Offensive & Defensive & Forensic Techniques for Determining Web User Identity

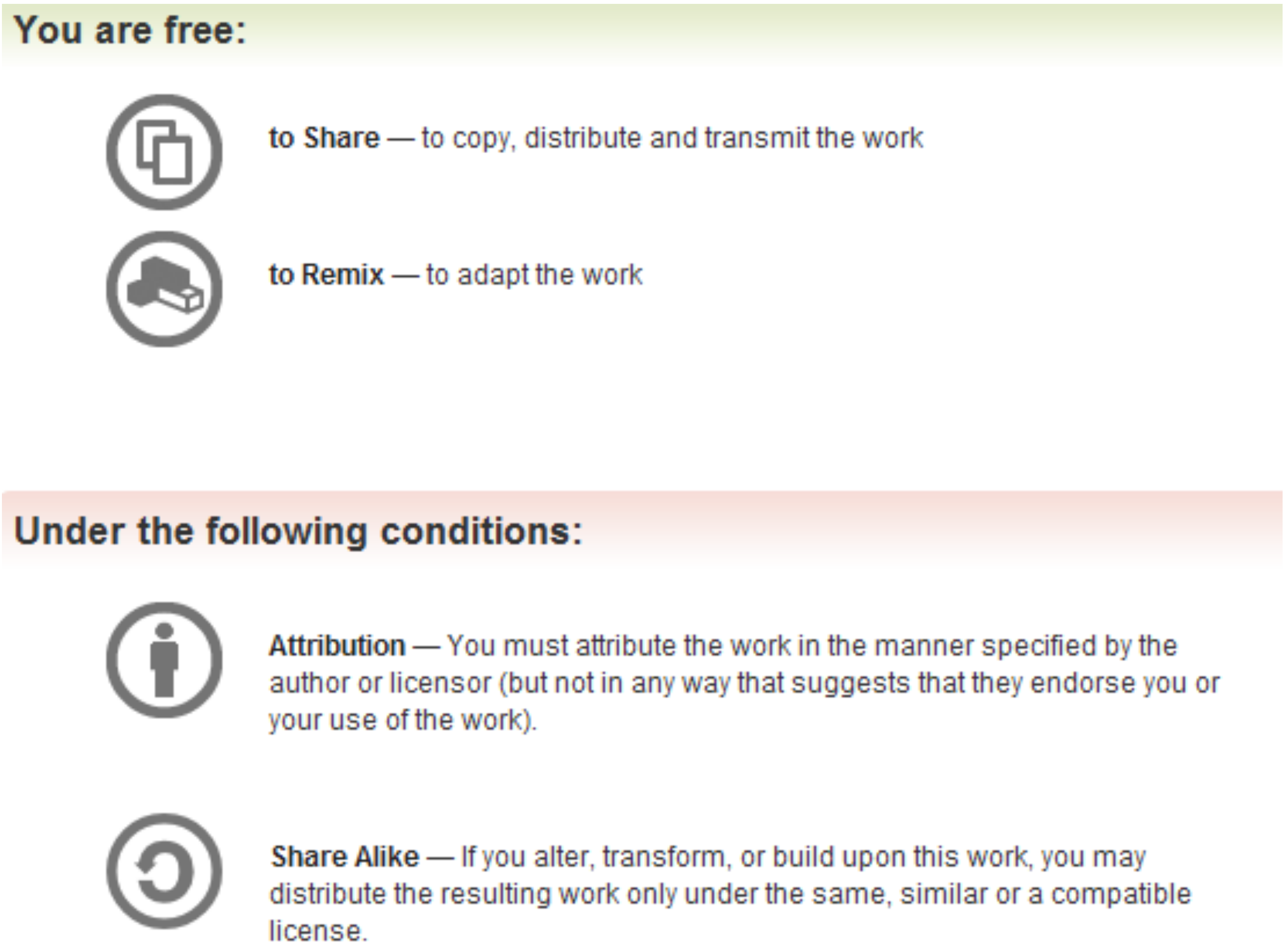
Part 2

Zachary Zebrowski
zak@freeshell.org

Approved for Public Release: 12-3046.
Distribution Unlimited

All materials is licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0/



You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Part 2 Outline

- How to obfuscate where you’re coming from
- How to protect against browser exposures
- Important Caveats

Obfuscation Content

- Simple Obfuscation
  - Borrowing a neighbors connection
  - Shell services
- Cloud services
- VPN Providers
- Anonymizers
  - Tor
  - Others
- Web browser “privacy” modes.
- Email

Borrowing a neighbors open network connection

- Easy to do (just select another Wi-Fi access point to connect too); free & plentiful (depending on neighborhood)
- You need not be "next door".
  - You can use antennas to extend ranges of your connection with an antenna up to 189 miles, or with a balloon (to overcome the shape of the earth) 260 miles with 6 watt amplifiers.
    - See http://en.wikipedia.org/wiki/Long-range_Wi-Fi
- It is (generally) not legal to connect to a neighbors network connection and use it for illicit purposes.
- It is (generally) not legal to "break" a neighbors "secured" wireless access point.
- It is (generally) legal to use a neighbors connection which is not protected by a password, and use it for "basic incidental personal" use.
  - See: http://compnetworking.about.com/od/wirelessfaqs/f/legal_free_illicit.htm for more info about legalities. ***I am not a lawyer***

REMINDER

- Just because you can steal a Wi-Fi connection, it doesn't mean you should.
  - Laws change.
  - **I do not want to see you go to jail.**
  - **<u>I am not a lawyer.</u>**

With that said…

- According to a Wakefield Research / Wi-Fi Alliance poll, 32% of those polled admit to borrowing a neighbors Wi-Fi network

Shell Accounts

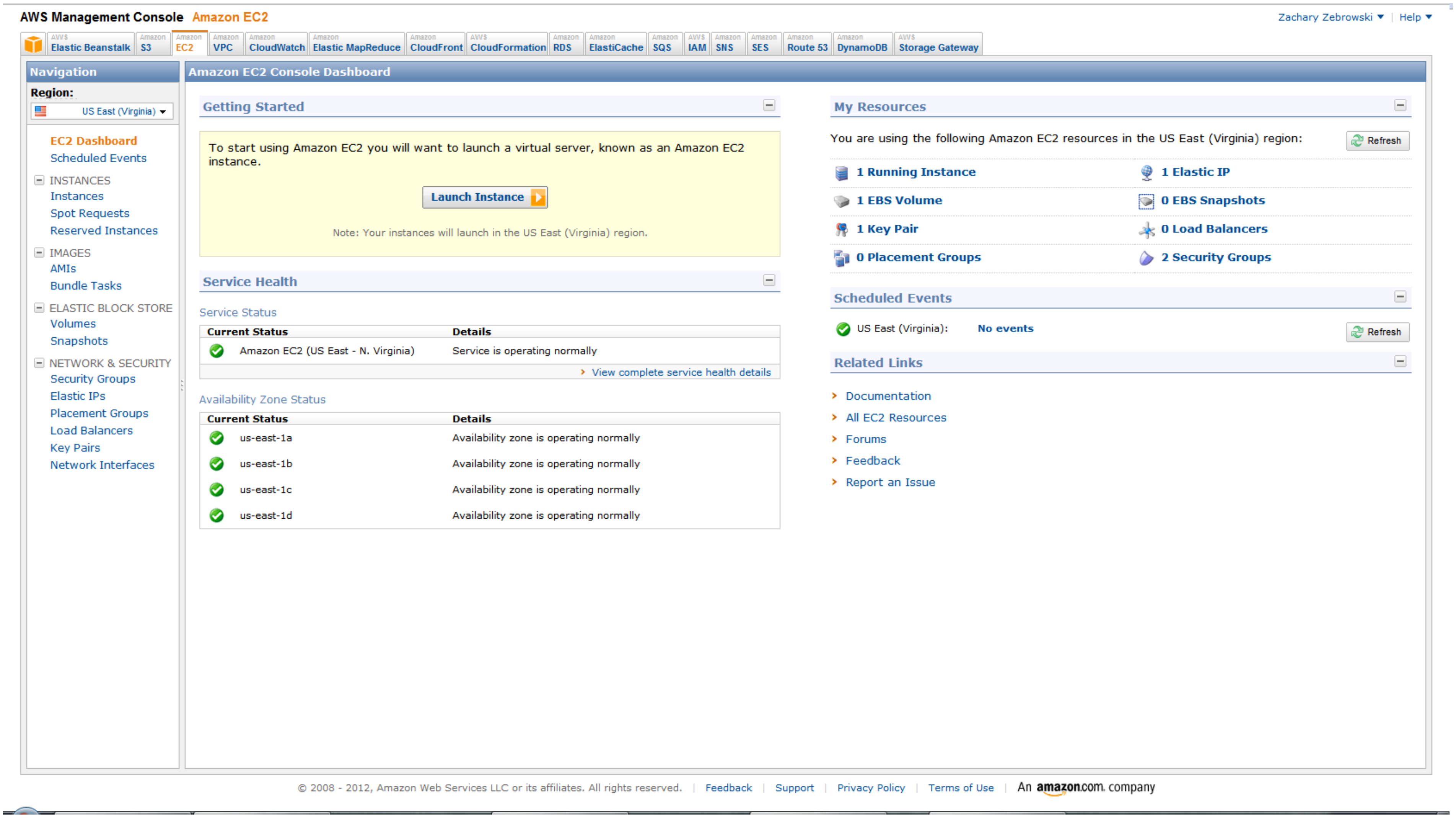
- What’s a shell?
  - A shell is a name for a command interface, like MSDOS. Shell services are generally associated with Linux OS’s. Generally, they are hosted on a machine different from your own. (A simple method to obfuscate where you are coming from.)

Who provides shell accounts?

- Freeshell.org
  - Longest & best “free” shell provider.
  - Cost: free, after a $1 donation to prevent spammers.
    - See also: http://sdf.org/?faq?MEMBERS?01 for “levels” of support.
      - Requires an upgrade to arpa status, a one time $36 dollar fee for outbound access
- Web Hosters
  - http://www.slicehost.com ($240 / year)
  - http://www.pair.com ($71 to $20,388 year, depending on package used.)
  - Go Daddy ($50 / year to $179 / year depending on package used)
  - (Prices valid in 2010).
- Your home PC
  - Use a dsl / cable connection ; install virtual box and your favorite Linux flavor

Cloud Services – create your own ssh box.

- Amazon EC2 cloud
- Another way to obfuscate where you're coming from.
- Costs money.
- Requires a credit card.
- Requires a valid phone number.
- They will disable your account if you do enough "bad" stuff – for example: wikileaks.
- Sort of a pain to create an account, sort of expensive after a while / understanding what costs money.



Amazon EC2 Console Dashboard

Getting Started

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (Virginia) region.

Service Health

Service Status

Current Status	Details
✓ Amazon EC2 (US East - N. Virginia)	Service is operating normally

› View complete service health details

Availability Zone Status

Current Status	Details
✓ us-east-1a	Availability zone is operating normally
✓ us-east-1b	Availability zone is operating normally
✓ us-east-1c	Availability zone is operating normally
✓ us-east-1d	Availability zone is operating normally

My Resources

You are using the following Amazon EC2 resources in the US East (Virginia) region:

1 Running Instance	1 Elastic IP
1 EBS Volume	0 EBS Snapshots
1 Key Pair	0 Load Balancers
0 Placement Groups	2 Security Groups

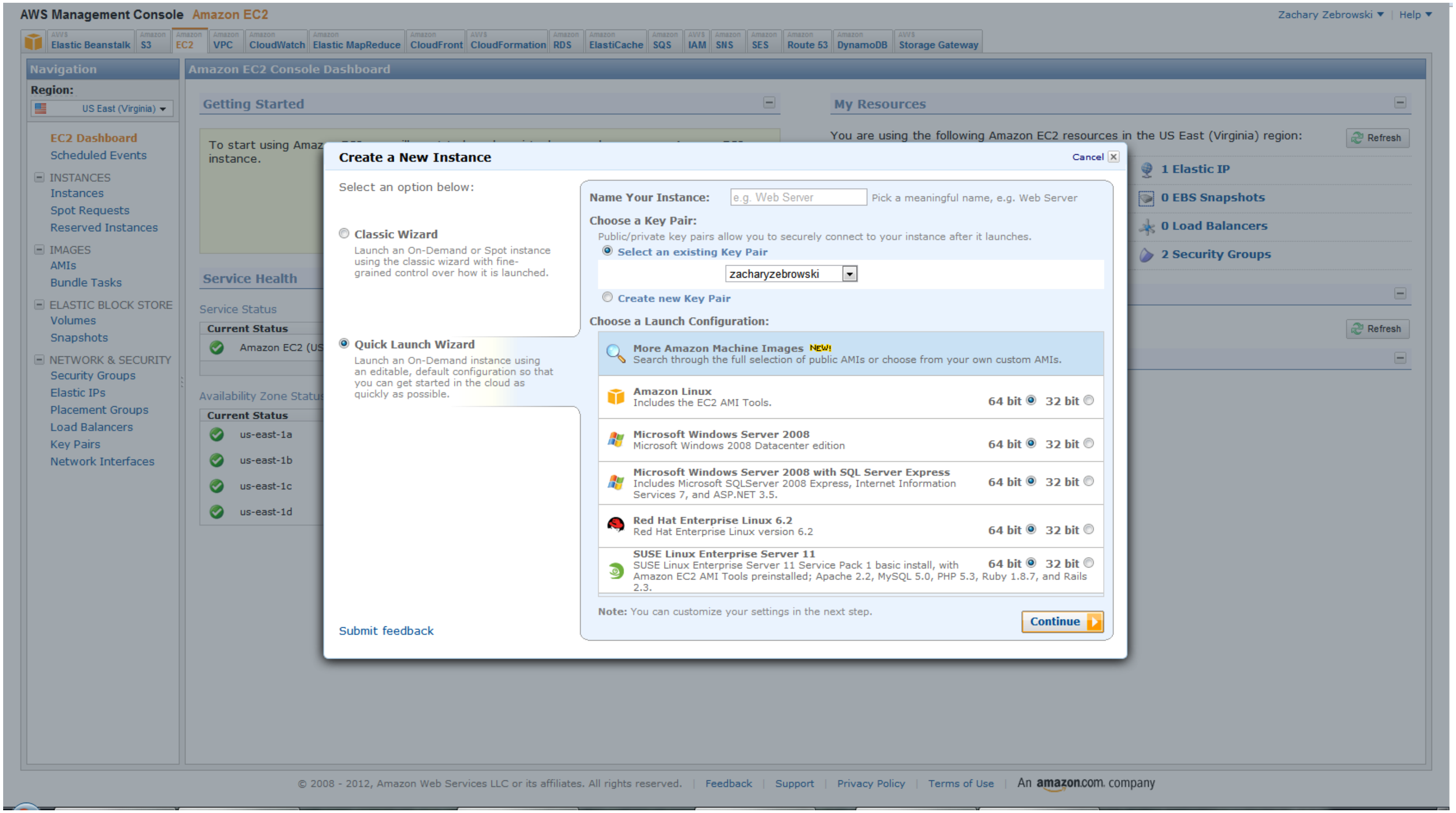
Scheduled Events

✓ US East (Virginia): No events

Related Links

- › Documentation
- › All EC2 Resources
- › Forums
- › Feedback
- › Report an Issue

© 2008 - 2012, Amazon Web Services LLC or its affiliates. All rights reserved. | Feedback | Support | Privacy Policy | Terms of Use | An amazon.com. company



To start using Amaz… instance.

Current Status	
✓	Amazon EC2 (US

Current Status	
✓	us-east-1a
✓	us-east-1b
✓	us-east-1c
✓	us-east-1d

You are using the following Amazon EC2 resources in the US East (Virginia) region:

- 1 Elastic IP
- 0 EBS Snapshots
- 0 Load Balancers
- 2 Security Groups

Create a New Instance Cancel ☒

Select an option below:

○ **Classic Wizard**
Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched.

● **Quick Launch Wizard**
Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible.

Submit feedback

Name Your Instance: e.g. Web Server Pick a meaningful name, e.g. Web Server

Choose a Key Pair:
Public/private key pairs allow you to securely connect to your instance after it launches.

● Select an existing Key Pair
zacharyzebrowski ▾
○ Create new Key Pair

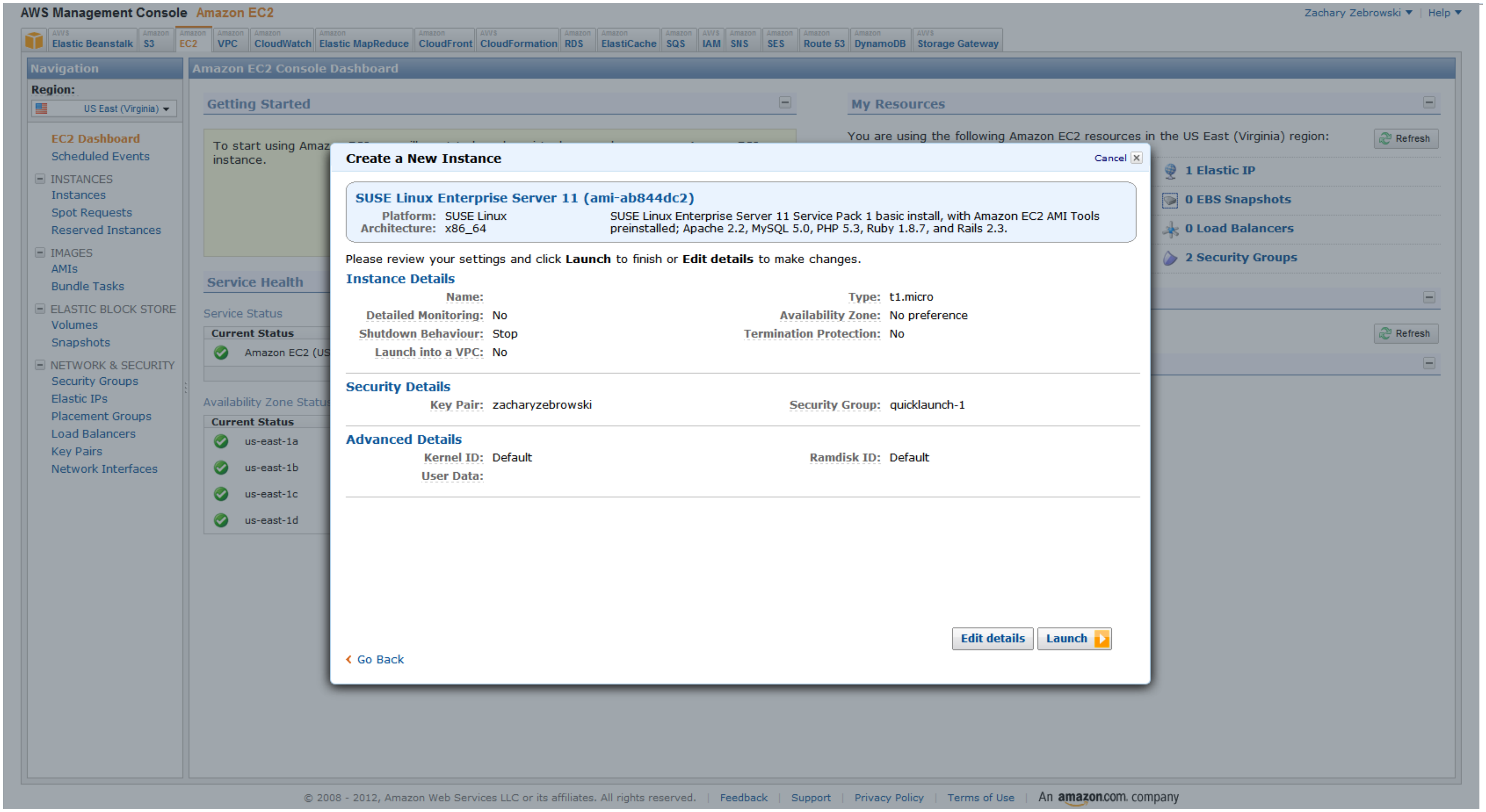
Choose a Launch Configuration:

More Amazon Machine Images NEW! Search through the full selection of public AMIs or choose from your own custom AMIs.		
Amazon Linux Includes the EC2 AMI Tools.	64 bit ●	32 bit ○
Microsoft Windows Server 2008 Microsoft Windows 2008 Datacenter edition	64 bit ●	32 bit ○
Microsoft Windows Server 2008 with SQL Server Express Includes Microsoft SQLServer 2008 Express, Internet Information Services 7, and ASP.NET 3.5.	64 bit ●	32 bit ○
Red Hat Enterprise Linux 6.2 Red Hat Enterprise Linux version 6.2	64 bit ●	32 bit ○
SUSE Linux Enterprise Server 11 SUSE Linux Enterprise Server 11 Service Pack 1 basic install, with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3.	64 bit ●	32 bit ○

Note: You can customize your settings in the next step.

Continue ▸

© 2008 - 2012, Amazon Web Services LLC or its affiliates. All rights reserved. | Feedback | Support | Privacy Policy | Terms of Use | An amazon.com. company



Create a New Instance

SUSE Linux Enterprise Server 11 (ami-ab844dc2)

Platform: SUSE Linux
Architecture: x86_64

SUSE Linux Enterprise Server 11 Service Pack 1 basic install, with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3.

Please review your settings and click **Launch** to finish or **Edit details** to make changes.

Instance Details

Name:		Type:	t1.micro
Detailed Monitoring:	No	Availability Zone:	No preference
Shutdown Behaviour:	Stop	Termination Protection:	No
Launch into a VPC:	No		

Security Details

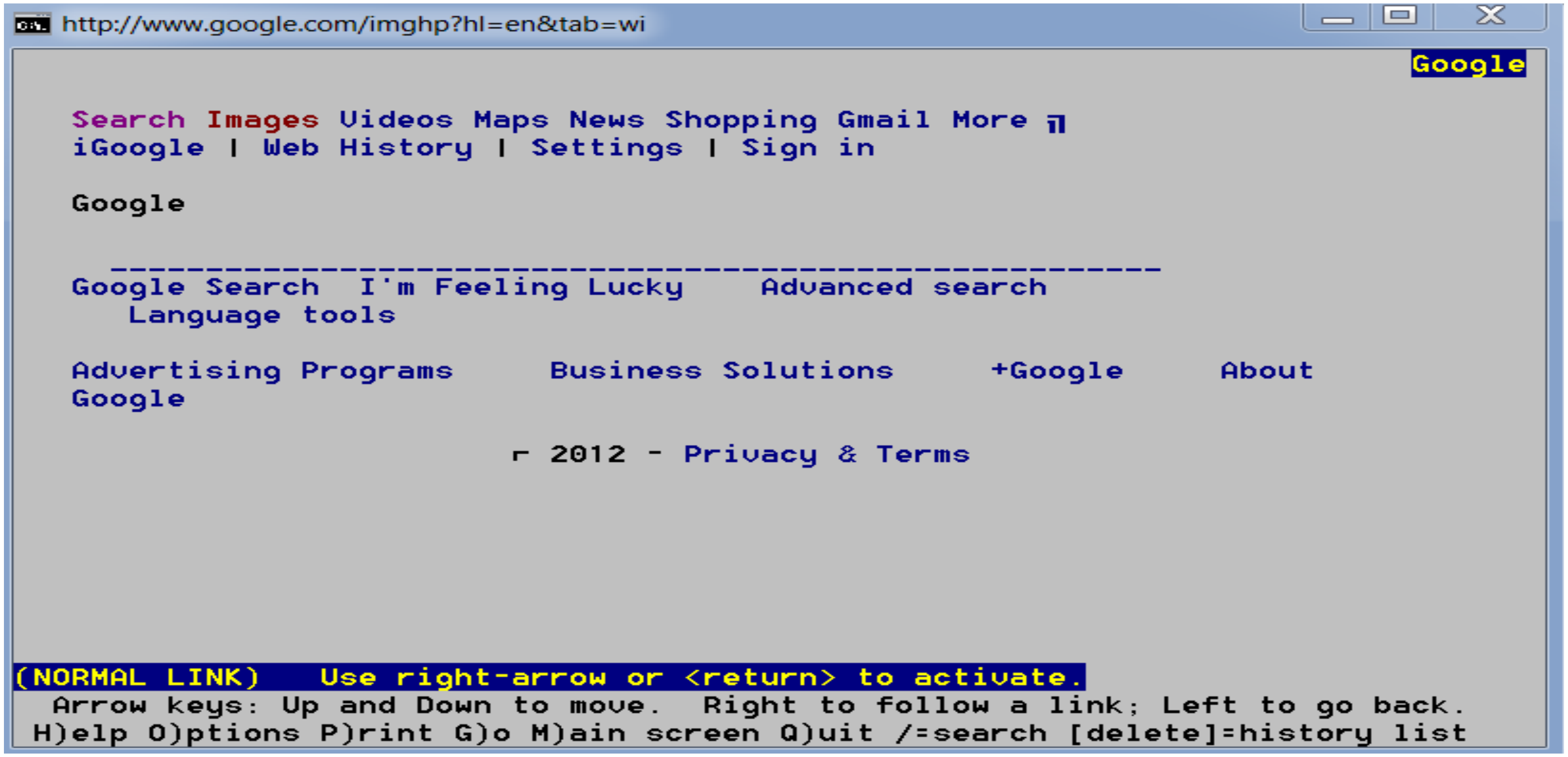
Key Pair:	zacharyzebrowski	Security Group:	quicklaunch-1

Advanced Details

Kernel ID:	Default	Ramdisk ID:	Default
User Data:			

Web Browsing via a Shell Account: Lynx

- Lynx is a simple text based web browser. A good tool to have if you're browsing on the command line.



```
http://www.google.com/imghp?hl=en&tab=wi

                                                                               Google

   Search Images Videos Maps News Shopping Gmail More ╖
   iGoogle | Web History | Settings | Sign in

   Google

     _______________________________________________________
   Google Search  I'm Feeling Lucky    Advanced search
      Language tools

   Advertising Programs     Business Solutions     +Google     About
   Google

                             r 2012 - Privacy & Terms

(NORMAL LINK)   Use right-arrow or <return> to activate.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Lynx Cheat Sheet

- Type lynx at command line. (Optionally with the URL you wish to go to).
- Use the up & down arrow keys to browse around the web page.
- Type G (for go) to go to another website.
- Press return to follow a URL link.

Lynx Lab

- Download & Install Lynx via http://lynx.isc.org/lynx2.8.7/index.html
- Start, and G)o to http://www.google.com
- Browse using <- -> /\ \/ pgup pgdown keys
- To follow a link, hit return.

VPN Providers

- VPN = Virtual Private Network
- There are numerous VPN services available commercially.
  - (Including freeshell.org)

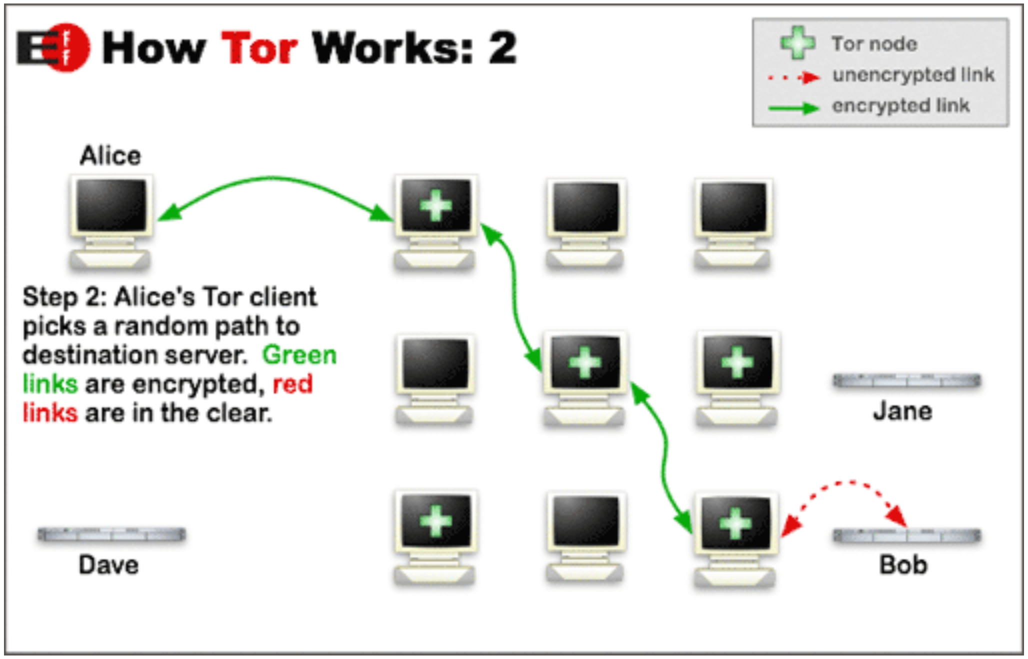
A note on mobile browsers that uses a proxy

- Browsers on mobile devices have different headers
- OperaMini – All traffic goes through opera-mini.net
  - Though it does include a HTTP_X_FORWARDED_FOR header with the client's IP ADDRESS.
    - Which may not appear, depending on how you set up your logs.
- Amazon silk hits a website twice, once from the client, once from the amazon cloud to "accelerate performance".

Anonymizers

- An anonymizer is a tool that allows you to improve your privacy and security on the internet.
- Tor
  - We will talk in depth about this in a second.
- Others
  - There are many.
  - Google “anonymous proxy”

Tor - How it works


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Source https://www.torproject.org/about/overview.html

Tor – Summary Info

- Tor is a socks proxy.
- A new Tor circuit is created every 5 minutes by default.
  - Can be changed via configuration options
- Runs on Windows / Linux / Mac / Android phone, etc.
- Tor is a bit slow.
  - But better since the latest version

Tor - What services are available

- Any TCP-based protocol
  - For any TCP-based protocol (telnet, ssh, nntp etc.), you can use TCP portmapping with 3proxy. For example, to map port 2200 of the local computer to port 22 (ssh) of my.ssh.server replace last string or add new string tcppm -i127.0.0.1 2200 my.ssh.server 22 to the 3proxy configuration from POP3. Now you can do ssh -p2200 127.0.0.1 to connect via SSH to my.ssh.server.
- See https://trac.torproject.org/projects/tor/wiki/TheOnionRouter/TorifyHOWTO/Misc or **http://preview.tinyurl.com/7pvwpnt**

Tor Software Bundles

- Software bundles for Windows / Mac / Linux allow for easy web browsing using tor.
  - Just double click on “Start Tor Browser” after you’ve downloaded the tor web bundle.
  - Also a chat client for IRC.

Tor – Hidden Web Sites

- *Tor allows clients and relays to offer hidden services. That is, you can offer a web server, SSH server, etc., without revealing your IP address to its users. In fact, because you don't use any public address, you can run a hidden service from behind your firewall.*
- Sites end in .onion, which isn’t routable on the internet, unless you’re running a tor client.
- Some “hidden” sites include:
  - Custom search engine for searching .onion sites
  - Wikileaks
  - **“One click and you will violate federal law” sites**
    - During October 2011, hacktivist collective Anonymous downed the servers of Freedom Hosting as part of OpDarknet, a campaign against child pornography. Anonymous stated in media releases that Freedom Hosting had refused to remove such sites as "Lolita City" and "Hard Candy," which it found to contain 100 GB of child porn. Anonymous released 1500 user names from these sites and invited the FBI and Interpol to follow up. (Source Wikipedia article below)
  - DANGER: You’re entering the dark side of the web.
- See http://en.wikipedia.org/wiki/.onion for various services

Tor – Hidden web sites part 2

- Why did I mention this?
  - It's good to know how wikileaks is hosted
  - It's good to know in case you need to set up something

- How to set up your own hidden service?
  - Follow tutorial:
  - https://www.torproject.org/docs/tor-hidden-service.html.en

- Example service:
  - http://3g2upl4pq6kufc4m.onion/ ← Duck Duck Go search engine

See also

- “How governments have tried to block tor”
  - http://www.youtube.com/watch?v=DX46Qv_b7F4
- Tor Metrics
  - http://metrics.torproject.org/index.html

Web browser “privacy” modes

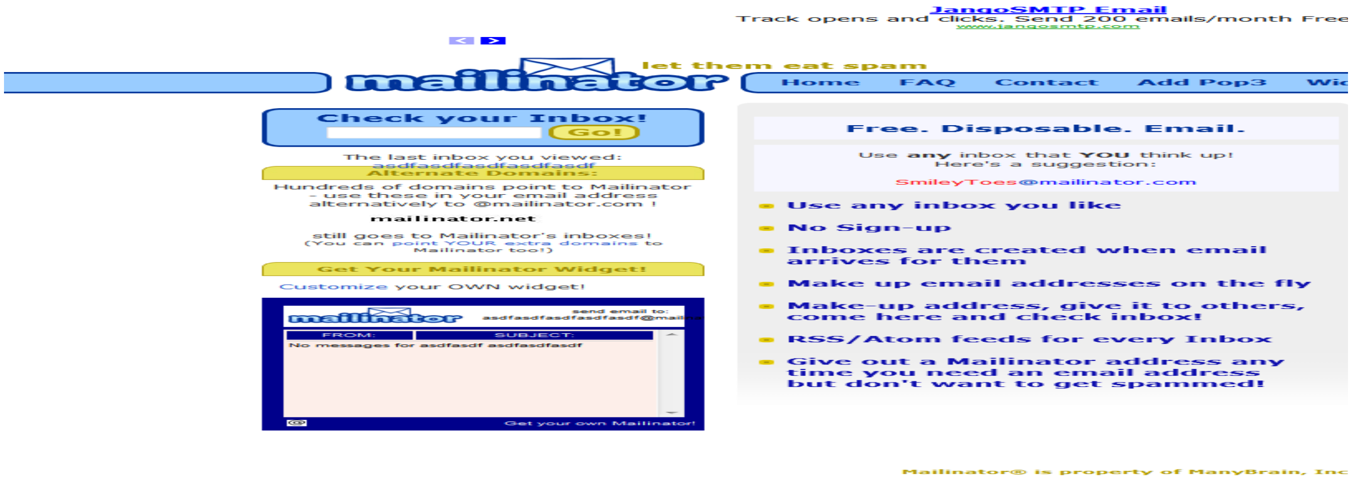
- Allows you to browse for a session without cookies / other methods being used.
- But in reality, there were some things that researchers were able to determine that still happened when you surfed via this technique.

Never Cookie

- A Firefox plugin which “blocks” evercookies.
  - From anonymizer.com
  - http://www.evercookiekiller.com/
  - Does not work with current (v12) Firefox.
    - Designed to work with v11.

Email Obfuscation Techniques

- Disposable email address
  - Mailinator has disposable email addresses
    - Randomly create a username and you have RSS / POP access to it. http://mailinator.com/index.jsp



JangoSMTP Email
Track opens and clicks. Send 200 emails/month Free
www.jangosmtp.com

The last inbox you viewed:
asdfasdfasdfasdfasdf

Hundreds of domains point to Mailinator - use these in your email address alternatively to @mailinator.com !

mailinator.net

still goes to Mailinator's inboxes!
(You can point YOUR extra domains to Mailinator too!)

Customize your OWN widget!

send email to:
asdfasdfasdfasdfasdf@mailina

No messages for asdfasdf asdfasdfasdf

Get your own Mailinator!

Free. Disposable. Email.

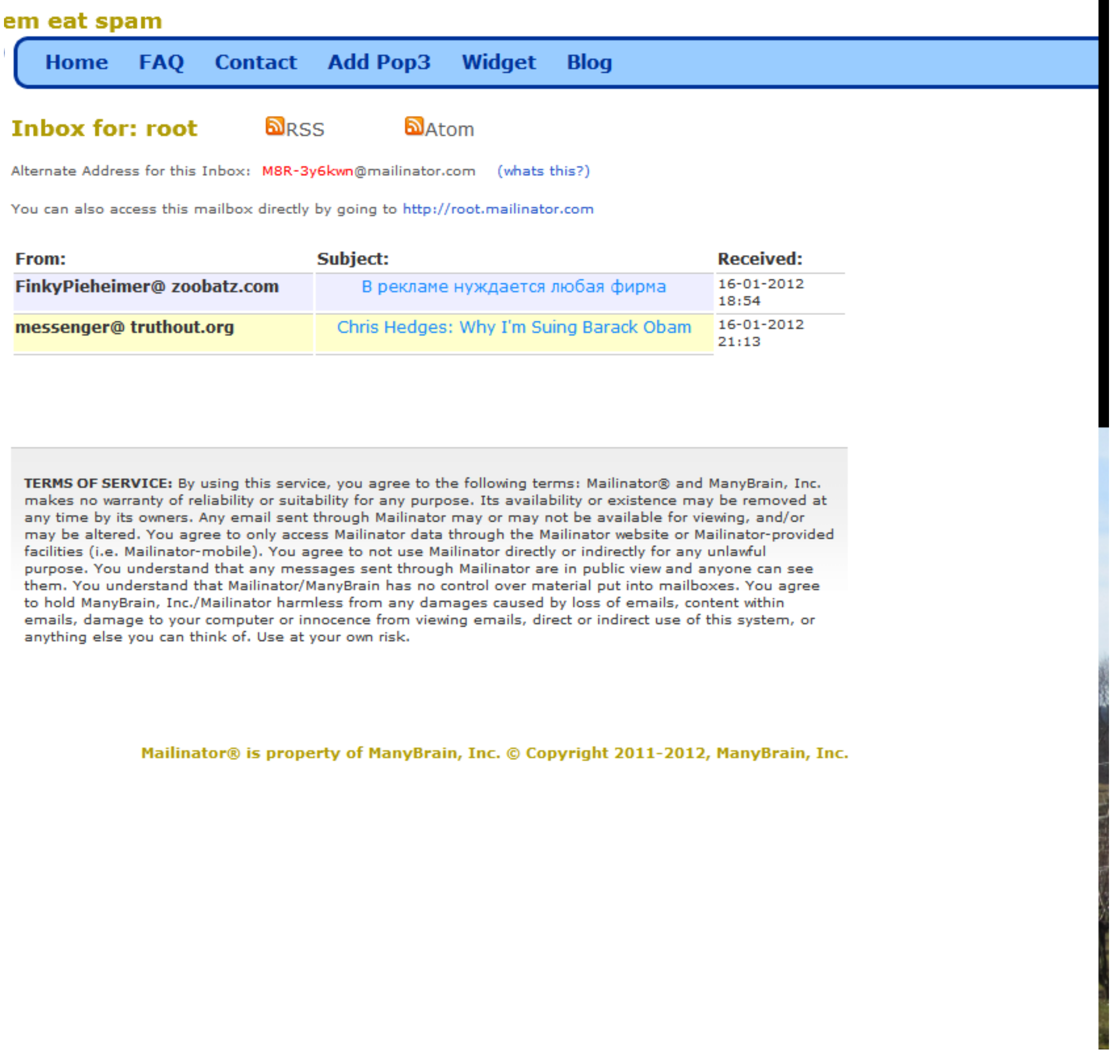
Use **any** inbox that **YOU** think up!
Here's a suggestion:

SmileyToes@mailinator.com

- Use any inbox you like
- No Sign-up
- Inboxes are created when email arrives for them
- Make up email addresses on the fly
- Make-up address, give it to others, come here and check inbox!
- RSS/Atom feeds for every Inbox
- Give out a Mailinator address any time you need an email address but don't want to get spammed!

Mailinator® is property of ManyBrain, Inc

Sample message listing



Inbox for: root RSS Atom

Alternate Address for this Inbox: M8R-3y6kwn@mailinator.com (whats this?)

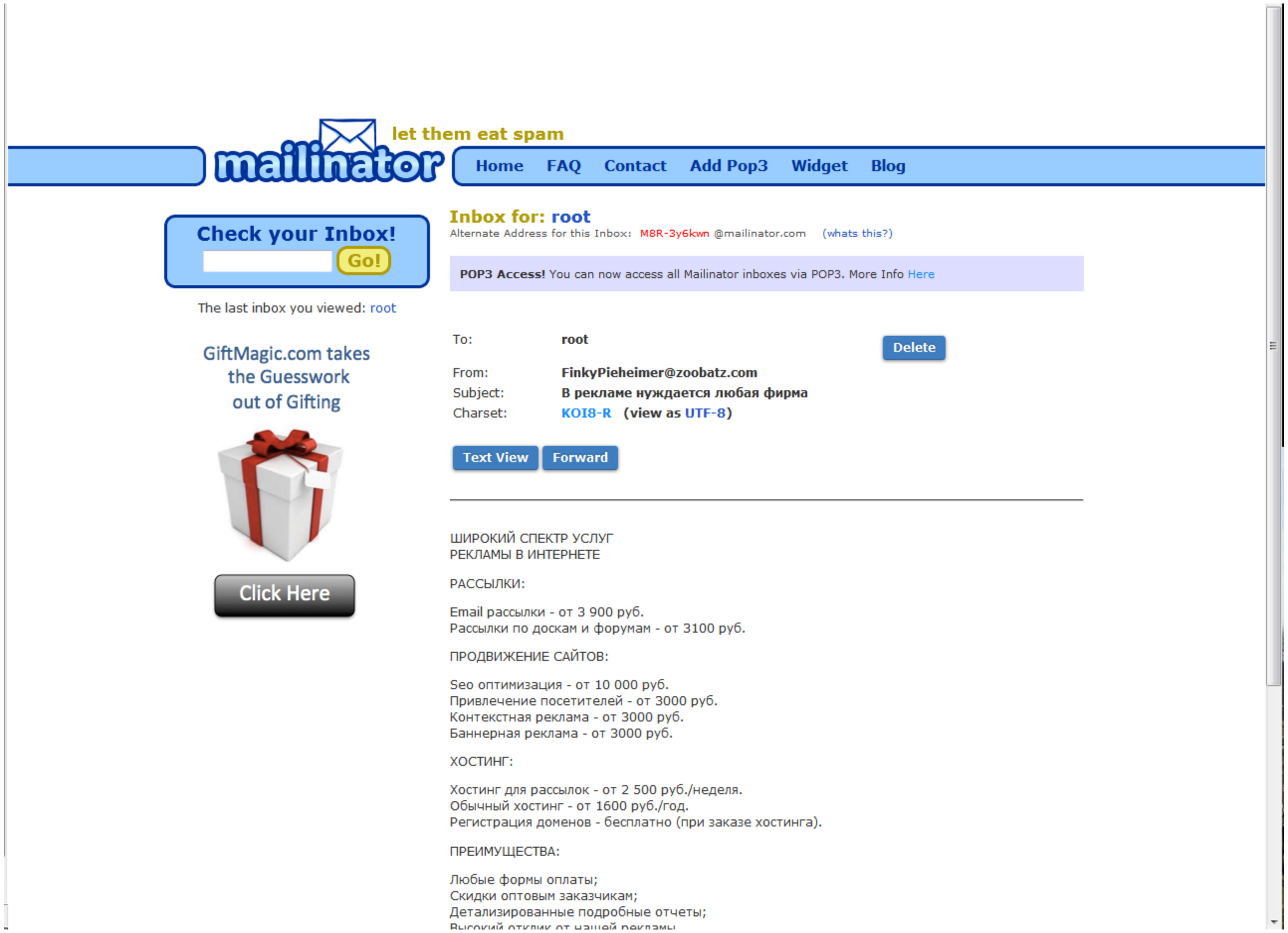
You can also access this mailbox directly by going to http://root.mailinator.com

From:	Subject:	Received:
FinkyPieheimer@ zoobatz.com	В рекламе нуждается любая фирма	16-01-2012 18:54
messenger@ truthout.org	Chris Hedges: Why I'm Suing Barack Obam	16-01-2012 21:13

TERMS OF SERVICE: By using this service, you agree to the following terms: Mailinator® and ManyBrain, Inc. makes no warranty of reliability or suitability for any purpose. Its availability or existence may be removed at any time by its owners. Any email sent through Mailinator may or may not be available for viewing, and/or may be altered. You agree to only access Mailinator data through the Mailinator website or Mailinator-provided facilities (i.e. Mailinator-mobile). You agree to not use Mailinator directly or indirectly for any unlawful purpose. You understand that any messages sent through Mailinator are in public view and anyone can see them. You understand that Mailinator/ManyBrain has no control over material put into mailboxes. You agree to hold ManyBrain, Inc./Mailinator harmless from any damages caused by loss of emails, content within emails, damage to your computer or innocence from viewing emails, direct or indirect use of this system, or anything else you can think of. Use at your own risk.

Mailinator® is property of ManyBrain, Inc. © Copyright 2011-2012, ManyBrain, Inc.

Sample email view



The last inbox you viewed: root

Inbox for: root

Alternate Address for this Inbox: M8R-3y6kwn @mailinator.com (whats this?)

POP3 Access! You can now access all Mailinator inboxes via POP3. More Info Here

To:	**root**
From:	**FinkyPieheimer@zoobatz.com**
Subject:	**В рекламе нуждается любая фирма**
Charset:	**KOI8-R (view as UTF-8)**

ШИРОКИЙ СПЕКТР УСЛУГ
РЕКЛАМЫ В ИНТЕРНЕТЕ

РАССЫЛКИ:

Email рассылки - от 3 900 руб.
Рассылки по доскам и форумам - от 3100 руб.

ПРОДВИЖЕНИЕ САЙТОВ:

Seo оптимизация - от 10 000 руб.
Привлечение посетителей - от 3000 руб.
Контекстная реклама - от 3000 руб.
Баннерная реклама - от 3000 руб.

ХОСТИНГ:

Хостинг для рассылок - от 2 500 руб./неделя.
Обычный хостинг - от 1600 руб./год.
Регистрация доменов - бесплатно (при заказе хостинга).

ПРЕИМУЩЕСТВА:

Любые формы оплаты;
Скидки оптовым заказчикам;
Детализированные подробные отчеты;
Высокий отклик от нашей рекламы

Can I Send Mail via mailinator address?

- Maybe – depends on your ISP
- How to configure:
  - http://borisbrodsky.com/2007/12/ubuntu-relay-email-server-thro-11.html

“Cypherpunk ; Mixmaster ; Mixminion” anonymous remailer email system

- See: http://en.wikipedia.org/wiki/Anonymous_remailer
- Easy to find a simple web page which you can anonymously send emails from a bogus email address to a real email address.

See also

- https://burnnote.com/

Burn Note enables you to communicate online as privately as a spoken conversation.

Each Burn Note can be viewed only once and then it is deleted. Deleted Burn Notes are completely erased from the Burn Note servers so it impossible for anyone to retrieve them. More details are available on our FAQ and our technical information page.

Burn Note is useful for private communication. For example Burn Note can be used to securely send a password. It can also be used to have an off-the-record conversation with a friend.

(via spymuseum.org)

Lab 6 – Browsing via Tor

- Browse in a non-tor browse to http://zak.freeshell.org/env.pl and note the variables shown.
- Download the tor browsing bundle from https://www.torproject.org/download
- Browse within the tor bundle to http://zak.freeshell.org/env.pl and note what has changed.
- Browse to another site and see if you can tell any differences.
- Also, try browsing to : http://3g2upl4pq6kufc4m.onion/ (Duck Duck go hidden service)

Lab 6B – Sending an email to mailinator.com

- Open outlook (or your favorite online server – Gmail)
- Send an email to: sampleforclass@mailinator.com
- Browse to : http://mailinator.com/maildir.jsp?email=sampleforclass
  - – wait for mail to show up.

Fixing / exploiting browser vulnerabilities

- Proxy Filters
  - Pollipio Installed by default w/ tor
- Using telnet to browse websites via proxy
- Using timed queries
- Use “new” features of html / JavaScript
- Breaking Tor

Proxy Filters

- Pollipio is a http filter, installed by default on Windows installations of TOR.
- It will filter out ads, JavaScript, cookies, etc.
- Other solutions exist for other types of OS's.

- But, as pollipo is known to be installed with TOR, you can configure attacks against the version of pollipo.

Telnet directly to a website

- You can use the program telnet to request an arbitrary page on a website, using the GET syntax.
- Example:

```
telnet host 80
Then:
GET /
```

Use timed queries

- To defeat time zone analysis, consider writing a script that will randomly request the page of interest at a random time of day.

Use new features of JavaScript

- If you can get the user to run a JavaScript command, you can then insert code that filters may not recognize.
- For example, the new location JavaScript API still works through TOR on the android, because JavaScript is not filtered.
  - For **older versions of TOR** on android

Trick the browser to open a session not being proxied through TOR

- If you can monitor another type of session (like ftp, or ldap request), and you can monitor that other session, you can determine the unproxied ip address.
  - Note! As of the latest version of the TOR browser bundles (as of April 2012), this trick does NOT work.
    - Unless you're using "advanced" installation of TOR, which does NOT include a bundled browser, which might have incorrect settings set.

Sorry, doh is not an acceptable word

If you know someone is going through TOR, you can exploit it.

- First, identify if the user is coming from a proxy, using IP Geolocation or other methods.
- Check to see if any long term cookies are set for the client.
- Know the version of the proxy filter
  - And see if that proxy has exploits.
- Trick the browser into doing something it shouldn't.
- Trick the user into doing something it shouldn't.
- Statistical use of looking at TOR packets to determine what content is looking over TOR.
  - There was a presentation at a security conference about this.
  - Similar to the "phoneme" attack against Skype to determine what a user is saying
- Statistical use of looking at a web browser connections to determine type of browser.
  - Written in a book entitled Silence on the Wire which mentions other active and passive techniques.
- Setup then monitor unencrypted traffic on an end node.

Defeating IP Geolocation techniques

- You can tell TOR what endpoint to use, if you need to come out of a certain country.
  - Use .exit special domain name to exit tor from a particular node.
    - Go to http://torstatus.blutmagie.de and pick a router name
    - Then browse to http://zak.freeshell.org/env.pl.someexit.exit where someexit is a router name.
    - You need to edit the config file to allow for exiting out of certain nodes as this is a security risk.

Questions?

- Break!
- See Also: http://en.wikipedia.org/wiki/Internet_privacy which is a good reference point too.
- Next up – Forensic database & log analysis