by a co-conspirator not named as a defendant herein. Based on my conversation with that agent, I have learned that on or about January 9, 2011 (around the time the Fine Gael website was defaced), the user of the Facebook account received an electronic message from another Facebook user with the name "Donncha Carroll" ["Carroll" is an English equivalent of the Gaelic "O'Cearrbhail"]. The message from "Donncha Carroll" contained computer code which produces the same defacement as appeared on the Fine Gael website when it was defaced.

ProTip: Don't use your personal Facebook account to send defacement code to FREEDOM FIGHTERS

engaged in certain forms of Internet chat, such as some of those detailed in this Complaint, may seek to cloak their true identities, including their true IP addresses, when engaged in online chat sessions.[13] Individual users may do this by using a "cloak key" that is unique to each computer network that hosts chat forum(s) in which the user participates. A cloak key employs an algorithm which uses, among other things, the user's IP address to generate a new, "cloaked" loginID. Accordingly, if a user with the same IP address logs into the same chat hosting computer network, the user's cloaked loginID should tend to be the same, regardless of whatever other aliases the user employs in chats. Based on the FBI's analysis of the chat sessions detailed above, it appears that the online nicknames palladium, polonium, and anonsacco shared one or more times the same cloaked loginID. Accordingly, it appears that these nicknames had been accessed from the same IP address and thus the same computer. In addition, on several other occasions since in or about June 2011 up to the present, the nicknames palladium and polonium shared loginIDs which had "Donncha" -- the defendant's first name -- as the associated username.

ProTip: Don't use your real first name as your username in

engaged in certain forms of Internet chat, such as some of those detailed in this Complaint, may seek to cloak their true identities, including their true IP addresses, when engaged in online chat sessions.[13] Individual users may do this by using a "cloak key" that is unique to each computer network that hosts chat forum(s) in which the user participates. A cloak key employs an algorithm which uses, among other things, the user's IP address to generate a new, "cloaked" loginID. Accordingly, if a user with the same IP address logs into the same chat hosting computer network, the user's cloaked loginID should tend to be the same, regardless of whatever other aliases the user employs in chats. Based on the FBI's analysis of the chat sessions detailed above, it appears that the online nicknames palladium, polonium, and anonsacco shared one or more times the same cloaked loginID. Accordingly, it appears that these nicknames had been accessed from the same IP address and thus the same computer. In addition, on several other occasions since in or about June 2011 up to the present, the nicknames palladium and polonium shared loginIDs which had "Donncha" -- the defendant's first name -- as the associated username.

ProTip: Don't use your real first name as your username in

engaged in certain forms of Internet chat, such as some of those detailed in this Complaint, may seek to cloak their true identities, including their true IP addresses, when engaged in online chat sessions.[13] Individual users may do this by using a "cloak key" that is unique to each computer network that hosts chat forum(s) in which the user participates. A cloak key employs an algorithm which uses, among other things, the user's IP address to generate a new, "cloaked" loginID. Accordingly, if a user with the same IP address logs into the same chat hosting computer network, the user's cloaked loginID should tend to be the same, regardless of whatever other aliases the user employs in chats. Based on the FBI's analysis of the chat sessions detailed above, it appears that the online nicknames palladium, polonium, and anonsacco shared one or more times the same cloaked loginID. Accordingly, it appears that these nicknames had been accessed from the same IP address and thus the same computer. In addition, on several other occasions since in or about June 2011 up to the present, the nicknames palladium and polonium shared loginIDs which had "Donncha" -- the defendant's first name -- as the associated username.

ProTip: Don't use your real first name as your username in

engaged in certain forms of Internet chat, such as some of those detailed in this Complaint, may seek to cloak their true identities, including their true IP addresses, when engaged in online chat sessions.[13] Individual users may do this by using a "cloak key" that is unique to each computer network that hosts chat forum(s) in which the user participates. A cloak key employs an algorithm which uses, among other things, the user's IP address to generate a new, "cloaked" loginID. Accordingly, if a user with the same IP address logs into the same chat hosting computer network, the user's cloaked loginID should tend to be the same, regardless of whatever other aliases the user employs in chats. Based on the FBI's analysis of the chat sessions detailed above, it appears that the online nicknames palladium, polonium, and anonsacco shared one or more times the same cloaked loginID. Accordingly, it appears that these nicknames had been accessed from the same IP address and thus the same computer. In addition, on several other occasions since in or about June 2011 up to the present, the nicknames palladium and polonium shared loginIDs which had "Donncha" -- the defendant's first name -- as the associated username.

ProTip: Don't use your real first name as your username in

Violation

Don’t contaminate

which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

Violation

Don’t contaminate

f. In a chat on or about July 31, 2011, at approximately 3:30 a.m., an individual using the alias "POW," later identified as the defendant, stated that "dumpster diving is all good i'm a freegan goddess." I know based on my investigation that "freegans" are individuals who practice eating and reclaiming food that has been discarded as part of an anti-consumerist movement. According to Chicago law enforcement authorities whom I have spoken to who have conducted surveillance of JEREMY HAMMOND, the defendant, in the course of their investigations of HAMMOND since 2005, HAMMOND is a "freegan." In conducting surveillance, agents have seen HAMMOND going into dumpsters to get food.

f. In a chat on or about July 31, 2011, at approximately 3:30 a.m., an individual using the alias "POW," later identified as the defendant, stated that "dumpster diving is all good i'm a freegan goddess." I know based on my investigation that "freegans" are individuals who practice eating and reclaiming food that has been discarded as part of an anti-consumerist movement. According to Chicago law enforcement authorities whom I have spoken to who have conducted surveillance of JEREMY HAMMOND, the defendant, in the course of their investigations of HAMMOND since 2005, HAMMOND is a "freegan." In conducting surveillance, agents have seen HAMMOND going into dumpsters to get food.

f. In a chat on or about July 31, 2011, at approximately 3:30 a.m., an individual using the alias "POW," later identified as the defendant, stated that "dumpster diving is all good i'm a freegan goddess." I know based on my investigation that "freegans" are individuals who practice eating and reclaiming food that has been discarded as part of an anti-consumerist movement. According to Chicago law enforcement authorities whom I have spoken to who have conducted surveillance of JEREMY HAMMOND, the defendant, in the course of their investigations of HAMMOND since 2005, HAMMOND is a "freegan." In conducting surveillance, agents have seen HAMMOND going into dumpsters to get food.

Violation

Keep personal life and hacking separate

Violation

Keep personal life and

FREEDOM FIGHTING separate

appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least one instance of unauthorized access to one of the Compromised Gmail Accounts by the Palladium IP Address, and several instances of unauthorized access by IP addresses allocated to the same Internet service provider in Ireland as the Palladium IP Address.[12]

appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least one instance of unauthorized access to one of the Compromised Gmail Accounts by the Palladium IP Address, and several instances of unauthorized access by IP addresses allocated to the same Internet service provider in Ireland as the Palladium IP Address.[12]

appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least one instance of unauthorized access to one of the Compromised Gmail Accounts by the Palladium IP Address, and several instances of unauthorized access by IP addresses allocated to the same Internet service provider in Ireland as the Palladium IP Address.[12]

ProTip: Don't connect to your target directly from your home IP address

Violation

Never operate from your home

(iv) The FBI in Chicago obtained information in the course of a separate investigation that HAMMOND may have been involved in hacks into the website of a white supremacist organization. According to that investigation, various IP addresses used to access the reported hacked accounts were connected to HAMMOND.

(iv) The FBI in Chicago obtained information in the course of a separate investigation that HAMMOND may have been involved in hacks into the website of a white supremacist organization. According to that investigation, various IP addresses used to access the reported hacked accounts were connected to HAMMOND.

Violation

Never operate from your home

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE. Based on the investigation, including information provided by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "wohoho," a/k/a devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE. Based on the investigation, including information provided by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "xoxoho," a/k/a devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE. Based on the investigation, including information provided by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "xoheho," a/k/a devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE. Based on the investigation, including information provided by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "xoxoho," a/k/a devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

Violation

Don’t reveal operational details

b. An FBI TOR network expert analyzed the data from the Pen/Trap and was able to determine that a significant portion of the traffic from the CHICAGO RESIDENCE to the Internet was TOR-related traffic. The Apple MAC Address was the only MAC address at the CHICAGO RESIDENCE that was connecting to known TOR network IP addresses. The defendant, using the alias "yohoho," has discussed with CW-1 that he used the TOR network. For example in a chat over a jabber service on or about February 2, 2012, at approximately 5:22 a.m., "yohoho" said that he could not play youtube videos because "it won't play over tor." On February 6, 2012, at approximately 4:31 p.m., "yohoho" complained that "tor's always up and down."

b. An FBI TOR network expert analyzed the data from the Pen/Trap and was able to determine that a significant portion of the traffic from the CHICAGO RESIDENCE to the Internet was TOR-related traffic. The Apple MAC Address was the only MAC address at the CHICAGO RESIDENCE that was connecting to known TOR network IP addresses. The defendant, using the alias "yohoho," has discussed with CW-1 that he used the TOR network. For example in a chat over a jabber service on or about February 2, 2012, at approximately 5:22 a.m., "yohoho" said that he could not play youtube videos because "it won't play over tor." On February 6, 2012, at approximately 4:31 p.m., "yohoho" complained that "tor's always up and down."

b. An FBI TOR network expert analyzed the data from the Pen/Trap and was able to determine that a significant portion of the traffic from the CHICAGO RESIDENCE to the Internet was TOR-related traffic. The Apple MAC Address was the only MAC address at the CHICAGO RESIDENCE that was connecting to known TOR network IP addresses. The defendant, using the alias "yohoho," has discussed with CW-1 that he used the TOR network. For example in a chat over a jabber service on or about February 2, 2012, at approximately 5:22 a.m., "yohoho" said that he could not play youtube videos because "it won't play over tor." On February 6, 2012, at approximately 4:31 p.m., "yohoho" complained that "tor's always up and down."

know that on or about August 4, 2011, the CW and an individual using the online nickname "palladium" exchanged private chat messages over the Internet. During the chat, the CW and palladium discussed the theft of palladium's online identity by another individual. Palladium inquired what he could do to prove his identity to the CW and stated, "I can post some info I have from really old opps," meaning prior computer hacking activity. Palladium continued, "I can explain something about the sun" and "I can give you some info I still have from the first fox LFI [hack]."[4] Later in the chat, the CW asked if a certain IP address[5] (the "Palladium IP Address") was used by palladium, to which palladium responded that the "ip [address] looks like a wifi I connect from." The CW also asked whether palladium uses "Perfect Privacy," a virtual private network[6] service located in Germany, to which palladium responded, "yes I use that vpn."

know that on or about August 4, 2011, the CW and an individual using the online nickname "palladium" exchanged private chat messages over the Internet. During the chat, the CW and palladium discussed the theft of palladium's online identity by another individual. Palladium inquired what he could do to prove his identity to the CW and stated, "I can post some info I have from really old opps," meaning prior computer hacking activity. Palladium continued, "I can explain something about the sun" and "I can give you some info I still have from the first fox LFI [hack]."[4] Later in the chat, the CW asked if a certain IP address[5] (the "Palladium IP Address") was used by palladium, to which palladium responded that the "ip [address] looks like a wifi I connect from." The CW also asked whether palladium uses "Perfect Privacy," a virtual private network[6] service located in Germany, to which palladium responded, "yes I use that vpn."

know that on or about August 4, 2011, the CW and an individual using the online nickname "palladium" exchanged private chat messages over the Internet. During the chat, the CW and palladium discussed the theft of palladium's online identity by another individual. Palladium inquired what he could do to prove his identity to the CW and stated, "I can post some info I have from really old opps," meaning prior computer hacking activity. Palladium continued, "I can explain something about the sun" and "I can give you some info I still have from the first fox LFI [hack]."[4] Later in the chat, the CW asked if a certain IP address[5] (the "Palladium IP Address") was used by palladium, to which palladium responded that the "ip [address] looks like a wifi I connect from." The CW also asked whether palladium uses "Perfect Privacy," a virtual private network[6] service located in Germany, to which palladium responded, "yes I use that vpn."

According to the records obtained from Google, and based on information provided by the Garda and the Garda Officers, it appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least

According to the records obtained from Google, and based on information provided by the Garda and the Garda Officers, it appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least

Violation

Don’t reveal operational details

Fine Gael website in around January 2011. Prior to O'CEARRBHAIL's arrest, the FBI had provided to the Garda certain chat logs obtained by the CW of communications in two online chat forums called "#sunnydays" and "#babytech."[8] Garda officers then showed certain of these chat logs to O'CEARRBHAIL during his post-arrest interview, in which O'CEARRBHAIL admitted participating in the Fine Gael hack described above.

know that on or about November 12, 2011, the CW and an individual using the online nickname "polonium" exchanged private chat messages over the Internet. During the chat, polonium stated "I know for a fact the FBI has a large amount of log files" from a server associated with Anonymous, and that "I was v&[9]", to which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

Fine Gael website in around January 2011. Prior to O'CEARRBHAIL's arrest, the FBI had provided to the Garda certain chat logs obtained by the CW of communications in two online chat forums called "#sunnydays" and "#babytech."[8] Garda officers then showed certain of these chat logs to O'CEARRBHAIL during his post-arrest interview, in which O'CEARRBHAIL admitted participating in the Fine Gael hack described above.

know that on or about November 12, 2011, the CW and an individual using the online nickname "polonium" exchanged private chat messages over the Internet. During the chat, polonium stated "I know for a fact the FBI has a large amount of log files" from a server associated with Anonymous, and that "I was v&[9]", to which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

know that on or about January 9, 2012, the CW and anonsacco exchanged Internet chat messages . During the chat, anonsacco stated, "I just got into the iCloud for the head of a national police cybercrime unit. I have all his contacts and can track his location 24/7."[10] Anonsacco then referenced "sunnydays", after which the CW inquired, "so who were you? if you know about !sunnydays," and "the channel name was leaked to feds. so clearly im interested in who you were," to which anonsacco responded, "I understand it was leaked. That caused me a lot of hassle. Could you understand that I don't want to align myself with a compromised screenname?" The CW then asked, "hassle how? you got raided? or people doxed[11] you?" Later, the CW asked, "so if you were raided, did they ask you about me?", to which anonsacco responded, "No. Not you personally."

know that on or about January 9, 2012, the CW and anonsacco exchanged Internet chat messages . During the chat, anonsacco stated, "I just got into the iCloud for the head of a national police cybercrime unit. I have all his contacts and can track his location 24/7."[10] Anonsacco then referenced "sunnydays", after which the CW inquired, "so who were you? if you know about !sunnydays," and "the channel name was leaked to feds. so clearly im interested in who you were," to which anonsacco responded, "I understand it was leaked. That caused me a lot of hassle. Could you understand that I don't want to align myself with a compromised screenname?" The CW then asked, "hassle how? you got raided? or people doxed[11] you?" Later, the CW asked, "so if you were raided, did they ask you about me?", to which anonsacco responded, "No. Not you personally."

Violation

Be paranoid

Virus (10:30:18 PM): don't start accusing me of [being an informant] - especially after you disappeared and came back offering to pay me for shit - that's fed tactics

Virus (10:30:18 PM): don't start accusing me of [being an informant] - especially after you disappeared and came back offering to pay me for shit - that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place

Virus (10:30:18 PM): don't start accusing me of [being an informant] - especially after you disappeared and came back offering to pay me for shit - that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place
Virus (10:30:36 PM): who's docs weren't even public

Virus (10:30:18 PM): don't start accusing me of [being an informant] - especially after you disappeared and came back offering to pay me for shit - that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place
Virus (10:30:36 PM): who's docs weren't even public
Virus (10:30:38 PM): gets owned

Virus (10:30:18 PM): don't start accusing me of [being an informant] – especially after you disappeared and came back offering to pay me for shit – that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place
Virus (10:30:36 PM): who's docs weren't even public
Virus (10:30:38 PM): gets owned
Sabu (10:32:29 PM): offering to pay you for shit?

Virus (10:30:18 PM): don't start accusing me of [being an informant] - especially after you disappeared and came back offering to pay me for shit - that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place
Virus (10:30:36 PM): who's docs weren't even public
Virus (10:30:38 PM): gets owned
Sabu (10:32:29 PM): offering to pay you for shit?
Virus (10:32:55 PM): yeah, you offered me money for "dox"

Virus (10:30:18 PM): don't start accusing me of [being an informant] – especially after you disappeared and came back offering to pay me for shit – that's fed tactics
Virus (10:30:31 PM): and then your buddy, topiary, who lives in the most random place
Virus (10:30:36 PM): who's docs weren't even public
Virus (10:30:38 PM): gets owned
Sabu (10:32:29 PM): offering to pay you for shit?
Virus (10:32:55 PM): yeah, you offered me money for "dox"
Virus (10:33:39 PM): only informants offer up cash for shit -- you gave yourself up with that one

HAPPY ENDING

Virus is still free

by CW-1 - were members of Anonymous, LulzSec, and/or AntiSec.[6] Based on my experience investigating computer crimes, I know that individuals involved in computer-related criminal activity often use multiple accounts and usernames, including IRC and Jabber usernames, to mask their identities. Also based on that experience, I know that it is possible, based on how online chats are logged by certain IM applications such as IRC and Jabber, as well as how individuals communicate with each other over the Internet, to associate an individual with two or more online aliases. For example, if during the course of an IM chat there is a question about the identity of an individual, others in the chat will often seek to verify the individual's identity by, among other things, asking questions about previous online interactions. In addition, if an IM user knows an individual by multiple aliases, the user may refer to that individual using different aliases during the same chat. At times, chat logs, including IRC and Jabber chat logs, will also identify that a user who previously logged in with a different alias is now logging in with a new name. Through these various methods, in the course of this investigation, I have identified a number of different online aliases that the defendant used to communicate with CW-1 and others, including the following: "anarchaos,"[7] "yohoho,"[8] "sup_g,"[9] "burn,"[10]

by CW-1 - were members of Anonymous, LulzSec, and/or AntiSec.[6] Based on my experience investigating computer crimes, I know that individuals involved in computer-related criminal activity often use multiple accounts and usernames, including IRC and Jabber usernames, to mask their identities. Also based on that experience, I know that it is possible, based on how online chats are logged by certain IM applications such as IRC and Jabber, as well as how individuals communicate with each other over the Internet, to associate an individual with two or more online aliases. For example, if during the course of an IM chat there is a question about the identity of an individual, others in the chat will often seek to verify the individual's identity by, among other things, asking questions about previous online interactions. In addition, if an IM user knows an individual by multiple aliases, the user may refer to that individual using different aliases during the same chat. At times, chat logs, including IRC and Jabber chat logs, will also identify that a user who previously logged in with a different alias is now logging in with a new name. Through these various methods, in the course of this investigation, I have identified a number of different online aliases that the defendant used to communicate with CW-1 and others, including the following: "anarchaos,"[7] "yohoho,"[8] "sup_g,"[9] "burn,"[10]

Violation

Never contaminate

through the morning of March 5, 2012: (i) the times at which physical surveillance in Chicago indicated that HAMMOND had entered, was inside, or had left, the CHICAGO RESIDENCE; (ii) the data from the Pen/Trap indicating Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE; and (iii) information obtained from CW-1, in Manhattan, about online communications between CW-1 and the defendant. Based on this analysis, as set forth below, Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE occurred during the time periods that HAMMOND is present inside the CHICAGO RESIDENCE, as confirmed by physical surveillance, and ceased, or at least continued but diminished, after HAMMOND was seen leaving the CHICAGO RESIDENCE. Similarly, information obtained from CW-1 about online activity by the defendant corresponded to the time periods that HAMMOND was confirmed to be inside the CHICAGO RESIDENCE as set forth below.

through the morning of March 5, 2012: (i) the times at which physical surveillance in Chicago indicated that HAMMOND had entered, was inside, or had left, the CHICAGO RESIDENCE; (ii) the data from the Pen/Trap indicating Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE; and (iii) information obtained from CW-1, in Manhattan, about online communications between CW-1 and the defendant. Based on this analysis, as set forth below, Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE occurred during the time periods that HAMMOND is present inside the CHICAGO RESIDENCE, as confirmed by physical surveillance, and ceased, or at least continued but diminished, after HAMMOND was seen leaving the CHICAGO RESIDENCE. Similarly, information obtained from CW-1 about online activity by the defendant corresponded to the time periods that HAMMOND was confirmed to be inside the CHICAGO RESIDENCE as set forth below.

Bonus: w0rmer

My name is Higinio Ochoa and until recently I have been also known as higochoa and w0rmer. I have spent the last few months fighting along side some of the best in the world.

On march 20th 2012 @ 10:30 am around 8 agents from the FBI stormed my apartment and put me under arrest. Shortly after I was taken to the Texas City field office where I turned over all evidence I had collected on myself,over the course of the last few months. I then spent the subsequent hours going over w0rmers timeline and confirming or denying my participation in various attacks. After FBI Agent Scott

or denying my participation in various attacks. After FBI Agent Scott Jenson was done explaining how unimpressed he was with both my expressed skills, and information I provided the systems administrator for the texas DPS. He then proceeded to interview me for the exact information concerning the breach of the texas DPS site.(It would seem to me niether the DPS administrator nor the FBI fully understand the "complexity" of SQL injections.) After faIling to get the printer

Techniques

Plumbing

It is boring.

You'll know it worked if nothing happens.

Put it in place first.

Paranoia doesn't work retroactively


HAWAII
DRIVER LICENSE
NUMBER 01-47-87441
06/03/1981
EXP 06/03/2008
McLOVIN
892 MOMONA ST
HONOLULU, HI 96820

Personas

Spiros: He knows my name, but my name is not my name. And you... to them you're only "The Greek."

The Greek: And, of course, I'm not even Greek.

Problem:

You are you.

Wednesday, October 10, 2012

Solution:

Be someone else.

Personas

- Danger to personas is *contamination*
  - Contact between personas (covers) contaminates both
  - Keep cover identities isolated from each other

Layered defense

- Fail safe technological solution
  - TOR all the things!
- Back stop persona
  - Primary cover alias as first identity
    - Secondary cover aliases (eg. handles)

Profiling data

Pitfalls

- Location revealing information
  - Weather
  - Time
  - Political events
- Profiling data

Practice

- Amateurs practice until they get it right, professionals practice until they can't get it wrong
- Practice makes perfect

Stringer: What you doing?
Shamrock: Robert's Rules says we got to have minutes of the meeting. These the minutes.
Stringer: Nigga, is you taking notes on a *criminal fucking conspiracy*?

No logs. No crime.

Staying Anonymous

Personal info is profiling info

Anti Profiling Guidelines

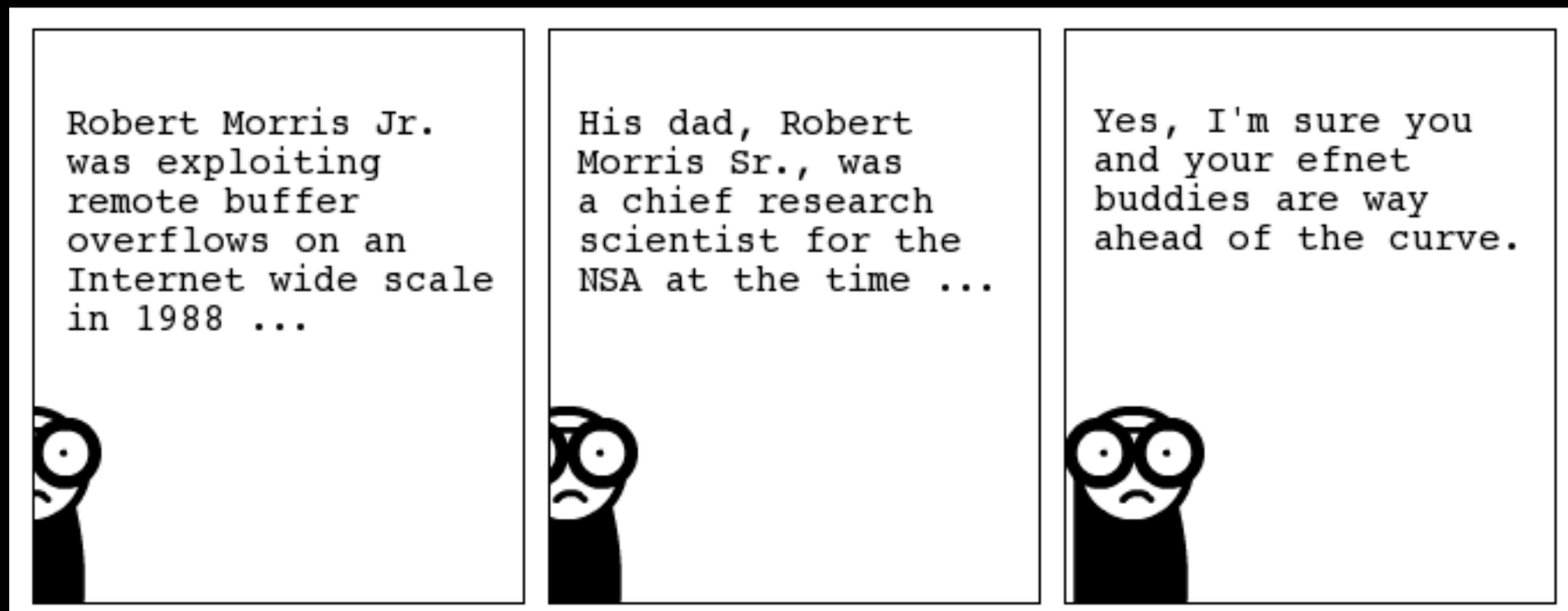
- Do not discuss personal information, e.g. where you are from
- Do not include personal information in your online identity, e.g. nick, username, etc
- Do not mention your physical traits, e.g. gender, tattoos, piercings or physical capacities

Guidelines, cont.

- Do not mention your profession, hobbies or involvement in activist groups
- Do not post information to the regular internet while you are anonymous in IRC.
  - Do not use Twitter and Facebook
- Do not post links to Facebook images
  - The image name contains a personal ID

Anti Location Profiling

- Do not keep regular hours / habits (this can reveal your timezone, geographic locale)
- Do not discuss your environment, e.g. weather, political activities, etc
- Do not use special characters on your keyboard unique to your language


Robert Morris Jr. was exploiting remote buffer overflows on an Internet wide scale in 1988 ...
His dad, Robert Morris Sr., was a chief research scientist for the NSA at the time ...
Yes, I'm sure you and your efnet buddies are way ahead of the curve.

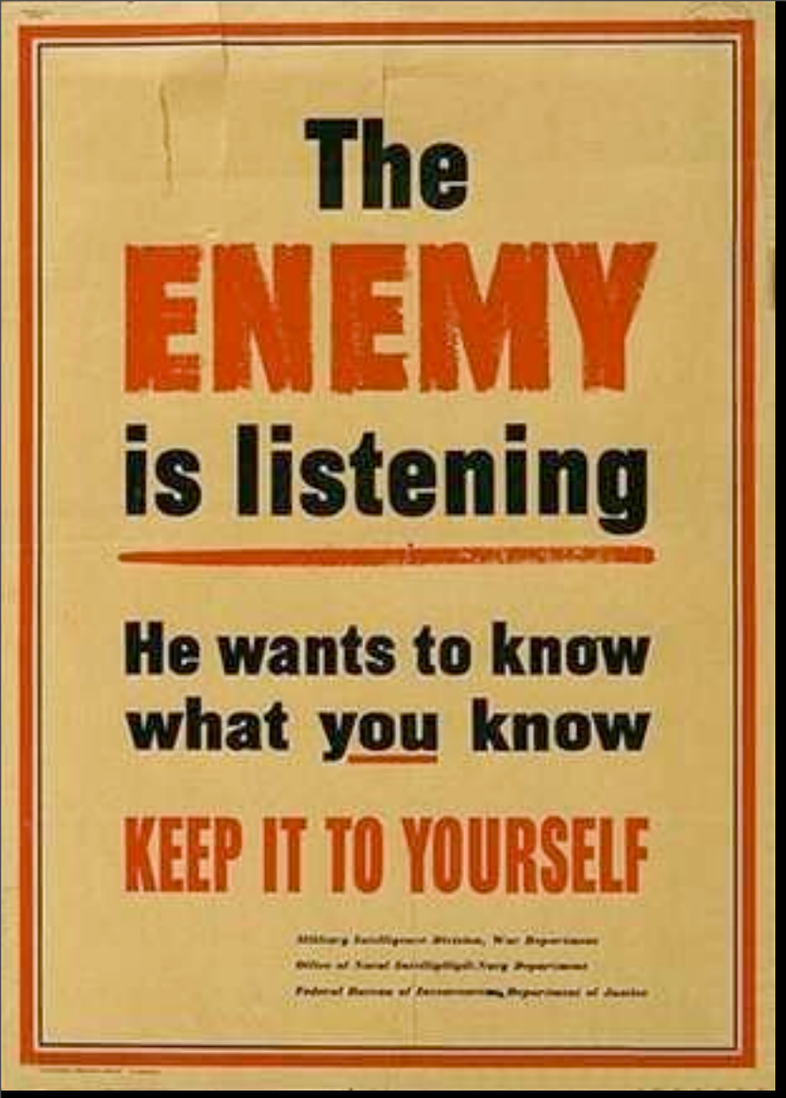
Hackers are no longer the apex predator

FREEDOM FIGHTERS are no longer the apex predator

That position has been ceded to LEO

That position has been ceded to LEO*

*Law Enforcement Officials


The
ENEMY
is listening
He wants to know
what you know
KEEP IT TO YOURSELF

Technology

VPNs vs. TOR

- VPNs provide privacy
- TOR provides anonymity
- Confuse the two at your peril

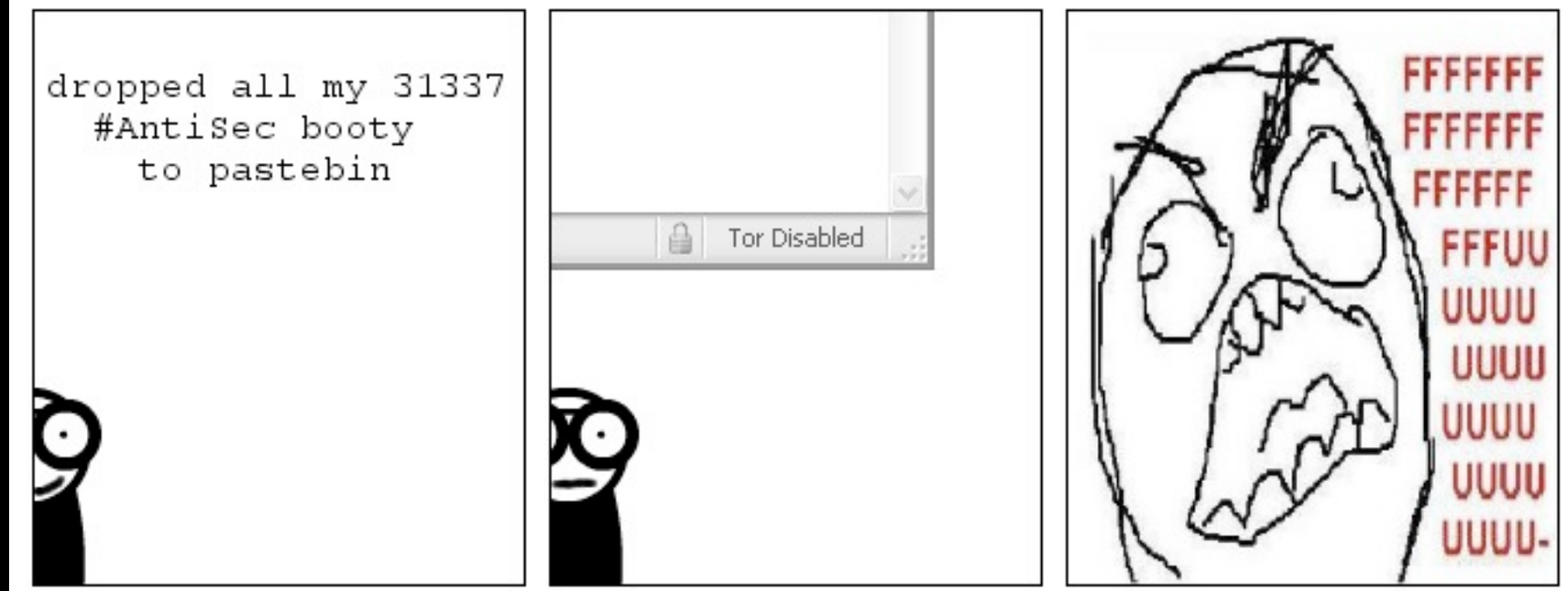
- TOR connection to a VPN => OK
- VPN connection to TOR => GOTO JAIL

On VPNs

- Only safe currency is Bitcoins
  - "Because they come from nothing"
- Purchase only over TOR
  - http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/

On Bitcoins

- Bitcoins are anonymous, not private
  - They can be traced
- Unique, uncontaminated, wallet per cover
  - Use mixers to

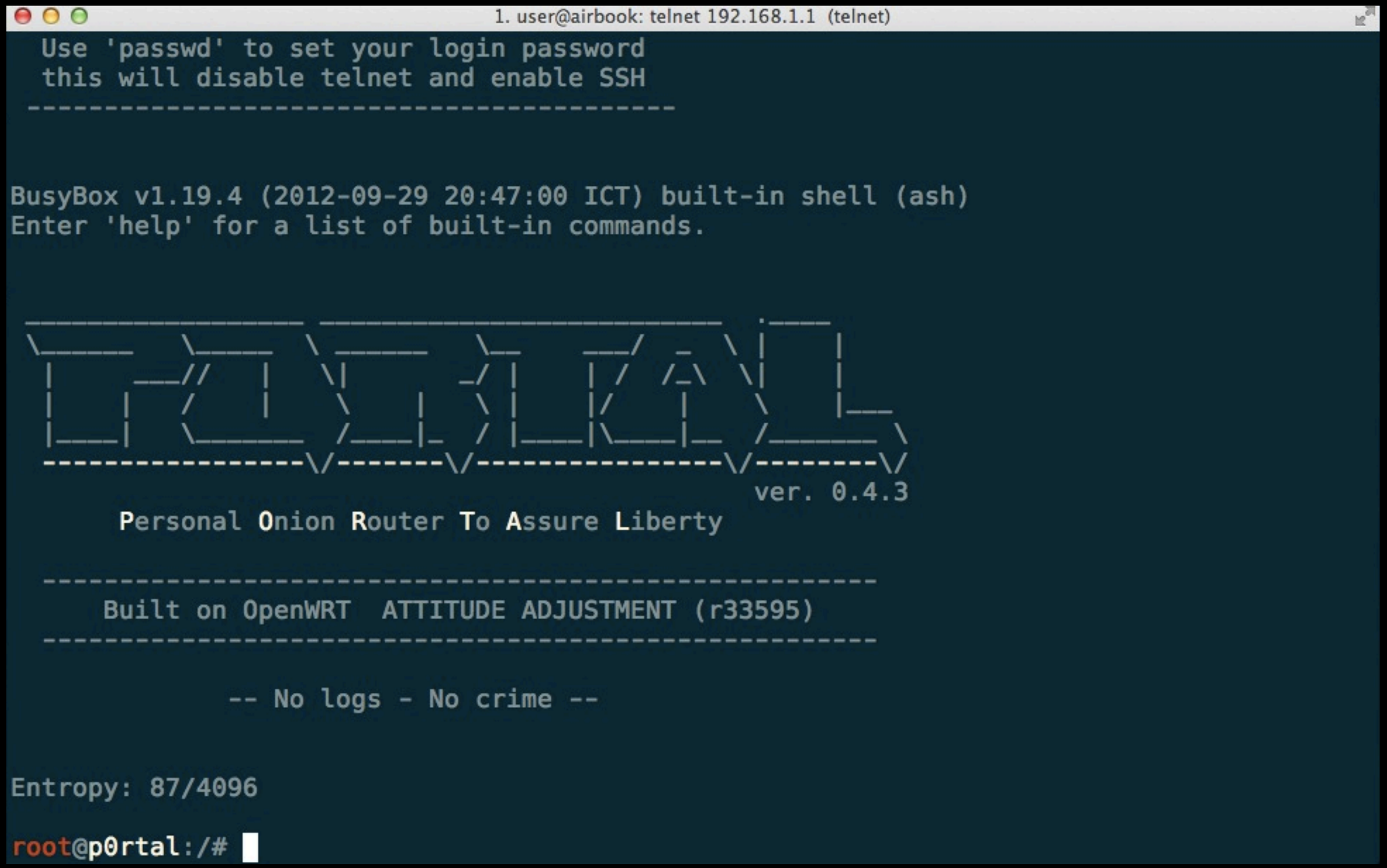

dropped all my 31337
#AntiSec booty
to pastebin
Tor Disabled
FFFFFFF
FFFFFFF
FFFFFF
FFFUU
UUUU
UUUU
UUUU
UUUU-

Fail closed

PORTAL

PORTAL

Personal **O**nion **R**outer **T**o **A**ssure **L**iberty


1. user@airbook: telnet 192.168.1.1 (telnet)
Use 'passwd' to set your login password
this will disable telnet and enable SSH
BusyBox v1.19.4 (2012-09-29 20:47:00 ICT) built-in shell (ash)
Enter 'help' for a list of built-in commands.
ver. 0.4.3
Personal Onion Router To Assure Liberty
Built on OpenWRT ATTITUDE ADJUSTMENT (r33595)
-- No logs - No crime --
Entropy: 87/4096
root@p0rtal:/#

PORTAL

- Router ensuring all traffic is transparently sent over TOR
  - Reduce the ability to make mistakes
- Use mobile uplink
  - Mobility (go to a coffee shop)
  - Reduce risk of wifi monitoring

PORTAL

- Uses tricks to get additional storage space on /

Hardware

- TP-LINK AR71xx personal routers
  - MR-11U
  - MR-3040
  - MR-3020
  - WR-703N

MR-3040 & MR-1IU

- Battery powered
  - Approx. 4-5 hrs per charge
- USB for 3G modem

http://grugq.github.com/portal

Conclusion


TIL: You can be famous. You can be a criminal.
but you can't be a famous criminal
RIP #lulz. RIP.

STFU

Questions?

If you hack, don't speak
If you speak, don't write
If you write, don't sign
If you sign, don't be surprised