

Workbook



SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

Home

Welcome to the SANS SEC487 Wiki



SEC487 Portal Version: 2.0.1 - Current Course Version E02_01

© SANS Institute 2019

Contained in the wiki, you will find:

- Electronic Copies of the Lab Guides
- Future course content

Course/Lab/Wiki Bugs or Suggestions

Please let us know if you find any bugs in the courseware/labs/wiki we need to fix. Also, reach out if you have suggestions to improve the course (for example: content/labs/tools that should be added, removed, or updated). The easiest ways to submit these improvements is by sending an email to updates@sec487.info or sending Micah a direct message on the SEC487 Slack group.

Addendum

Things change fast in the OSINT world and we do our best to keep this course updated. We also want you to learn from the other students that share their tips and tricks in class. To keep you supplied with the latest OSINT skills and info from your peers, we developed the course Addendum.

Wiki Change Log

Our course is ever-evolving due to the changes in OSINT tools, sites, and techniques. Our wiki too changes. Our change log of major changes can be found at changelog.md.

Wiki Updates

To update the wiki inside your SEC487 VM, launch a terminal window and type: sudo wi ki up. sh. You will be prompted for your password and then your wiki will update.

Addendum

We all know that the field of OSINT moves pretty fast; faster, in-fact, than we can keep up with in our books and blog posts. Students and instructors of SEC487 are constantly suggesting new tools and techniques that'd be amazing for the class. I maintain a private document of all those links and such so that, when I make the changes to the course, I can include those terrific resources.

What I realized is that, me keeping a *private* repository does not help *you*. I know of a bunch of extra material that will eventually be in the class but it may be new to you.

This document is an attempt at getting you *what will be in the next course update* in a raw form but a timely manner. The document will change over time and I'm hoping it helps you keep current and continue to learn.

--- *Micah (WebBreacher)*

Day 1 Content

*

Day 2 Content

- User name enumeration (similar to WhatsMyName) - <https://github.com/sherlock-project/sherlock>
- Sock puppet profile images - <https://www.generative.photos/>

Day 3 Content

- Satellite Imagery - <https://satellites.pro/>

Day 4 Content

*

Day 5 Content

- Monitoring Section - talkwalker (like Google Alerts) - <https://www.talkwalker.com/>
- International Address Formats - <https://www.bitboost.com/ref/international-address-formats.html>

Wiki Changes

Below are the major changes that we've made in this wiki. Most recent changes are at the top.

December 2019

- Added content to addendum.md
- Added satellites.pro, Sherlock, generative photos.

NetWars Questions for SEC487

To make the class more fun and make sure that people of all skill levels are challenged, we have created a NetWars server for SEC487 students. This server contains a bunch of optional OSINT challenges for you to solve.

Below are the credentials for the server. *Please do not share them outside the class.*

This is an optional part of class. Most questions have `Hints` to help you along.

Server: <https://sec487-e01.labs.sans.org/>

User: SEC487-CTF

Password: Somewhere80bj ecti ve7Sal t7

Single click link: <https://SEC487-CTF:Somewhere8Objective7Salt7@sec487-e01.labs.sans.org>

1. Log into the server using the credentials above.
2. Register for an account using the `Register` button in the upper right of the page.
3. Log into the web application using your new credentials.
4. Click on the `Questions` link at the top of the page.
5. Submit your answers!

Order of Labs

Day 1 Labs

- Setup
 - OSINTing People
 - Mapping Minds and Cases
 - Hunchly
 - Searching for IP
 - Managing Passwords - Optional
 - Slacking It - Optional
-

Day 2 Labs

- Harvesting Web Data
 - Web Analytics
 - Metadata Analysis
 - Retrieving Files Challenge - Optional
 - About My Home
 - Finding Emails
 - Finding Users
 - Reversing Images
-

Day 3 Labs

- People Searching

- Facebooking
 - Tweet Analysis
 - Twitter Bot Analysis
 - Aerial Adventure
 - Location Challenge - Optional
-

Day 4 Labs

- Domains and IPs
 - Domain Challenge - Optional
 - Wireless OSINT
 - Spiderfoot
 - Government Trivia
 - Business OSINT
-

Day 5 Labs

- Tor
 - HaveIBeenPwned
 - International Issues
 - Solo CTF
-

General Labs

- Cached Content

Setup

Table of Contents

- Objectives
- Preparation
- Step-by-step Instructions
 - Setup VM VPN (In-class students only)
 - Practice disconnecting the VPN
 - Practice Updating the Electronic Workbook
 - Join Slack (optional)

Objectives

- Log into and configure OSINT virtual machine
- Configure VPN [Not for remote students]
- Become comfortable with using the interface
- [OPTIONAL] Join the SEC487 Slack group

Preparation

You need internet access

Your host computer must already be joined to the class network and be able to reach the internet using a web browser. If you cannot launch a web browser and reach a web site such as <https://google.com>, please troubleshoot your host's networking before proceeding with this lab. Your VM's network adapter should be in NAT mode (bridged mode may also work depending upon the network).

Step-by-step Instructions

There is a video walkthrough for this lab. [Click here to view it.](#)

Setup VM VPN (*In-class students only*)

In-class VPN

If you are taking the class via OnDemand, Simulcast, or vLive, skip the following section. The VPN is for students in a live classroom.

1. Get your student number from the instructor

Your instructor will assign you a student number. With this, you will modify the domain name of the host your system will VPN to so that your traffic is going to its own server. We do this so that your searches are isolated from the other students and, if your IP address gets blocked on some system, we can reassign you another system so that you can continue to complete the labs.

Using a VPN protects the data traveling to and from your computer while you are conducting your assessments. It can also be used to bypass filtering one your computer's local network. So if you are using a hotel's Wi-Fi network and they are preventing the use of Tor, we may be able to connect our system to a VPN server on the internet and then send our Tor traffic through the VPN, bypassing the hotel's inspection of the traffic.

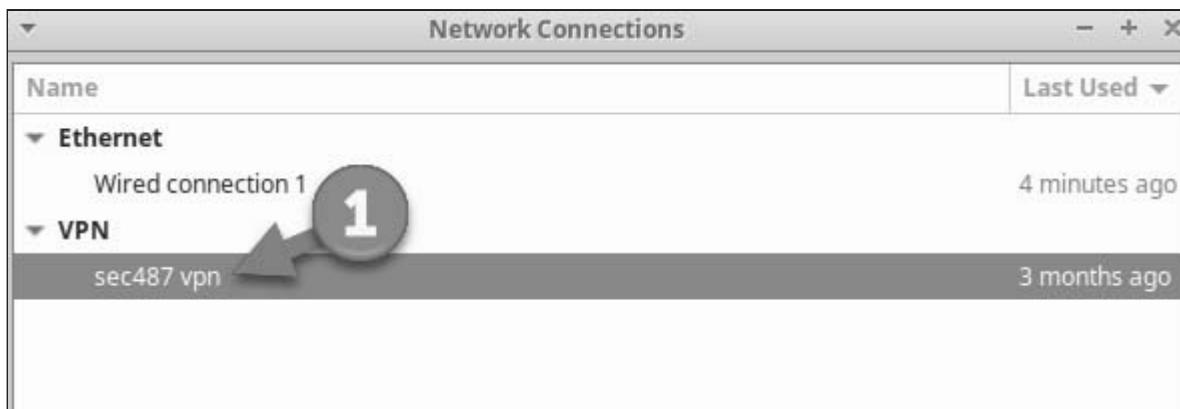
Record your student number in your notes.

2. Let's configure the VPN now. In the upper right of the VM, there is an icon with two arrows, one

 pointing up and one down. Left click those arrows so that the configuration menu appears (arrow 1 below).



3. Click on Edit Connections... (arrow 2 above). This allows us to reconfigure the network settings of your system. You should see the screen below.



4. Double click on the sec487 vpn entry (arrow 1 above).

We need to change the host name of the VPN server to which your VM will connect.

5. Change the contents of the Gateway: field from `studentXXXXXXXXXX.sec487.info` to read: `student#.sec487.info` and insert the student number you received from the instructor into the `#` place in the host name.

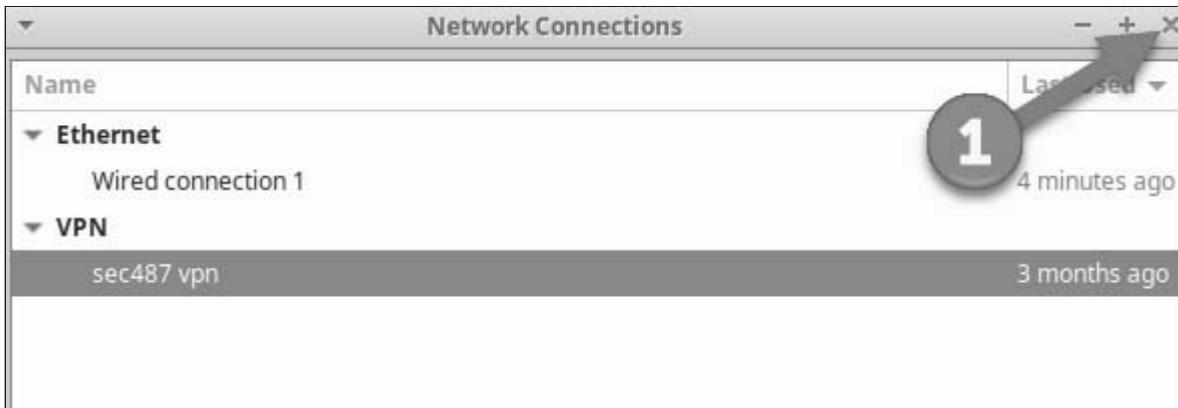
For example, if the instructor assigned you to be student 5, your Gateway: field contents should read: `student5.sec487.info` (as shown below at arrow 1).



Common error

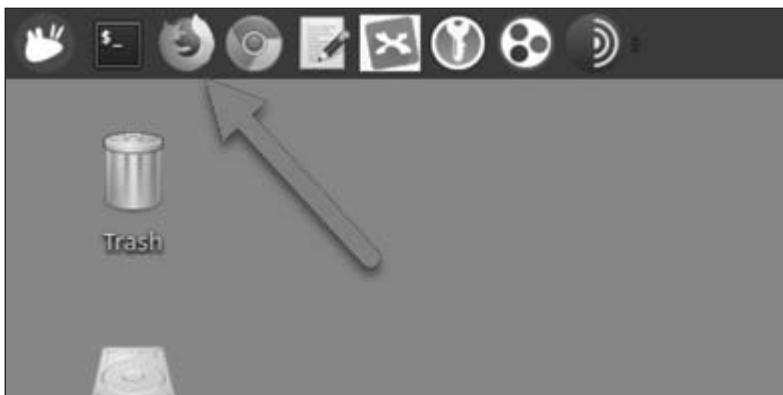
Please make sure that the Gateway: field only contains the `student#.sec487.info` content. Any extra spaces, letters, or numbers will cause this VPN setup to fail.

6. Click the Save button at the bottom of the window (arrow 2 above) to save the content.
7. Press the close button (X) on the Network Connections window to close it (arrow 1 below).



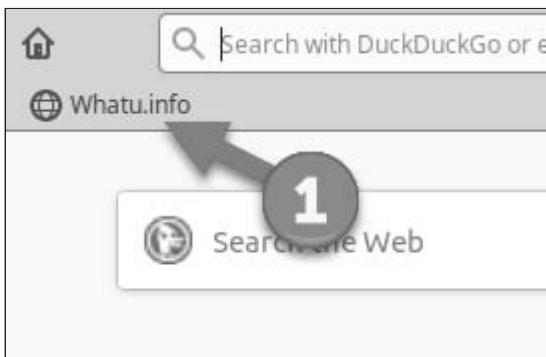
Before we engage the VPN, let's check to see if your VM has a connection to the internet by launching the Firefox web browser and visiting a site that shows you what IP address your system is using to browse the internet.

8. Launch the Firefox web browser by clicking the Firefox icon in the upper left of the menu bar (it may already be running if you are using it to read these lab directions).



9. Click the Whatu.info Firefox bookmark.

We placed a bookmark in the bookmarks bar for Whatu.info (a site we created for checking browser information). Click that bookmark once to visit the <https://whatu.info> web site.



This site will show you what IP address it sees your browser using.

10. Note the IP address displayed in the Your IP address: box (arrow 1 below).

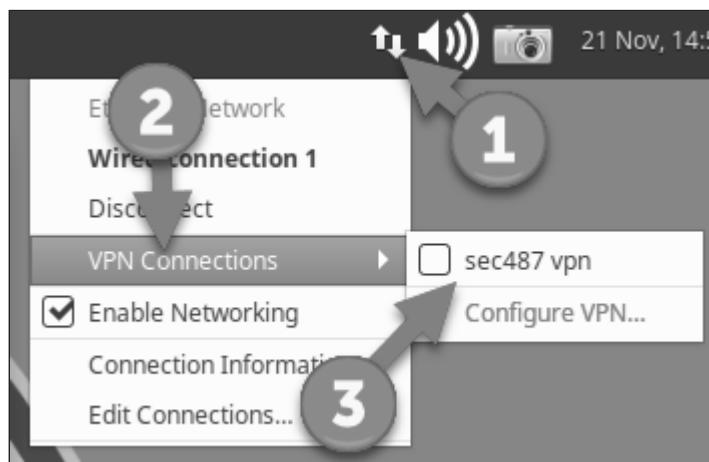
This is how your browser appears to other sites.

This page echoes back to you several pieces of data that web sites 'know' about you. This is a great awareness tool for you to see how your device presents itself to other sites. It also leverages your location services to show your IP location and such. It is not 100% accurate.

Item	Value
Your IP Address:	1
Your User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
HTTP Referrer:	

Write down what the site reports your system's IP address is.

11. Click once on the arrows icon (arrow 1 below) and then mouse-over the VPN Connections option (arrow 2 below). To start the VPN to the remote server, left click the "sec487 vpn" item (arrow 3 below).



Wait for the connection to be established. If everything worked well, the double arrow icon in the menu bar should now show computer icon  noting that the VPN was successful.



Troubleshooting

If your VM did not connect to the VPN, go back ensure that the host name entered is like `student1.sec487.info` (but with your student number instead of the "1")



Still having issues?

Contact your instructor.

12. Press the reload icon in the Firefox web browser (arrow 1 below) to reload the `https://whatu.info` web page. The IP address reported should be different than what it was before the VPN connection was created.



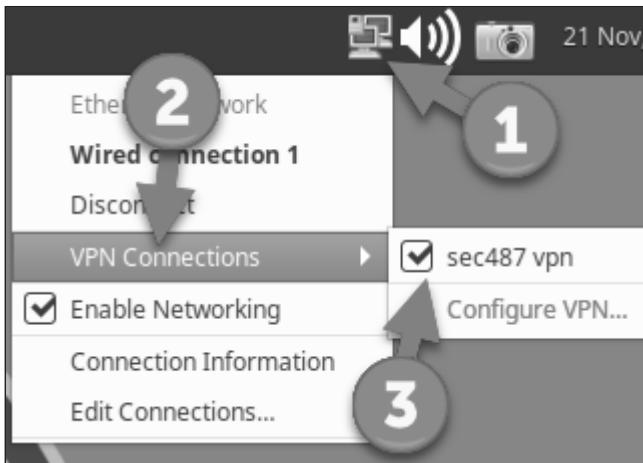
Write down what the site reports your system's IP address is with the VPN enabled.

Practice disconnecting the VPN

You will need to sometimes turn the VPN connection off. Doing this is simple.



1. Click the  icon in the system menu bar (arrow 1 below) to drop down the networking menu.



2. Move your mouse over top of the VPN Connections entry (arrow 2 above) and then move it right to the "sec487 vpn" (arrow 3 above).

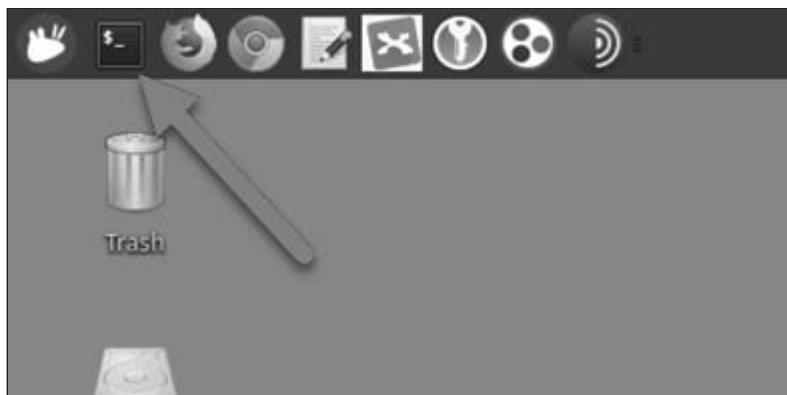
That "sec487 vpn" should have a check mark on the left of it showing it is enabled (as shown above). To disable it, just click the words "sec487 vpn" once.

When you do that, the  icon in the menu bar will change to the non-VPN state that looks like .

3. Press the reload icon in the Firefox web browser to reload the web page and see that the IP address reported should be the same as you noted before we turned the VPN on.
4. You may close the Whatu.info web page tab in your browser as we have completed this section of the lab.

Practice Updating the Electronic Workbook

1. We need to ensure that your electronic course materials are up-to-date. Ensure that your VPN is disabled and open a terminal window by clicking the terminal icon in the task bar.



2. In that terminal window, type: `sudo wikiup.sh` and press `Enter` ("1" in the image below).

A screenshot of a terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main area shows the command `sudo wikiup.sh` being run. The terminal output includes:

```
student@sec487 (15:19:25) :~$ sudo wikiup.sh
[sudo] password for student:
HEAD is now at 57b07bf removing test dir
Already up to date.
HEAD is now at 99e4b43 updated content
Warning: Permanently added the RSA host key for IP address '...' to the
list of known hosts.
remote: Enumerating objects: 34, done.
remote: Counting objects: 100% (34/34), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 20 (delta 5), reused 20 (delta 5), pack-reused 0
Unpacking objects: 100% (20/20), done.
From wiki:WebBreacher/sec487-wiki-e02
  99e4b43..f413d92 master      -> origin/master
Updating 99e4b43..f413d92
Fast-forward
 labs/setup/index.html      | 127 ++++++
 labs/setup/media/image1.png | Bin 0 -> 718 bytes
 labs/setup/media/image10.png| Bin 1264 -> 6833 bytes
```

The terminal window is annotated with three numbered arrows: "1" points to the `Enter` key, "2" points to the password entry field, and "3" points to the progress bar for file transfers.



No Dots When Typing Password

When you type in your password for this command, there will be no feedback from the system (no `*` show up when you type your password). This is normal. Just type your password and press the `Enter` key.

3. You will be asked to enter your student user password (arrow 2 above). Your password should be `Securi ty487` unless you changed it.

Let the update process complete. It may take a while to finish depending upon the network and your computer speeds and the amount of new data to be downloaded into your system (arrow 3 above).

- When the process completes, type: `exit` and press `Enter` to close the window.



Reload Your Browser Page

In your Firefox web browser, make sure to reload the wiki page so that you can see the new content.

Join Slack (optional)

- In a web browser, visit <https://sec487.info/joinslack> to join the SEC487 Alumni Slack group.
- Fill in the email address you wish to use for Slack (arrow in the image below). You will need to verify the address so you do need to be able to receive an email.

The screenshot shows a web browser window for Slack. At the top, it says '# slack'. Below that, there's a heading 'Join the Slack workspace' followed by a bolded 'SEC487alum'. Underneath, a question asks 'What is your email address?' with a placeholder 'you@example.com'. A large, dark grey arrow points from the bottom right towards this input field. To the right of the input field, there's a 'Verify email' button. On the right side of the screen, there's a grey sidebar featuring two user icons: a man with glasses and a woman, both with speech bubbles above them. One of the speech bubbles contains three dots, and another contains a PDF icon.

3. You will receive an email that has directions on how to verify your account. Follow those directions.



Please check your email!

We've sent an email to test@example.com with instructions for joining this team.

We need you to verify your email address so you can finish creating your account.

To continue, go open the email.

(You can close this window now.)

4. There is a lab that you will do later in the day that has instructions on how to configure Slack in your VM if you wish. Close and exit the Firefox web browser.

The lab is completed. You may close the Firefox web browser if desired.

This page intentionally left blank.

OSINTing People

Table of Contents

- Objectives
- Goals
- Preparation
- Instructions
 - Targets
 - Flags
 - Documentation
 - Scoring

Objectives

- Find as many flags as you can about a human target on the Internet

Goals

1. Choose one of the targets below
2. Using passive/non-interactive techniques, find as many of the flags as you can about the target
3. Try to use sources other than Wikipedia to gather your results.
4. Document each flag and where you found it (URL)

Preparation

VPN if problems

Instructions

There is a video walkthrough for this lab. [Click here to view it.](#)

Targets

Choose one to research. DO NOT INTERACT WITH THEM IN ANY WAY! (No friending, connecting, social engineering the targets, their families, friends, or coworkers.)

1. Amiya Kumar Mallick (India)
2. Maia Chiburdanidze (Georgia)
3. Marcel Herrmann Telles (Brazil)
4. Nadia Murad (Iraq)
5. Cristiano Ronaldo (Portugal)
6. Lee Soo-jung (United States)

Flags

1. Aliases or nicknames
2. Username(s) for online accounts
3. E-mail(s)
4. Personal phone number(s)
5. URLs to social media profiles

6. Date and place of birth
7. Schools attended
8. Jobs (current and past)
9. Home addresses (both past and current)
10. Pet names
11. Hobbies
12. Avatars or profile photos that the target uses on social media
13. Places visited in last five years
14. Favorite food, drink, and music
15. Favorite sports team
16. Official government identification number (SSN / Passport)
17. Mother's maiden name
18. Family member names and relationships (mother, father, spouse, kids, ...)
19. Negative press about the target

Documentation

1. Record your activities in your favorite documentation application. If you do not have a favorite one, there is a spreadsheet (arrow 1 below) in the VM's student home directory in the /home/student/labs/osinting-people/ directory (arrow 2 below).



2. This file can be opened using LibreOffice Calc application (similar to Microsoft Excel) from the menu system (arrows 1 and 2 below).



3. Remember to record the location or URL where you found the information.

Scoring

1. When finished, score your work.
2. 1 point for every validated flag (if you find multiples of a flag, each one gets an additional point so if you find 1 email address you get 1 point but find 3 of them and you get 3 points)

This page intentionally left blank.

Mapping Minds and Cases

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step Instructions
 - XMind
 - Screenshot App
 - Maltego Casefile
 - Adding Entities to a Graph

Objectives

- Populate a MindMap file
- Gain experience taking a screenshot in the VM
- Manipulate data in Maltego's Casefile

Goals

1. Use the MindMap application to populate the `/opt/tools/osinttools/OSINT_Maps.xmind` template with meaningful data.
2. Take a screenshot of a web page
3. Use Maltego's Casefile to manipulate the `maltego_princess_bride.mtgI` file

Preparation

XMind Resolution

The resolution for the virtual machine's display should be set to 1024x768 or greater so that the XMind application's window displays properly. If your virtual machine's screen is less than that value, you will need to move the window around using its border.

No VPN

Step-by-step Instructions

There is a video walkthrough for this lab. [Click here to view it.](#)

XMind

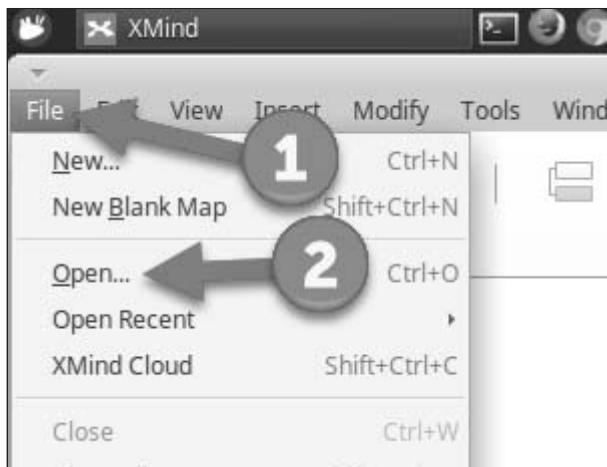
Let's start our documentation lab with the MindMap application. We are using the free version of the application from XMind.net.

1. Launch the application by clicking the XMind icon in the menu bar (shown below).



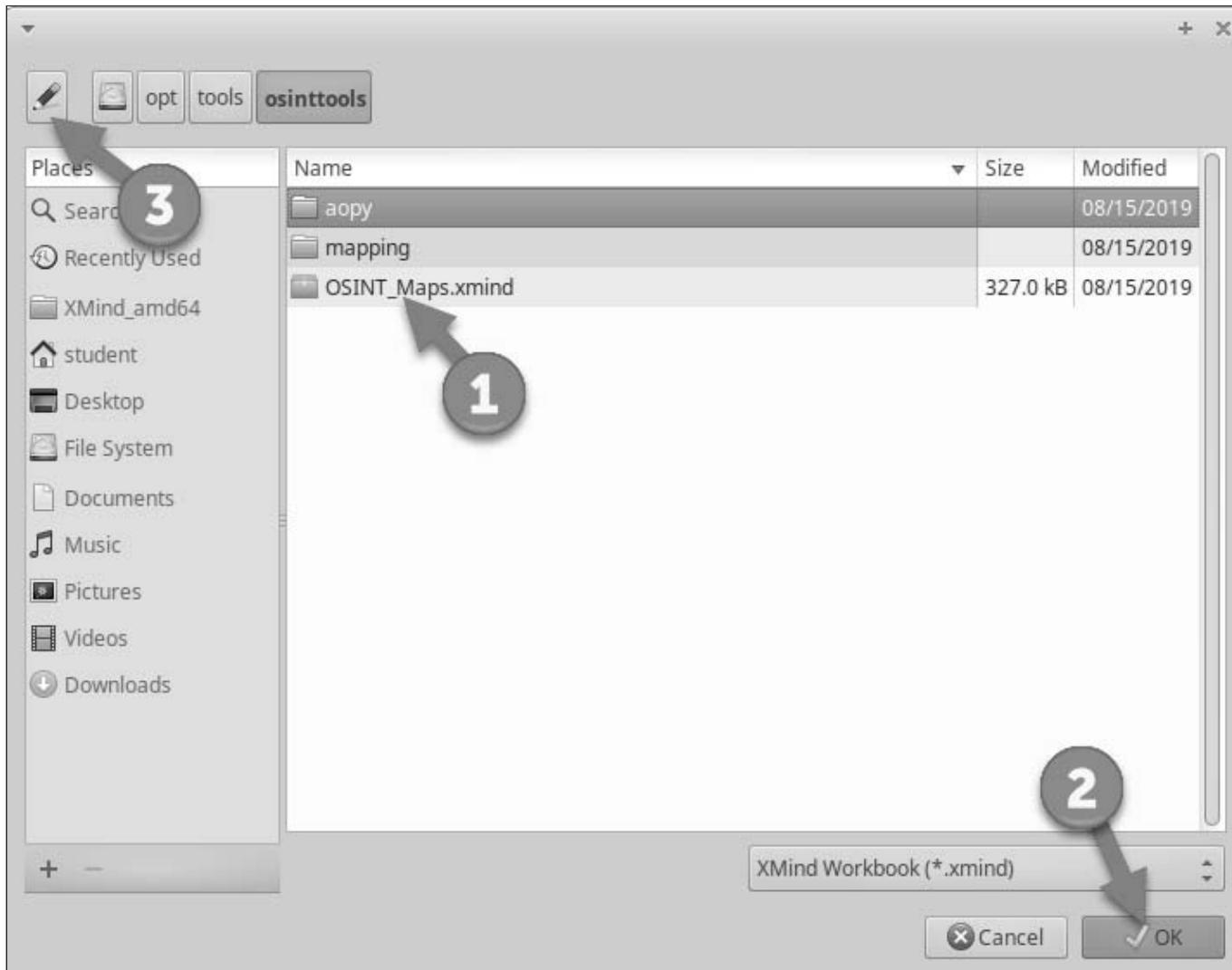
We have a template file for you to use.

2. To load the template, in the application select the File menu item then Open...



The first time you do this, the Open dialog box will most likely be in the Recently used section.

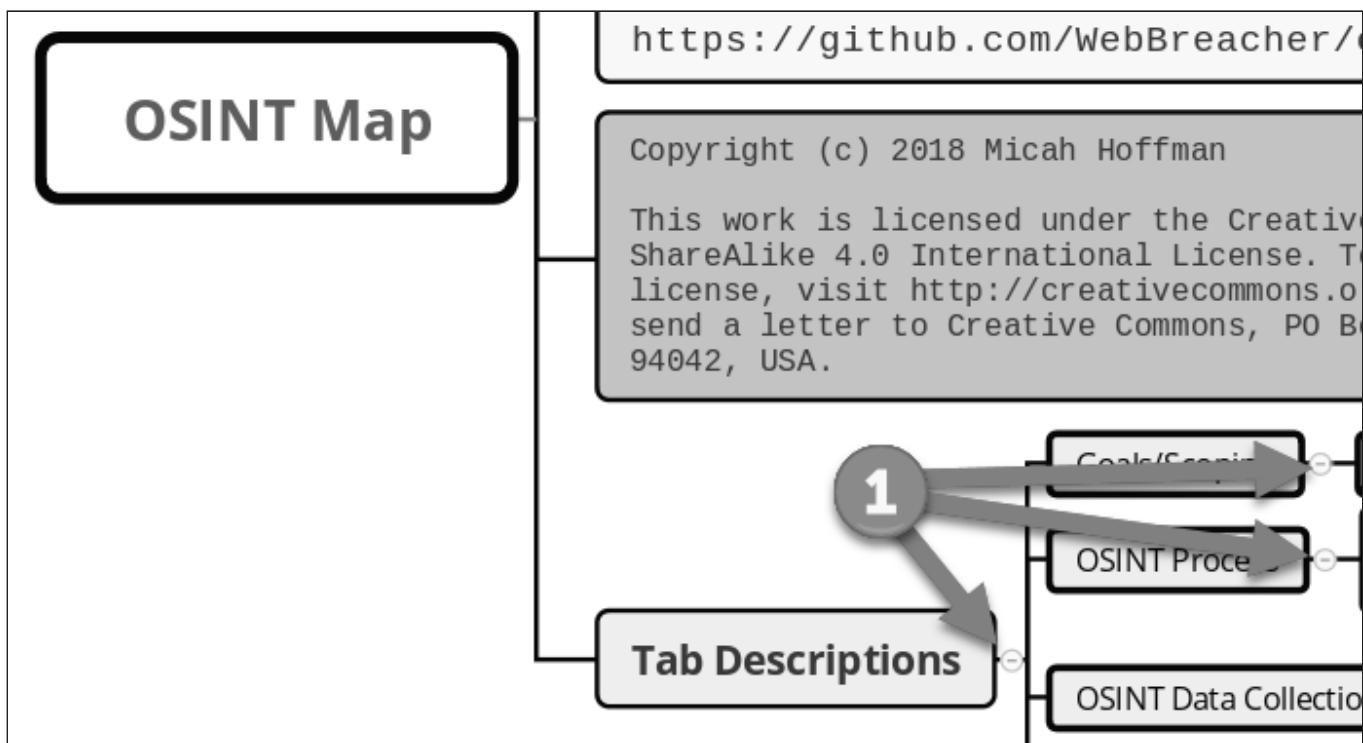
3. If it is on Recently Used, then double click the `OSI NT_Maps. xmind` file (arrow 1 below) and press the "OK" button (arrow 2).



If you do not see the file needed for this lab in the main window, click on the pencil (arrow 3 above) and then type: /opt/tools/osinttools into the Location: field and press Enter. You should now see the file you need.

4. The document will load (this may take a little bit of time) and you should see the data in the main window of the application.
 - Zooming in and out are important skills to have as your MindMaps may get quite large once you begin adding images to them. You can zoom in and out by using the buttons to increase or decrease the zoom or via holding down the left `CONTROL` key and using the scroll wheel to move in and out. Alternatively, you can use the `CONTROL +` (press control and the plus character) to zoom in or `CONTROL -` to zoom out.

- Moving around the sheet (the workspace) is done by clicking and holding the middle mouse button (if you have one), using a scroll wheel on a mouse, and via the slider bars on the bottom and right sides of the window.
- Choose which you would like to do and move down the window to view the Legal Issues node.
- Child nodes can be collapsed by clicking the "-" under the parent node (arrows at 1 below). It will then change to a "+" and, if you click it again, it will expand the child nodes.



5. Zoom out now so that you can see the entire MindMap sheet on one page.

Depending on your computer and VM display sizes, your ability to read the content on the screen will vary. You should see something that looks like the image below.

OSINT_Maps x

OSINT Map

Tab Descriptions

- Goals/Scoping: The initial tab is for defining your engagement.
- OSINT Process: Modelled after OSINT Process (Yoga) The process tab will help guide you through your data collection.
- OSINT Data Collection: The data collection tab is where your data you harvest would be entered (results from searches, screen shots and any other interesting data).
- Additional Resources: The last tab has additional resources to round out your data collections(Ex: additional areas to search, tools and collection of OSINT sites).

Intro Goals/Scoping OSINT Process OSINT Data Collec... 80%

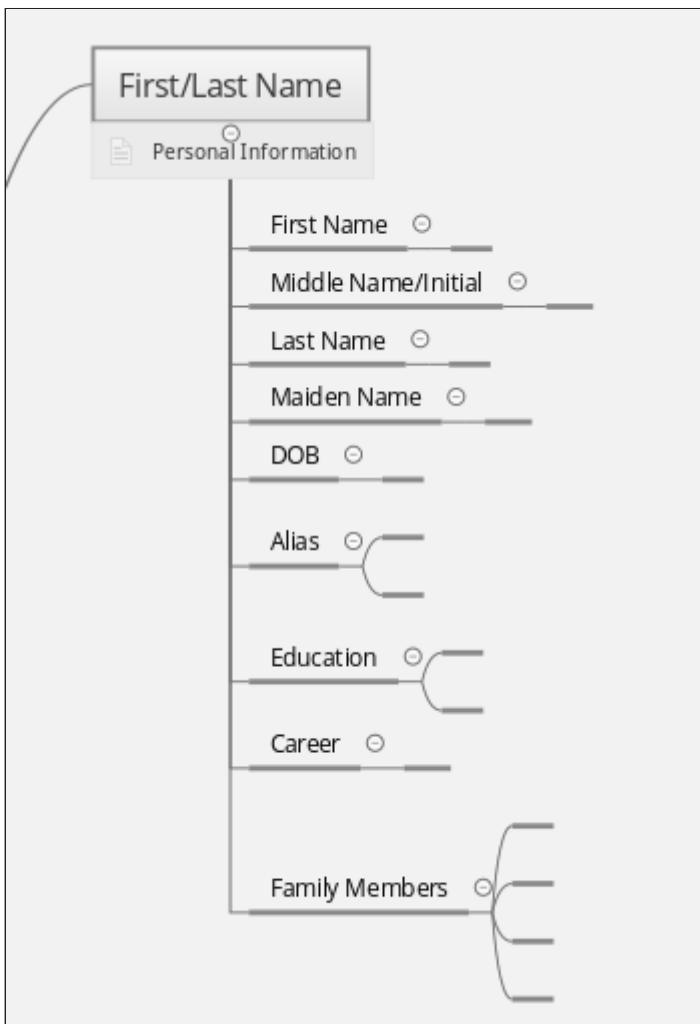
Moving to another tab is simple using the tabs along the bottom left of the window. This file has multiple tabs: Intro, Goals/Scoping, OSINT Process, OSINT Data Collection, and Additional Resources. We are in the Intro tab now.

6. Click on the OSINT Data Collection tab to shift to that tab's content.

Intro Goals/Scoping OSINT Process OSINT Data Collec... 80%

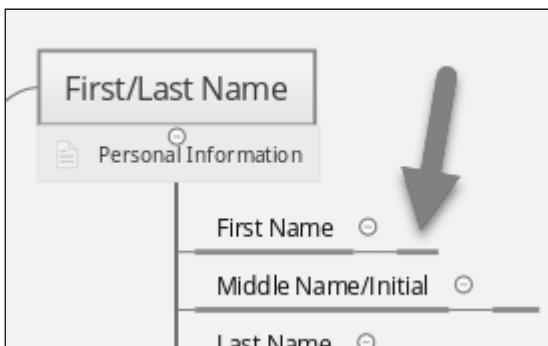
Using your zooming, clicking and expanding skills, browse around this sheet and examine the different content in the various categories.

This MindMap is a template that you can customize and use to keep track of your OSINT work. Let's add some content to it. To do this, we need to get to the correct node to add data. We will use the First/Last Name node as our start. This node should look like the below image.

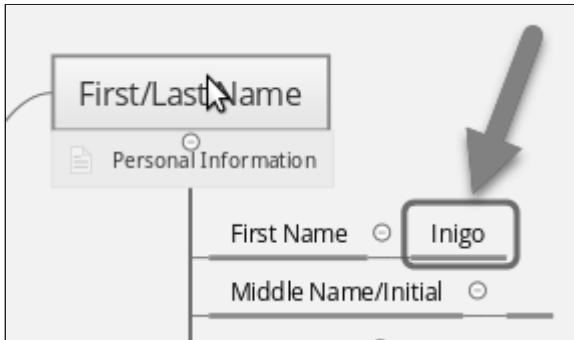


To add content to a node, we click it and type our data into it. Notice there is a blank node to the right of the "First Name".

7. Click the blank space to the right of the "-" on the same line as the First Name node. It should highlight the node.



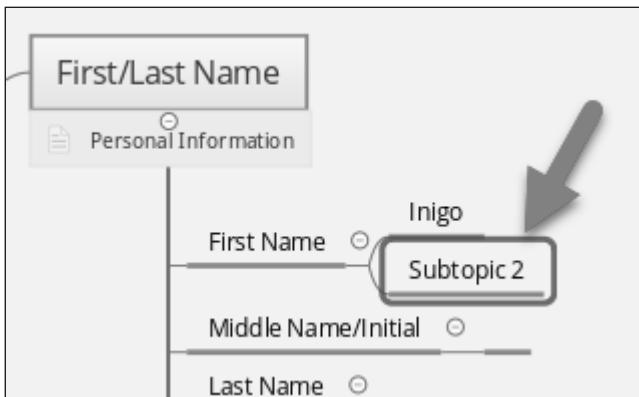
8. Type in our target's first name `Ini go` and press enter.



To add a child node, we use the `tab` key on our keyboard.

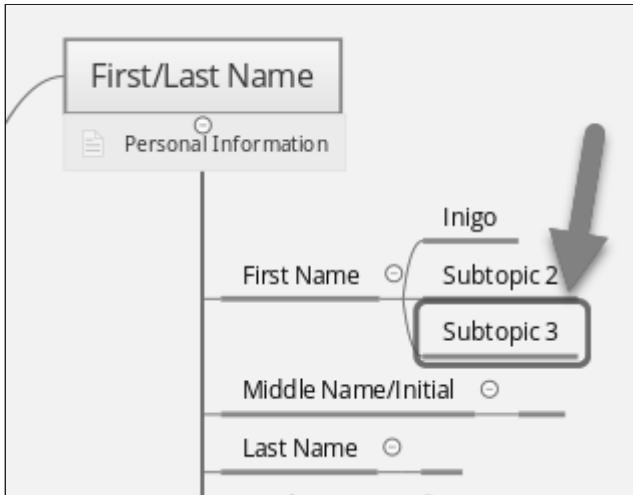
9. Click one time on the First Name node to highlight it and then press the Tab key on your keyboard.

A new child node (Subtopic2) should appear to the right of the First Name node since there was already a blank node.



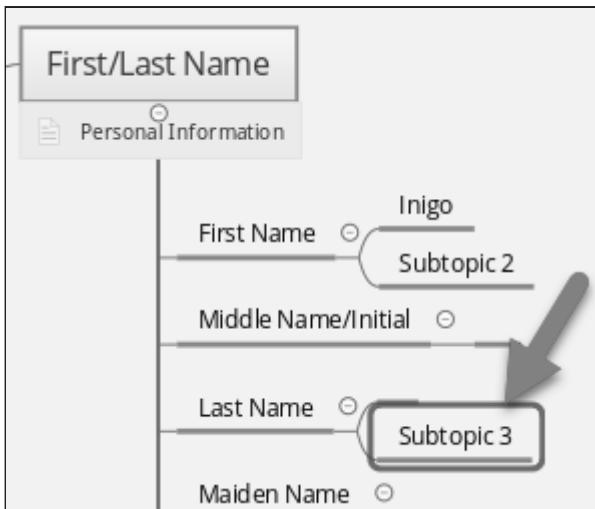
10. Press the `Enter` key while that node is highlighted to create a peer node (at the same level of indentation).

Ensure the node you just created is selected (click once on it if it does not have a blue border as shown above) and press the `Enter` key to create a peer node.



Nodes can be moved by clicking and dragging them to their new parent. So, let's say that we wanted the Subtopic3 node that was created above to be realigned under the Last Name node. We could move it by clicking and dragging it down to the new parent and then releasing. As you move the node down, you will notice that the application suggests connecting to each node you pass by making a red connection to each node. When this red line is highlighting the Last Name node, we release our hold and drop the node into its new place. Try that now.

- Move the node by clicking and dragging it down to the new parent and then releasing.



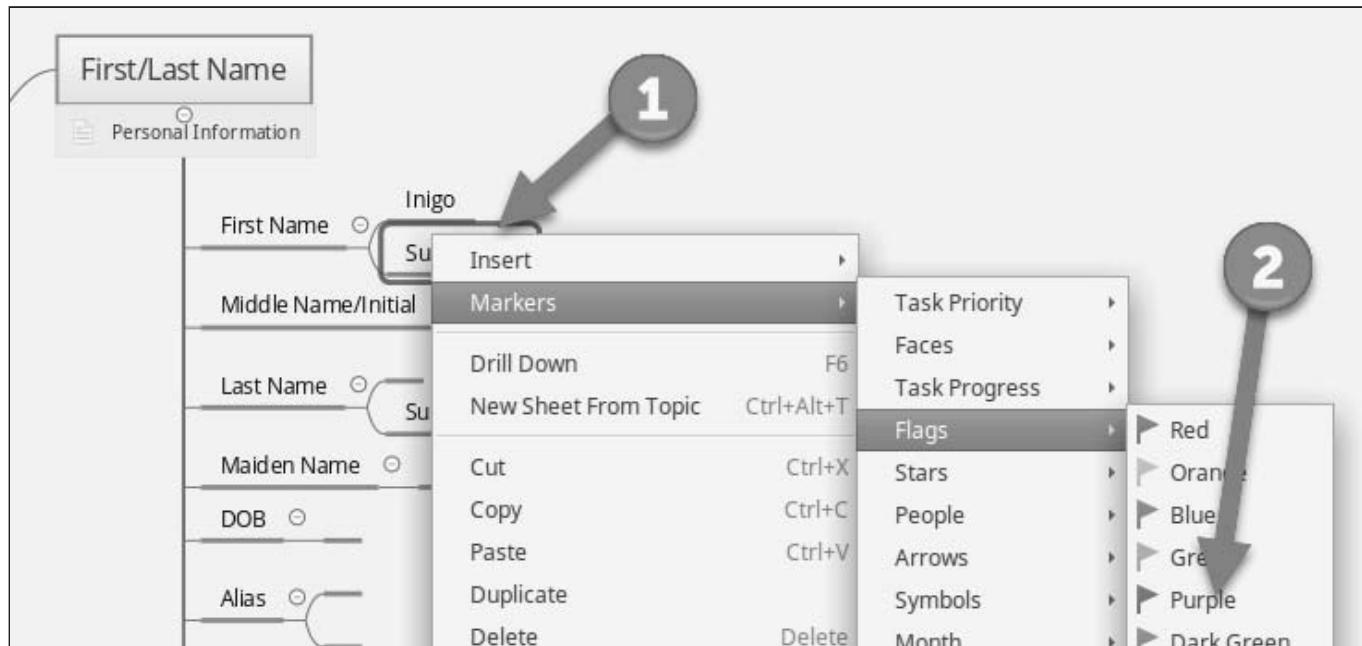
Removing or deleting nodes can be done by clicking the node once and then pressing the **Delete** key on your keyboard or right-clicking on it and selecting the Delete function.

There are other actions you can perform on nodes by right clicking on them too. Go and explore that if you wish.

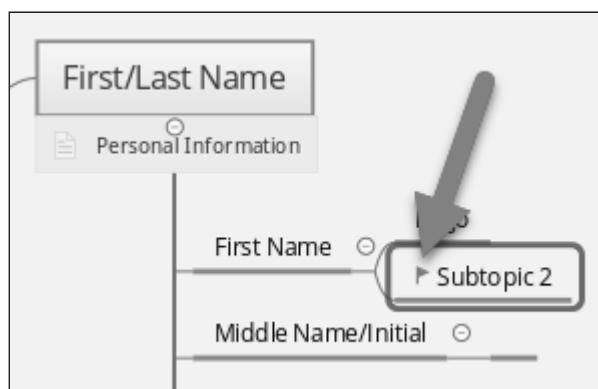
Because we can move nodes around and collapse or expand node trees, MindMaps are helpful tools in our organization of our assessment data. We can also tag items with icons and flags to help us remember where the good data is, what to ignore, or other things.

We can right click on a node (arrow 1 below), then, when the contextual menu appears, choose Markers, pick the type of marker we want to tag the node with and click it.

12. In our example, let's tag the "Subtopic2" with a purple flag.



Once you click the Purple flag your display should appear as below.

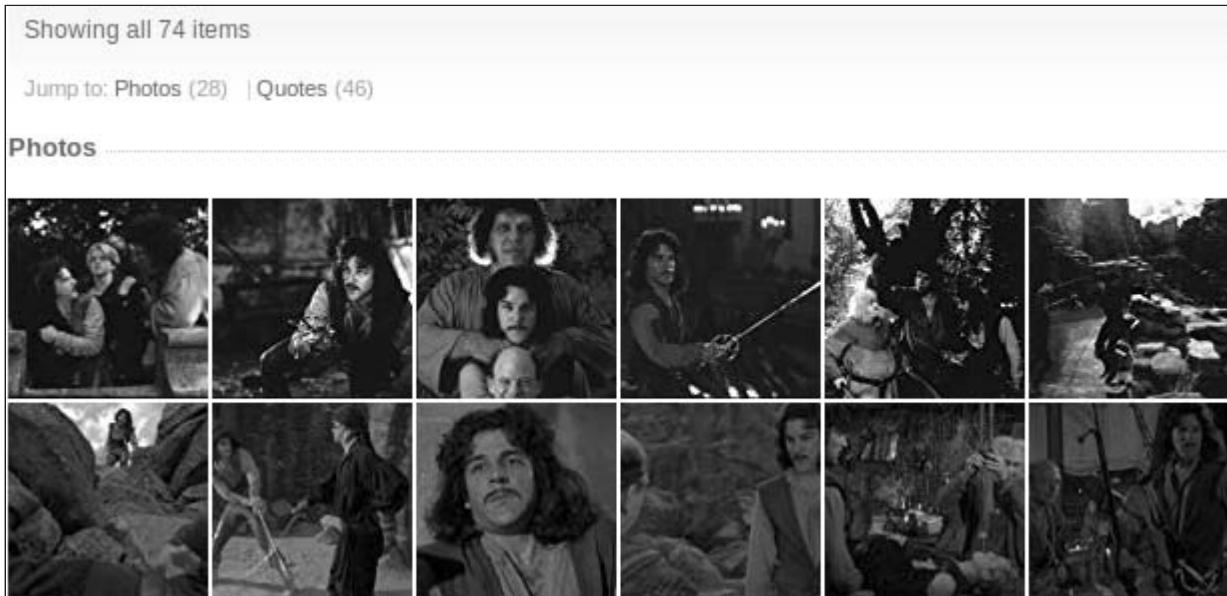


You and your team should create a key of what the markers in your MindMaps mean so that you use them consistently across the team.

Screenshot App

1. Let's add an image to the MindMap by capturing it in the VM's screenshot application.
2. Visit the <https://sec487.info/es> page in a web browser.

We will capture images of Inigo Montoya on this page (see image below). Scroll so that the images of Inigo Montoya are in the browser.



3. Left click on the Camera icon in your taskbar (arrow 1 below).



Doing this will:

- Allow you to drag the cursor over a region of the screen to capture an image
- Darken the screen
- Change the cursor to a crosshair (+)

4. Click and move the cursor over the images of Inigo Montoya and release the mouse. This should bring up a window asking what you would like to do with the image you just captured (see image below).

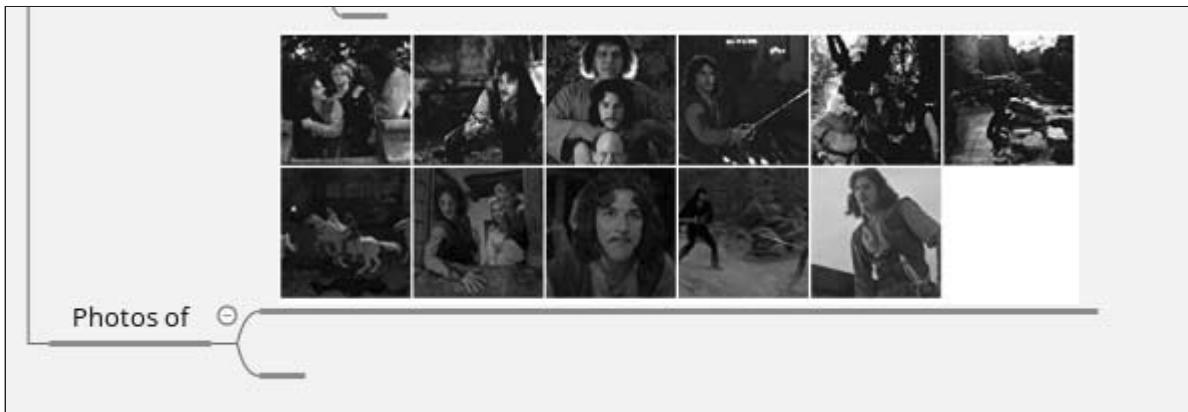


The most common actions you might wish to take are to save the image (arrow 2) or copy it to the clipboard so you can paste it into another application (arrow 3).

5. Choose the Copy to the clipboard option (arrow 3 above) and press the OK button (arrow 4 above).

With the image copied into your system's memory, we can switch back to the MindMap and paste it into a node. The perfect place for this image is in First/Last Name -> Photos of.

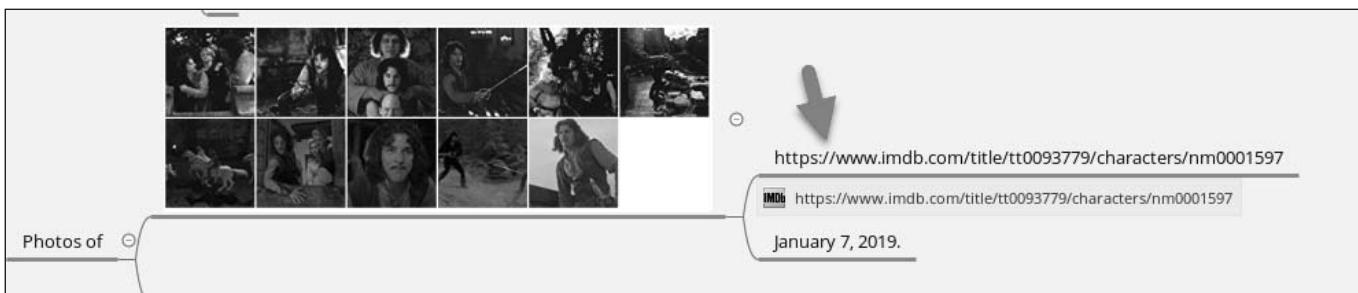
6. If your MindMap has a "Photos of" node, click once on it (shown below) and press CONTROL v to paste the contents of memory into a new node. If it does not have one already, create the node and paste the image.



We need to document where we got this image.

7. Press the Tab key and then type: <https://www.imdb.com/title/tt0093779/characters/nm0001597> (or copy and paste it from your browser's URL bar).

Consider adding the date you took the screen capture to the node too as we did below (arrow 2).

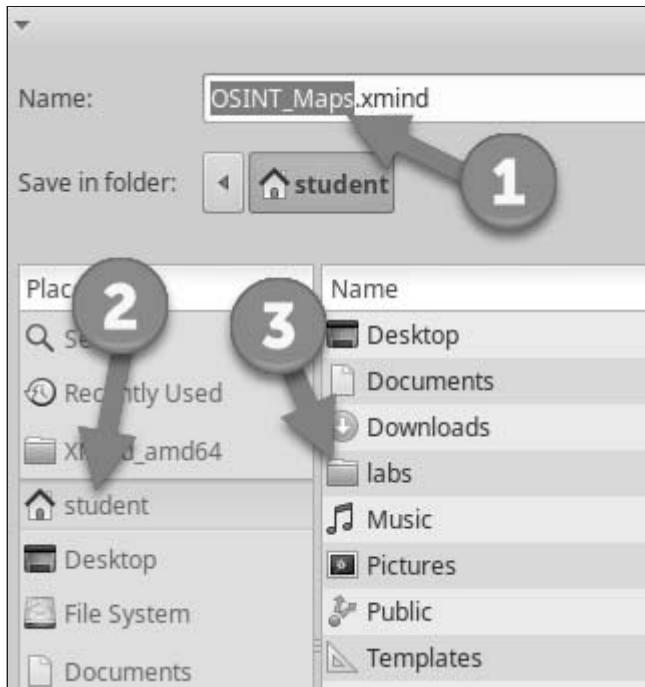


8. [Optional] Fill out more of this tab with your (or fictitious) data

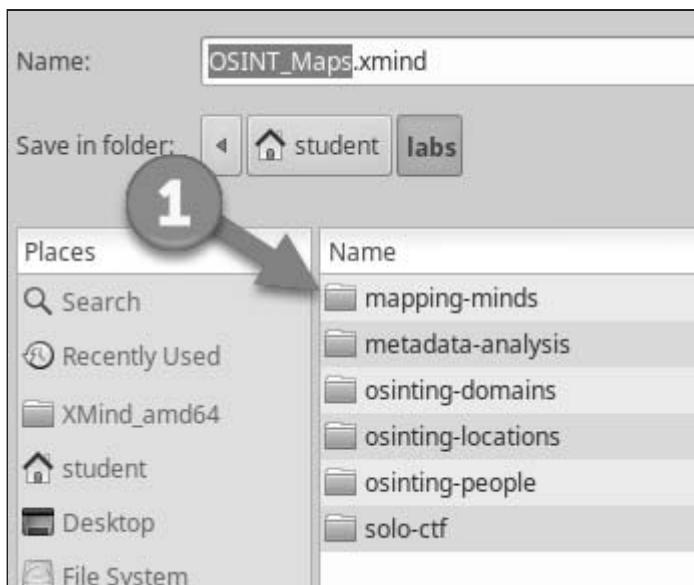
Take the skills you learned above and fill out the more of the sheet with your personal data or that of a fictitious person you may be performing OSINT on.

Once you have content, you will need to save it.

9. The File menu has the Save As... option to allow you to save your work. Choose a name for your file (arrow 1 below) and then select the /home/student/labs/ directory by clicking the student item on the left (arrow 2) and then double click the labs item on the right (arrow 3).



- Double click the mapping-minds folder (arrow 1 below) and then press the OK button in the lower part of the window.



We will be using XMind in future labs but, for now, we are finished.

- Click on the File menu item and go down to the Exit option to quit the program.

If you have not already saved your work, it will prompt you to do so now.

Maltego Casefile

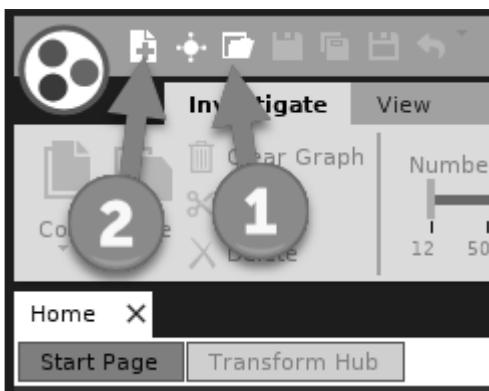
We use Casefile to analyze data and show relationships between entities whether they are people, web sites, groups, documents, or phrases. Maltego Casefile allows us to create a "graph" and then add entities to it. While the other versions of Maltego (Community, Classic, and XL) can be used to show relationships and grab data from remote web sites, Casefile cannot grab its own data. We either import data into Casefile from a CSV file or create our graphs manually.

Adding Entities to a Graph

1. Casefile can be launched from the taskbar by clicking once on the Maltego three-dot icon shown below.



2. You can either create a new graph by clicking on the New Graph icon (arrow 1 below) or, if you would like to modify a file we already created, open an existing Maltego file using the Open a graph option (arrow 2) and navigating to `/home/student/I abs/mappi ng-mi nds/maltego_pri ncess_bri de.mtgl`.



Casefile comes with standard entities in its palettes that work for a wide range of investigative needs. You can purchase even more entities or create your own. Let's populate the graph with entities according to the scenario below.



Navigation

Moving around the graph is completed by right clicking the graph background and dragging. We can also zoom in and out using the scroll wheel.

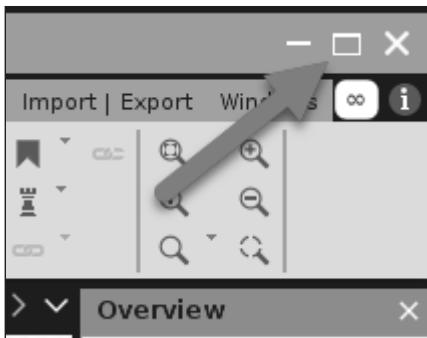
3. Let's create a new graph using the scenes, actions, and characters from the movie *The Princess Bride*. Here are the people and actions that can be mapped in the new graph.

There are entities in the palettes corresponding to the words in bold below.

- Male – Westley
 - Westley has an alias of "Dread Pirate Roberts"
 - Loves (relationship) Princess Buttercup
 - Hates (relationship) Prince Humperdinck
- Female – Princess Buttercup
 - Loves (relationship) Westley
 - Hates (relationship) The Dread Pirate Roberts
 - Hates (relationship) Prince Humperdinck
- Government Official – Prince Humperdinck
 - Rules and lives in the city of Guilder
 - Hates (relationship) The Dread Pirate Roberts

Before we explore Casefile further, let's maximize the window size so we can see more of the interface.

4. Press the maximize button in the upper right of the window as shown below.



On the left side are the palettes from which we can pull our entities.

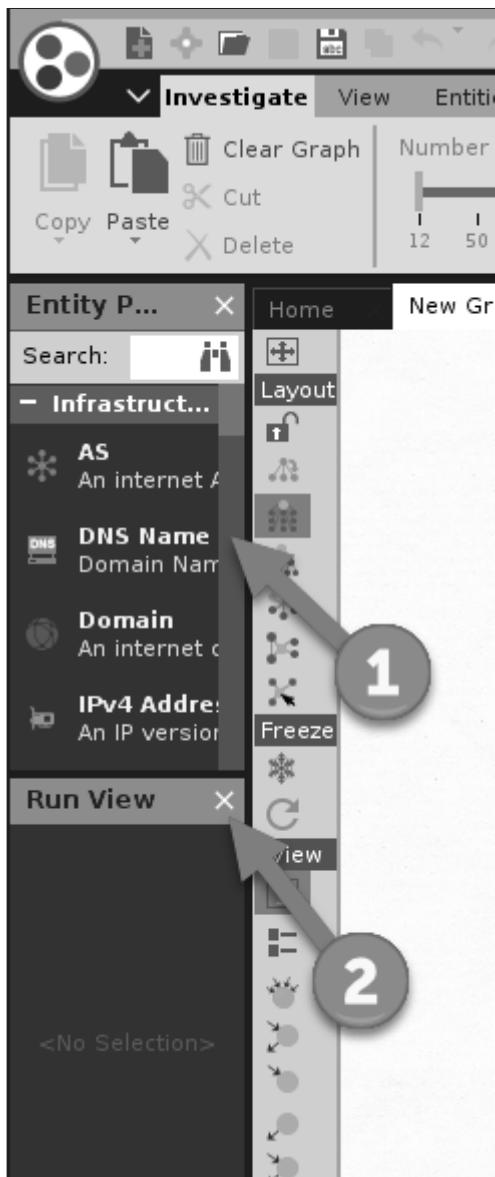
Screen Size

You may need to move some of the window pane borders around to better see the items on the left. Move the cursor in between the "Entity P..." window and the home graph. The cursor will change to a "resize" one.

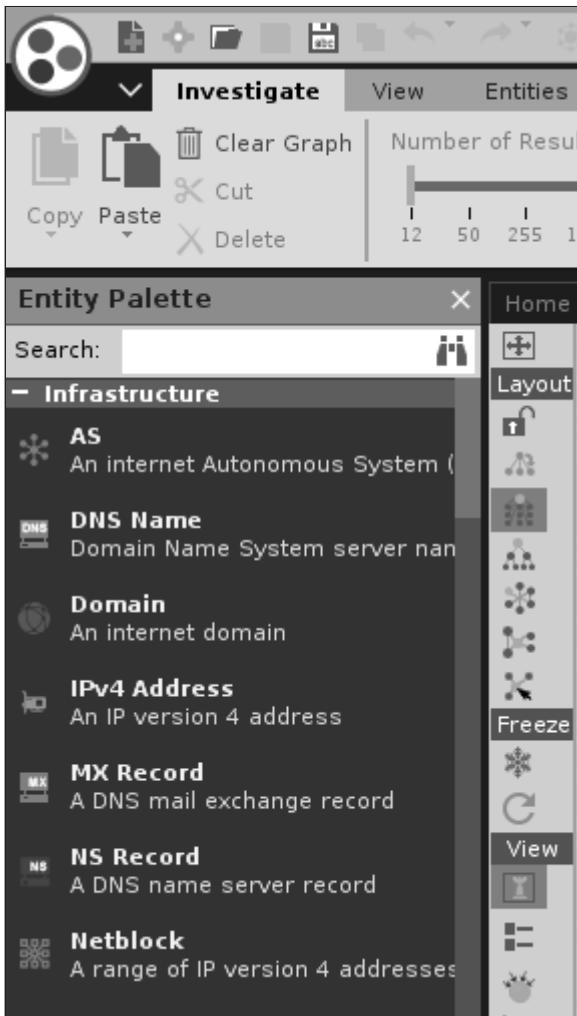
Click and drag the "Entity P..." (Entity Palette) window pane border (arrow 1 below) to make it larger.

A screenshot of the Entity Palette window, which is currently the active pane. A large gray arrow points to the vertical border between the Entity P... palette and the Home graph area. The number '1' is overlaid on the arrow. The Entity P... palette contains a search bar and a list of entity types: Events, Conversation, Conversation, and Incident. The Home palette contains icons for Layout, Lock, and other navigation options.

5. We can close the Run View pane as we will not be using that. Click the white X in the upper right of the pane.



Change the interface windows to look like the one below.

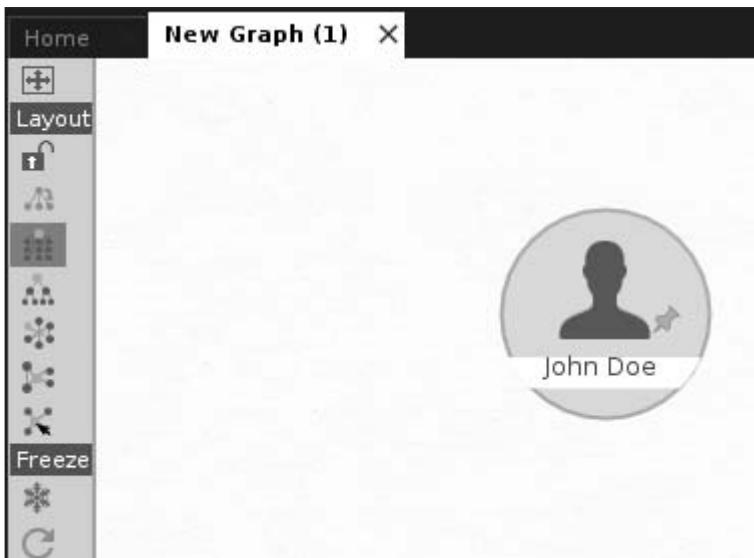


We can scroll up and down in the Entity Palette or use the Search: field to find entities or entities that we want to drag onto the graph. Let's start with the first entry in the above scenario:

- Male – Westley
 - Westley has an alias of "Dread Pirate Roberts"
6. In the Search: field, type `male` and the view should change to show "Female" and "Male" entities (arrow 1 below).



7. Click and drag the Male entity from the palette to the graph. Your graph should now have a "John Doe" entity on it.



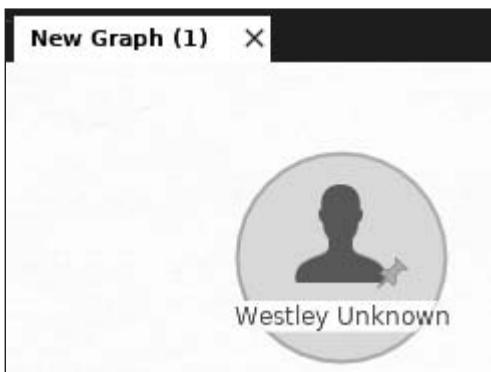
8. Double click on the entity and it will launch another window that allows you to change the properties of the entity.
9. Change the Full Name field to be Westley Unknown (since we do not know his last/surname). It should look like the image below.

The screenshot shows the 'Details' window for an entity named 'Westley Unknown'. At the top, there are tabs for 'Summary', 'Attachments (0)', 'Notes', and 'Properties (3)'. Below the tabs, the entity's name is displayed in bold. A placeholder profile picture is shown next to the name. The gender is listed as 'Male' with the note '[maltego.Male]'. There is a bookmark icon. The main body of the window contains three input fields: 'Full Name' (containing 'Westley Unknown'), 'First Names' (empty), and 'Surname' (empty). The entire window has a dark theme.

Notice in this Details window we can add notes, add a picture, attach files, and edit/add other properties about this entity if we desired.

10. We are finished with the entry for now so click the OK button in the lower right of the window.

Our "John Doe" has transformed into "Westley Unknown".



We know that Westley has an alias of Dread Pi rate Roberts . Let's go back to the palette and find the Alias entity.

11. You can either search for it or remove the filter we made for the word "male" by pressing the trash can icon and then scrolling down the window until you see the entity you want.
12. However you choose to find the alias entity, click and drag it onto the graph near the "Westley Unknown" entity.

13. Double click the alias entity and change the Alias field to be Dread Pi rate Roberts then click OK.

My graph looks like the one below but yours may look different depending on where you placed the entities on the graph.



We have the alias and the person, but there is no relationship yet showing that "Westley Unknown" is known as the alias "Dread Pirate Roberts".

14. To make the relationship, make sure that the "Westley Unknown" icon is not already selected (it should look like the picture above), then click and drag on the "Westley Unknown" entity and release.

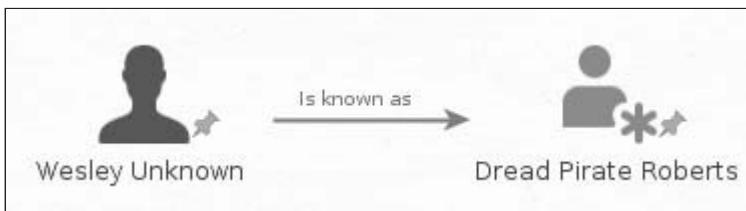
When you move your mouse somewhere around the screen you should see that there is an arrow moving around the screen with your cursor.

15. Click once on the Dread Pirate Roberts alias entity to show that you want to connect the two.

The Properties window should pop up asking you to specify details about this relationship.

16. We are going to enter Is known as in the Label field and then click OK.

Now our graph is starting to look like an OSINT investigation. It should look similar to the image below.

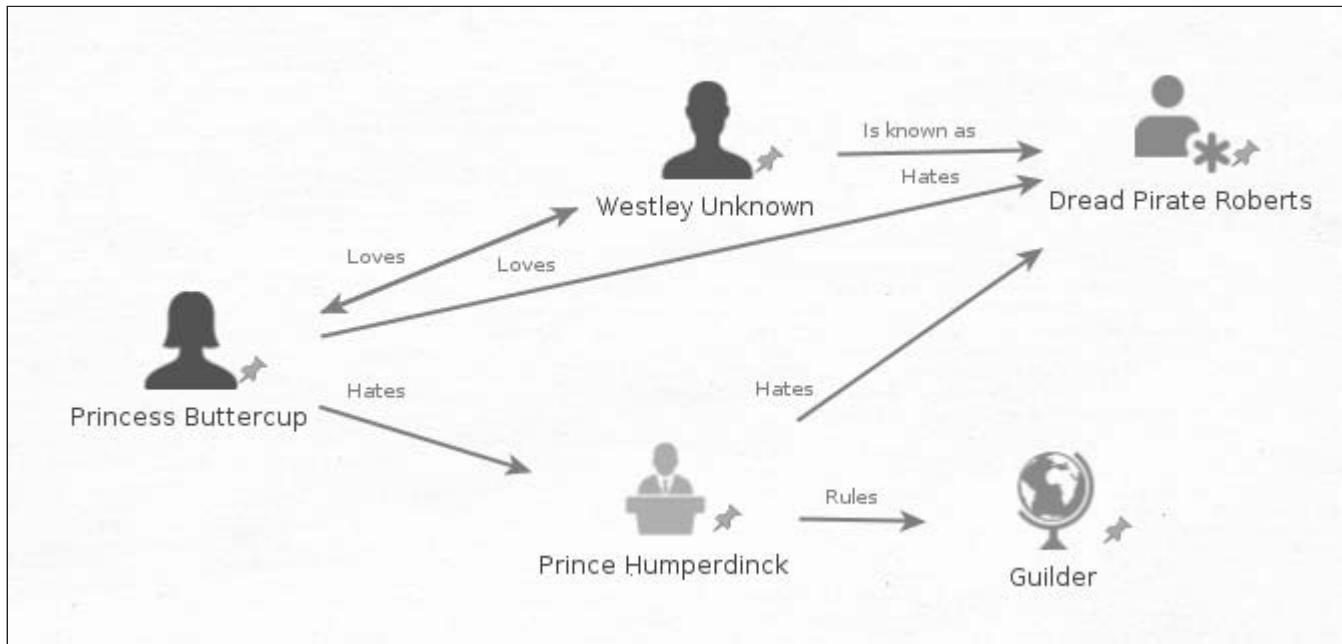


17. Go ahead and continue to populate the graph according to the scenario outlined above.

As you will soon realize, when you put more entities on the graph and establish the relationships, the graph becomes very busy and hard to see all the relationships. You can easily

drag each entity on the graph around to manually position it in a meaningful manner but there is an easier way: using the Layout buttons.

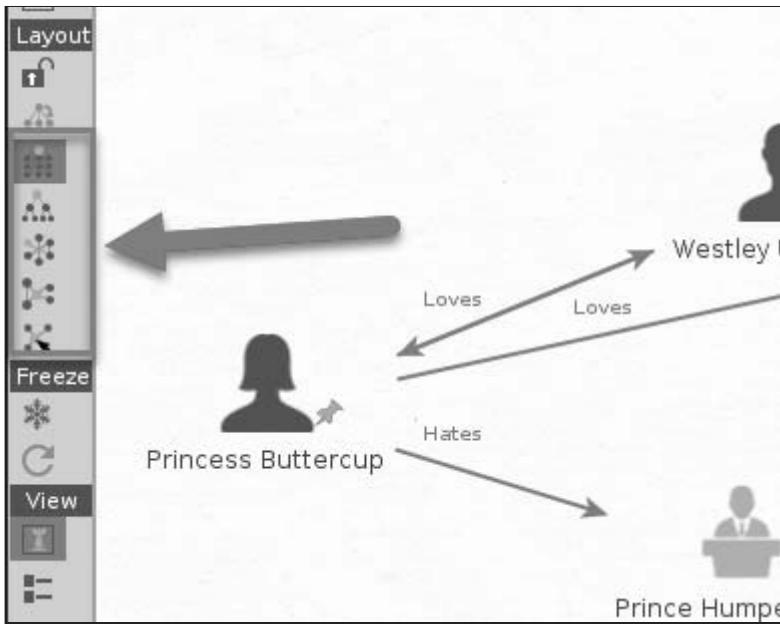
Our graph should look something like the one below (you can load this graph if you'd like, as it is saved as `maltego_princess_bri.de.mtg1` in the `/home/student/labs/mapping-minds/` folder).



Between the palette and the graph are the Layout, Freeze and View buttons. Let's use those now to reorganize the data. You can use your graph or load the pre-populated one in the labs folder.

The layout buttons reorient the nodes in specific fashions.

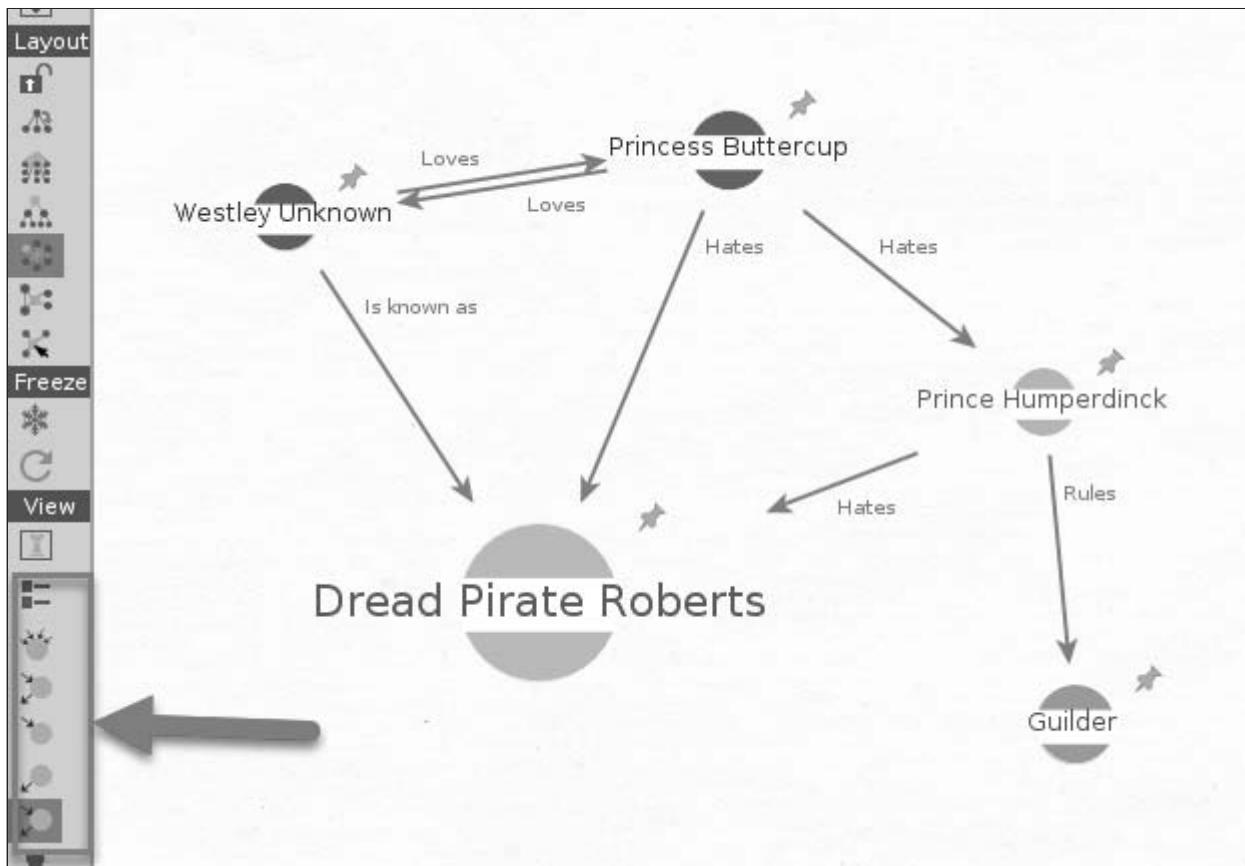
18. Experiment by pressing each of these icons and observing how the nodes shift and reveal the highly-connected nodes.



Once the layout buttons are pressed, we can move nodes around the graph manually to best situate them for analysis. Although this graph is not complete with all known relationships and nodes, we can evaluate the contents based upon the numbers of incoming and/or outgoing links. The more links, the bigger the bubble icons. For this, we use the icons in the View section.

When we click on these icons, the entity icons shift to bubbles of varying sizes as shown below. You will need to re-click the layout buttons if you choose the bubble views so that the entities adjust to their larger sizes in the graph.

19. Click on each of the View icons and examine the results.



You may continue to experiment with the layouts, views, and the other features of Maltego Casefile. These are merely the basic skills that you need to use the tool and understand some of its strengths.

20. When you have finished, you may click the Maltego logo in the upper left of the window (arrow 1 below), save your work (arrow 2), and exit (arrow 3).



21. Your lab is completed.

OnDemand Students

OnDemand students should proceed to Lab 1.5 - Hunchly after completing this lab. Students taking the class in a live or vLive setting, your instructor will determine when lab 1.5 is run.

The lab is completed. You may close the Firefox web browser.

Hunchly

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step Instructions
 - Retrieve a license
 - Method 1: Using your own license
 - Method 2: Using the free license from your SANS portal account
 - Method 3: Register for a free 30 day license
 - Install the License into Hunchly
 - Use Hunchly for Documentation

Objectives

- Download a valid Hunchly license
- Install that license in the Hunchly application within your VM
- Use Hunchly to document a case

Goals

1. Retrieve a valid Hunchly license
2. Install that license in the Hunchly application within your VM
3. Use Hunchly for OSINT documentation:
 - Create a new case

- Insert Selectors
- Collect data from web sites browsed using Google Chrome
- View the Hunchly Dashboard

Preparation

VPN if problems

Step-by-step Instructions

There is a video walkthrough for this lab. Click here to view it.

Retrieve a license

For this lab you need to choose 1 of the following 3 methods of retrieving a valid Hunchly license to install in the virtual machine for our labs. Any of the three will allow you to perform the activities needed to successfully complete the SEC487 course.

1. Using your own paid license
2. Logging into your SANS portal account and downloading the free license that you get from being in this course. This option will only work if your SANS portal account is tied to the purchase of this class. If someone else purchased the class for you (for instance a buyer or purchasing person at your organization), your Hunchly license may be tied to their account and not your portal account.
3. Registering for a free, 30 day trial license from the <https://hunch.ly> site

 Cannot Do Any of These?

If you cannot do any of these methods, please talk to your instructor.

Page down this document to read the directions for the method that you would like to use.

Method 1: Using your own license

If you have a valid Hunchly license file and you would like to use it in the class VM, follow the directions below.

1. Drag your valid Hunchly license file, most likely named `hunchly.license.key`, from your host system to your VM as shown in the image below.



2. Drop it on your Desktop in the VM (as shown in the image below).



3. Now you are ready to import into Hunchly.

Method 2: Using the free license from your SANS portal account

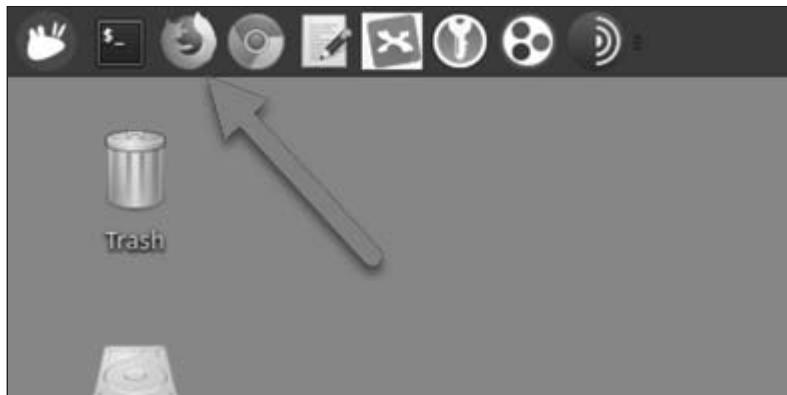
If you want to use the license that comes with the course, you can log into your SANS portal account <https://www.sans.org> and download that license provided that:

- You have paid or have been invoiced for the SEC487 class AND
- You have either started class or are within 1 day of starting the class AND
- You have your email and password to the SANS portal AND
- You didn't have a third party sign you up for the class with their email

If you meet them all, follow the instructions below. If you do not, skip to Method 3.

Doing this within the web browser within the SEC487 VM will save you steps. Let's use that approach.

1. Launch the Firefox web browser from the taskbar.



2. Visit the <https://www.sans.org> web site.
3. Click on the `Login` link in the upper right of the window.

A screenshot of the SANS.org website homepage. At the top, there is a navigation bar with links for "Training", "Online Training", "Programs", "Resources", "Vendor", and "About". To the right of these links are "Login" and "Join Community" buttons, and a search bar with a magnifying glass icon. A large grey arrow with the number "1" on it points from the text "Click on the trash icon" to the "Login" button. The main content area features a banner with the text "Cyber Security Training, Certification, and Research." and "Security West 2019". Below the banner, there is information about the event: "May 16 | San Diego, CA" and "Cyber Security Courses".

4. Enter your username (email) and password and click the "Login" button.



5. Look down the "Account Dashboard" page to find the Hunchly License SEC487 link on the right side of the page. Click the link. *If you do not have a link on the page, skip the rest of these Method 2 instructions and move to Method 3 because this will not work.*

The screenshot shows the SANS Account Dashboard. At the top right, it says "Welcome, Micah Hoffman". Below the header, there's a navigation bar with links: "Find Training", "Live Training", "Online Training", "Programs", and "Resources". The main title "Account Dashboard" is displayed prominently. On the left, there's a sidebar with "Account Details" containing links like "Account Profile", "Communication Preferences", "My Orders", "My Webcasts", "My Applications", "My Account Secret", and "Logout". Below that is "My GIAC Certification" with links for "Practice Tests" and "Certification History". The main content area has three sections: "My Online Training" (with a list starting with "..."), "My Links" (with a list starting with "..."), and a large grayed-out section. A callout bubble with the number "1" is overlaid on the "My Links" section, pointing to the "Hunchly License SEC487" link.

Account Details

- Account Profile
- Communication Preferences
- My Orders
- My Webcasts
- My Applications
- My Account Secret
- Logout

My GIAC Certification

- Practice Tests
- Certification History

My Online Training

-
-

My Links

-
-
-
- Hunchly License SEC487
-

6. The next page will display the license file, show the date when the license will expire (#1 in the image below) and also provide a `Download` button. Click that button to download the license. The license should be valid for several months.

The screenshot shows the SANS Institute website with a search bar and navigation links for Find Training, Live Training, Online Training, Programs, Resources, Vendor, and About. The main content area displays a "Hunchly License Instructions" page. It includes a message about a trial license file for the SEC487 class, a "License" section with fields for "For", "User", and "Expires", and a "Key" section containing PGP signed data. A large "Download" button is at the bottom. Two numbered arrows point to specific parts of the license key: arrow 1 points to the expiration date, and arrow 2 points to the end of the PGP signature block.

Welcome, Micah Hoffman +Q

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

Hunchly License Instructions

Below is your Hunchly trial license file that you will use in the virtual machine for our SEC487 class. Please press the "Download" button once and save the file on the computer that you will be using in class. Further instructions about what to do with this file will be given once you get into class.

License

For: Open-Source Intelligence Gathering and Analysis Training Event

User: micah@[REDACTED]

Expires: Aug 25, 2019

Key:

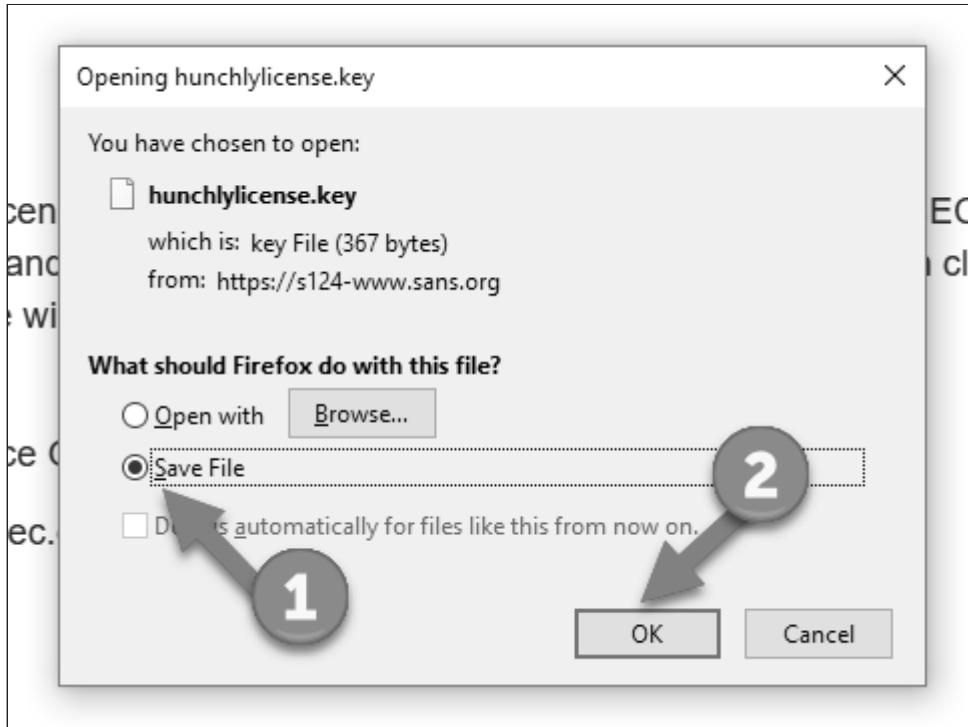
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

1 [REDACTED], 2019-08-25
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iJwE [REDACTED] 1Vmvt
QLvZ [REDACTED] 5yBo8
th8C [REDACTED] RLRNu
mAMJNpPlRnIxeoSPjjo=
=zOK3
-----END PGP SIGNATURE-----
```

Download

7. Your computer should then prompt you to download a file named `hunchlylicense.key`. Choose to save that file on your computer (within your VM) and click the `OK` button.

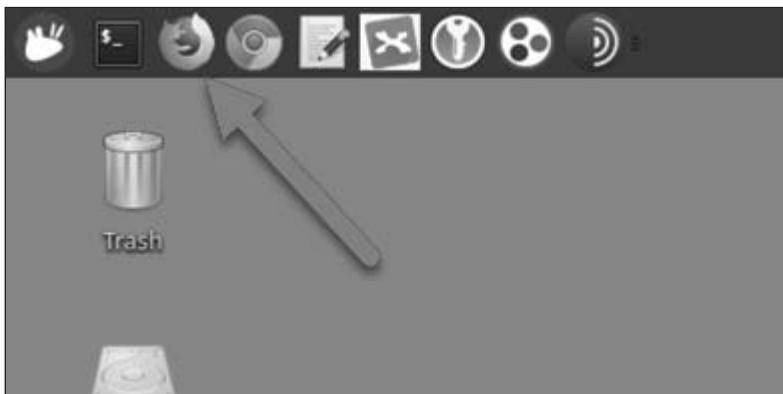


8. Now you are ready to import into Hunchly.

Method 3: Register for a free 30 day license

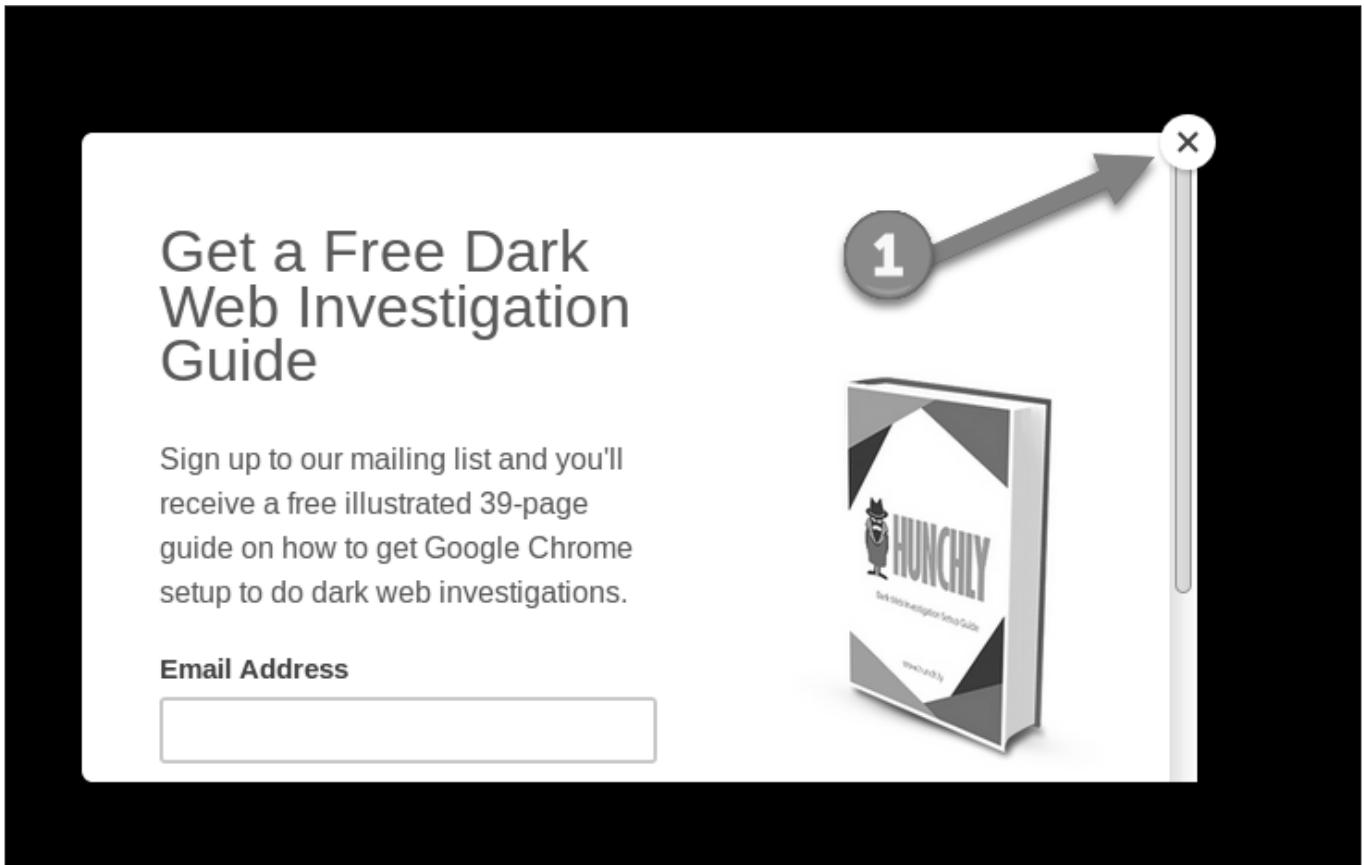
If you are not able to use any of the methods above to get a valid license, you can request one directly from the <https://hunch.ly//try-it-now> site. *These licenses require you to give Hunch.ly a valid email address where they can send your license.*

1. Launch the Firefox web browser from the taskbar.



2. Visit the <https://hunch.ly//try-it-now> site.

3. You may get a pop up box asking if you want a "Free Dark Web Investigation Guide". You can get it or just click the X in the upper right of the window (#1 below) to close that box.



4. Fill out the form on the web page with your information (image below). The email address must be one that you can access so that you can receive the email with the license file in it. Then click the Start Now button (#5 below).

First Name *

1 Micah

Last Name *

2 Hoffman

Email Address *

3 my@email.address

Industry *

4 Cybersecurity ▾

* All fields are required

5 Start Now

The form consists of five input fields and one button. Step 1 is 'First Name' with value 'Micah'. Step 2 is 'Last Name' with value 'Hoffman'. Step 3 is 'Email Address' with value 'my@email.address'. Step 4 is 'Industry' with value 'Cybersecurity' and a dropdown arrow. Step 5 is a large grey button labeled 'Start Now'. Below the first three steps is a note: '* All fields are required'.

5. Check your email for a new email from support@hunchly and download the hunchly license.key file that is attached to that email (image below).



Different Looking Email is Normal

Your email may appear different from the image below. We used a Gmail address for this test and so the image below is from Gmail. Whatever email system you use should allow you to download the attached hunchly license.key file from the email.

Your 30 Day Trial of Hunchly ➤ [Inbox](#)

Hunchly Support support@hunch.ly via netorg3986042.onmicrosoft.com
to [REDACTED]

Thank you for requesting a 30 day trial license for Hunchly. Your license key is attached to this email.

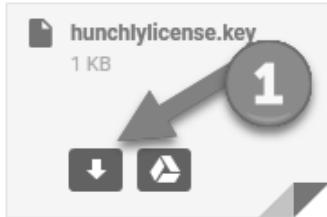
The best place to start is our Getting Started series of tutorials and videos here: [Getting Started](#).

If you have not done so yet, please:

1. Install Google Chrome [here](#)
2. Download Hunchly for your operating system [here](#).
3. Put the attached hunchlylicense.key in your Hunchly data directory. This is by default in Documents/HunchlyData

If you require any assistance please visit our [knowledgebase](#) or email support@hunch.ly

Team Hunchly

A screenshot of an email attachment preview for a file named "hunchlylicense.key". The file is 1 KB and has a document icon. A large grey arrow points from the file name towards the "Open" icon (a document with a play button). A circled number "1" is overlaid on the arrow.

[Reply](#) [Reply all](#) [Forward](#)

6. Drag your valid Hunchly license file named `hunchlylicense.key` from your host system (if you used your host system to access your email) to your VM as shown in the image below.



7. Drop it on your Desktop in the VM (as shown in the image below).

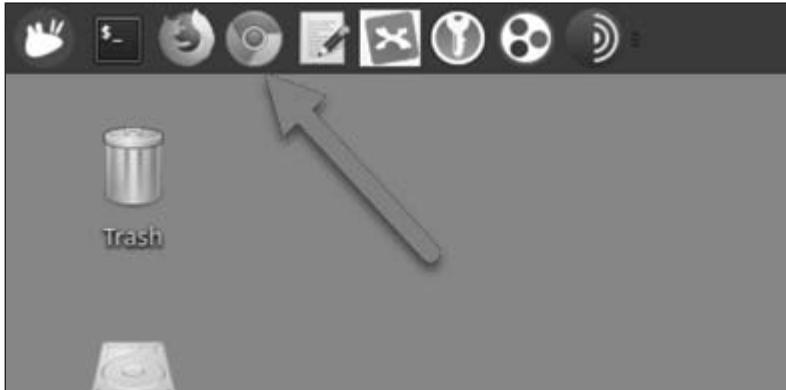


8. Now you are ready to import into Hunchly.

Install the License into Hunchly

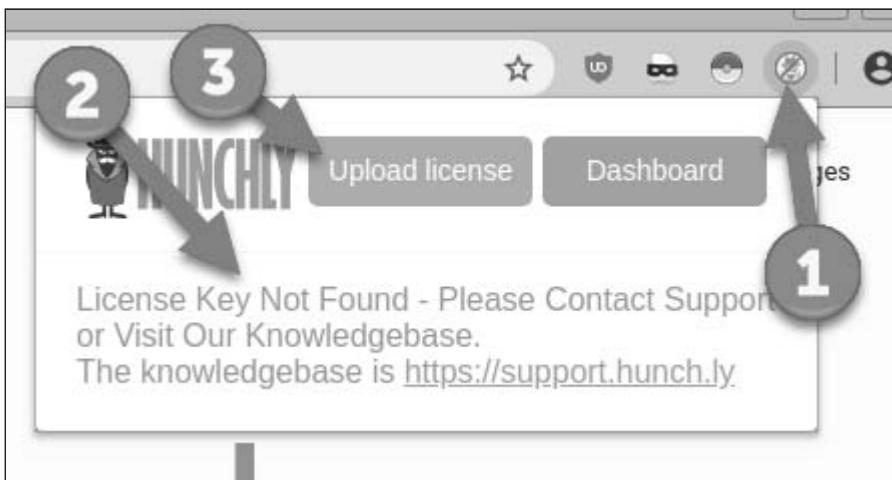
Since the Hunchly application is an extension to the Google Chrome browser, we need to launch the Chrome web browser for this portion of the lab.

1. Click on the Chrome icon in the menu bar.

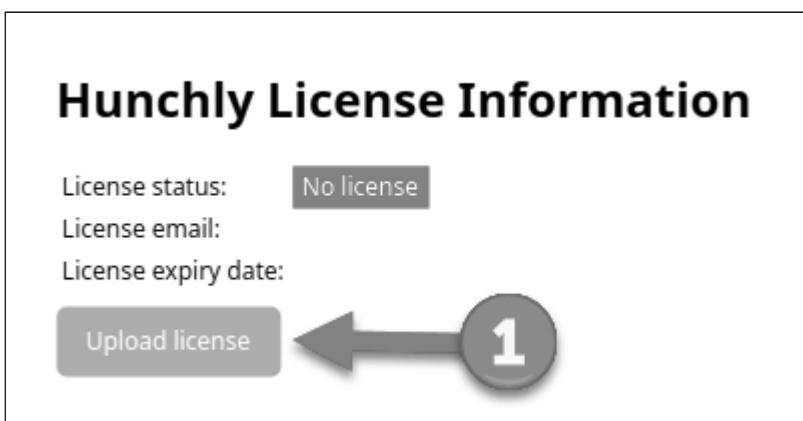


Hunchly has a dashboard where you control and review content it has recorded.

2. To access the Upload license button, click once on the Hunchly icon (arrow 1 below) and you should see the drop-down menu showing that you do not have the license installed (arrow 2).



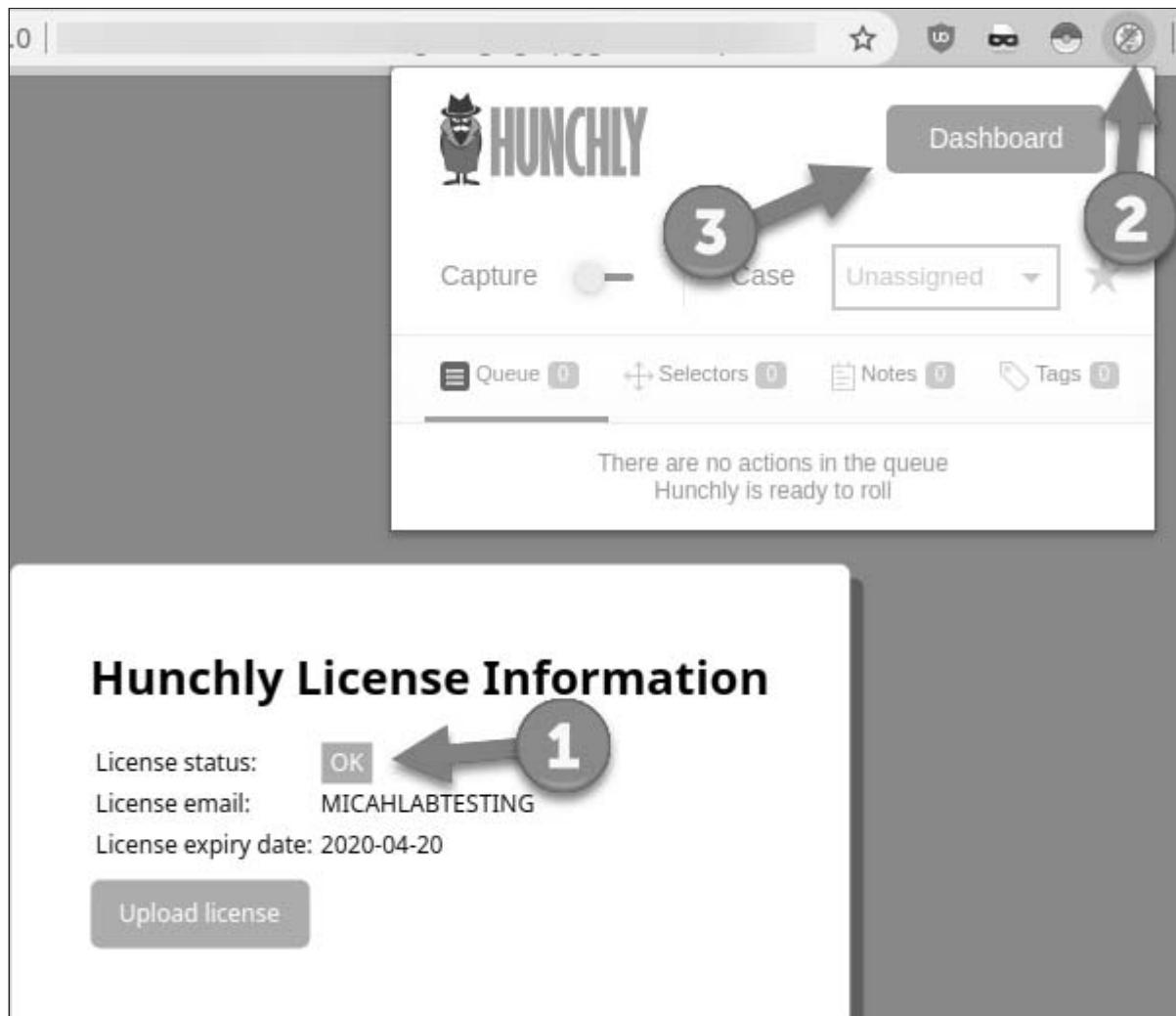
3. Click the `Upload License` button in the middle of the window (arrow 3 above).
4. Click the `Upload License` button in the middle of the new window (arrow 1 below).



5. Now Hunchly wants you to find the `hunchlylicense.key` file that you moved onto the virtual machine's Desktop. Click on the Desktop (arrow 1) and then the file (arrow 2). Finally, click the Open button (arrow 3) at the bottom of the window to accept your choices.



6. Hunchly should now have a valid license and show the OK message on your screen (arrow 1 below). The other information from your license will be different from the image below. If you see the OK message, click once on the Hunchly icon (arrow 2 below) and then click on the Dashboard button (arrow 3).



⚠ Something Go Wrong?

If you don't see similar images in your browser, let your instructor know.

Use Hunchly for Documentation

The Hunchly Dashboard should now be shown on the screen (shown below).

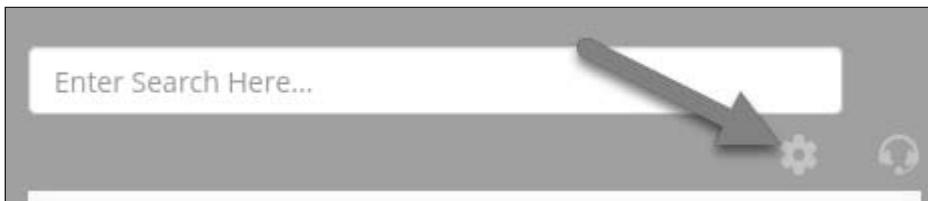
The screenshot shows the Hunchly 2.2.0 application interface. At the top, there's a navigation bar with 'Hunchly' and 'Edit' buttons, and a title 'Hunchly 2.2.0'. Below the navigation is a toolbar with 'Case', 'To Do', 'Export', 'Selectors (0)', and 'Tags (0)'. The main area displays two rows of metrics:

Unassigned :	Pages viewed	Searches performed
Created November 22, 2019 11:01 AM Active Case	0	0
Photos tagged	Selector matches	Notes taken
0	0	0

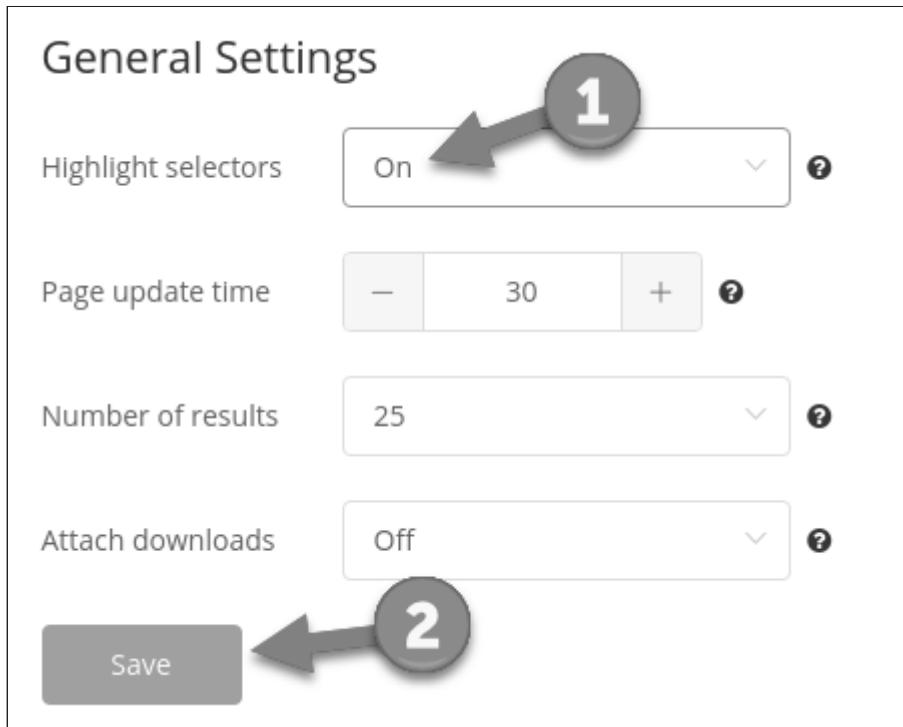
To the right of these metrics is a sidebar titled 'Selectors' with a note: '+ Adding a new selector will scan all case files for the new selector. This may take a minute or two.' It includes buttons for '+ Add', '+ Bulk add', and 'Export matches'. Below this are sections for 'Selector' and 'Count' with dropdown menus.

At the bottom of the dashboard are tabs for 'History (0)', 'Notes (0)', 'Photos (0)', 'Attachments (0)', 'Searches (0)', and 'Data (0)'. The 'History' tab is selected. A message indicates it shows the history of viewed pages from newest to oldest. It also shows 'Showing 0 of 0 total pages', sorting by 'Newest', and a search bar.

1. Let's make Hunchly more useful by turning on selector highlighting. With this on, whenever Hunchly views a selector you've input, it will highlight that string in yellow to make it stand out on the web page. In the Hunchly Dashboard window, click the settings gear button (below).



2. Scroll down in the settings area and click the "Highlight Selectors" then change the setting to "On" (arrow 1 below). Then click the **Save** button (arrow 2 below).



3. Click on the Hunchly Logo or the Back button (below) to go back to the main dashboard.



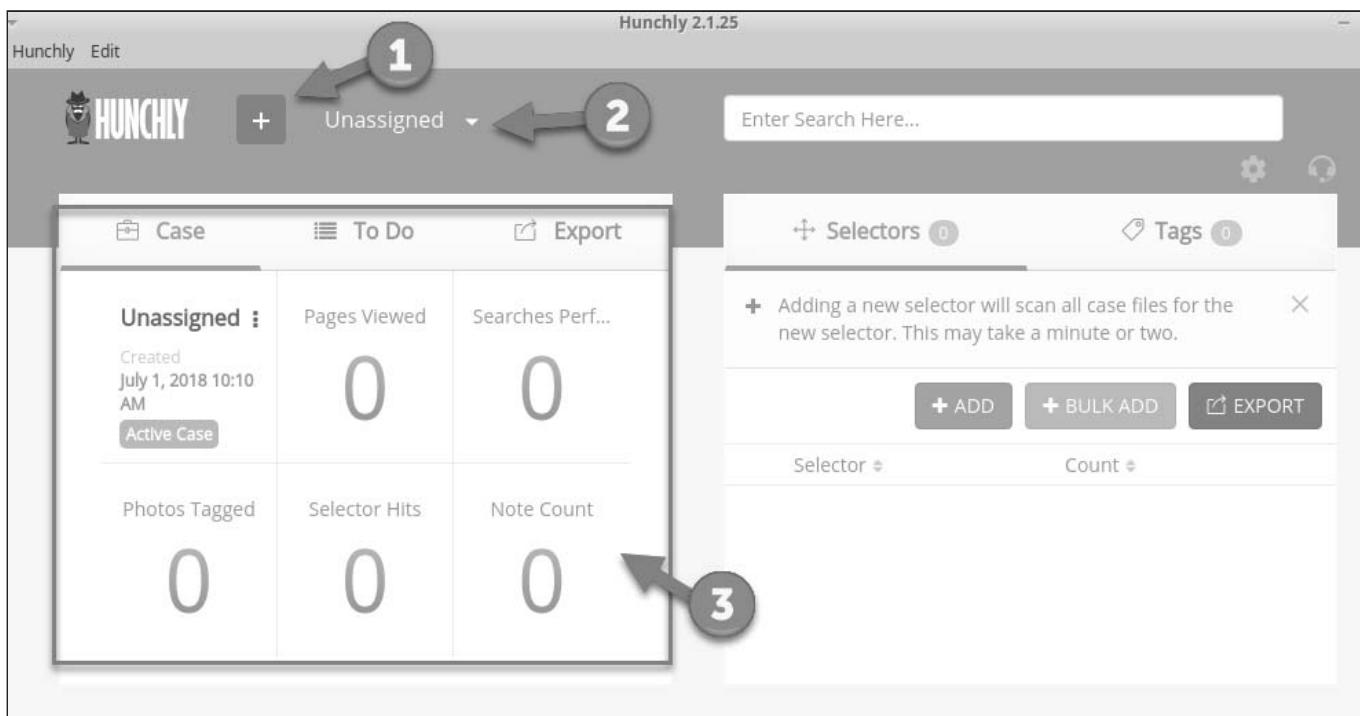
By default, Hunchly has a single "Unassigned" case (arrow 2 below). Cases are how you segment the different work you perform. When you work an OSINT task for client 1, you create a new case for "client1" and then configure Hunchly to record data there. Need to switch to client 2's case? No problem. Create or switch cases in the app and now client 1's data remains in the client1 case and client 2's data is sent to their case.



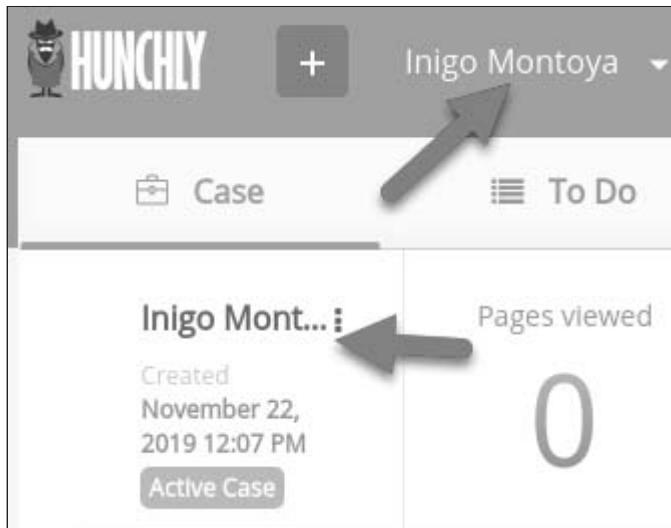
Check What Your Current Case Is

It is important to remember and check what case Hunchly is sending data to before you begin each assessment session. Contaminating cases with the searches of another customer shows poor process and can ruin an assessment.

4. We will begin a new case by clicking the + button on the left of the window (arrow 1 below) and then select New case. Once we start adding content to the case by searching web sites, the summary of that data will appear in the box below the case name (arrow 3).

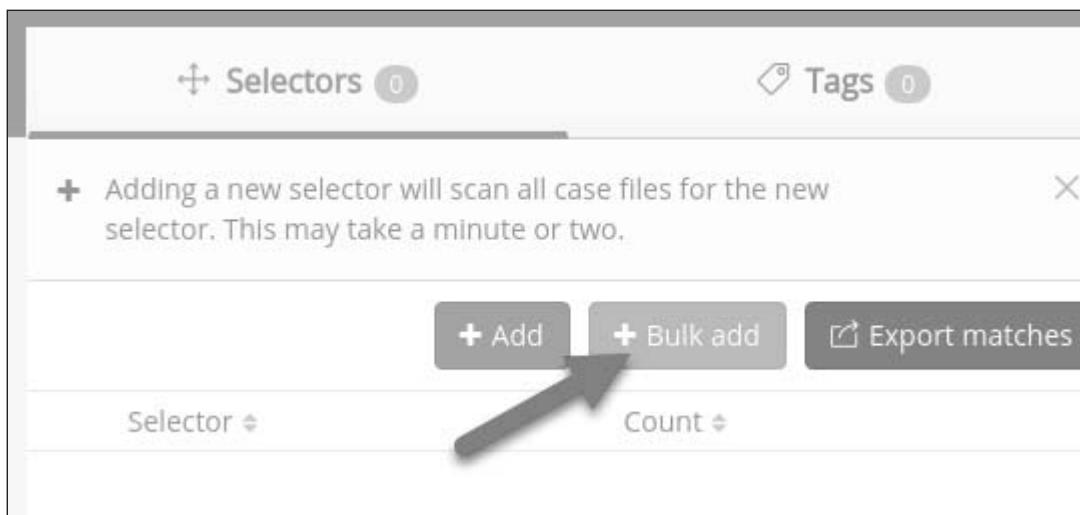


5. Enter your new case's name in the Add New Case window. For this lab, we will call it `I ni go Montoya`. When completed, click the Save button in the lower right of the window.
We can see (arrows in the image below) that we are now using this case as the active one instead of the Unassigned one.



Hunchly scours and highlights keywords in the content it records. These keywords, or *selectors*, can be names, numbers, passwords, phrases, or anything textual that may appear in a web page. We will start our case with some starting selectors.

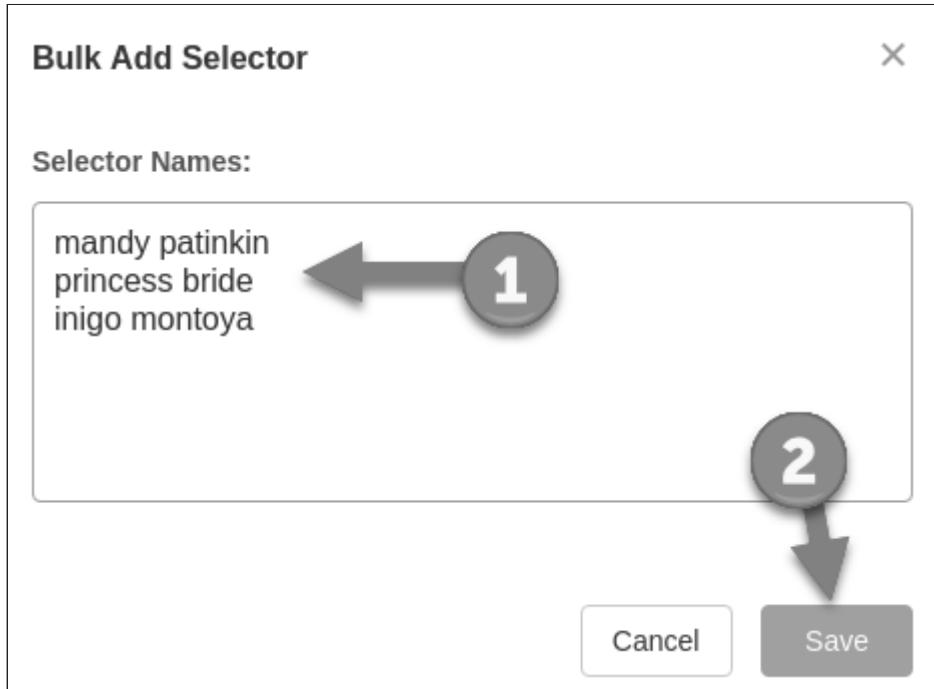
6. Click the orange + Bulk add button on the right side to add multiple selectors (arrow in image below).



7. Enter the following strings in the field with a return after each (as shown in image below).

- mandy pati nki n
- pri ncess bri de
- i ni go montoya

When finished, click the green Save button (arrow 2 below).



You are almost ready to begin searching the internet for information about your target "Inigo Montoya".

The icon for Hunchly in Google Chrome should look like with a red line through it. This tells us that Hunchly is not recording your actions.

8. We need to click on that Hunchly icon in Google Chrome (arrow 1 below) and click on the `Capture` switch (arrow 2) to turn on Hunchly's recording features. You can choose the case you want to work on (arrow 3).



With Hunchly on, we can begin our searches and investigation of the "Inigo Montoya" person.

Leave the Hunchly dashboard running and switch back to Google Chrome.

9. In Google Chrome, visit <https://www.google.com>.
10. Type: "Inigo Montoya" (with the quotes) into the Google search field and click enter.



Hunchly not only records all the searches and web pages you visit, but it also highlights the page content when it sees one of the selectors that you entered. The resulting page should look something like the one below (although the results may be different). Look for the yellow-highlighted selectors in the page content. See how easy it is to pick them out? Thanks, Hunchly!

"Inigo Montoya"

All Images Videos Shopping News More Settings Tools

About 905,000 results (0.71 seconds)

Videos

Hello, My name is Inigo Montoya.... Clare Elaine YouTube - Nov 13, 2010	"Hello My Name Is Inigo Montoya" chaplinblinks YouTube - Sep 14, 2011	The Princess Bride (11/12) Movie CLIP - My Name Is Inigo ... Movieclips YouTube - Feb 11, 2015	Inigo Montoya Fictional character Inigo Montoya is a fictional character in William Goldman's 1973 novel <i>The Princess Bride</i> . In Rob Reiner's film adaptation, he was portrayed by Mandy Patinkin. In both the book and the movie, he was originally from Andalucia and resided in the fictional country of Florin. Wikipedia

Inigo Montoya - Wikipedia
https://en.wikipedia.org/wiki/Inigo_Montoya ▾
Inigo Montoya is a fictional character in William Goldman's 1973 novel *The Princess Bride*. In

Go ahead and try some of your own searches. You are trying to get some test data into Hunchly, so you can see the other cool things it does. Some suggested sites to visit:

- Try a Bing, DuckDuckGo, or Yandex search for Mandy Patinkin .
- Visit the IMDB page for The Princess Bride <https://www.imdb.com/title/tt0093779/>.

When you have visited 3-4 more web sites, go visit the Hunchly dashboard to see what it collected.

11. Switch back to the Hunchly Dashboard application which should look similar to the image below (of course your dashboard will have references to the content you browsed and will look different than the image below).
 - The box with the "1" arrow pointing to it shows the summary of data collected including number of searches and number of selector hits.
 - The "2" box shows tabs you can use to get more details about what was collected. The image below shows the content from the history tab and that 8 items were found in there.

- Arrow "3" is the beginning of where you see the details from the history and other tabs. See it shows 8 items? Same as next to the History tab above it.
- The box at arrow 4 highlights the data that shows the number of times Hunchly viewed each selector.

The screenshot shows the Hunchly application interface. At the top, there's a navigation bar with a logo, a search bar, and a gear icon. Below the navigation bar is a summary card for 'Inigo Montoya' with metrics: Pages viewed (8), Searches performed (2), Photos tagged (0), Selector matches (12), and Notes taken (0). To the right of the summary card is a 'Selectors' panel with a table showing three entries: 'mandy patinkin' (Count 6), 'princess bride' (Count 3), and 'inigo montoya' (Count 3). Below the summary card is a horizontal navigation bar with tabs: History (8), Notes (0), Photos (0), Attachments (0), Searches (2), and Data (11). The 'History' tab is selected. A large arrow labeled '3' points to the 'History' tab. Another arrow labeled '4' points to the 'Selectors' table. The main content area below the navigation bar shows a list of recent pages viewed, starting with 'Inigo Montoya - Wikipedia' (https://en.wikipedia.org/wiki/Inigo_Montoya) viewed on November 22, 2019, at 12:18 PM. The page was viewed by 'mandy patinkin, princess bride ...and 1 more'.

12. Click on the History or Searches tabs and scroll down to examine what Hunchly recorded.

As mentioned briefly above, in addition to tagging text-based selectors, we can also tag images (for example avatar or profile pictures) by right clicking on them. When Hunchly finds these in other pages it will alert you.

Right Click to Add Selectors

While you are browsing web sites, you can right click any word(s) or image(s) and store them as selectors or write notes about them. A good example of when this would come into play might be if you started a Google search with a person's name, Mandy Patinkin, and then found a PIPL.com web site link. When you clicked that, it showed his phone number. You would want Hunchly to store that and highlight future pages it sees with that content, so you highlight that text and then go down to Hunchly and store text as selector.

13. If you have more time:

- Feel free to browse other sites
- Right click and add Hunchly notes and selectors on new web pages and then examine the content that Hunchly recorded

14. When you are done, please turn Hunchly off in Google Chrome so that it stops capturing content by clicking the Hunchly extension icon (arrow 1) and then the `Capture` option (arrow 2 below).



In this image, Hunchly is off since the Hunchly icon has a red line through it.

15. After that, you may close Google Chrome and Hunchly Dashboard.

Discount for Purchasing Hunchly

If you like Hunchly and find it useful, you can purchase a copy from the <https://hunch.ly/> web site at a 15% discount using the code: `sanssec487`. Your SEC487 license will expire in 5 months from when you started the class.

Searching for IP

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step Instructions
 - Find Materials
 - Report Findings

Objectives

- Practice using advanced search engine queries
- Locate places that hold illegal files with SANS and GIAC intellectual property
- Log and report the places you found content

Goals

Using search engines, your goal is to find pirated copies of courseware and test questions on the internet. Both SANS and GIAC regularly scan the internet for proprietary, intellectual capital that has been posted to file sharing and other web sites. In this lab, you are going to help find these files.

For your awareness, below are links to current GIAC certifications and SANS courses which you may need for search terms in your queries.

- GIAC certifications can be found at <https://www.giac.org/certifications/categories>.
- SANS courses can be found at <https://www.sans.org/courses>.

- Using search engines, find SANS and GIAC intellectual property on the internet that are not housed on official SANS and GIAC web sites.
- Submit your findings via the <https://sec487.info/searchingforip> online form.

Preparation

VPN if problems

VPN Use

Since this lab may have a large amount of googling, you might want to start with the class VPN on and turn it off if you have issues/slowness.

Document with MindMap or Hunchly

Consider using a MindMap to track your work in this lab.

Step-by-step Instructions

There is a video walkthrough for this lab. [Click here to view it.](#)

Find Materials

For this lab, you can and should use multiple search engines like <https://google.com>, <https://duckduckgo.com>, <https://bing.com>, and <https://yandex.com>.

Click Here to See Some Potential Search Strings



Below are some suggestions about what search terms you may wish to use but feel free to create your own:

- GIAC search terms

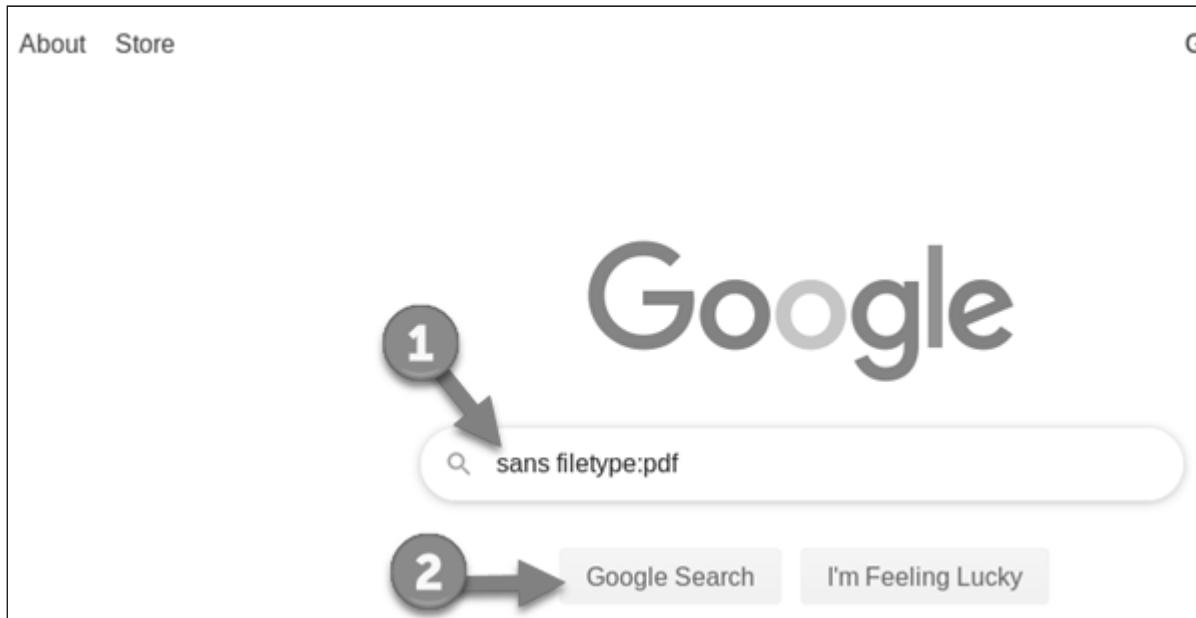
- "verified questions"
- "real exam questions and answers"
- "real braindump"
- Non-GIAC web sites that have pages like the following may house these files:
 - `http://example.com/vendors/giac/gcia-exam.htm` (Remember to look for exams other than the GCIA as well.)
 - `GSEC-t-8440.htm` (Where the exam name (`GSEC`) last four numbers (`8440`) change from file to file)
 - `GSEC_flashcards` (Substitute other GIAC certifications for the `GSEC` string)
 - VCE is a common testing engine format so you can do searches like `GCIH VCE`
- SANS terms
- These files will almost always have the following file extensions: `.pdf`, `.mp4`, `.mp3`, `.zip`, and/or `.tar.gz`
- Sites that have been found to have these files in the past are:
 - `certcollection.org`
 - `downturk.org`
 - `ebay.com`
 - `fastrls.com`
 - `googledrive`
 - `mega.nz`
 - `mshare.io`
 - `nitroflare.com`
 - `raptidgator.net`
 - `vminhsang.name.vn`
- `SANS big collection`
- `certcollection baseline`

When you find a site that has files you think are SANS or GIAC property, submit them to the <https://sec487.info/searchingforip/> web form.

Looking for a little more help? Continue reading below.

1. Using a web browser, visit a search engine (we will use <https://google.com>). We are choosing to start our search broadly and then refine it as we go. Our initial search terms will be `sans`

filetype:pdf (arrow 1 below) which looks for results with the word sans in them and is also a PDF file. Press the "Google Search" button (arrow 2) when ready.



Different Results

Your results will look different from the images below but you can follow along and see our thought processes and then make your own choices.

2. We should see many results for PDFs with the word sans in them that are hosted on the sans.org web site (arrows at 1 below).

Google search results for "sans filetype:pdf":

- [PDF] Incident Handler's Handbook - SANS.org
https://www.sans.org › incident › incident-handlers-handbook
Abstract. One of the greatest challenges facing today's IT and preparing for the unexpected, especially in response
- [PDF] SANS 2019 Events Calendar - SANS.org
https://www.sans.org › media › vendor › 2019-SANS-Ever
SANS 2019 Events Calendar. SANS is the most trusted a
for information security training and security certification i
- [PDF] SANS 2019 Incident Response (IR) Survey
https://www.sans.org › reading-room › whitepapers › incid
SANS 2019. Incident Response (IR) Survey: It's Time for
Written by Matt Bromiley. August 2019. Sponsored by: DF

Those are official documents and not what we are looking for. Let's refine the Google query to remove those: sans filetype:pdf -site:sans.org . See the -site:sans.org at the end? We are telling Google to remove any results that are hosted on the sans.org domain.

3. That search gave results that still have official SANS and GIAC domains in them (arrows at 1 below).

Google search results for `sans filetype:pdf -site:sans.org`:

- [PDF] Frequently Asked Questions -**
<https://www.sans.edu> · downloads › SANS-T
The SANS Technology Institute is a master's exclusively on cybersecurity degree program 2005 ...
- [PDF] SANS and GIAC Certifications**
<https://www.giac.org> · pdfs › NICE-Mapping-C
SANS and GIAC Certifications in alignment Workforce Framework. Ensuring a trained ar

A large number '1' is circled in the top left corner, with two arrows pointing from it to the first two search results.

Let's add the `sans.edu` and `giac.org` domains to be ignored. This changes our search query to: `sans filetype:pdf -site:sans.org -site:sans.edu -site:giac.org`.

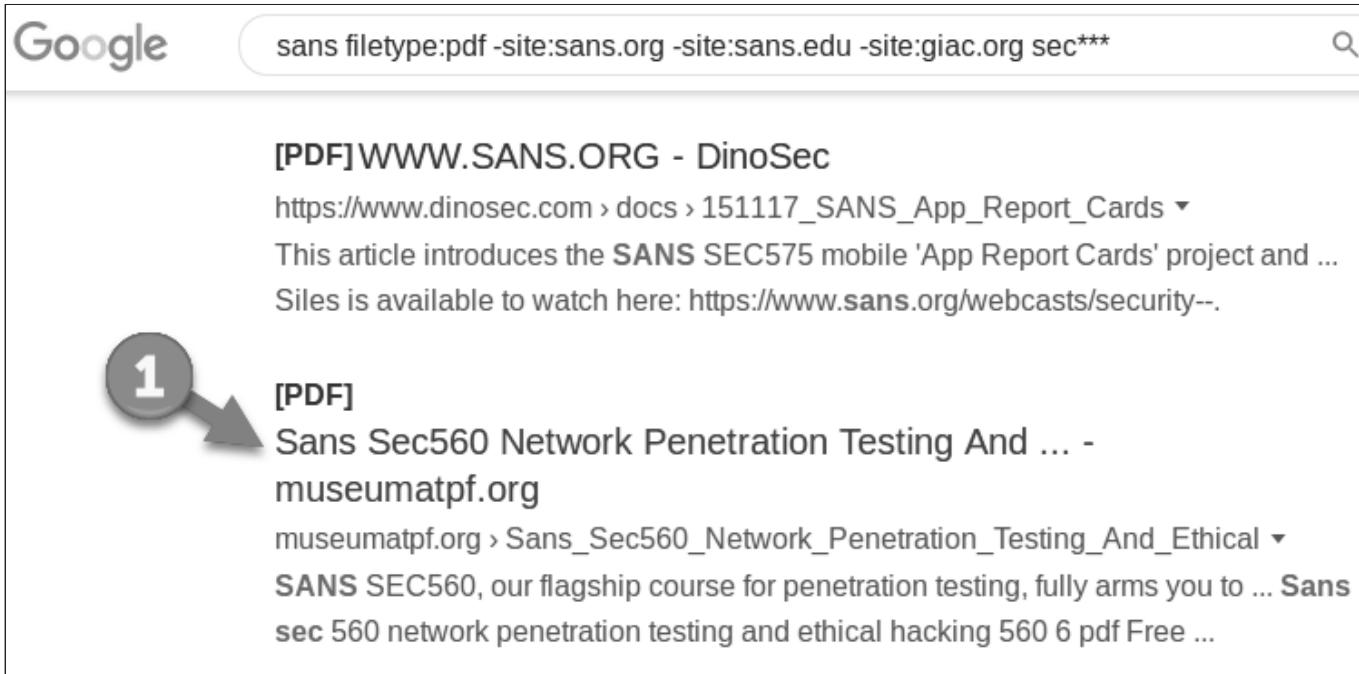
4. OK. Now we are seeing results outside of the official web sites SANS and GIAC maintain (image below). This is good but doesn't seem to be giving us the illegally-posted content we are supposed to be finding.

Google search results for "sans filetype:pdf -site:sans.org -site:sans.edu -site:giac.org":

- [PDF] SANS TRAINING**
https://www.energy.gov › sites › prod › files › cioprod › docume...
SANS Training Voucher Program Registration Procedures ...
program, the OCIO will cover only registration fees for SANS
- [PDF] the SANS 2017 Data Protection Survey - Ir...**
https://www.infoblox.com › wp-content › uploads › infoblox-wh...
by B Filkins - 2017 - Cited by 4 - Related articles
Ransomware, insider threat and denial of service are considered sensitive data by respondents to the 2017 SANS Data Protection Survey.
- [PDF] NIST Cybersecurity Framework Policy Tem...**
https://www.cisecurity.org › 2019/08 › NCSR-SANS-Policy-Tem...
gives the correlation between 35 of the NIST CSF subcatego...
SANS policy templates. A NIST subcategory is represented by

Let's add the `sec***` string to the query. This tells Google to look for documents with the letters `sec` and then three other characters in them. Here we are looking for things like "`sec560`", "`sec487`", and similar strings but will also get false positives like the word "`secure`" since it matches our string. This changes our search query to: `sans filetype:pdf -site:sans.org -site:sans.edu -site:giac.org sec***`.

5. Ah. For us, this query started paying off. Look at the second entry in our results (arrow 1 below). It looks a little suspicious. It is on an odd domain, has our keywords in the PDF, and looks like it has some sales language.



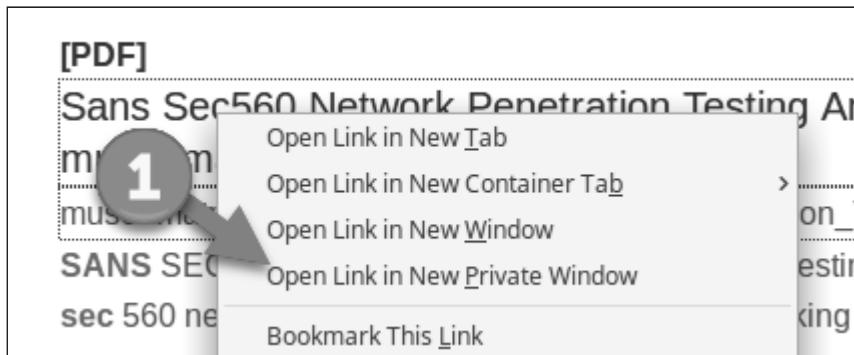
Google search results for [PDF]WWW.SANS.ORG - DinoSec

https://www.dinosec.com › docs › 151117_SANS_App_Report_Cards ▾
This article introduces the **SANS SEC575** mobile 'App Report Cards' project and ...
Siles is available to watch here: https://www.sans.org/webcasts/security--.

1 [PDF]
Sans Sec560 Network Penetration Testing And ... - museumatpf.org
museumatpf.org › Sans_Sec560_Network_Penetration_Testing_And_Ethical ▾
SANS SEC560, our flagship course for penetration testing, fully arms you to ... **Sans sec** 560 network penetration testing and ethical hacking 560 6 pdf Free ...

Since we have no idea about the safety of this PDF (it could have malware in it), let's open it in a New Private Window to isolate it.

6. We will right click on the document and select "Open Link in New Private Window" (arrow 1 below).



When the window opens, we will look at the document and examine the content.

7. We now see some of the telltale indications that someone has scanned in some SEC560 books and is trying to sell them. The image below shows the URL that we need to capture (1), images of the books (2), and the indication that the buyer will get ebooks (3) if they purchase this product.

1

2

3

4

5

6

Book Descriptions:
Sans Sec560 Network Penetration Testing And Ethical is nice books to read or download to add to your book collection

How it works:

1. Register for FREE 1st month.
2. Download your desired books
3. Easy to cancel your membership.
4. Joint with more than 80.000 Happy Readers.

3

This is what we are looking for! Keep this page open for reference.

Report Findings

1. Open a new browser window and visit the web form at <https://sec487.info/searchingforip>.
2. Fill out the form using the information you found. Below (arrow 1), we pasted the URL to the resources we found and then inserted the date we found it on the site (arrow 2).

SEC487 Searching for IP Lab Submission Form

This form is for students to submit their findings from one of the SANS SEC487 Labs where they look for proprietary/restricted data online.

* Required

1. Paste the URL to the discovered content (Example: <https://example.com/pdfs/sans560.pdf>) *



2. What date did you find this content? (Sometimes things disappear from the internet) *



3. Continue to fill out the rest of the form with as much detail as possible.
4. When you have completed this entry, repeat the process of discovery, documentation, and reporting for additional findings until your instructor tells you the lab is over.

Managing Passwords

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step Instructions

Objectives

- Create a new password manager database using KeePassXC
- Store passwords in KeePassXC
- Use the KeePassXC password generator

Goals

1. Start KeePassXC and create a new database
2. Add the user name and password for the SEC487 VM to the database
3. Save the database
4. Use the KeePassXC password generator to create a password that is 21 characters, and composed of upper and lower case letters and numbers.

Preparation

No VPN

Step-by-step Instructions

There is a video walkthrough for this lab. Click here to view it.

We will be using the open source password manager KeePassXC (<https://KeePassXC.org/>) for this lab. It is free, has strong encryption, and the KeePass-family of applications work on macOS, Windows, and Linux. Throughout the rest of the course, you will be authenticating to a variety of systems and sites. You can use KeePassXC to record those logins and security questions to a local, encrypted database.

An additional feature that we will explore is the password generator feature of the application.

1. We launch the application by clicking once on the KeePassXC application in the menu bar.

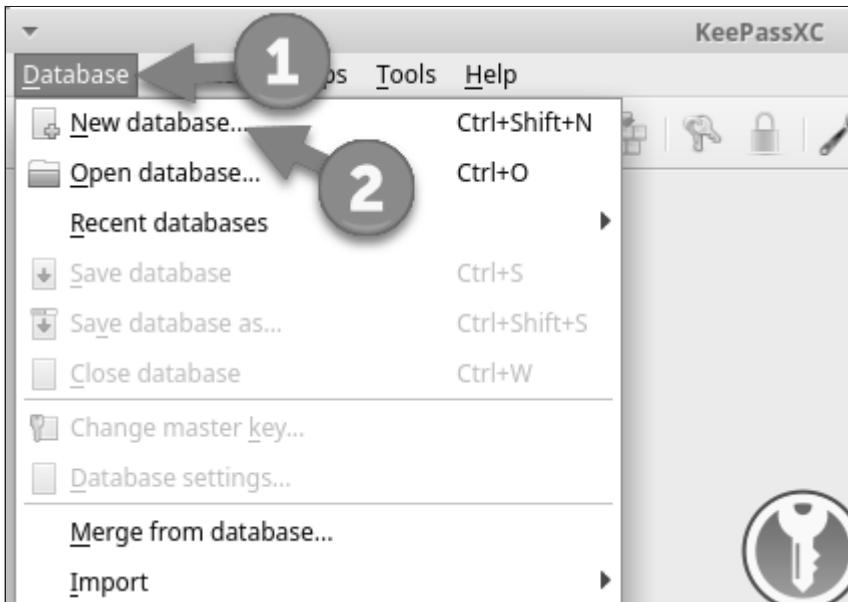


The first time you use KeePassXC you will need to create a database to store your passwords inside.

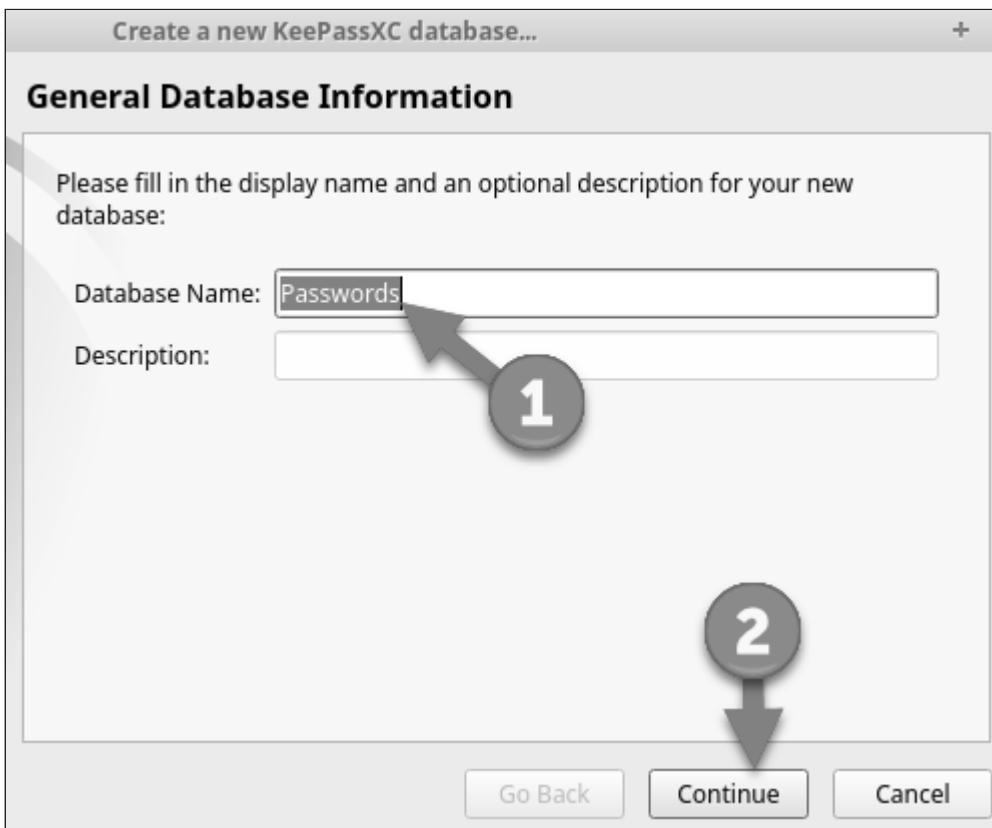
⚠ Tip

You only have to do this the first time.

2. To do this, click on the Database menu item at the top left of the KeePassXC application window and then selected New Database.



3. Enter a name for the database (arrow 1 below) and click the Continue button (arrow 2).



4. Accept the default values for the KeePassXC Encryption Settings by clicking the Continue button (arrow 1).



The way KeePassXC works is that there is a master key that unlocks all the passwords inside of the database. We need to create a strong password.

Choosing Your Own Password

While you can use any password or passphrase you wish for this lab, we suggest using the class password so that if you forget the password during class (you will be learning lots of different things and, well, sometimes we forget), you can refer to the book or ask a friend what the password should be.

Choosing Your Own Password - Warning

If you choose a password known only to you and you forget it, your data inside the KeePassXC application is irretrievable.

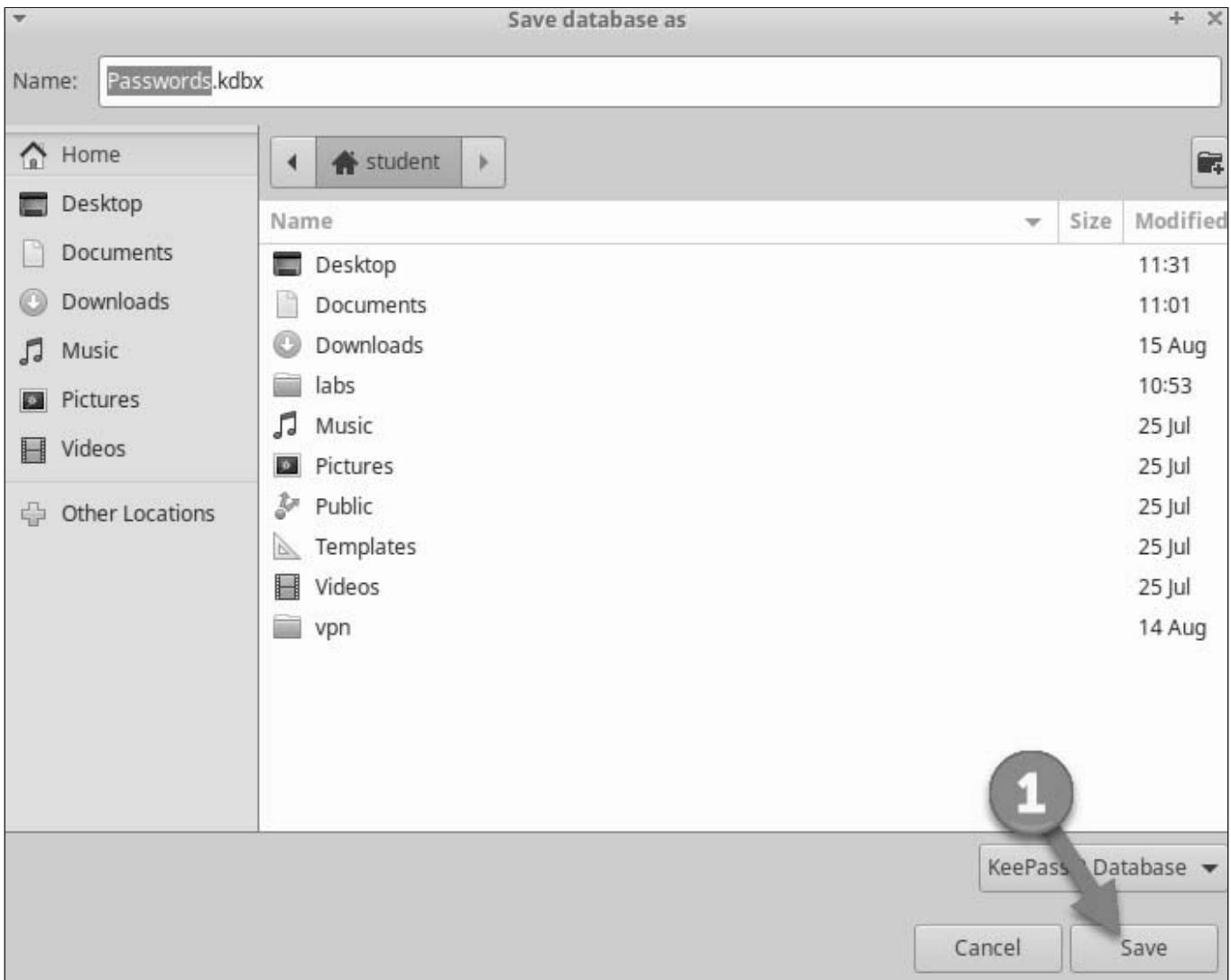
The password we suggest you use is: This is a long 1.

- Enter that (or the password you chose) into the password fields (shown below).



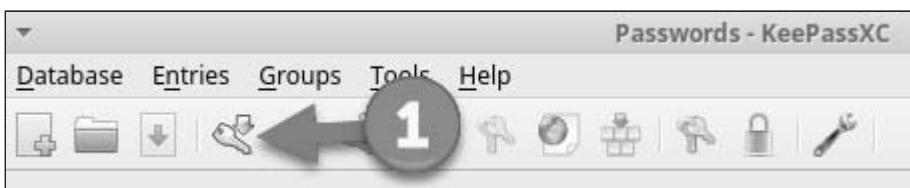
If you wish to see what you typed, click the eyeball icon  on the far right of the field.

- Click the OK button when you have finished.
- We will need to tell KeePassXC where to save the database and what to name it. We will keep the defaults (saved in `/home/student` and filename of `Passwords.kdbx`) as shown below. Click the Save button.



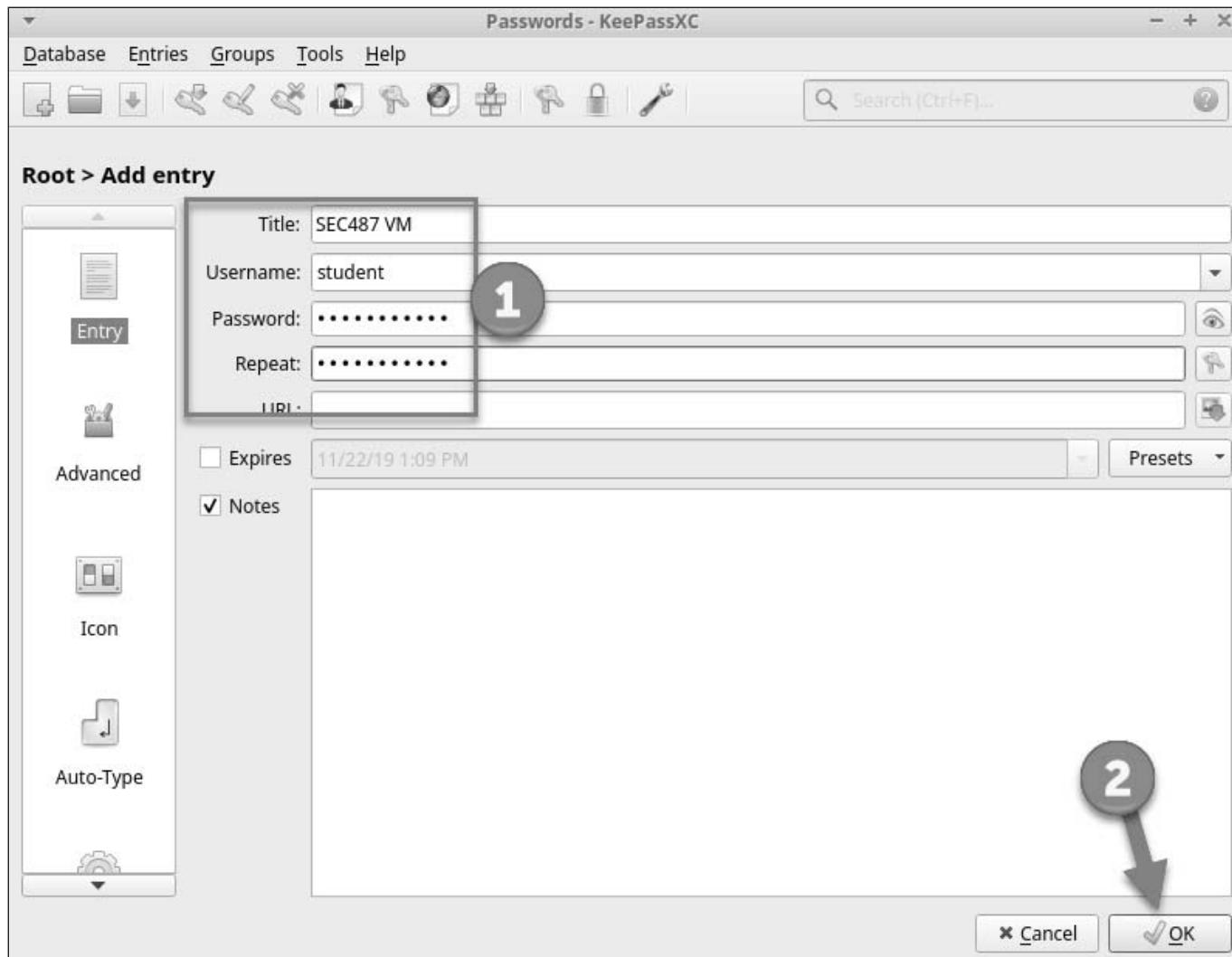
Our first entry will be for the SEC487 VM user name and password. While it seems silly to enter this inside a database that you must open from an application that you can only access once you have the user name and password to log into the system, entering it here can be useful. Some people copy their KeePassXC databases to USB drives or store them on cloud servers so that they can access from other systems or their mobile devices.

8. To create a new entry, click the Add New Entry button.



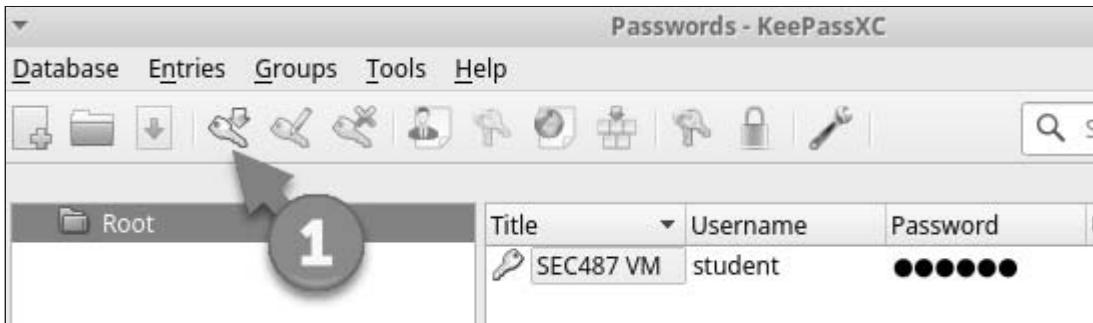
The title should be something like SEC487 VM . Then fill in the rest of the data (User name: student ; Password: Securi ty487 ; Repeat: Securi ty487) (arrow 1 below).

- When you have completed, click the OK button (arrow 2) to save this record.

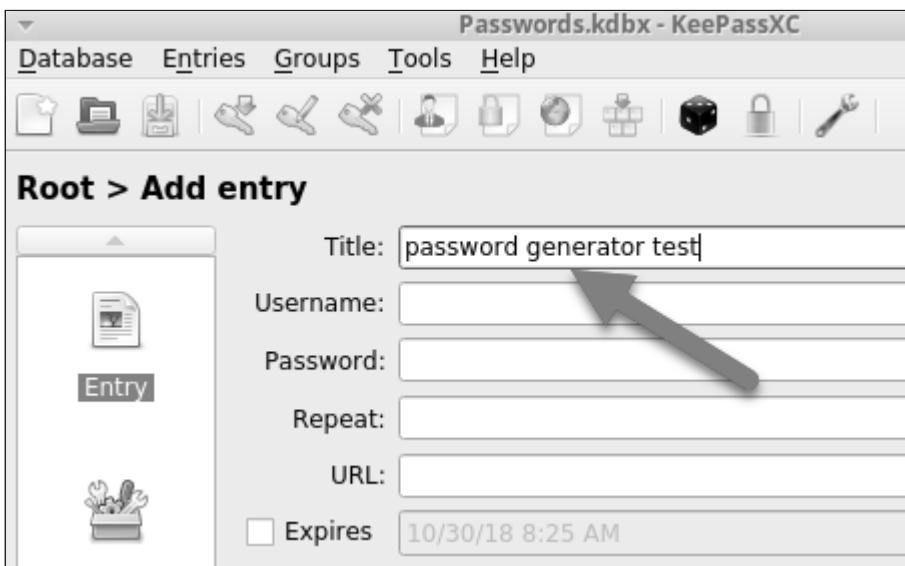


The KeePassXC application ships with a password generator to make it easier to create a pseudo-random password from certain character sets. Have you ever had to create an 8-12 character password using lowercase and uppercase letters, numbers, and the characters semicolon, hyphen, and forward slash? It gets challenging to make good passwords with all these constraints. The password generator helps with this task.

- Create another new entry by clicking the key with the green arrow.



11. We will name this password generator test in the title field.



To the right of the password "Repeat" field is a button which is used to generate a new password.

12. Click this button.



13. I like to see the passwords that are created so I click the eyeball button on the far right to see the passwords.

For this example, let's use the following password creation rules. Passwords must:

- Contain uppercase characters

- Contain lowercase characters
 - Contain numbers
 - Be at least 21 characters long
14. We need to change the length from 16 characters to 21.

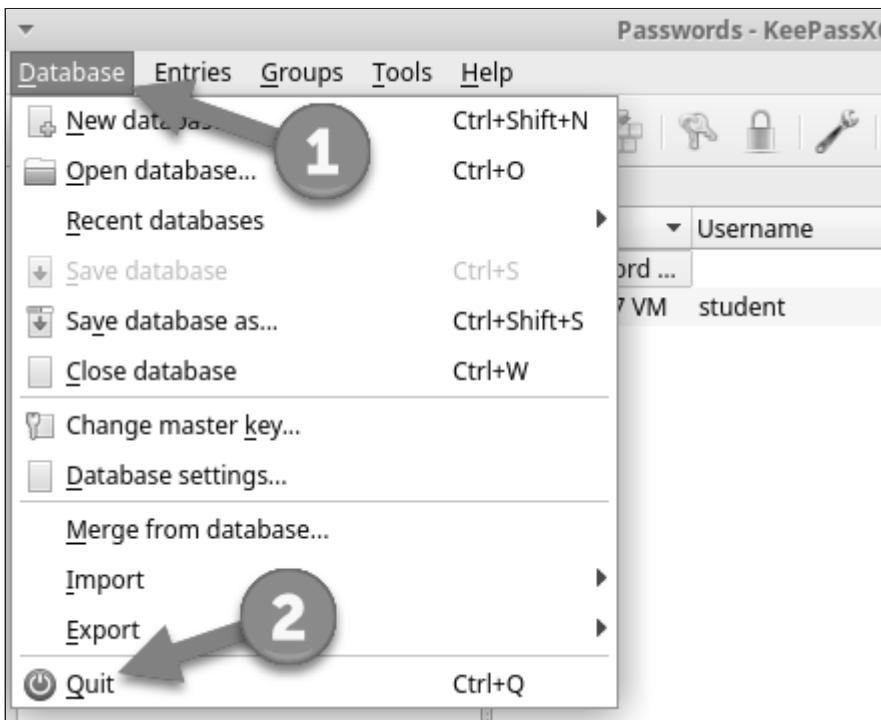
You can see in the image below that it choose a password (arrow 1) for us. Arrow 2 points to the place where we alter the number of characters in the password.



⚠ Unique Passwords

Since this is a password generator, the password shown in the Password: field in your KeePassXC will be different than the one shown above.

15. When you are happy with the password that was generated click the Accept button (arrow 3 above) to move it to the password and repeat fields.
16. Then click the OK button at the bottom of the record to close it.
17. We have completed our editing. Close the KeePassXC application by clicking the Database menu option (arrow 1) and then the Quit (arrow 2).



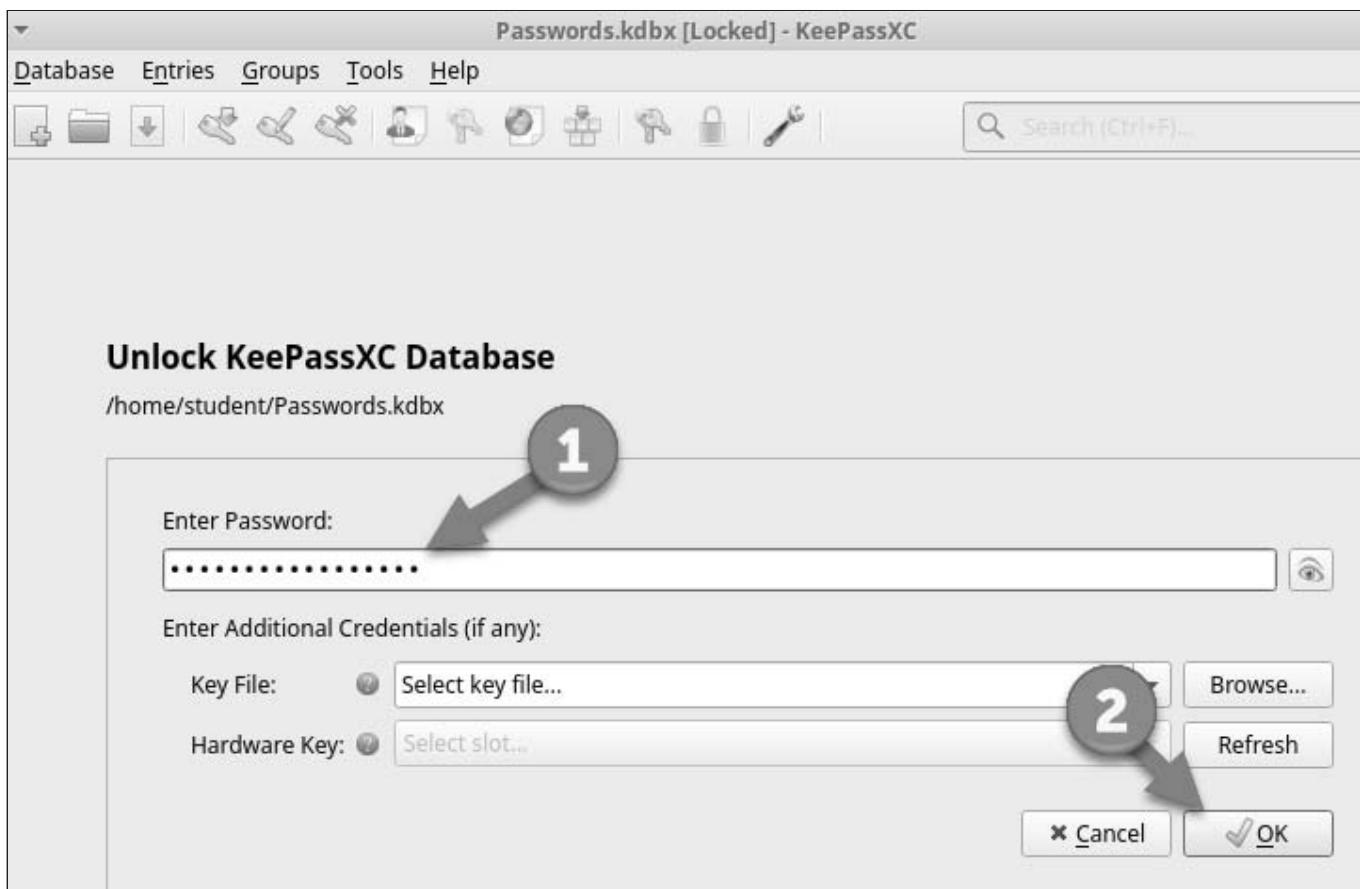
Now that we have a good database with a couple of records in it, let's get back into it and see what it looks like when we want to use it.

18. Click the KeePassXC icon in the menu bar to launch the application.

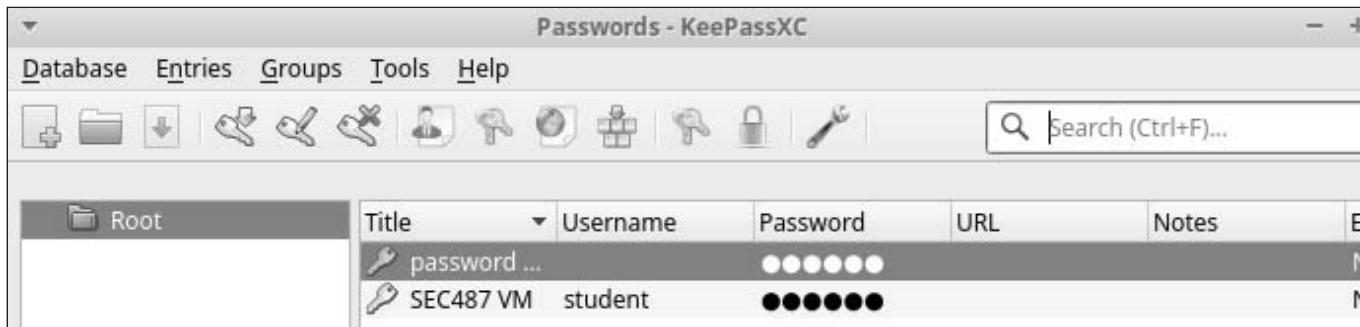


When it opens, it will remember the last database opened and request the password key for it.

19. Enter the `This is a long 1.` string (or whatever password you made for the master password) and click OK.



If successful then KeePassXC should have reopened and you should be able to see the two records you just created.



20. The lab is finished. You may close the KeePassXC application now.

This page intentionally left blank.

Slacking It

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions

Objectives

- Gain confidence in using Slack, navigating the application, and understanding what content can be found.

Goals

1. Log in to the SEC487alum Slack
2. Make your first post in the `#firstpost` channel

Preparation

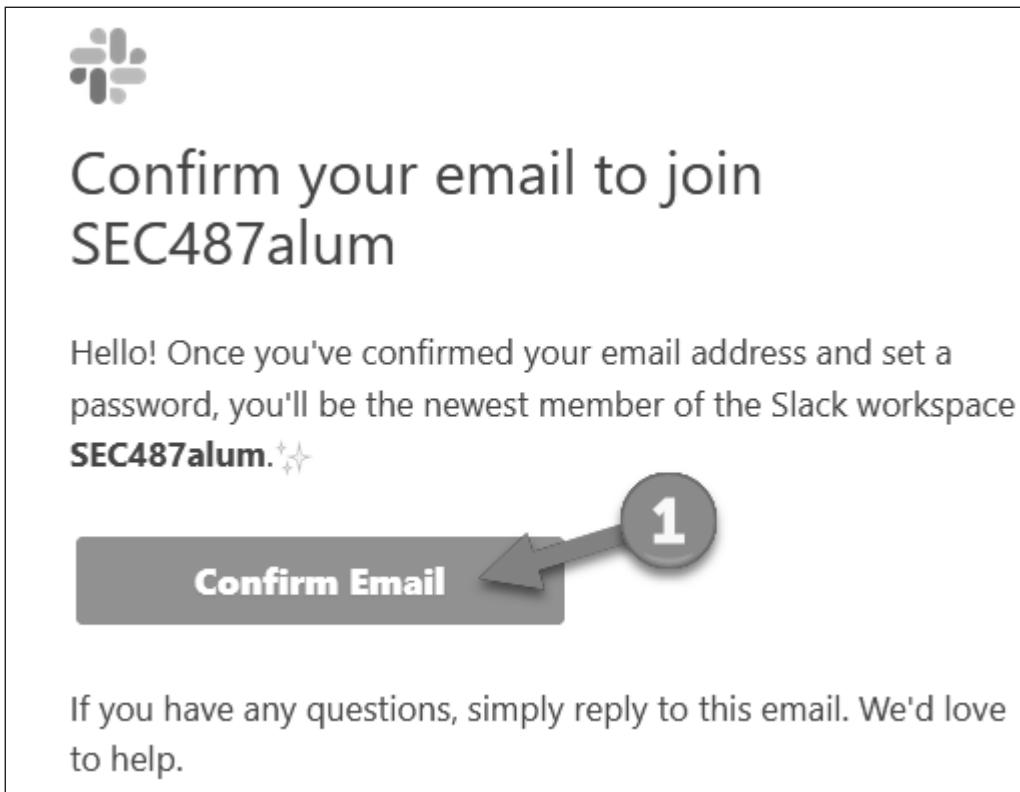
No VPN

Step-by-step instructions

The SEC487 class has a Slack online group so that students and instructors can talk about OSINT and course-related topics. This optional lab explains how you gain access to this resource.

We understand that some people (or their companies) might not want the Slack application installed on their host systems so we added it to the VM! Before gaining access to the Slack content, you need to request an account using the link from an earlier lab (<https://sec487.info/joinslack>).

1. You should get an email in the account you used to sign up for the Slack that looks like the email invite below. Click the Confirm Email button (arrow 1 below).



2. You will be redirected to Slack.com's web site to fill in their registration form. Enter in the appropriate data like a name (arrow 1 below), a password (arrow 2), uncheck the box asking for permission to send you spam emails (arrow 3), and then click the Create Account button (4).

Join the Slack workspace SEC487alum

Full name

Full name

1

Your name will be displayed with messages you send.

Password (required)

Password

2

Passwords must be at least 6 characters long, and can't be things like "password", "123456", or "abcdef".

It's ok to send me email about the Slack service.

Create Account

3

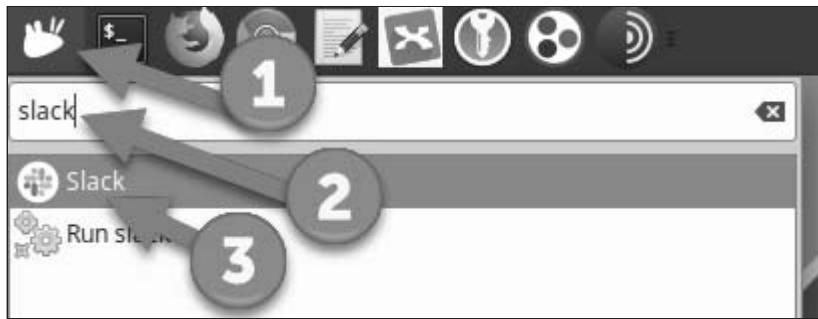
4



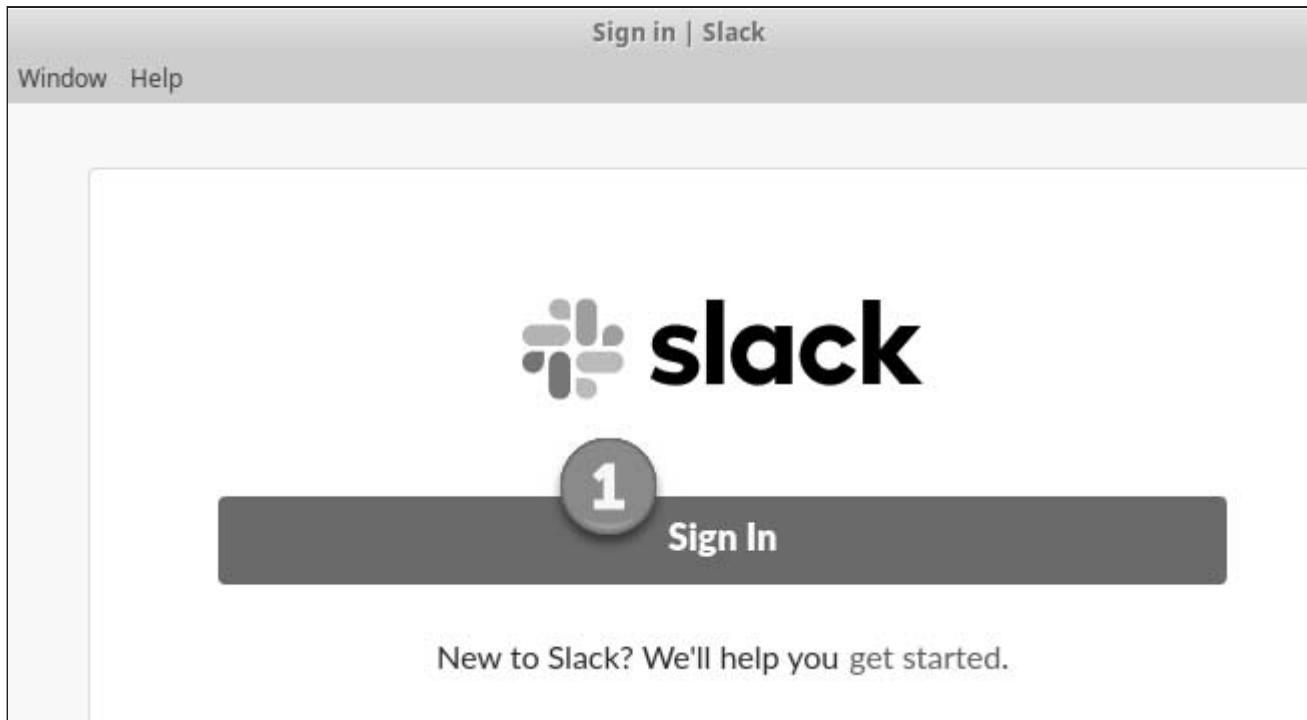
Many Methods to Access Slack

Now you can launch the Slack application in your VM. You also can use the Slack mobile applications on your phones/tablets, the web version, or a version of the Slack application installed on your host system. You choose.

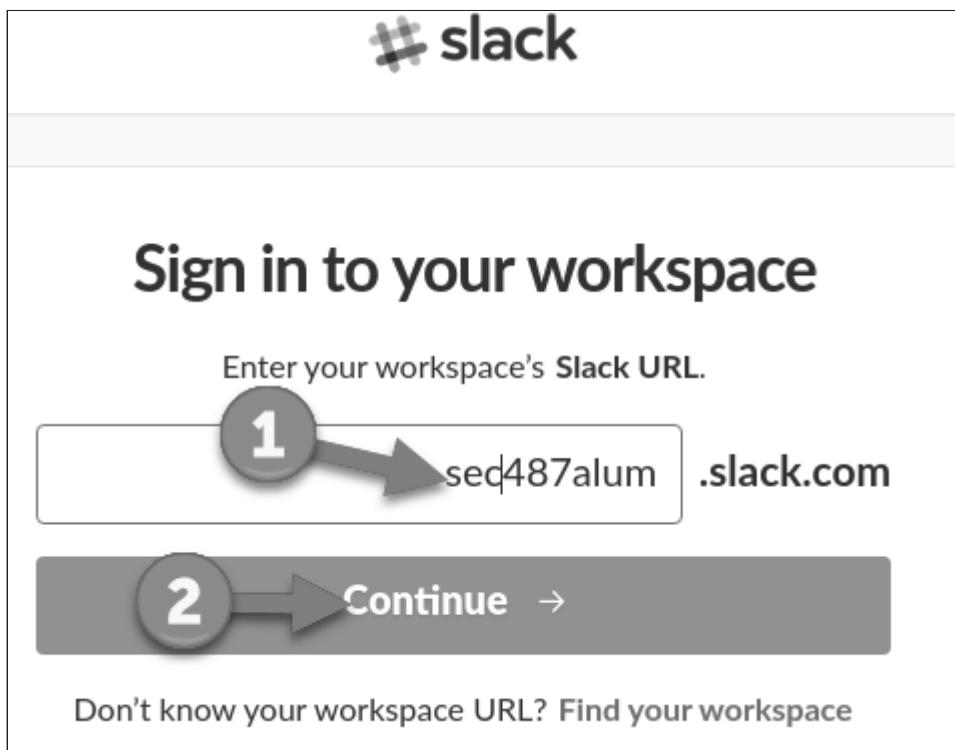
3. To launch the Slack application installed in the VM, click on the white mouse in the blue circle in the taskbar (arrow 1 below). When the menu drops down, type the word slack (arrow 2), and then click the Slack application shown below it (arrow 3).



- When you launch the application (inside the VM), click the Sign In button which will then open a web page.



- Slack now asks for the workspace name. Enter `sec487al um` (arrow 1) and click Continue (arrow 2).



6. You will need to enter the email address and password you used for your Slack account and click Sign In.

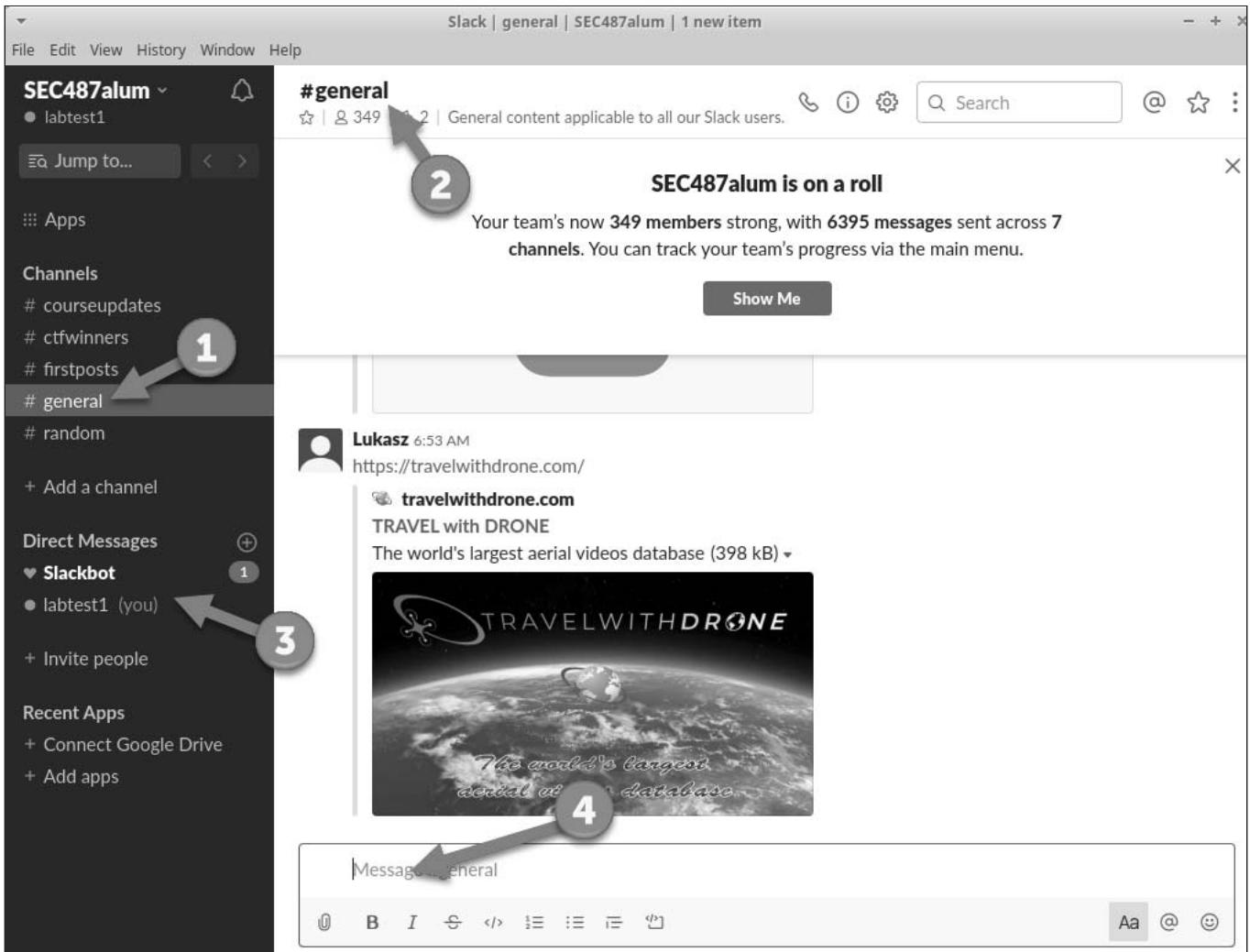
The screenshot shows the Slack sign-in form. The title "Sign in to SEC487alum" is at the top, followed by the URL "sec487alum.slack.com". A text input field for the email address has "1 example.com" entered. A text input field for the password has "2 word" entered. A large button labeled "3 Sign in" is positioned below the password field. Below the form are links for "Remember me" (with a checked checkbox) and "Forgot password? · Forgot which email you used?".

7. You will be asked to launch the Slack application (shown below). click Remember my choice for slack links (arrow 1) and then the Open link button (arrow2).

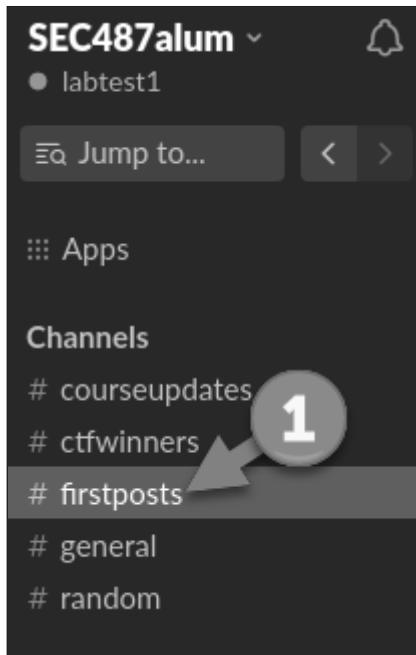


8. Let's orient you to the window and how to use Slack. It is an elegant design and user-friendly. You should see a window like the one below. We have pointed out different pieces of the window.

- Channels (arrow 1) - Think of these as different rooms to have specific conversations in. At the start, you are joined to several channels: general, random, ctfwinners, courseupdates, and firstposts. Channels are referred to using the `#channel` format.
- Current Channel (arrow 2) - At the top of the window you will see the name of the current channel you are viewing. For the picture below, it is the general channel.
- Direct Messages (arrow 3) - If you want to send a private message to another person in the Slack, you can click the + next to the Direct Messages label and enter the user's name.
- Post field (arrow 4) - At the bottom of the window is the area to type what you want to post.



- Change to the #firstposts channel by clicking on that channel's name (arrow 1 below).



10. Fill in the post field at the bottom of the window with something you want everyone in the channel to see. Write `Hi` or `My first post!` or something else (arrow 2 below) and click the Enter key to send it.



Channel Description

There may be a description of what kinds of conversations should be discussed in the channel description area at the top of the window (arrow 1 below).

#firstposts

WebBreacher created this channel today. This is the very beginning of the #firstposts channel. Purpose: As part of a SEC487 lab, we ask students to make their first post to Slack. This is the place for those. (edit)

+ Add an app  Invite others to this channel



Today

 **WebBreacher** 8:50 PM
joined #firstposts.

 **WebBreacher** 8:50 PM
set the channel purpose: As part of a SEC487 lab, we ask students to make their first post to Slack. This is the place for those.

 Pinned
 **WebBreacher** 8:51 PM
Welcome to the Slack and congrats on making your first post! We hope you are enjoying the SEC487 class and continue OSINT conversations in this group.

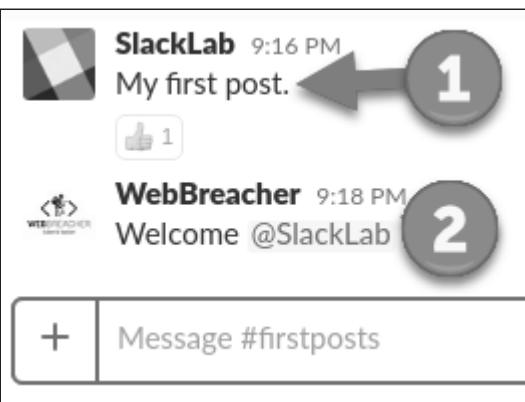


My first post.



bold _italics_ ~strike~ `code` `preformatted` >quote

After posting something, you will see it posted to the channel. People can respond to your post and post other content. You can see in the image below the first post and WebBreacher responded. The way he did it, it would have sent an alert to the SlackLab user because he "tagged" the user in his post by using the `@user` format. You can also see that someone responded to the first post with an emoji thumbs up!



 **SlackLab** 9:16 PM
My first post.

 1

 **WebBreacher** 9:18 PM
Welcome `@SlackLab`

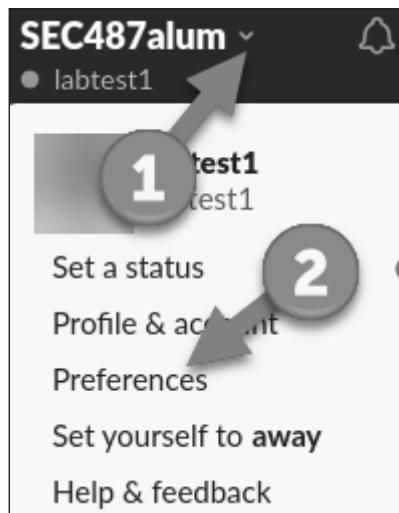
 Message #firstposts

Now that you know how to post and move around in the application, you may wish to alter your user preferences to customize your experience.

- To visit the preferences menu, click the v next to the SEC487alum heading in the top left of the window.

The screenshot shows a Slack channel interface. At the top, a message from 'WebBreacher' at 1:04 PM reads: 'set the channel purpose: Is there a typo in the courseware? Do you have suggestions for other content? Put that info in here!'. Below this, the channel header shows '#coursewaresuggestions' was created by WebBreacher on December 9, 2017. A large button labeled 'Join Channel' is visible, with a callout arrow pointing to it. Another button labeled 'See More Details' is also shown with a callout arrow.

There are a variety of settings in this area. Feel free to change them as you see fit.



- When you are ready to exit the preferences area click the `ESC` key or click the X in the upper right.

Your preferences for SEC487alum

Notifications

Language & Region
Messages & Media
Themes
Sidebar
Mark as Read
Accessibility
Advanced

Notifications

Notify me about...

[About notifications](#)

All new messages
You'll be notified for every new message

 from SEC487alum
Good morning everyone!

Direct messages, mentions & keywords
You'll be notified when a teammate mentions you, sends you a direct message, or uses one of your keywords

 from SEC487alum
Hi @labtest1

Nothing
You won't receive notifications from Slack.
Note: you will still see badges (1) within Slack

 from SEC487alum
Hi!

Notify me about replies to threads I'm following

Use different settings for my mobile devices

When you click the close application X in the upper right of Slack to close it, it will stay running and keep you logged in.

EC487alum 

[About notifications](#)

message.  from SEC487alum
Good morning everyone!

words  from SEC487alum
e mentions  from SEC487alum
Hi @SlackLab

Check out the # icon on the right of the toolbar (arrow 1 below).



- You will see a blue dot in this # icon when someone has posted in a channel that you are joined to. This is your signal to go into Slack and take a look at what was posted.
- When you receive a new mention (someone uses the @YOURNAME in a post), a red dot will appear in this # icon and (depending upon how you configured the application preferences) a pop-up window may appear indicating a new message has been posted.
- If you ever want to exit out of Slack on your system, right click the # icon and select Quit.

13. The lab is finished. You can keep Slack up and running through the course if you'd like.



OPSEC ALERT!

We are not using this VM for anything sensitive. If you were performing a sensitive assessment from it, you would most likely not want something like Slack running on the same system that you are performing your OSINT work upon. Slack will use the system VPN and network connections to send and receive traffic. Consider installing Slack on your host system or mobile device.

Harvesting Web Data

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions

Objectives

- Use Censys.io to retrieve OSINT data from HTTPS Certificates

Goals

1. Your customer, a web development company, is trying to find one of their ex-employees (Kevin). All they have is the old domain that the employee said was theirs: mnksmith.com. Can you find an email address for him?
2. Use the <https://censys.io> web site to find an email address associated with the mnksmith.com domain HTTPS certificates.

Preparation

Yes VPN

Limited Censys.io Requests Per IP

The censys.io web site only allows 10 searches per IP address per day. Use them for the lab first and then you can do other queries if you'd like.

Step-by-step instructions

Our goal is to find the email address of a user associated with the mnksmith.com domain. We know that sometimes web sites use HTTPS and, to do this, they must have a TLS or SSL certificate. These certificates can have useful data in them. We will use the Censys.io web site to see if it captured content that may be useful in the target domain's HTTPS certificate.

1. In Firefox, visit the <https://censys.io> web site.
2. Scroll down the page until you see the Search Certificates button (arrow 1 below). Depending on your screen width, the web page may look different than below. Click that button to perform a certificate search.



Screen Size

Depending on the width of your browser window, the Censys page may look like the below image or the fields may be next to each other.

Search Censys Data

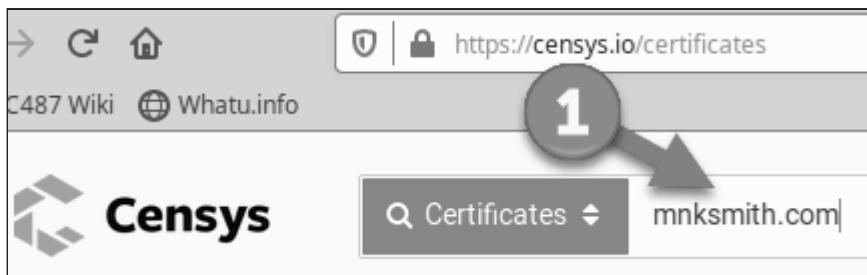
Search IPv4 →

Search Certificates → **1**

Search Websites →

More About Data →

3. You are going to type: mnksmi th. com into the field (arrow 1 below) and then press your Enter key.



This should take your browser to the https://censys.io/certificates?q=mnksmith.com page.

4. Scroll down the page (or visit the additional pages of results) and you will see the entry below which has the email address in it.

CN=server.mnksmith.com

- Let's Encrypt Authority X3
- 2017-03-17 - 2017-06-15
- server.mnksmith.com
- parsed.names: server.mnksmith.com

⚠ C=US, ST=IN, L=Indianapolis, O=MnK Smith, CN=192.168.*:

- C=US, ST=IN, L=Indianapolis, O=MnK Smith, emailAddress= [REDACTED]@mnksmith.com
- 2017-06-13 - 2022-12-04
- *.mnksmith.com, 127.0.0.1, 192.168.1.10, 192.168.1.20, ...

Record the email address you see in your notes.

This email address is a pivot point for our investigation. We will pause our work here and continue researching this email in the coming labs.

This lab is completed. If you have time, you can perform more queries, sign up for a free account, and look for other interesting content such as unknown IP addresses and domain names.

Click Here to See Our Findings ▼

Email Address: kevin@mnksmith.com

Web Analytics

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Retrieve the UA Code
 - Find Other Domains with that Code
 - Analyze the Data

Objectives

- Find the Google Analytics code of a web site
- Find other domains/web sites that use that code
- Perform OSINT on those sites and find out why they have the same code

Goals

1. Find the Google Analytics code used on the <http://www.city-data.com/> site
2. Use that code to find other sites that also use it
3. Determine what the common factors are for those sites (why do they all use the same code?)

Preparation

VPN if problems

Step-by-step instructions

As this is a challenge lab, our directions will be more sparse than normal. This is to get you to try things on your own.

Retrieve the UA Code

1. Launch a web browser (Firefox or Chrome) and visit the <http://www.city-data.com/> site.
2. Right click on the page and choose View Page Source.
3. Use the Find command to search for UA- in the source code of the page. Extract the UA- code with the numbers in it and write that down in your notes.

Find Other Domains with that Code

1. In your web browser, visit <http://spyonweb.com>, <https://builtwith.com> (remember to search for the domain here and not the UA code), or visit <https://urlscan.io/api/v1/search/?q=UA-XXXXXX> (replace the UA-XXXXXX with the code you found).
2. Record all the other domains that also have that UA- code found in their code.

Analyze the Data

Here, we are going to leave this for you to figure out. Why are all these sites using the same Google Analytics code?

 Click here for a hint



What company owns all those domains?



Click Here to See Our Findings



1. UA code for city-data.com is UA-892232 .
2. Other sites using that code as of November 2018

```
photo-dictionary.com
readperiodicals.com
shareranks.com
the-linking-light-ministries.blogspot.com
www.advameg.com
www.americoreignrelations.com
www.bankencyclopedia.com
www.biologyreference.com
www.chemistryexplained.com
www.city-data.com
www.deathreference.com
www.discoveriesinmedicine.com
www.everyculture.com
www.fashionencyclopedia.com
www.filmsreference.com
www.foodbycountry.com
www.healthisforchildren.com
www.hospital-data.com
www.humanities.com
www.madehow.com
www.medicalorders.com
www.musicbanter.com
www.mythencyclopedia.com
www.nationsencyclopedia.com
www.nonprofitfacts.com
www.notablebiographies.com
www.photo-dictionary.com
www.politiciansissues.com
www.presidentprofiles.com
www.pressreference.com
www.readabstracts.com
www.readperiodicals.com
www.referenceforbusiness.com
www.scienceclariified.com
www.sexencyclopedia.com
www.surgeryencyclopedia.com
www.trademarkencyclopedia.com
www.waterencyclopedia.com
www.weatherexplained.com
```

3. Reason for same Google Analytics code is that all of these sites are owned/run by Adavmeg, Inc. <http://www.advameg.com>. DNS is all similar and so is the Whois data for the majority of these sites.

This page intentionally left blank.

Metadata Analysis

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Extract metadata from DOCX file
 - Examine JPG metadata
 - Map the image GPS coordinates

Objectives

- Understand how to examine the metadata within files from a Linux command line
- Get comfortable with mapping the GPS coordinates for geotagged images

Goals

Instead of a scenario for this lab, we have a puzzle.

1. Using Linux command line tools, extract metadata from the `/home/student/labs/metadata-analysis/thismetadata.docx` file and follow the instructions that you find.
2. Examine the metadata of the four JPG images in the same directory as the DOCX file and extract the GPS coordinates of the images.
3. Display each GPS coordinate on a map and determine the country name for that image.

Challenge!

- Find the real locations where the woman.jpg and hotel.jpg pictures were taken (the metadata locations are not correct).

Preparation

No VPN

Step-by-step instructions

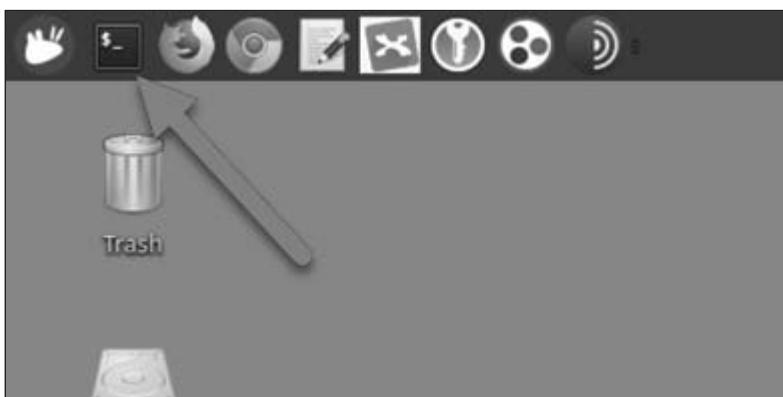
Extract metadata from DOCX file

The de-facto tool for Linux command line metadata extraction is the exiftool. We will use it in both parts of this lab.

👉 Document with MindMap or Hunchly

Consider using a MindMap to track your work in this lab.

1. Our first step is to launch a terminal window by clicking the terminal icon in the menu bar.



In the terminal, change directories to the place where your lab files are.

2. Type: `cd labs/metadata-analysis` then press Enter.
3. Take a look at what files are in the directory by typing: `ll` (that is 2 lowercase "L"s) which is a shortcut/alias for the `ls -AFIB` command then press Enter.

You should see 5 files in the directory (shown below). We will work with the Word document first and then with the images.

```
student@sec487 (14:55:12) :~$ cd labs/metadata-analysis

student@sec487 (14:55:15) :~/labs/metadata-analysis$ ll
total 13908
drwxr-xr-x  2 student student    4096 Dec  5 13:43 .
drwxrwxr-x 11 student student    4096 Dec  5 13:43 ..
-rw-r--r--  1 student student 6609554 Dec  5 13:43 field.jpg
-rw-r--r--  1 student student 3091276 Dec  5 13:43 hotel.jpg
-rw-r--r--  1 student student 12574 Dec  5 13:43 metadata.docx
-rw-r--r--  1 student student 2923143 Dec  5 13:43 ocean.jpg
-rw-r--r--  1 student student 1585725 Dec  5 13:43 woman.jpg
```

Using the exiftool from the command line is simple. We type: `exiftool FILENAME` where the FILENAME is the name of the file that we want to examine.

4. Type: `exiftool metadata.docx` then press Enter.

The exiftool will display a large amount of data that will scroll off the screen. You can slide the scroll bar up to view it if you like but the majority of what we need for the lab, should be viewable at the bottom of the output (shown below).

Application	: Microsoft Office Word
Doc Security	: None
Lines	: 10
Paragraphs	: 2
Scale Crop	: No
Heading Pairs	: Title, 1
Titles Of Parts	: Here is the fancy Title
Company	: Princess Bride Imports LLP
Links Up To Date	: No
Characters With Spaces	: 1444
Shared Doc	: No
Hyperlinks Changed	: No
App Version	: 16.0000
Title	: 1-
Subject	: 2-
Creator	: Dread Pirate Roberts
Keywords	: 3-
Description	: Micah Hoffman
Last Modified By	: 4
Revision Number	: 2017:07:14 00:45:00Z
Create Date	: 2017:11:26 18:39:00Z
Modify Date	



For the lab, the main content you need is in the title, subject, and description fields shown above. For an assessment, all the information in the metadata should be recorded. The exiftool has a variety of output options that could be useful in your work: CSV (add `-csv`), JSON (`-j`), and short (`-s`) formats are some of the more useful ones. Let's export the metadata into a CSV file so that we can store it for later.

5. To do this type: `exiftool -csv metadata.docx > metadata.csv` then press Enter.
6. To check the first 10 lines of that CSV file, type: `head metadata.csv` then press Enter.

You will see the CSV formatted metadata content (shown below).

```
student@sec487 (14:56:31) :~/labs/metadata-analysis$ head metadata.docx.csv
SourceFile,ExifToolVersion,FileName,Directory,FileSize,FileModifyDate, FileAccess Date,FileInodeChangeDate,FilePermissions,FileType,FileTypeExtension,MIMEType,Zip RequiredVersion,ZipBitFlag,ZipCompression,ZipModifyDate,ZipCRC,ZipCompressedSize ,ZipUncompressedSize,ZipFileName,Template,TotalEditTime,Pages,Words,Characters,A pplication,DocSecurity,Lines,Paragraphs,ScaleCrop,HeadingPairs,TitlesOfParts,Com pany,LinksUpToDate,CharactersWithSpaces,SharedDoc,HyperlinksChanged,AppVersion,T itle,Subject,Creator,Keywords,Description,LastModifiedBy,RevisionNumber,CreateDate,ModifyDate
metadata.docx,10.80,metadata.docx,,,12 kB,2019:12:05 13:43:23-05:00,2019:12:05 1 3:43:23-05:00,2019:12:05 13:43:24-05:00,rw-r--r--,DOCX,docx,application/vnd.open xmlformats-officedocument.wordprocessingml.document,20,0x0006,Deflated,1980:01:0 1 00:00:00,0x6cd2a4df,346,1312,[Content_Types].xml,Normal.dotm,3 minutes,1,215,1 231,Microsoft Office Word,None,10,2,No,"Title, 1",Here is the fancy Title,Prince ss Bride Imports LLP,No,1444,No,No,16.0000,1- If you are reading this,"2- then y ou have ""finished"" this section.",Dread Pirate Roberts,,3- Visit the https://sec487.info/c5 site for details.,Micah Hoffman,4,2017:07:14 00:45:00Z,2017:11:26 18:39:00Z
```

Now you have a copy of the metadata that you can post-process in Excel or Libre Calc if you'd like. Let's use the exiftool to extract a single tag from the metadata. Above we saw something interesting in the "Description" field.

7. Type: `exiftool -Description metadata.docx` then press Enter to retrieve that single field/tag (shown below).

```
student@sec487 (14:56:49) :~/labs/metadata-analysis$ exiftool -Description metadata.docx
Description :
```

We are finished with this section of the lab, but, oh wait. There was a URL in the metadata (in the image above) which you may want to visit in a web browser.

Examine JPG metadata

We can use the same technique as above to see the EXIF data in the images in a directory. The latitude and longitude data we need is in the "GPSPosition" tag. We can tell exiftool to output it in a decimal degrees format to seven degrees of precision using the `-c %+..7f` flag. While we could dump all the EXIF data for each file and then comb through it (which, if this were a real case, you

may wish to do to preserve the metadata external to the file), we can perform this task MUCH more rapidly by pulling just that one tag.

1. To do this extraction, you type: `exiftool -c %+..7f -GPSPosition *.jpg` then press Enter.

This tells the exiftool to pull that single tag value for all JPG files in the current directory. Your output should include the file name and latitude and longitude reported in the image's metadata (shown below).



Only Looking at Metadata

Since this is a lab on the metadata of the image, we are not examining what the content of the image is. In a real assessment, you would analyze all aspects of the files.

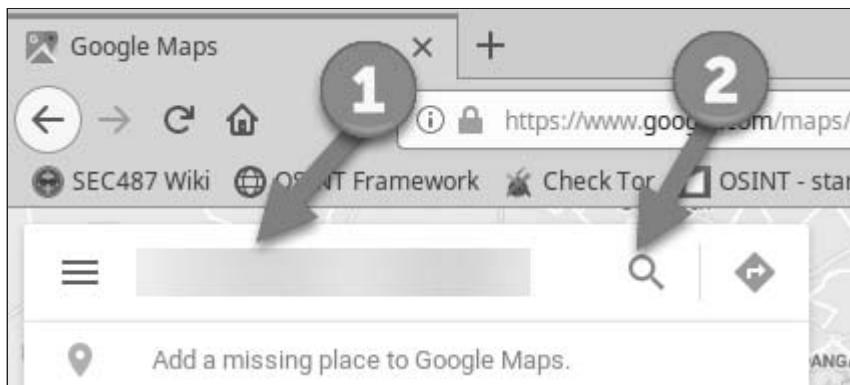
```
student@sec487 (14:57:22) :~/labs/metadata-analysis$ exiftool -c %+..7f -GPSPosition *.jpg
===== field.jpg
GPS Position          :
===== hotel.jpg
GPS Position          :
===== ocean.jpg
GPS Position          :
===== woman.jpg
GPS Position          :
4 image files read
```

In the above image, we see the file name (such as `field.jpg`) and then the GPS Position tag pulled from its metadata (for example: `+9.9999999, +1.1111111`).

2. Record this data in your notes and below.

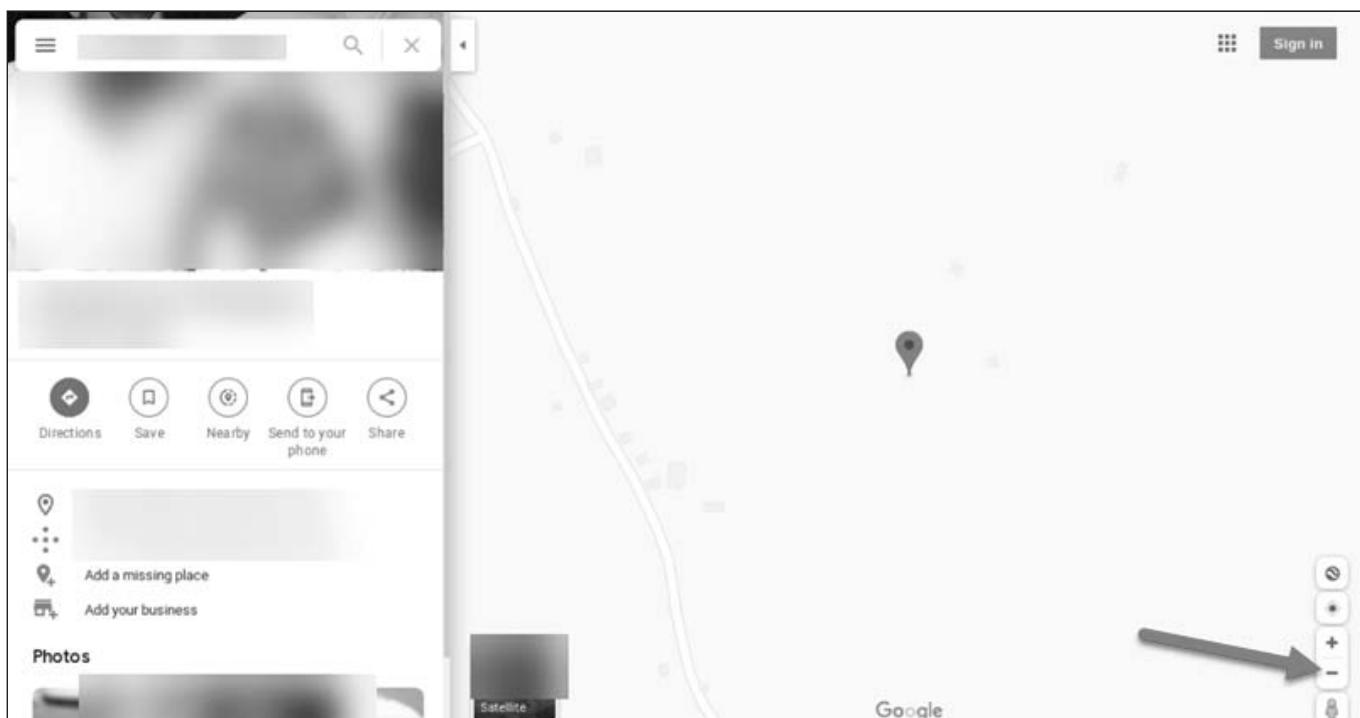
Map the image GPS coordinates

1. In your web browser, visit the <https://www.google.com/maps> web page.
2. In the upper right of the web page should be a form field with the words "Search Google Maps" in it (arrow 1 below). Click once in that field and press `CONTROL v` to paste the coordinates then press the Enter key or click the magnifying glass icon to perform the search (arrow 2).



The window should change and show you the map contents for those coordinates (shown below). Sometimes there is no labeled map content at the exact coordinates (shown below) and you may need to zoom out to see the name of the country where this image was taken.

3. Zoom out by clicking the - on the right.



When you decrease the zoom level you will see the shape, and possibly the name, of the country where this image was located.

Your challenge is to perform the conversion of coordinates and then lookup all 4 images on a mapping site (Google Maps, <https://www.openstreetmap.org/>, or any other).

4. Record the data you discover in your notes.

5. This lab is completed. When finished, close the web browser and the terminal. If you would like, you can save the gedit file or close it without saving its contents.

Click Here to See Our Findings ▼

Metadata in Word DOCX file:

```
student@sec487 (22:08:38) : ~/labs/lab3.4$ cat metadata.docx.csv
SourceFile,ExifToolVersion,FileName,Directory,FileSize,FileModifyDate, FileAccessDate,FileInodeChangeDate,FilePermissions,FileType,FileTypeExtension,MIMEType,ZipRequiredVersion,ZipBitFlag,ZipCompression,ZipModifyDate,ZipCRC,ZipCompressedSize,ZipUncompressedSize,ZipFileName,Template,TotalEditTime,Pages,Words,Characters,Application,DocSecurity,Lines,Paragraphs,ScaleCrop,HeadingPairs,TitlesOfParts,Company,LinksUpToDate,CharactersWithSpaces,SharedDoc,HyperlinksChanged,AppVersion,Title,Subject,Creator,Keywords,Description,LastModifiedBy,RevisionNumber,CreateDate,ModifyDate
lab3.4_metadata.docx,10.10,lab3.4_metadata.docx,.,12 kB,2018:01:06 15:39:24-05:00,2018:01:07 10:47:29-05:00,2018:01:07 10:47:29-05:00,rw-r--r--,DOCX,,application/vnd.openxmlformats-officedocument.wordprocessingml.document,20,0x0006,Deflated,1980:01:01 00:00:00,0x6cd2a4df,346,1312,[Content_Types].xml,Normal.dotm,3 minutes,1,215,1231,Microsoft Office Word,None,10,2,No,"Title, 1",Here is the fancy Title,Princess Bride Imports LLP,No,1444,No,No,16.0000,1- If you are reading this,"2- then you have ""finished"" this section.",Dread Pirate Roberts,,3- Visit the https://sec487.info/c5 site for details.,Micah Hoffman,4,2017:07:14 00:45:00Z,2017:11:26 18:39:00Z
```

```
$ exiftool -Description metadata.docx
Description : 3- Visit the https://sec487.info/c5 site for details.
```

```
$ exiftool -c %+_7f -GPSPosition *.jpg

filed.jpg: +22.7478439, +77.8940663
hotel.jpg: +26.4568930, +29.5460780
ocean.jpg: +9.2713936, +2.2990486
woman.jpg: -28.2842654, -71.0055342
```

Countries you should have discovered.

File name	Country
field.jpg	India
hotel.jpg	Egypt
ocean.jpg	Benin
woman.jpg	Chile

Challenges:

As for the challenges, talk to your instructor once you think you have the locations of the hotel and woman pictures.

This page intentionally left blank.

Retrieving Files Challenge

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Questions for gastonbachelard.org site files
 - Retrieve the files
 - Analyze the Files
- Answers for for gastonbachelard.org site files

Objectives

- Use Wget to retrieve files from web sites
- Use tools to extract data from those files to answer exercise questions below

Goals

1. Retrieve only PDF files from the <https://gastonbachelard.org/wp-content/uploads/> site.
2. Using those files, answer the questions below.

Preparation

No VPN

Step-by-step instructions

Questions for gastonbachelard.org site files

1. What are the names of the PDF document(s) where Julien's first and last name appear as the author?
2. Who was the manager of the nouvel_esprit.pdf document?
3. A person named Noudelmann was from a certain university. What was the name of the university?
4. What is the email address of a person with a first name of Chevrier?
5. What date and time was the COGITAMUS_Lettre-Bachelard_No6_Printemps-Ete-2012.pdf document created?
6. What file was created by Paolo using CorelDraw?
7. Extract all the URLs for YouTube videos.

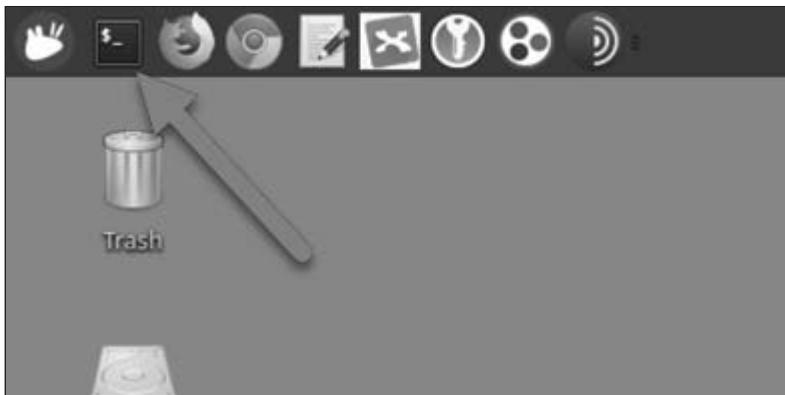
As this is a challenge lab, these instructions will give you a push in the right direction, but you will need to figure out some of the techniques yourself.

The end goal is most important: get us the answers to the above questions. How you choose to do it is up to you. Write a Python script. Use command line tools. Manually examine the documents. Again, does not matter HOW you do it, just that you do it.

We will give you some hints how you can accomplish this in the text below.

Retrieve the files

1. Launch the terminal window by clicking the terminal icon in the upper left of the menu bar.



2. Let's make a directory to store the files that you will retrieve. To do this in the command line we run the `mkdir` command to "make a directory". You could also do this via the GUI interface. Type: `mkdir labs/retrieving-files` then press Enter.
3. To move the terminal window into that directory, type: `cd labs/retrieving-files` then press Enter. Your screen should look similar to the content below.

```
student@sec487 (10:37:17) : ~$ mkdir labs/retrieving-files  
student@sec487 (10:37:19) : ~$ cd labs/retrieving-files/  
student@sec487 (10:37:27) : ~/labs/retrieving-files$
```

4. We will need to make another directory for the `gaston` site. Type: `mkdir gaston` then press Enter.
5. Type: `cd gaston` then press Enter to change into that new directory.
6. Now let's download those files from the `gastonbachelard.org` site. We are going to use a different `wget` command here. Type: `wget -m -np -nd -A .pdf --no-check-certificate -e robots=off https://gastonbachelard.org/wp-content/uploads/` then press Enter.

What does this command do? We break down each flag and switch below but for more information, take a look at <https://www.gnu.org/software/wget/manual/wget.html>.

- `-m` - Mirror the site
- `-np` - Do not move up to the parent directories on the web site to retrieve files.
- `-nd` - Do not store the files in their directory locations where they were found on the web site. Just put them all in the current directory.

- `-A .pdf` - Only retrieve files with an extension of .pdf.
- `--no-check-certifi cate` - Do not examine the HTTPS certificate for errors.
- `-e robots=off` - Ignore the robots.txt file if there is one.

Your computer should be retrieving files from the server now.



This will take a while!

You will be downloading many files from this web site. Depending upon your internet connection speed and your computer, this could take from 5 minutes to 30 or more. You can press `CONTROL c` at any time to stop the downloading of the files before they are all downloaded.

Analyze the Files

To examine the metadata of the files, the `exiftool` is going to be your best/fastest tool. To examine the text-based content of the files, you have choices.

1. Open each file and manually search through it.
2. Write a custom Python or other script.
3. From inside the directory where the files are on the file system, use something like `pdftotext` to convert PDFs to text files. This will create a file that is a text file and ends in a .txt extension of each .pdf file. Then you can analyze them using text-based tools like `grep`. To accomplish this, `cd` into the `gaston` directory and use a command like:

```
for a in `ls *.pdf` do pdftotext $a done
```

4. Install use a special tool like `pdfgrep` to search inside PDFs

From here on, you are on your own to find the answers to the questions. Good luck!

Answers for gastonbachelard.org site files

This site continuously adds files to these directories so your results may vary from those below. We ran these analyses in November 2019 and will show our work so that you can confirm results.

Click Here to See Our Findings ▼

1. What are the names of the PDF document(s) where the word Julien appears in the author metadata field?

```
$ exiftool -Author *.pdf | grep -B1 -i Julien | grep -B1 Author  
===== AAGB_Librarie_bon-de-commande.pdf  
Author : Julien  
--  
===== Bulletin-Adhesion.pdf  
Author : Pennecot Julien  
--  
===== COGITAMUS_Lettre-Bachelard_No2_Pri nttemps-Ete2010.pdf  
Author : Julien  
--  
===== COGITAMUS_Lettre-Bachelard_No4_Pri nttemps-Ete-2011.pdf  
Author : Julien
```

2. Who was the manager of the nouvel_esprit.pdf document?

```
$ exiftool -Manager nouvel_esprit.pdf  
Manager : Jean marie Tremblay
```

3. A person named Noudelmann was from a certain university. What was the name of the university?

```
$ pdfgrep -i "noudelmann" *.pdf | grep -i uni  
COGITAMUS_Lettre-Bachelard_No10_Pri nttemps-ete_2014.pdf: 14h30-15h15 : François NOUDELMANN  
(Université Paris VIII), Imagination morte
```

4. What is the email address of an account with chevrier in the local-part?

```
$ pdfgrep -h -P "chevrier@*.fr" *.pdf  
chevrier.logistique@u-bourgogne.fr 5 rue de l'école de Droit
```

5. What date and time was the COGITAMUS_Lettre-Bachelard_No6_Printemps-Ete-2012.pdf document created?

```
$ exiftool -CreateDate COGITAMUS_Lettre-Bachelard_No6_Printemps-Ete-2012.pdf  
Create Date : 2012:06:20 20:46:37+02:00
```

6. What file was created by Paolo using CorelDraw?

```
$ exiftool -Creator -CreatorTool -File Name *.pdf | grep -B2 -A1 -i corel  
===== 2012-semi nai re-GB-heri tage-napl es. pdf  
Creator : Paolo  
Creator Tool : Corel DRAW  
File Name : 2012-semi nai re-GB-heri tage-napl es. pdf
```

7. Extract all the URLs to YouTube videos.

```
$ pdfgrep -h -P "https?://.*youtube\.com/watch.*" *.pdf  
  
http://www.youtube.com/watch?v=Id3GX9D0rLI&feature=youtu.be  
https://www.youtube.com/watch?v=QqhH9ZiV4bk  
https://www.youtube.com/watch?v=wDbNfVTPFsE  
https://www.youtube.com/watch?v=A04aLAd490o  
https://www.youtube.com/watch?v=GXjRyOnvNn0  
https://www.youtube.com/watch?v=eTYLaKT0i4U  
https://www.youtube.com/watch?v=D_9dnDN-J08  
https://www.youtube.com/watch?v=AETD4e9P4cM  
http://www.youtube.com/watch?v=k9Ynv
```

About My Home

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Examine Real Estate Sites
 - Use Reverse Phone Lookup

Objectives

- Gather OSINT data about a home from real estate web sites
- Execute phone number reverse lookups to find an owner/address

Goals

Your customer tells you that she is concerned for her safety. She has a vacation home and has been receiving taunting emails with pictures from inside her apartment. Your customer said that she redid her place a year ago and the pictures she is receiving are from before the renovation. She would like you to figure out how the emailer is getting these pictures. Your customer's address is: 2660 S Ocean Blvd, Apt 105N, Palm Beach, FL 33480.

Your customer also mentions that while in California at her main home, she found a dog wandering around Santa Barbara's beach. The dog had no microchip but did have a tag with a phone number:

805-895-0484. When she called the phone, no one would answer, and it would just ring and ring. Can you help her find the owner?

1. Using the address of your customer's apartment, visit real estate sites and find images inside your client's home.
2. Try using <https://google.com> and <https://thatsthem.com> to find the owner of the dog and where they live.

Challenge!

Here are some additional things to look for if you have time:

1. Can you find images of the kitchen that show appliances and other items on the kitchen counters?
2. Can you find who is the current owner of that property?

Preparation

VPN if problems

Step-by-step instructions

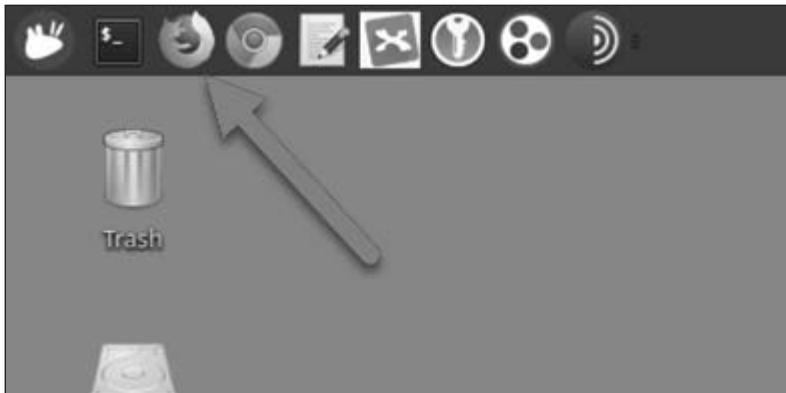
Examine Real Estate Sites

Your customer provided you her vacation apartment's address (2660 S Ocean Blvd, Apt 105N, Palm Beach, FL 33480). Let's get an understanding of where that is and what it looks like using Google and some real estate web sites.

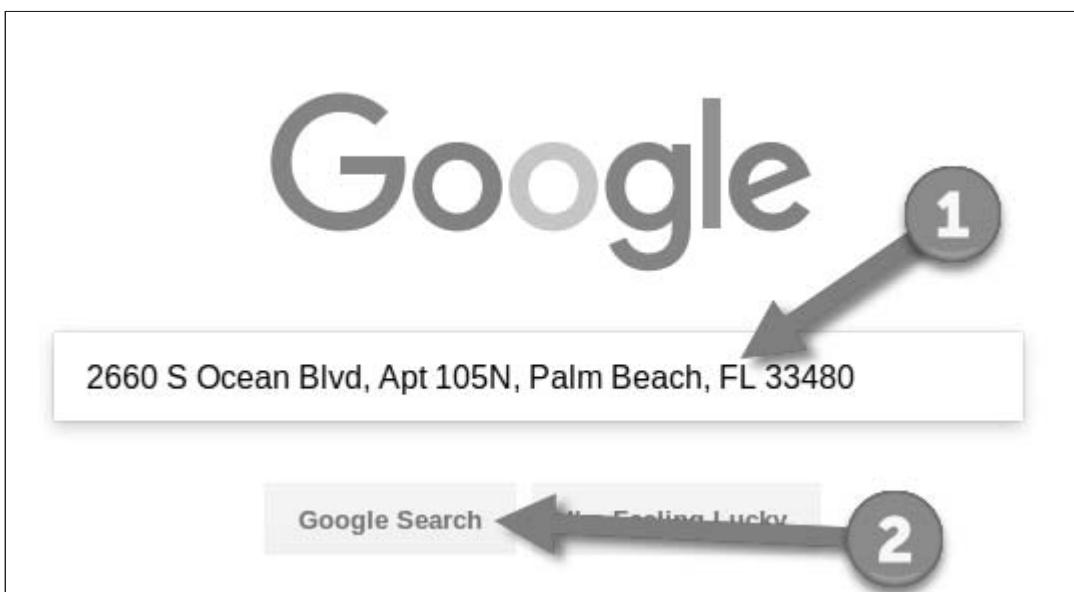
💡 Use Hunchly or a MindMap

Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

1. Launch the Firefox web browser by clicking the Firefox icon in the upper left of the menu bar.

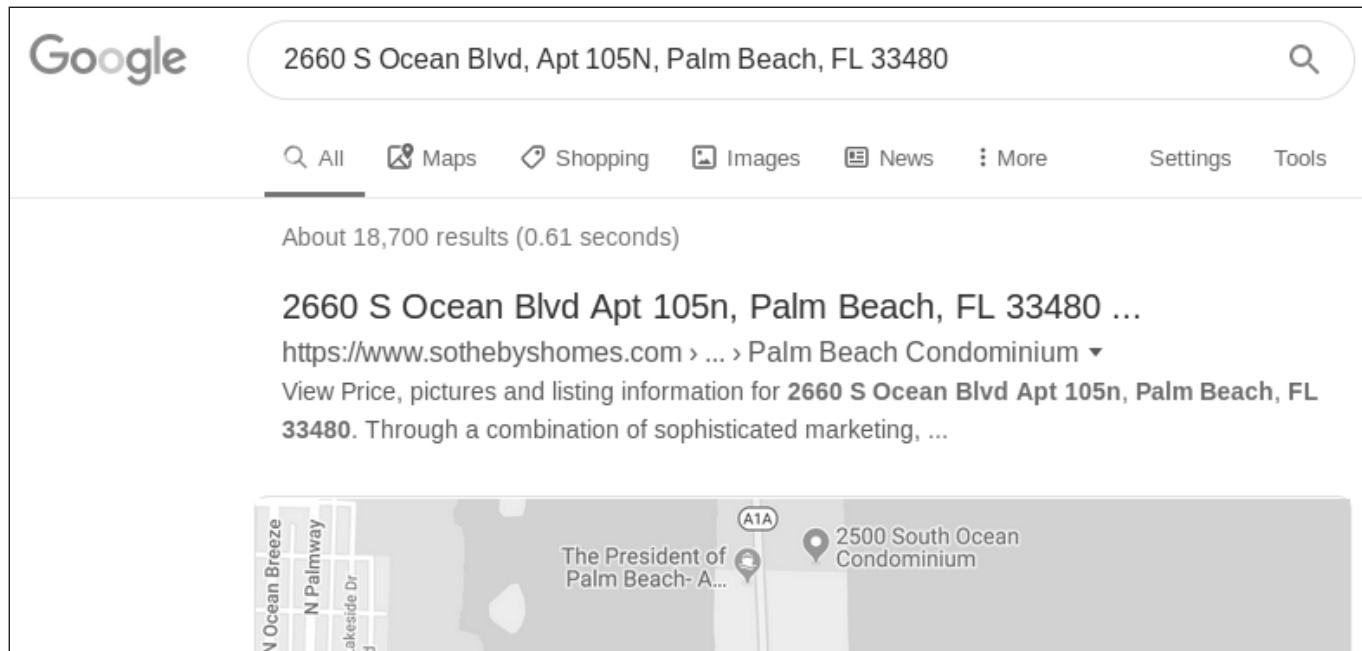


2. Visit the <https://www.google.com> web site.
3. In the main search field type: 2660 S Ocean Bl vd, Apt 105N, Palm Beach, FL 33480 and press Enter (or click the Google Search button).



This should show you results similar (but yours may be different) to the ones below. See that most of these sites are real estate companies? The challenge is figuring out which ones have the best and most-relevant data for the data we need to find. Under normal (non-lab)

circumstances, you may visit a variety of these sites to figure out what data each contains about your target location. Because this lab is time-constrained, we will focus your efforts on a couple of these results.



4. Scroll down the page until you get to the Sothebys <https://www.sothebyshomes.com/palmbeach/sales/0076539> results for that apartment. In our search, it was the first result.

The result you want looks like the one above.

If you don't see it in your results, visit it manually by typing: <https://sec487.info/c1> into your URL bar and pressing Enter.

The detailed page for the apartment now shows in your browser. One thing that we can also find is pictures of the property from previous viewings/listings. These can sometimes leak data about the inside of the place. In the image below, you can see there images from inside the apartment. Let's look through them and see if there is anything useful.

5. Click the right arrow on the screen (arrow 1 below) to make the slideshow advance or choose the image you wish from the panel at the bottom of the area (arrow 2 below).

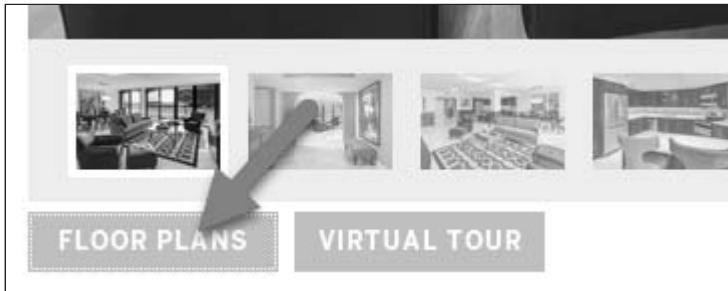


You should see images inside the apartment. Document this (and other images inside the house) by taking screenshots, noting the URL and content, and/or tagging them in Hunchly.



While documenting these images, begin to create a mental floor plan as to how these rooms fit together. Look at the cues in the images, the angles, the flooring and wall coverings to see which rooms can be seen from which angle.

If you click the FLOOR PLANS button below these images, you should see the floor plan for the apartment (image below). With this as our guide, and the images from the other slides, we can recreate what the inside of the apartment looked like.



6. [OPTIONAL] Depending upon your time, you may wish to create the report showing an image of the inside of the apartment and then show which room and the direction the picture was taken from. An example from the kitchen image above is shown below as an example below.



This image mark-up can help audience visualize the point of view of the person taking the photo but it is time-consuming and may not be required for your assessment.

Now, back to our customer and their request. We have some pictures from inside the apartment. We know when they were taken and can show them to her to see if they matched the ones sent in the emails.



Visiting Multiple Sites

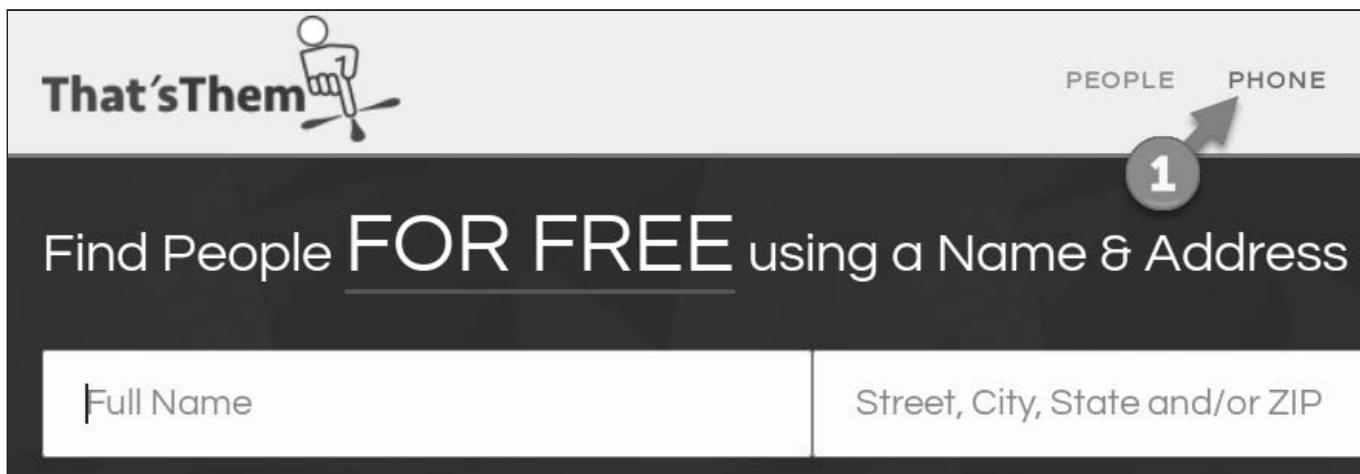
Due to time constraints, we visited a single real estate site. In a real-world assessment, you would have searched Google images, reviewed a variety of other real estate sites, looked in apartment rental sites for this listing, and possibly performed reverse image searches on each of these images to find other places that stored images about this apartment.

Use Reverse Phone Lookup

Your customer also asked you to check into the owner of the dog she found in California on the Santa Barbara beach. The phone number 805-895-0484 was on the dog's tag. For this effort, since the phone number looks like one found in the United States, you will use a reverse phone number search engine. Using a generic search engine such as DuckDuckGo or Bing will be less-useful as they will have a variety of results that promise to show the address and owner of the phone but are just baiting you to pay them money to see the content.

We will rely on thatsthem.com to find the phone number-owner's address.

1. You can visit the main site (<https://thatsthem.com>) in Firefox, click the PHONE link in the upper right of the window (arrow 1 below), and enter the phone number to search in the field. Alternatively, visit <https://sec487.info/c3> (<https://thatsthem.com/phone/805-895-0484>) in your browser to go directly to the results.



Browser Width

If your browser window is not wide enough, the above links will show as a pancake icon that you can click (shown below) then click the "phone" link.

The screenshot shows the homepage of [That'sThem](#). At the top left is the logo, which features a stylized figure holding a magnifying glass over a key. To the right of the logo is a large, bold text "Find People FOR FREE". In the top right corner, there is a navigation menu icon consisting of three horizontal lines.

This screenshot shows the search interface for a phone number. At the top, the [That'sThem](#) logo is visible along with navigation links for PEOPLE, PHONE, ADDRESS, EMAIL, and IP. Below the logo, the text "Find People FOR FREE using a Phone Number" is displayed. A search bar contains the phone number "805-895-0484". To the right of the search bar is a "SEARCH" button. Two numbered arrows, one pointing left from the search bar and one pointing right towards the search button, are overlaid on the interface.

We now have confirmation that this phone number most likely belongs to John Cleese at the 1813 Fernald Point Ln, Santa Barbara, CA 93108 address (image below). This search engine also provides a potential email address to contact Mr. Cleese. This may be helpful to your customer and should be included in the report.

This screenshot displays the search results for "John Cleese". The top section shows his name in large, bold letters. Below this, his address is listed: "1813 Fernald Point Ln" and "Santa Barbara California 93108". A detailed table follows, showing various pieces of information:

Phone Number	805-895-0484
Email Address	Jcleese@msn.com
Length of Residence	Available
Household Size	Not Available
IP Address	192.88.129.85

A large arrow points to the "Available" status under the "Length of Residence" row.



Checking Your Data

A final step might be to insert the 1813 Fernald Point Ln, Santa Barbara, CA 93108 address into a mapping program (<https://www.google.com/maps>) and then include a picture of that area (shown below) in your report to give your customer an idea of where the home is located so she can see if that was near where she found the dog.



2. This lab is completed. When finished, close the web browser.

Finding Emails

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Use theHarvester

Objectives

- Harvest email addresses from open sources using theHarvester
- Become more comfortable using command line Linux commands

Goals

Your customer, an internal security team for the Illy Coffee company headquartered in Italy, has received information that they want checked out. Someone alerted them that some of their employees use the illy.com email addresses in non-company web sites (for example: social media, personal ecommerce, etc.).

1. Use theHarvester to find the emails associated with the illy.com domain name

Preparation

Yes VPN

since we will be using the Google.com web site.

Step-by-step instructions

Use theHarvester

Our first step in the investigation is to find email addresses that use the `@illy.com` email domain. To do this we could scour Google, Bing, DuckDuckGo, forums, and the rest of the internet. Perhaps we could use a tool instead? `theHarvester` is a good one to start with.

Other Email Tools

Spiderfoot, Recon-`ng`, and others have email retrieval features too. If you are truly looking to find as many email addresses as possible for your customer, you should probably run several of these tools to ensure a good coverage. For our lab, we don't have time to run all those tools, so we will just use `theHarvester`.

1. Launch the terminal window by clicking the terminal icon in the upper left of the menu bar.



2. Change directories to the one with the tool in it by typing: `cd /opt/tools/theHarvester`, then press Enter.

```
Terminal
File Edit View Terminal Tabs Help
student@sec487 (12:25:51) : ~$ cd /opt/tools/theHarvester/
student@sec487 (12:26:11) : /opt/tools/theHarvester$
```

A screenshot of a terminal window titled "Terminal". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main area shows a command-line session. The user types "cd /opt/tools/theHarvester/" and presses Enter. The terminal then displays the current directory as "/opt/tools/theHarvester\$".

`theHarvester` is a python program and has several switches which you can see (shown below).

3. Type: `python theHarvester.py -h`, then press Enter to see the flags and switches you can use in the tool.

```
student@sec487 (09:16:57) : /opt/tools/theHarvester$ python theHarvester.py
```



Usage: theharvester options

```
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
      googleplus, google-profiles, linkedin, pgp, twitter, vhost,
      virustotal, threatcrowd, crtsh, netcraft, yahoo, all

-s: start in result number X (default: 0)
-v: verify host name via dns resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
```

For our purposes, we will have theHarvester run its searches on the `illy.com` domain and use the google data source (shown above).

4. To launch the application, we need to type: `python theHarvester.py -d illy.com -b google`, then press Enter.

```
student@sec487 (08:41:26) : /opt/tools/theHarvester$ python theHarvester.py -d
illy.com -b google
```

When finished, you should see a list of IP addresses and domain names on the screen. theHarvester is a multipurpose tool: it will get email addresses, IP addresses and domains. Right now, we are only interested in the email accounts it found.

5. Scroll up in the window to find the "Emails found" section (shown below).



You Will Get Different Results

The emails that you retrieve in this lab will appear in a different order than what is shown in the screenshot below. You may also not have some that were found below or may have ones that we didn't find. These cases are expected outcomes since, over time, the internet changes.

```
Harvesting results

[+] Emails found:
-----
info@illy.com
caninfo@illy.com
emailandrea.illy@illy.com
udc.usa@illy.com
levy@illy.com
doe@illy.com
Adam.Paige@illy.com
Giovanna.Gregori@illy.com
giovanna.gregori@illy.com

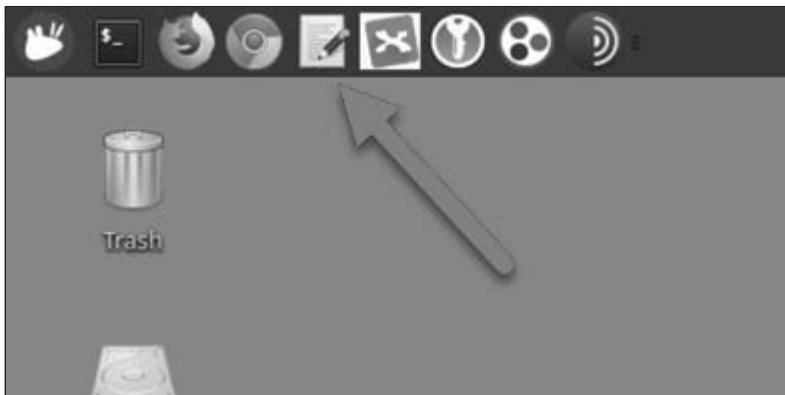
[+] Hosts found in search engines:
-----
```



Do you see a false positive in the above list? In your results, you may see the `emailandrea.illy@illy.com` entry, shown at the red arrow in the image. theHarvester found it but based on the other records and the email pattern of `firstname.lastname@illy.com`, we should research this odd entry and see why it doesn't follow the correct pattern. Our tools will frequently retrieve extra content that is irrelevant to our current project and represents false positive data. Remember to review the data and remove these before processing and reporting. Your data may or may not have false positives in it.

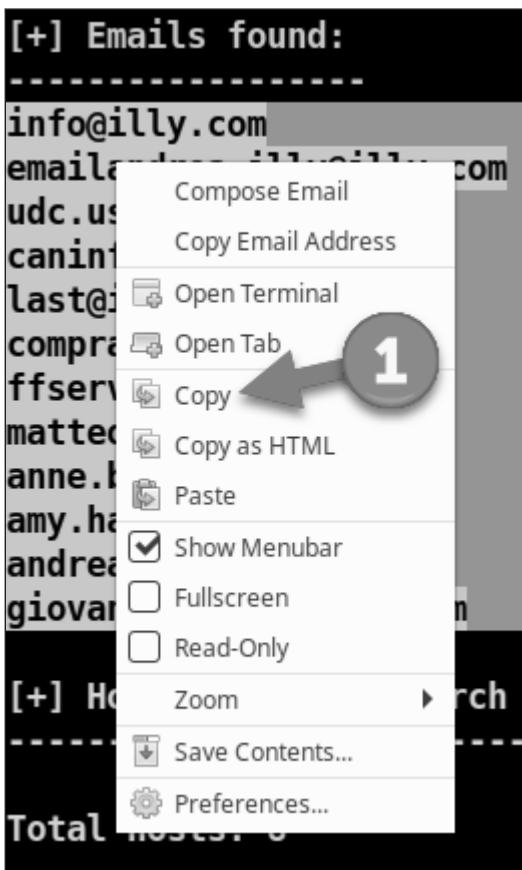
We need to select the email addresses in this window and copy them into a text document.

6. We will use the gedit text editor which you open by clicking the icon in the menu bar (shown below).



7. Select the email address content in the terminal window by clicking and dragging the mouse from the first email to the last one.

This will cause the text to be highlighted (arrow 1) and invert the colors on the screen (shown below).



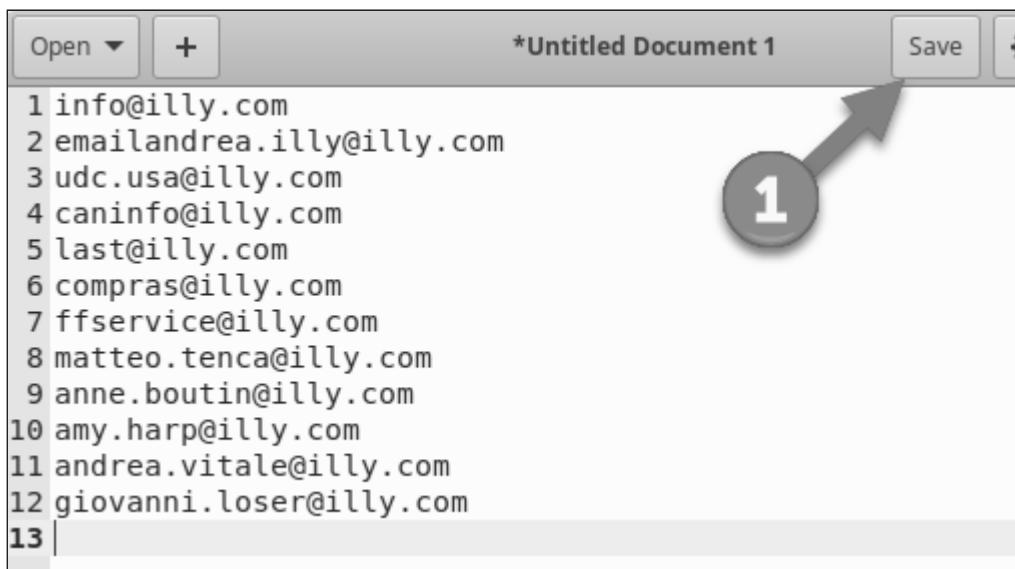
8. Copy the contents of the screen by clicking on the Edit window menu item and dragging down to "Copy", right-clicking on the content and selecting "copy" (arrow 2 above) or by pressing the SHIFT CONTROL c keys at the same time.

CONTROL c Does Not Copy in the Terminal

Using the `CONTROL c` keys will not work to copy content as they would in Windows because, in a Linux terminal, that is the command to exit a certain application or stop a process.

9. Once copied, switch to the gedit window and paste by pressing `CONTROL v` (hold the `CONTROL` or `CTRL` key and press the `v` key once).

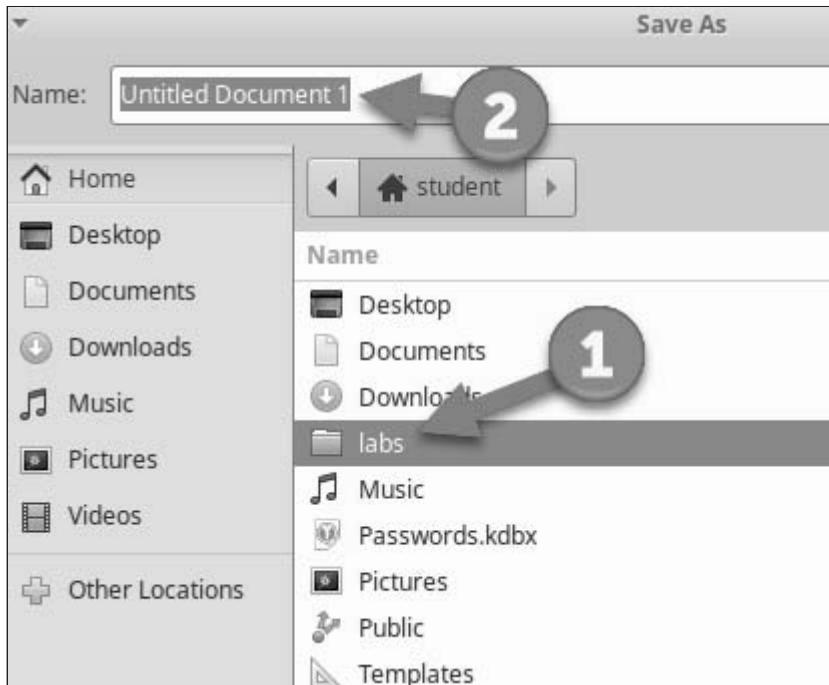
You now should have multiple email addresses in the gedit document (looking somewhat like the below image).



10. Save the document by clicking the Save button in the top right of the window (arrow 1 above).

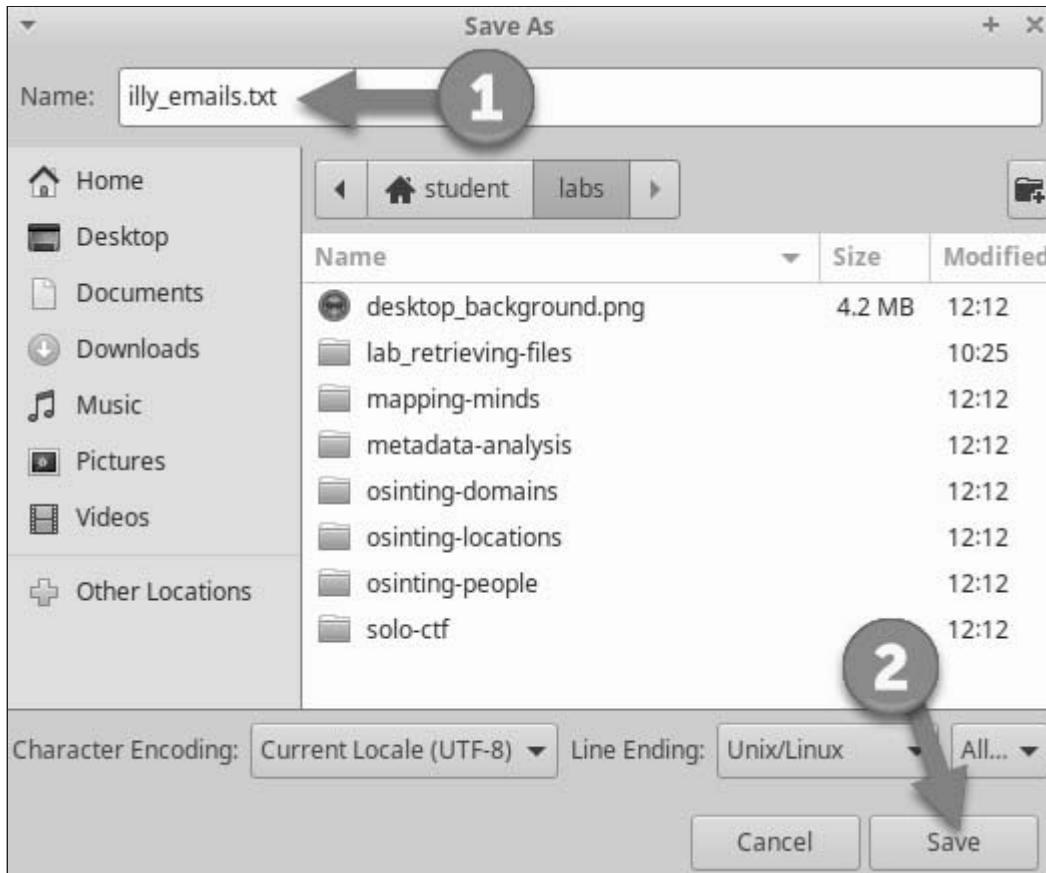
When that button is clicked you will be prompted for where you want to save and what you want the file name to be.

11. Double click the "labs" directory to switch to that directory (arrow 1 below).



At the top of the window is the field for the file name (it currently shows "Untitled Document 1" at arrow 2 above).

12. Delete that default file name (arrow 1 below) and name this file `illy_email_s.txt` and click the Save button in the lower right of the window (arrow 2 below).



13. You can close the gedit application by pressing the X in the upper right of the window.

You now have a text file with all the email addresses theHarvester found for the illy.com domain.



Using All the Sources

This is not an exhaustive list. In real investigations, you would continue to run tools and find other email addresses, add them to this list, remove duplicates, and repeat until you were satisfied that you had enough. For our purposes, we have "enough" now and the data is in a format we can use in another program too!

At this point, you may copy the emails and paste them into your MindMap or into a report.

Finding Users

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Keybase Profile
 - Use Recon-ng Profller
 - Optional EyeWitness
 - Export results from Recon-ng
 - Extract the URLs from the CSV
 - Automate web surfing using EyeWitness

Objectives

- Rapidly discover many places where a user name might be used
- Become comfortable using Recon-ng (version 4) to find a user name across many web sites

Goals

For this lab, you will start with the <https://keybase.io/inigomontoya> profile. Many times when we are OSINTing, we find that a target has linked an account that has a different user name than we knew about. Pivoting our focus to that one can open up our investigations.

We want to find accounts that this user has under a different user name (not inigomontoya). The target has at least 2 other accounts under a different user name. Find them and look in the bio area for a line starting "Lab answer = ". Find that answer.

1. Visit <https://keybase.io/inigomontoya> and find the linked account
2. Use the Recon-ng Profller module to find web sites using that new account name
3. Visit the bio of the other site(s) and find the phrase after "Lab answer = "

[OPTIONAL Goals]

1. Export the results from Recon-ng to a CSV
2. Extract the URLs from the CSV
3. Use the EyeWitness tool to automatically retrieve web site content

Preparation

VPN if problems

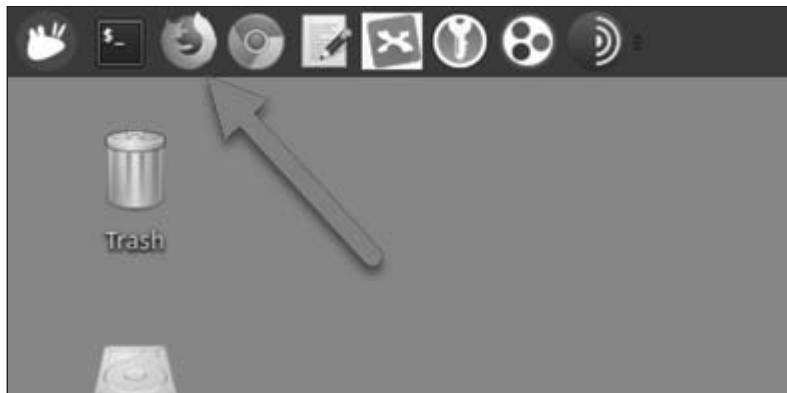
 Document with MindMap or Hunchly

Consider using a MindMap to track your work in this lab.

Step-by-step instructions

Keybase Profile

1. Launch a web browser and visit <https://keybase.io/inigomontoya>



The page should look like the image below.

A screenshot of a web browser window. The address bar shows the URL "https://keybase.io/inigomontoya". The main content area displays a Keybase user profile for "inigomontoya". The profile picture is a black and white photo of a man with a mustache. To the right of the profile picture, there is a summary: "1 device", the handle "inigofrancismontoya", and a "gist" indicator. A large, semi-transparent gray arrow points from the bottom right towards the handle "inigofrancismontoya".

inigomontoya (Inigo Montoya) [+](#)

← → ⌛ ⌄ https://keybase.io/inigomontoya

SEC487 Wiki OSINT Framework Check Tor OSINT - start.me

Search Keybase

1 device
inigofrancismontoya • gist

inigomontoya
Inigo Montoya

I am looking for a 6 fingered man
Madrid, Spain

From an OSINT perspective, this page has many interesting pieces of information:

- Profile image/avatar

- Reported location where the user "lives"
- Friends and followers
- Devices and names (<https://keybase.io/inigomontoya/devices>)

Each of these may have pivot points for some investigations.

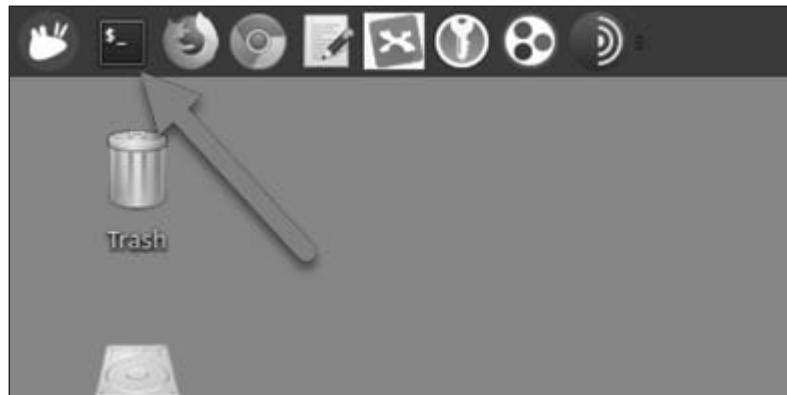
2. There is a GitHub account named `inigofrancismontoya` shown on the image above. Record that user name.
3. Let's visit that GitHub profile and see if we see information that might corroborate that it is this user's account. Click on the link to the <https://github.com/inigofrancismontoya> web site.

The screenshot shows a web browser window with the GitHub homepage loaded. The URL in the address bar is <https://github.com/inigofrancismontoya>. The page features a prominent 'Create your own GitHub profile' section with a 'Sign up' button. Below this, there is a large placeholder image of a person with long hair and a mustache. To the right of the image, there are tabs for 'Overview', 'Repositories 1', 'Stars 0', and 'Followers 0'. Under the 'Popular repositories' heading, there is a single entry: 'myfirstrepo'. At the bottom of the profile section, it says '4 contributions in the last year'.

We see the same profile image as the KeyBase.io site. There may be other data on the site too. For our purposes, this looks like the profile/user name we are looking for.

Use Recon-*ng* Profiler

1. Launch a terminal window by clicking the terminal icon in the menu bar.



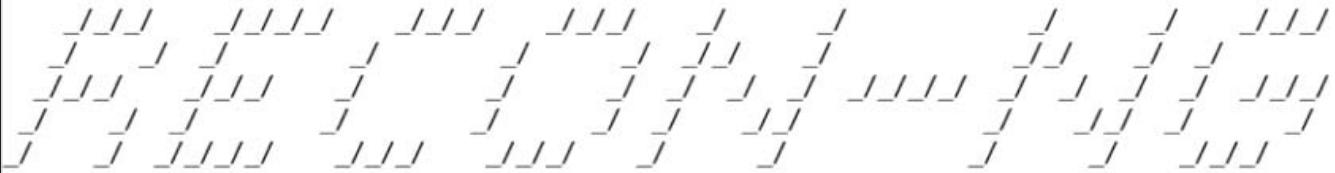
2. In the terminal window, type: `cd /opt/tools/recon-ng/`, then press Enter to change directories to the Recon-*ng* application location.
3. In this directory, you will launch the interactive Recon-*ng* application by typing: `./recon-ng --no-analytic --no-version`, then press Enter.

The `--no-analytic` is important to protect your and your customer's privacy as it shuts off the Google Analytics traffic that Tim Tomes uses in the project.

The `--no-version` prevents your system from reaching out to the internet and checking if the version installed on your system is the most recent. If it is not, then it will not run until you update it. Using this flag will bypass that check.

```
student@sec487 (15:37:14) : /opt/tools/recon-ng/$ ./recon-ng --no-analytic --no-version
```

```
student@sec487 (15:04:15) :/opt/tools/recon-ng$ ./recon-ng
```



Sponsored by...



```
[recon-ng v5.1.0, Tim Tomes (@lanmaster53)]
```

```
[6] Reporting modules  
[3] Import modules  
[1] Recon modules
```

1

```
[recon-ng][default] > |
```

You can see that all the import and reporting modules are installed in your version of Recon-*ng*. Additionally, arrow 1 points to the single recon module we installed, Profiler.

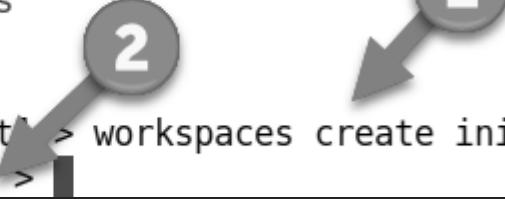
Before you start using the module, you need to create a workspace to segment your data. To create a new workspace, you need to choose a workspace name. For this case, we will call it *inigo*.

4. Type: `workspaces create i ni go` (Ensure that you use the word "workspaces" with an s on the end as shown at arrow 1 below), then press Enter.

You should see the prompt at the bottom of the window showing `[recon-ng][i ni go]` instead of the word "default" (arrow 2 below). This shows you were successful in adding and switching to a new workspace.

```
[6] Reporting modules
[3] Import modules
[1] Recon modules

[recon-ng][default] > workspaces create inigo
[recon-ng][inigo] >
```



You now need to load the module you wish to use.

5. Type: `modules load profiler`, then press Enter to select that module.

The prompt should now show `[recon-ng][inigo][profiler]` indicating that you have moved into the profiler module.

6. Set the profile you wish to use by typing: `options set SOURCE inigofrancismontoya`, then press Enter.

```
[recon-ng][inigo][profiler] > options set SOURCE inigofrancismontoya
SOURCE => inigofrancismontoya
```

Other Methods of Inputting Usernames

Recon-ng uses databases to store information. We can insert records into the `profiles` database table and this module will iterate over each and look them up. If you have more than one target user name, you may wish to add each to the `profiles` table using `db insert profiles`. When you press Enter, it will ask you for the user name and other details. Just enter the user name and press Enter for each of the other fields (leaving them blank).

7. To have Recon-ng perform the user name lookups for us, we type: `run`, then press Enter.

You will see positive and negative results and, perhaps a few errors or timeouts, scroll up the screen while the application runs. When you have the prompt back (shown below), you should see at least 2 accounts that were found with that user name.

```
-----
SUMMARY
-----
[*] 2 total (2 new) profiles found.
[recon-ng][inigo][profiler] >
```



What our customer asked for was other profiles using this secondary user name. We should have found the GitHub account and probably at least one other. Let's look in the profiles table for any additional data. To do that, we type: `show profiles` and press Enter.

```
[recon-ng][inigo][profiler] > show profiles
```

rowid	username	resource	url	category	notes	module
1	inigofrancismontoya	about.me	https://about.me/inigofrancismontoya	social		profiler
2	inigofrancismontoya	GitHub	https://api.github.com/users/inigofrancismontoya	coding		profiler

8. Looks like we found the `https://about.me/inigofrancismontoya` profile. Visit that in your browser. Check that user's bio (arrow 1 below) for the "lab answer".

INIGO MONTOYA
Sailing in Madrid, Spain

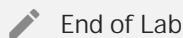
Take my class

1

Greetings, I'm Inigo.

Lab answer = [redacted]

You can take my class with a click on the button above.



The lab is over. If you have more time, consider learning some additional tricks with Recon-ng and EyeWitness below.

Optional EyeWitness

The next parts of this lab are written for your information. Many times when we run this profiler module (or others), we receive many responses back. Pulling that data out by hand is cumbersome

and inefficient. Below, we show you how to export the content from Recon-ng and then, using another tool, visit the web sites and take screenshots of them.

Export results from Recon-ng

You may wish to export all the found accounts locations from Recon-ng and include them in your report to your customer. To do this, we will need to move into the reporting/csv module.

1. Go back to the terminal window and type: `modules load reporting/csv`, then press Enter.

This will move your prompt out of the profiler module and over to the reporting CSV export one. Your prompt should have changed to reflect the new module location.

To export data, we need to tell Recon-ng what database table to export. All our data has been stored in the `profiles` database table.

2. Type: `options set TABLE profiles`, then press Enter.

This sets the variable telling Recon-ng where to pull the data from.

3. Next, send the command to export the data to a CSV file by typing: `run`, then press Enter.

These steps and their results are shown below for your information. Your CSV file should now be in the `/home/student/.recon-ng/workspaces/ini go/results.csv` file.

```
[recon-ng][ini go][profiler] > modules load reporting/csv
[recon-ng][ini go][csv] > options set TABLE profiles
TABLE => profiles
[recon-ng][ini go][csv] > run
[*] 2 records added to '/home/student/.recon-ng/workspaces/ini go/results.csv'.
[recon-ng][ini go][csv] >
```

4. We are now done with Recon-ng so type: `exit`, then press Enter to return to the terminal prompt.

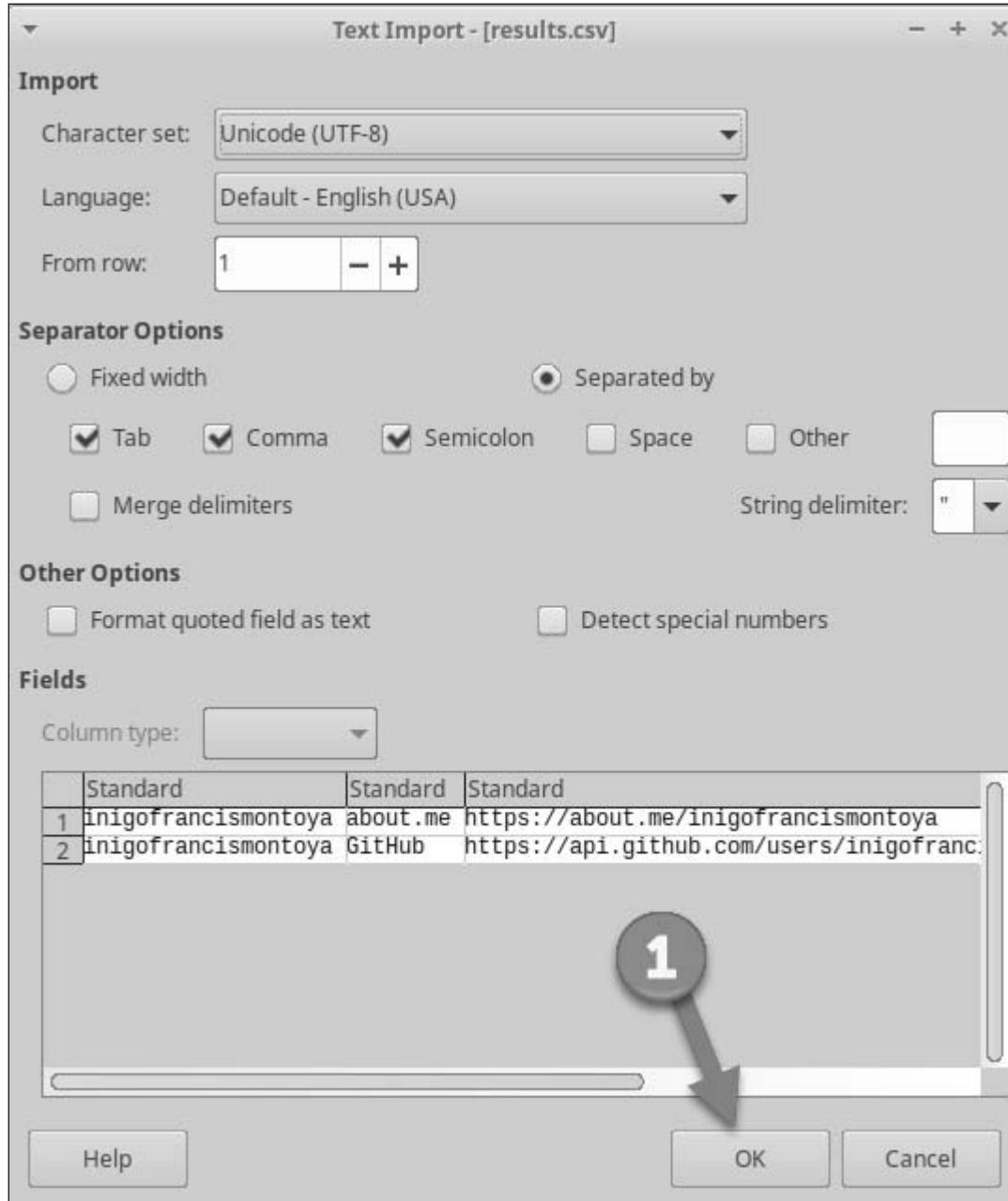
Extract the URLs from the CSV

Since this is a CSV, let's use a spreadsheet application to view it. On your Linux VM, you have LibreOffice Calc which can be launched via the terminal or from the application menu

1. In the terminal window, type: `libreoffice /home/student/.recon-ng/workspaces/ini go/results.csv`, then press Enter.

This will open LibreOffice's spreadsheet application, Calc, in a new window. It should recognize this as a valid CSV file and ask you to confirm how it should be imported.

- Accept the default import by clicking the OK button (below).

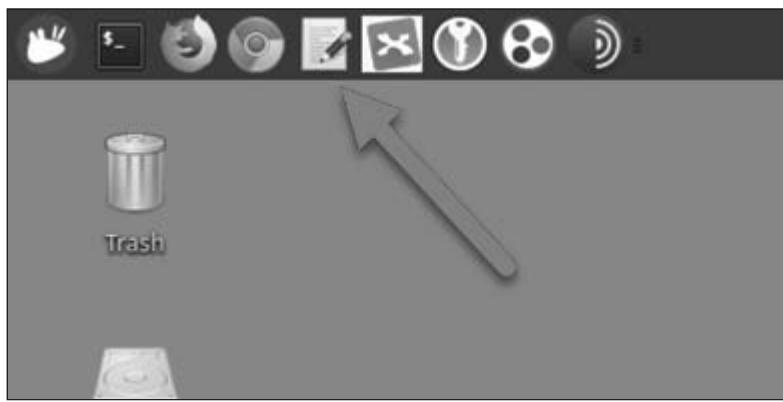


- To save all the URLs to their own file, put your cursor on the C1 cell and click and drag down, selecting all the URLs in that column. In our case, we only have a few URLs but if you used a different profile name for the Recon-ng module, you may have many more.

	A	B	C	D	E	F
1	inigofrancismontoya	about.me	https://about.me/inigofrancismontoya	social		profiler
2	inigofrancismontoya	GitHub	https://api.github.com/users/inigofrancismontoya	coding		profiler
3						

4. Copy that content by pressing CONTROL c on the keyboard or going to the Edit menu and choosing Copy.

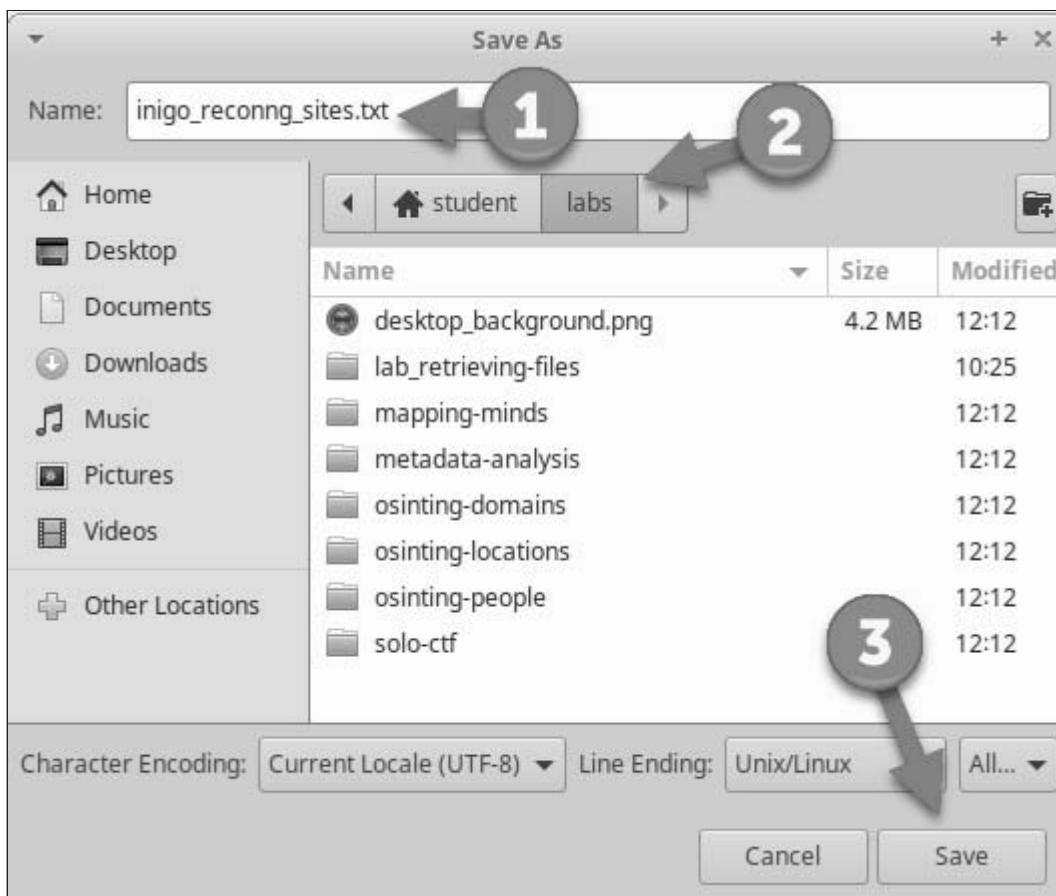
5. Open the gedit program so that we can paste these URLs into a text file.



6. When gedit opens, paste the contents of the clipboard by pressing CONTROL v or going to the Edit menu and selecting Paste. Your gedit document should look similar to the image below.



7. Save the data into a text file by pressing CONTROL s or using the File menu and choosing Save.
8. Navigate to the /home/student/labs directory and name the file inigo_reconng_sites.txt and click Save.



9. Close the gedit application.

We now have the URLs in a file. We can save the CSV into another format if we wished (perhaps an Excel XLS or XLSX). We do not need to for our lab. The CSV format worked for our needs.

10. Close the LibreOffice Calc application and either save the file or do not (your choice).

Automate web surfing using EyeWitness

Now you will use the EyeWitness tool from Chris Truncer (<https://github.com/FortyNorthSecurity/EyeWitness>, <https://sec487.info/yf>) to take each URL in our file, visit the web site, take a picture of the web site as it would appear in our web browser, and then compile these images into a single HTML document we can view? It greatly decreases the manual work you might have to do by rapidly visiting the URLs and it is installed on your system in /opt/tools/EyeWitness.

Running EyeWitness

You must run EyeWitness from inside the /opt/tools/EyeWitness directory. If you do not, you will get errors.

1. In a terminal window, move into the EyeWitness directory by typing:

```
cd /opt/tools/EyeWitness, then press Enter.
```

2. You will run EyeWitness and give it the location of the Recon-ng output URLs from the above steps.

UserAgent

The about.me web site does not respond well to non-browser web requests. If you make the request without changing your User Agent to pretend to be a normal web browser, you will get a 401/403 response back and no valid content. To combat this, we will tell EyeWitness to pretend to be a web browser.

3. To run the tool, type:

```
/EyeWitness.py --user-agent 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36' --web --timeout=30 --max-retries=2 -f /home/student/abs/ini/go_reconng_sites.txt
```

4. Then press Enter.

```
student@sec487 (16:25:35) : /opt/tools/recon-ng$ cd .. /EyeWitness/  
  
student@sec487 (16:25:37) : /opt/tools/EyeWitness$ ./EyeWitness.py --user-agent  
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/72.0.3626.121 Safari/537.36' --web --timeout=30 --max-retries=2 -  
f /home/student/abs/ini/go_reconng_sites
```

EyeWitness will cycle through each URL and make the web request. Status messages about its progress will appear on the screen. All images and data that it collects are stored in the /opt/tools/EyeWitness/MMDDYYYY_HHMMSS folder (where MMDDYYYY is the month, day, and year the tool was run and the HHMMSS is the hour, minute, and second it was run). Take note of this location and remember to archive and remove that data when you clean up this assessment.

```
#####
#                               EyeWitness                               #
#####
#          FortyNorth Security - https://www.fortynorthsecurity.com      #
#####
Starting Web Requests (2 Hosts)
Attempting to screenshot https://about.me/ini_gofrancismontoya
Attempting to screenshot https://api.gitHub.com/users/ini_gofrancismontoya
Finished in 8.40729808807373 seconds

[*] Done! Report written in the /opt/tools/EyeWitness/11252019_164422 folder!
Would you like to open the report now? [Y/n]
```

Once completed, it will ask if you wish to see the report file (which will be named differently than the one above).

5. Type: `y`, then press Enter. EyeWitness will launch Firefox and display the report.
6. You can scroll through each site and view the HTTP headers on the left and the screenshot of the URL on the right.

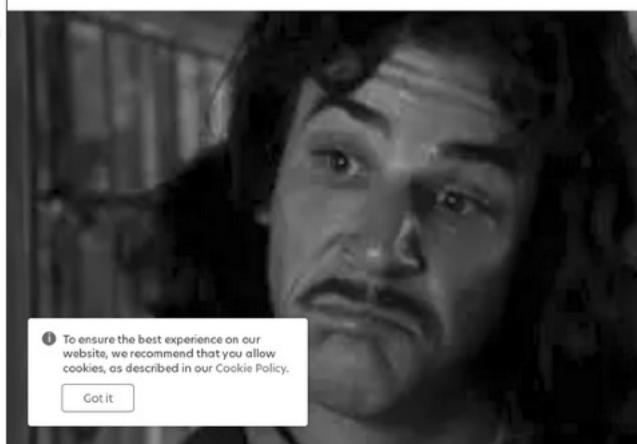
With this information you can prioritize which sites you may wish to visit first to find more data on your subject.



Different Results Are OK

Since the EyeWitness tool uses the current date/time stamp for the directory name, your output will look different from the above.

Uncategorized

Web Request Info	Web Screenshot
<p>https://about.me/niogofrancismontoya Resolved to: 3.83.0.146</p> <p>Page Title: Inigo Montoya - Madrid, Spain about.me Date: Mon, 25 Nov 2019 21:44:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 124960 Connection: close Server: nginx Vary: Accept-Encoding Set-Cookie: aboutme_anon_id=2cdc9129-532b-4f8d-8474-bed0f8df3416; Max-Age=31536000; Path=/; Expires=Tue, 24 Nov 2020 21:44:25 GMT; HttpOnly X-Frame-Options: DENY ETag: W/"1e820-R6BYyLTyHbar++NmInIUDzLv6ic" Response Code: 200</p> <p>Source Code</p>	

7. To close the terminal, type: `exit` in the terminal window, then press Enter.
8. This lab is completed.

 Click Here to See Our Findings ▼

The answer to the lab is "That's inconceivable!" as shown below.



This page intentionally left blank.

Reversing Images

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Image Search with Google Chrome (The Easy Method)
 - Image Search with Firefox

Objectives

- Use reverse image search engines to identify the subjects of several images

Goals

The https://start.sec487.info/image_lab.html page has images on it that need analysis. Each image has at least one attribute that you need to find about it. You may use any search engine you wish although Yandex, Google, and Bing have the highest success rates.

Your goals are to answer the trivia questions about each image.

1. Carpet image - What is the name and location where this image was taken?
2. Dog image - What breed of dog is this?
3. Car image - What kind of car is this and in what country is it made?
4. Landscape image - What is the name of this geographic landmark and where is it located?
5. Church image - What is the name of this building and where is it located?

Preparation

No VPN

Step-by-step instructions

💡 Try Using Hunchly or a MindMap

Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

The process for discovering information about these images is similar for each of the images. It is:

- Visit an image search engine
- Give it the URL to the picture you wish to search for
- Perform the search
- Examine and evaluate the results
- Verify results if needed

You may use any reverse image search tool for the analysis of these images. We found that the following sites had the most accurate results:

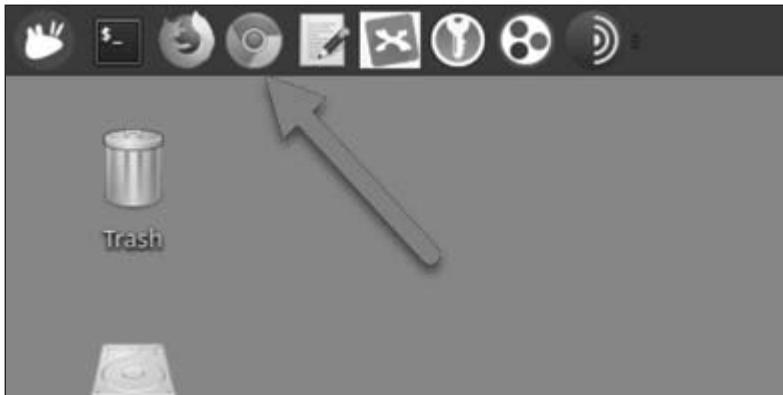
- <https://images.google.com/>
- <https://yandex.com/images/>
- <https://www.bing.com/images/>

Below, we will walk through the first reverse search and then let you repeat your actions with each of the other images. Remember to try different search engines in class to get the feel for them and the content they respond with.

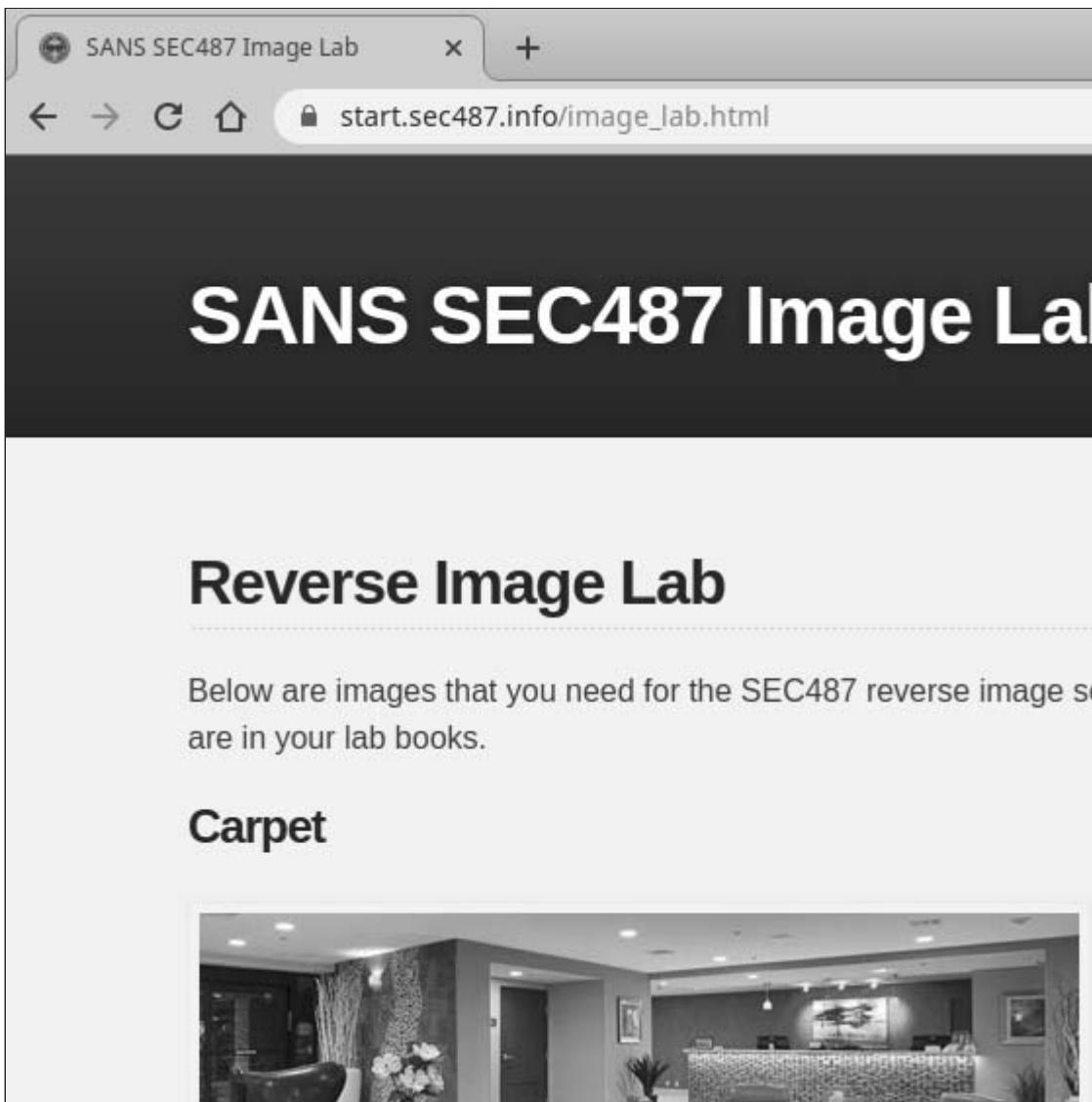
Image Search with Google Chrome (The Easy Method)

If you use the Google Chrome browser, you can simply right click on an image and Search Google for image to send each image to Google's reverse image search tool, as shown below.

1. Launch Google Chrome web browser by clicking on its icon in the task bar.



2. Visit the https://start.sec487.info/image_lab.html web site



The screenshot shows a web browser window with the title bar "SANS SEC487 Image Lab". The address bar contains the URL "start.sec487.info/image_lab.html". The main content area features a large header "SANS SEC487 Image Lab" and a section titled "Reverse Image Lab". Below this, a text block reads: "Below are images that you need for the SEC487 reverse image search exercise. These images are in your lab books." A sub-section titled "Carpet" is shown with a thumbnail image of a carpeted hallway.

Reverse Image Lab

Below are images that you need for the SEC487 reverse image search exercise. These images are in your lab books.

Carpet



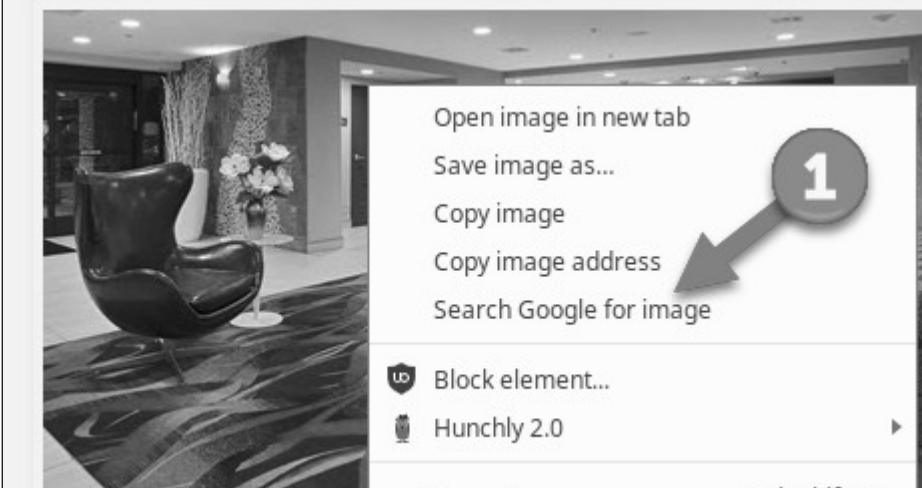
We will start with the Carpet image and send it to Google's Image Search.

3. Right click on the image you wish to send (in this case, the Carpet image), and choose Search Google for image from the contextual menu that pops up (arrow 2 below).

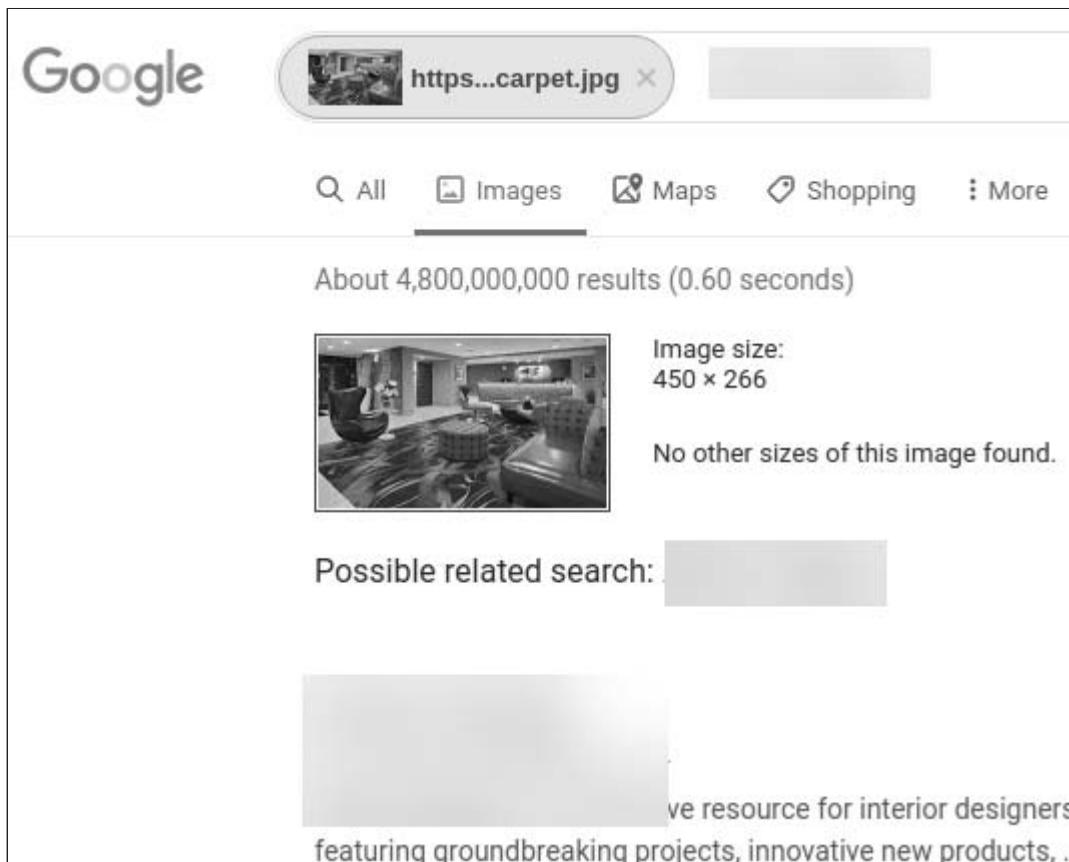
Reverse Image Lab

Below are images that you need for the SEC487 reverse image are in your lab books.

Carpet



This will open a new tab, upload the image to Google, and perform the search for you (as shown in the image below). Remember that, with Google Image Search, you may need to provide additional contextual cues to the search engine to help it narrow results.



4. Continue through the other images and find the answers to the trivia questions above.

Image Search with Firefox

If you'd like to try using Firefox for image searching, the instructions are below.

Note

For your benefit, we are going to show you how to search for the same image as above but on a different search site. You can use whatever site(s) and browser you wish for this exercise.

1. Visit the https://start.sec487.info/image_lab.html web site in Firefox.

The screenshot shows a web browser window with the following details:

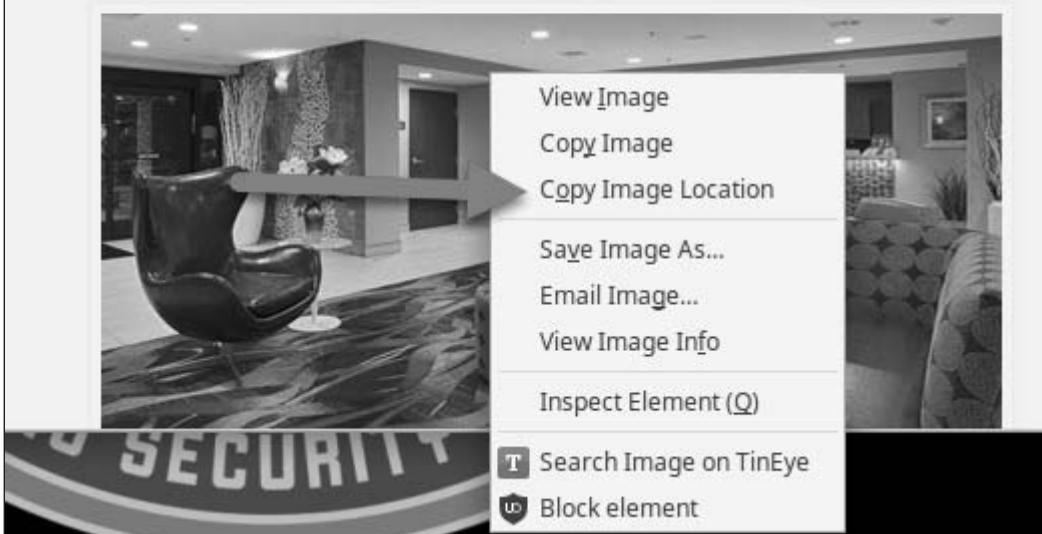
- Address Bar:** https://start.sec487.info/image_lab.htm
- Toolbar:** Home icon, Lock icon, Search bar with placeholder "Search", three dots, a bookmark icon, and a star icon.
- Page Headers:** OSINT Framework, Check Tor, OSINT - start.me
- Section Header:**

Reverse Image Lab
- Text:** Below the header, there is a paragraph: "Below are images that you need for the SEC487 reverse image search in your lab books."
- Image:** A large black and white photograph of a modern interior space. It features a large, dark, egg-shaped chair on the left, a patterned rug, and a reception desk in the background.

2. Right click on the image you wish to search and select Copy Image Location. This will place the URL for that image into your computer's memory.

in your lab books.

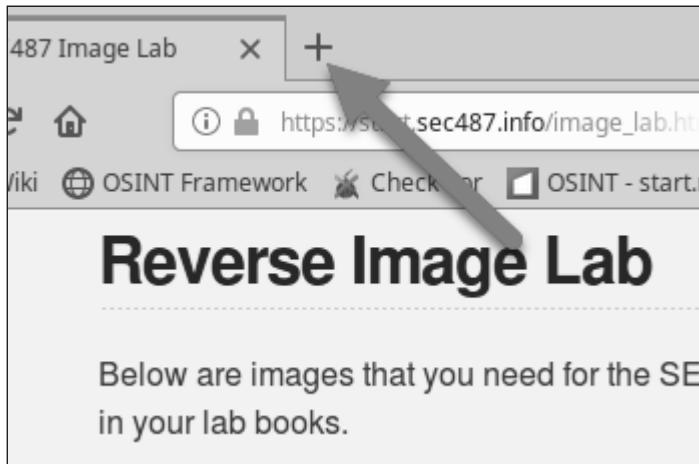
Carpet



Save Image Locally

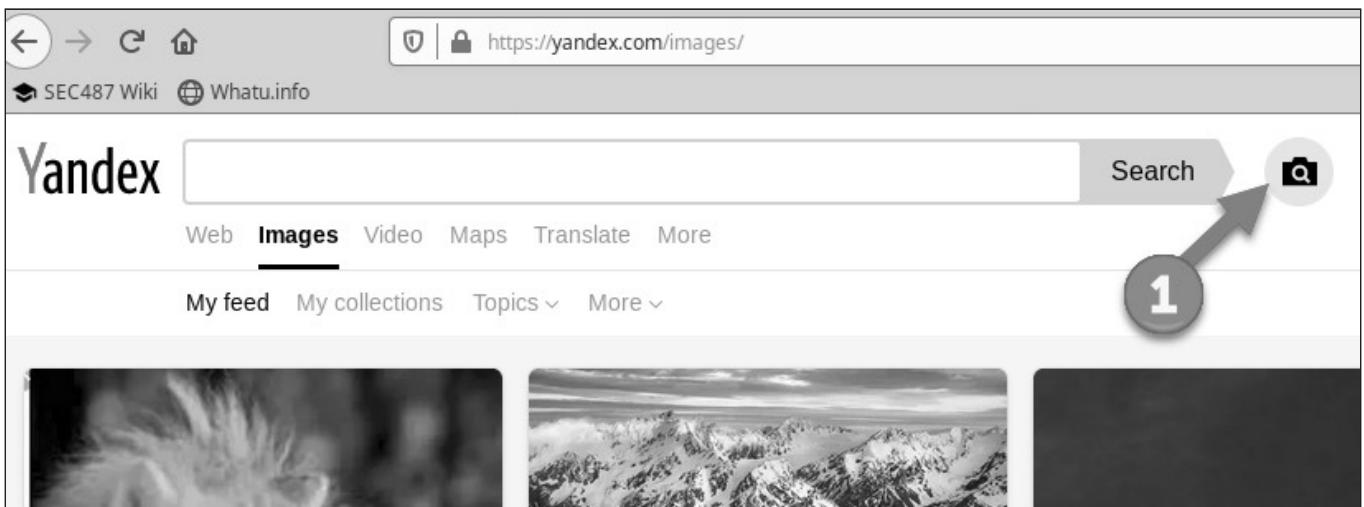
When doing this for an assessment, you may need to or want to save the image locally to your computer and then upload it to search engines.

3. Open a new tab by clicking the new tab icon (shown below).



4. Visit the image search engine you wish to use. We are going to try Yandex's site so enter <https://yandex.com/images/> in the URL bar and press Enter (or click the link).

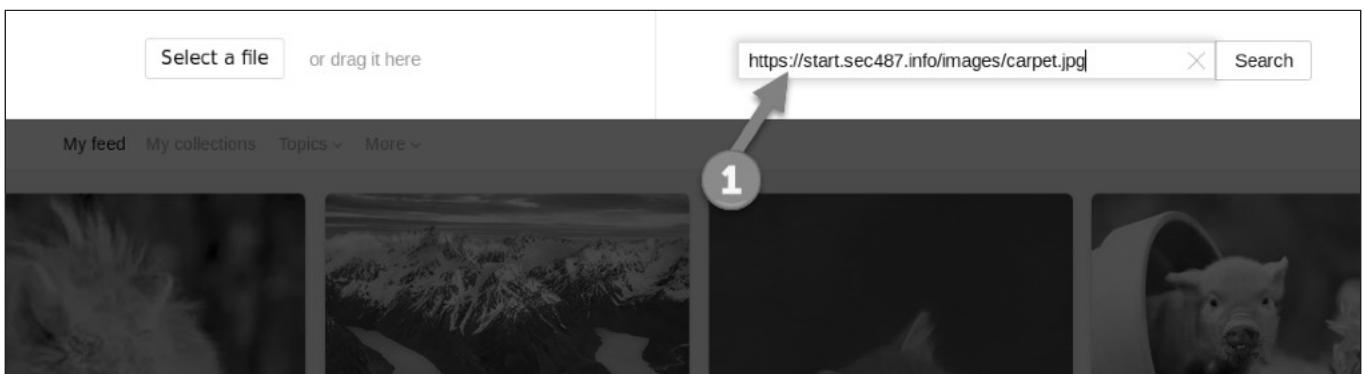
5. In the search field, you should see a picture of a camera on the right side (arrow 1 below). Click this icon.



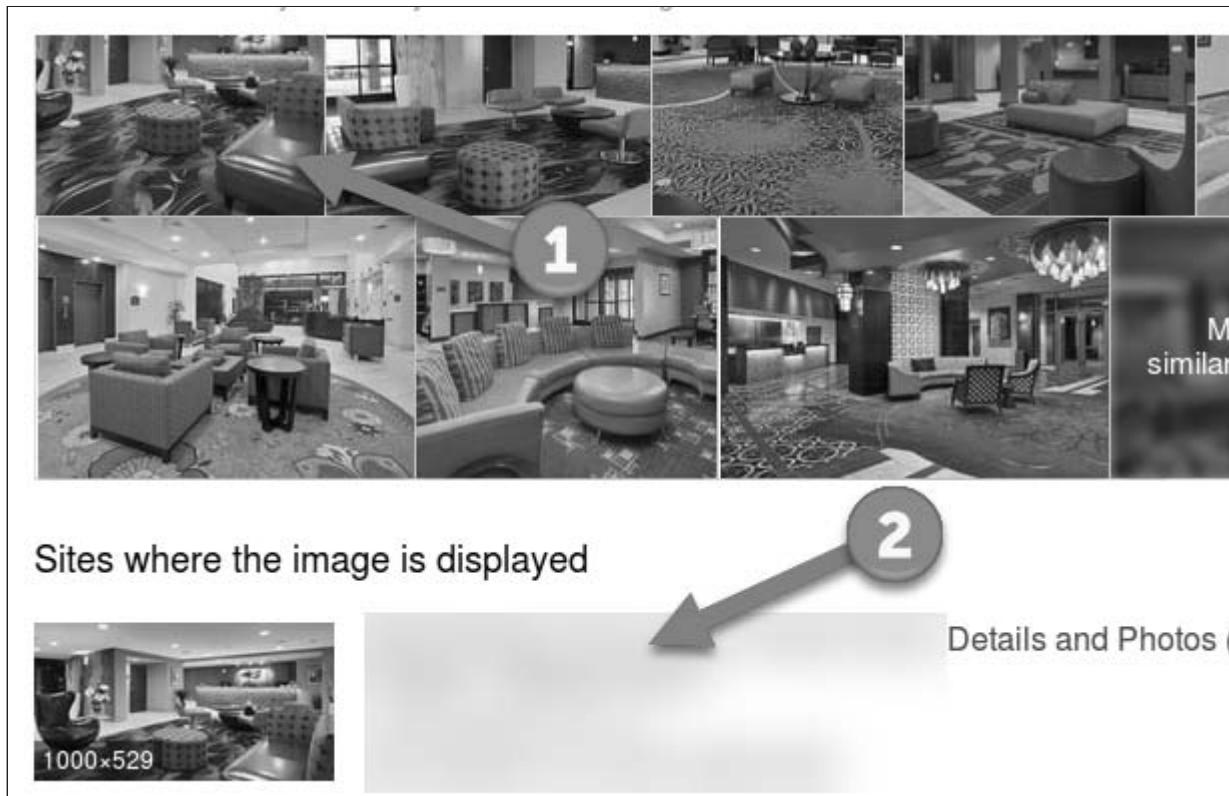
6. Paste in the URL to the image you wish to search for (you may need to go back and copy it into the computer's memory again) and press enter to perform the search.

Russian Language

This page may appear in Russian. It is easy to figure out where to paste the URL to the image and infer the button next to it performs the search.



7. Scroll down the results page and see that Yandex matched your image (arrow 1 below) and discovered a site that hosts it (arrow 2 below). We blurred this out so that you can perform the lab and discover this location yourself.



8. Repeat these steps with the other images on the https://start.sec487.info/image_lab.html web site.
9. When finished, close the web browser. The lab is finished.

Click Here to See Our Findings ▼

1. Carpet Image - Hotel Best Western Plus Fresno Airport, CA from <https://www.hotels.com/ho121339/best-western-plus-fresno-airport-hotel-fresno-united-states-of-america/>
2. Dog Image - Louisiana Catahoula Leopard Dog from <https://versatilehuntingdog.com/breeds/louisiana-catahoula-leopard-dog/>
3. Car Image - Bucci Special is a V12-powered Argentinian supercar from <https://www.motor1.com/news/39379/bucci-special-is-a-v12-powered-argentinian-supercar-video/>
4. Landscape Image - Tres Hermanas (Three Sisters) Falls, Peru from https://athebest.com/snax_item/tres-hermanas-falls-peru-914-m-2999-ft/. This also shows up as Air Terjun Chemerong Tertinggi in search engines. You may need to translate that or pull up other pages.
5. Church Image - Cathedral of the Immaculate Conception in Moscow, Russia from <http://travelever.com/arts/20-most-beautiful-churches-and-cathedrals-in-moscow/>

People Searching

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Visit people search engine
 - Examine Gravatar Content
 - Find the Twitter account
 - Find the oldest tweet

Objectives

- Become comfortable using people search engines
- Gain experience using cached versions of data

Goals

Remember when your customer (earlier lab) asked you to get an email address for their former employee Kevin? They want more details about him now. That customer wants you to confirm that that Kevin is "their" Kevin by getting biographical data about him such as his last name and city of residence.

The customer also thinks that Kevin tweeted some sensitive data from his personal account before September 2017. They don't know what his Twitter handle was and want you to see if you can confirm or deny if he tweeted sensitive data.

1. Using people search engines, look up the email address: kevin@mnksmith.com

2. Find the Twitter account associated with the email

Challenge!

- Find the oldest tweet from that account

Preparation

No VPN

Step-by-step instructions

Visit people search engine

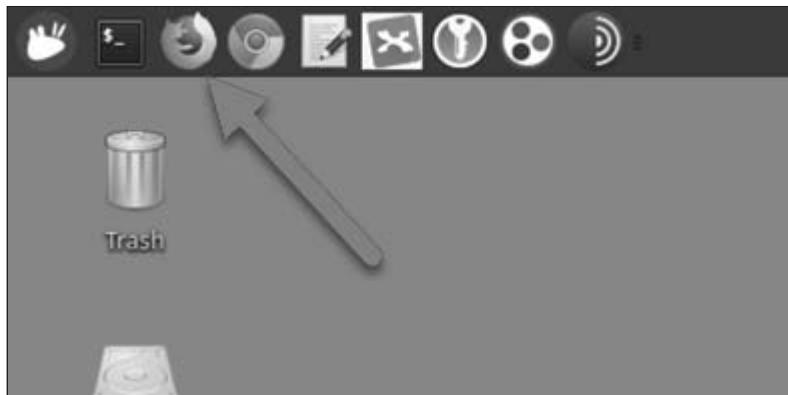
We found the kevin@mnksmith.com email account in an earlier lab. Now you will use a people search engine to search for data about this user. We are specifically looking for the Twitter account associated with the email.



Document with a MindMap or Hunchly

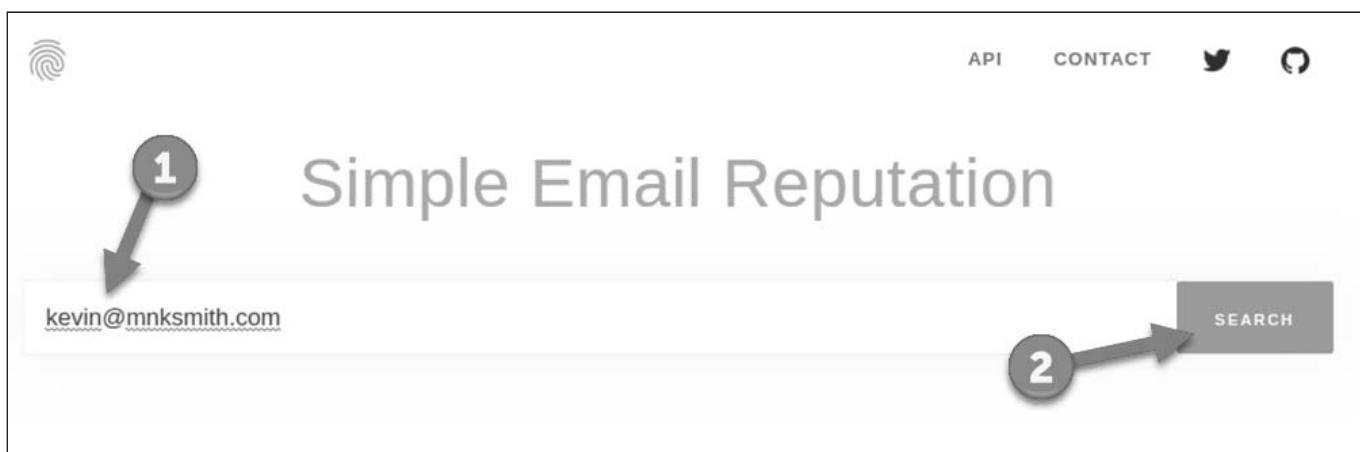
Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

1. Launch the Firefox web browser by clicking the Firefox icon in the upper left of the menu bar.



Since we are searching for an email address, we cannot use some of the people search engines that only allow us to search on names and phone numbers. We will use <https://emailrep.io>.

2. In Firefox, visit <https://emailrep.io> and allow the page to load.
3. Type: `kevi n@mnksmi th. com` into the search field and click the SEARCH button.



The website should return data like we show in the image below. Your search may reveal more or fewer sites associated with the email. Notice the Gravatar account (arrows at 1 below)? That might be interesting to examine further.

LOW REPUTATION

This email address has been seen in 3 reputable sources on the internet, and has profiles on well known sites like Gravatar and Twitter. We've observed no malicious or suspicious activity from this address.



You should see other OSINT data about that email account as you scroll down the page. (Your screen content might be different from the images below.)

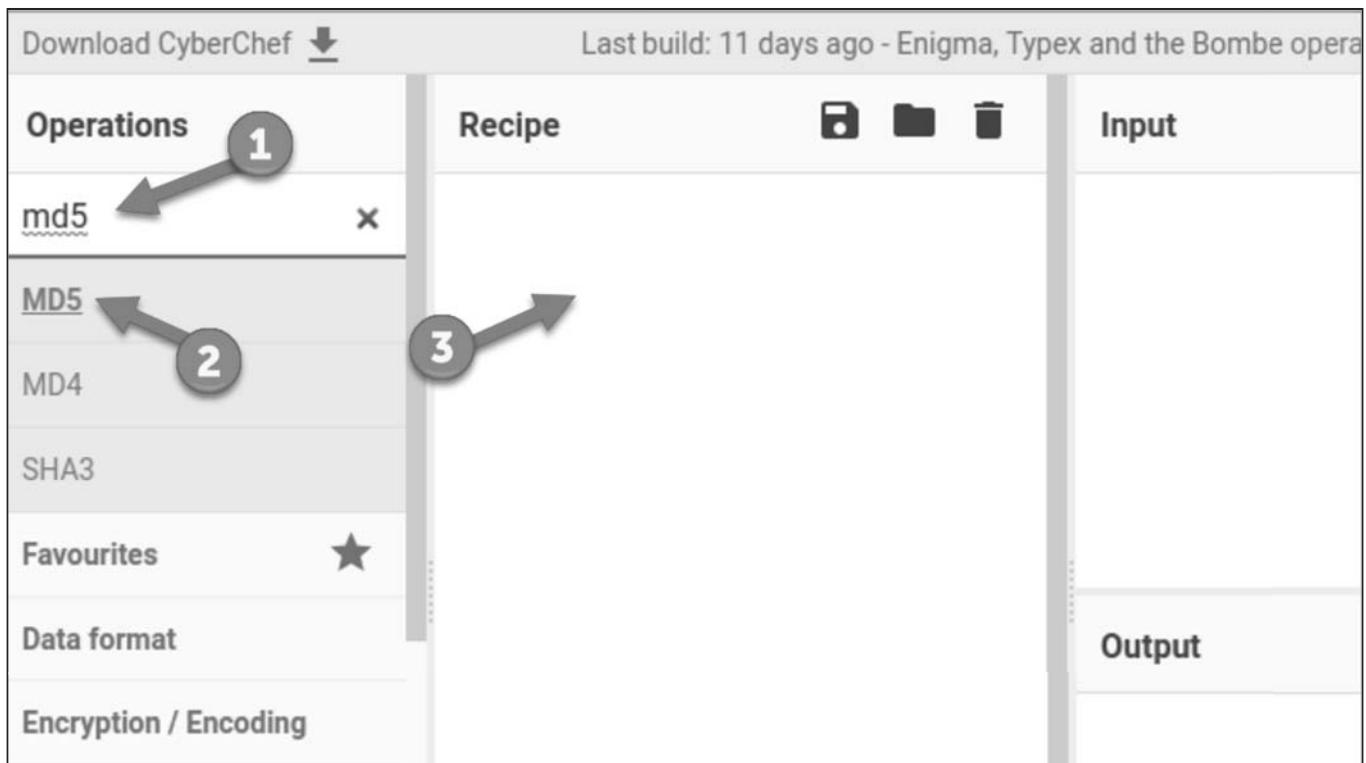
```
curl emailrep.io/kevin@mnksmith.com
{
  "email": "kevin@mnksmith.com",
  "reputation": "low",
  "suspicious": false,
  "references": 3,
  "details": {
    "blacklisted": false,
    "malicious_activity": false,
    "malicious_activity_recent": false,
    "credentials_leaked": false,
    "credentials_leaked_recent": false,
    "data_breach": false,
    "first_seen": "never",
    "last_seen": "never",
    "domain_exists": true,
    "domain_reputation": "low",
    "new_domain": false,
    "days_since_domain_creation": 1810,
    "suspicious_tld": false,
    "spam": false,
    "free_provider": false,
    "disposable": false,
```

Examine Gravatar Content

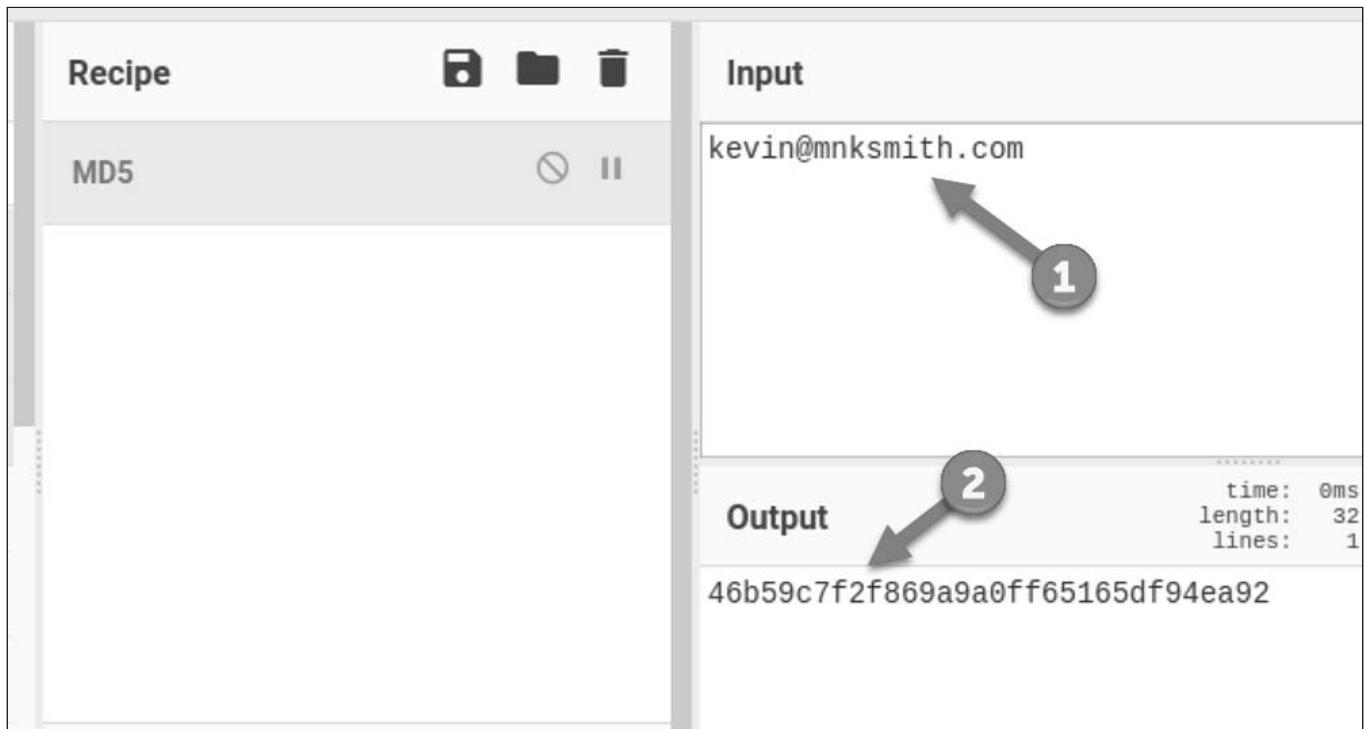
1. To search for an email account on the Gravatar site we need to change the email address into an MD5 hash (For details on how we know this, check out <https://en.gravatar.com/site/implement/hash/>). To perform this task, visit the CyberChef web site at <https://gchq.github.io/CyberChef/>.
2. On the left (arrow 1 below), type `md5` in the Search... field to bring up all the MD5 operations CyberChef can perform.

The screenshot shows the CyberChef web application. At the top, there is a download link "Download CyberChef" with a dropdown arrow, and a message "Last build: 11 days ago - Enigma, Typex and the Bombe operations added for ...". The interface is divided into three main sections: "Operations" (left), "Recipe" (center), and "Input/Output" (right). The "Operations" section contains a search bar labeled "Search..." with an arrow pointing to it from the list below, and a list of operations including "Favourites" (marked with a star), "To Base64", "From Base64", "To Hex", "From Hex", "To Hexdump", "From Hexdump", "URL Decode", and "Regular expression". The "Input" and "Output" sections are currently empty. A large number "1" is circled in the "Search..." field area, indicating the step to type "md5".

3. Once you type in the md5 string, the operations underneath it should change as shown below. Drag the MD5 underneath the search field (arrow 2 below) from its location into the panel on the right (arrow 3 below) and drop it.



- Now type the `kevin@mnksmith.com` email address in the Input field on the right of that window (arrow 1 below). The MD5 hash we need for Gravatar can be found in the Output window pane below the input one (arrow 2 below).



5. The MD5 should be 46b59c7f2f869a9a0ff65165df94ea92. We take that MD5 hash and add it to the end of the Gravatar URL to make: <https://gravatar.com/> 46b59c7f2f869a9a0ff65165df94ea92. Open that link in your browser and it should redirect you to the Gravatar account that uses the kevin@mnksmith.com email (<https://en.gravatar.com/kev21986>).

Shown below we can see a larger image of the avatar, that this user lives in Indianapolis, IN (the HTTPS certificate from the earlier lab had a location of Indianapolis, IN too lending credence that this may be our target), and a Twitter account @respectTheCode.

The screenshot shows a Gravatar profile page for a user named Kevin. At the top right is a link to WordPress.com. The profile information includes a large thumbnail image of a man with long hair and a beard sitting at a desk with a laptop, labeled with a circled '1'. Below the image is a 'Find Me Online' section. It lists a Twitter link (@respectTheCode) with a 'Follow' button and 138 followers, labeled with a circled '2'. There is also a note at the bottom stating 'Gravatar allows you to manage all of your online identities in one place on the web.', labeled with a circled '4'. The top left of the page has a 'What Is Gravatar?' link, a 'How to Use Gravatar' link, and a 'Help' link.

Notice we have other pivot-points that need to be recorded in our MindMap or notes (if we were using Hunchly, we would add these pieces of data as selectors):

- The user name for the Gravatar account is kev21986 which we could pivot on and look for other accounts on the internet that use it.
- We have the avatar image (arrow 1) which we could reverse image search.
- There are some old web site links at the bottom of the profile we could investigate.
- There is a Twitter account @respectTheCode to investigate.

- The respectTheCode account name (arrow 2) is another pivot point to see if there are other places on the internet it is used as a user account.

You may not realize it but there is other data that Gravatar has about this user that you cannot see in this view.

- Click the JSON link (<https://en.gravatar.com/kev21986.json>) (arrow 4 above) to show the data in JSON (JavaScript Object Notation) format and reveal the additional content shown below.

JSON	Raw Data	Headers
Save Copy		
<pre> preferredUsername: kev21986 ▼ thumbnailUrl: "https://secure.gravatar.com/avatar/46b59c7f2f869a9a0ff651" ▼ photos: ▼ 0: ▼ value: "https://secure.gravatar.com/avatar/46b59c7f2f869a9a0ff651" type: "thumbnail" ▼ name: givenName: "Kevin" familyName: "Smith" formatted: "Kevin Smith" displayName: "Kevin" ▼ aboutMe: "Co-Founder of App Press and Invisions Technical Arts." currentLocation: "Indianapolis, IN" ▼ accounts: ▼ 0: domain: "twitter.com" display: "@respectTheCode" url: "http://twitter.com/respectTheCode" username: "respectTheCode" verified: "true" shortname: "twitter" </pre>		

Viewing the JSON data, it is easier to read the content that may be important. We also learned that this Kevin person from Indianapolis, IN (arrow 2) and has a last name of Smith (arrow 1); two pieces of information that our client asked us to find.

Find the Twitter account

The kevin@mnksmith.com email account is connected to the respectTheCode Twitter account according to this Gravatar site.

1. Visit the <https://twitter.com/respectthecode> site in your web browser.

The web site is shown below. While it does not have the same avatar image (you should be copying the one that is there and adding to your MindMap or Hunchly), we see that the name on the account is Kevin (arrow 2) and that there is more than 1 tweet (arrow 3).

A screenshot of a Twitter profile page. The profile picture is a black circle with the text "espect theCode" in white. The name "Kevin" is displayed above the handle "@respectTheCode". Below the handle, it says "Joined January 2011". To the right of the profile picture, there are statistics: Tweets 10, Following 170, Followers 127, and Likes 49. Below these stats is a navigation bar with three tabs: "Tweets", "Tweets & replies", and "Media". The "Tweets" tab is selected. A single tweet is listed: "Kevin @respectTheCode · 19 Apr 2018 Verifying myself: I am respectthecode on Keybase.io. FaI6chczJT7gskV1UYCkqdECMkvwKKu03GZf / keybase.io/respectthecode...". Below the tweet are icons for reply, retweet, like (with a count of 1), and a retweet button.

Looks like we may have found the target's Twitter account. We would still like to confirm it using other sources but for this lab, we will say that we are confident enough that it is our target's account.

Find the oldest tweet

This should be simple, right? To find the oldest tweet, simply scroll down the window and the oldest tweet will be at the bottom.

According to the image below, and if you visit Twitter as an unauthenticated user, April 19, 2018 is the oldest tweet. But is this really the oldest tweet from the account?

Kevin
@respectTheCode

Follow

Verifying myself: I am respectthecode on Keybase.io.

FaI6chczJT7gskV1UYCkqdECMkvwKKu03GZf /

Translate Tweet

respect(theCode);

respectthecode (Kevin) on Keybase

End-to-end encryption + digital signing with anyone. Open source for iOS, Android, macOS, Linux, and Windows.

keybase.io

3:03 PM - 19 Apr 2018

The answer is no.

Challenge!

Click Here to See How We Found the Oldest Tweet

1. If you use the Twitter search field to search for `to: respectthecode` you will find Twitter conversations where people replied to this account in January 2011. Since these are replies, we understand that this account tweeted on or before 14 January 2011.

G GRANITE @greygranite · 18 Jan 2011
Replies to @respectTheCode
@respectTheCode oh well this might be a re-run... I have never seen it before.
(a food safe)

M Margaret Padgett @moogritt · 14 Jan 2011
Replies to @respectTheCode
@respectthecode means spell check is #interfering.

M Margaret Padgett @moogritt · 14 Jan 2011
@respectthecode dot your I'd and cross your t's.

We cannot see those tweets for some reason (they may have been removed). So the oldest tweet we can see from that account is from 31 July 2011.

Kevin @respectTheCode · 31 Jul 2011
Technology + Politics = Facepalm via @techcrunch http://bit.ly/neUMjJ

This lab is completed. When finished, close the Firefox web browser.

This page intentionally left blank.

Facebooking

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Find a Photo
 - Find Facebook account from email

Objectives

- Gain experience using Facebook searches to achieve your OSINT goals

Goals

1. Find a photo posted to Facebook tagged to Basra, Iraq from 23 February 2008.
 - Extract the name of the Facebook user that posted the photo.
 - Extract the names of the 4 people in the photo.
2. Find the Facebook user account name of the user with an email of johndoe@example.com

Challenge!

- Can you find the entity ID for that Facebook user with the email of johndoe@example.com?

Preparation

Yes VPN

Start VPN connection (see lab 1.0).

 Need a Valid Facebook Account

You will need to be authenticated to Facebook as a valid user during the lab.

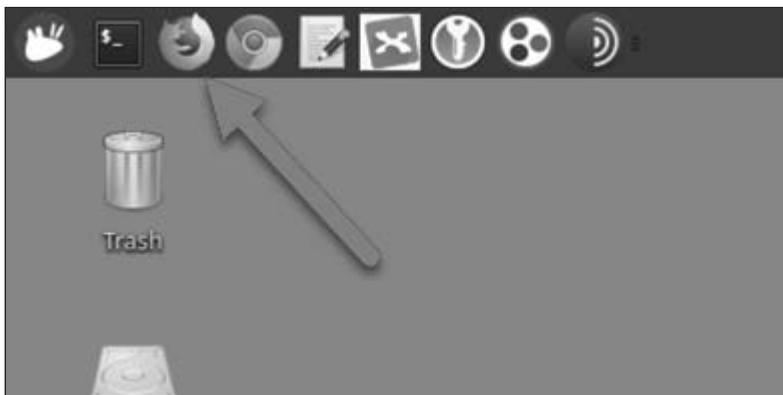
Step-by-step instructions

Find a Photo

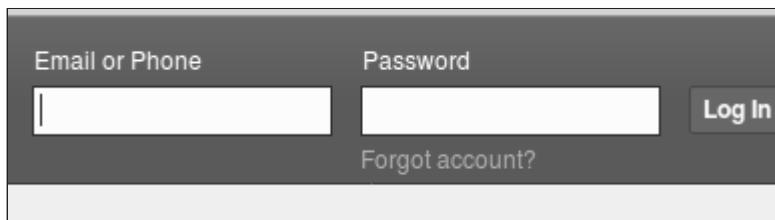
 Documentation

Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

1. Our first step is to launch a Firefox browser window by clicking the Firefox icon in the menu bar.



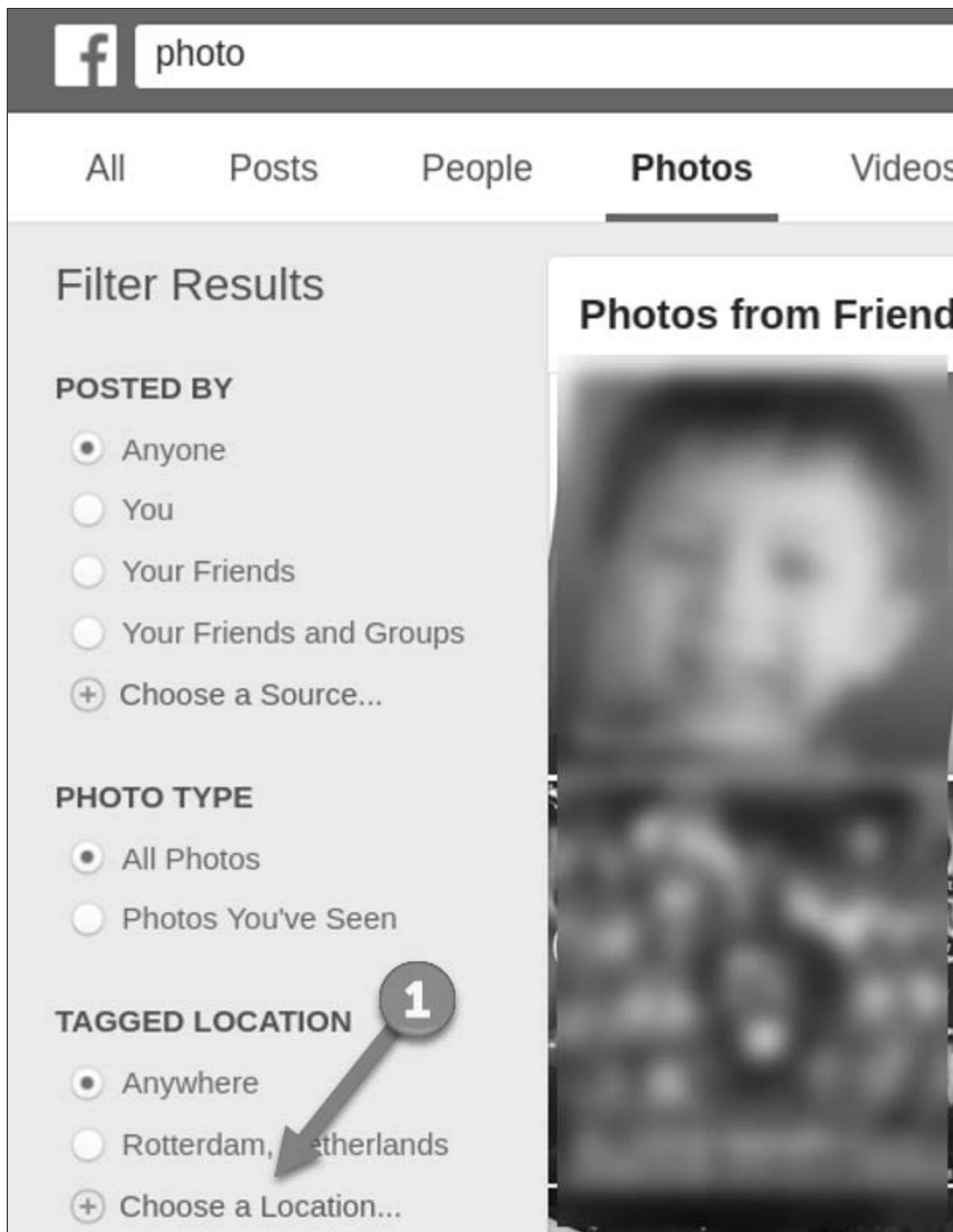
2. In the browser, visit the <https://www.facebook.com> site.
3. Log into the site using your user name and password (sock puppet or other account) in the fields shown in the image below.



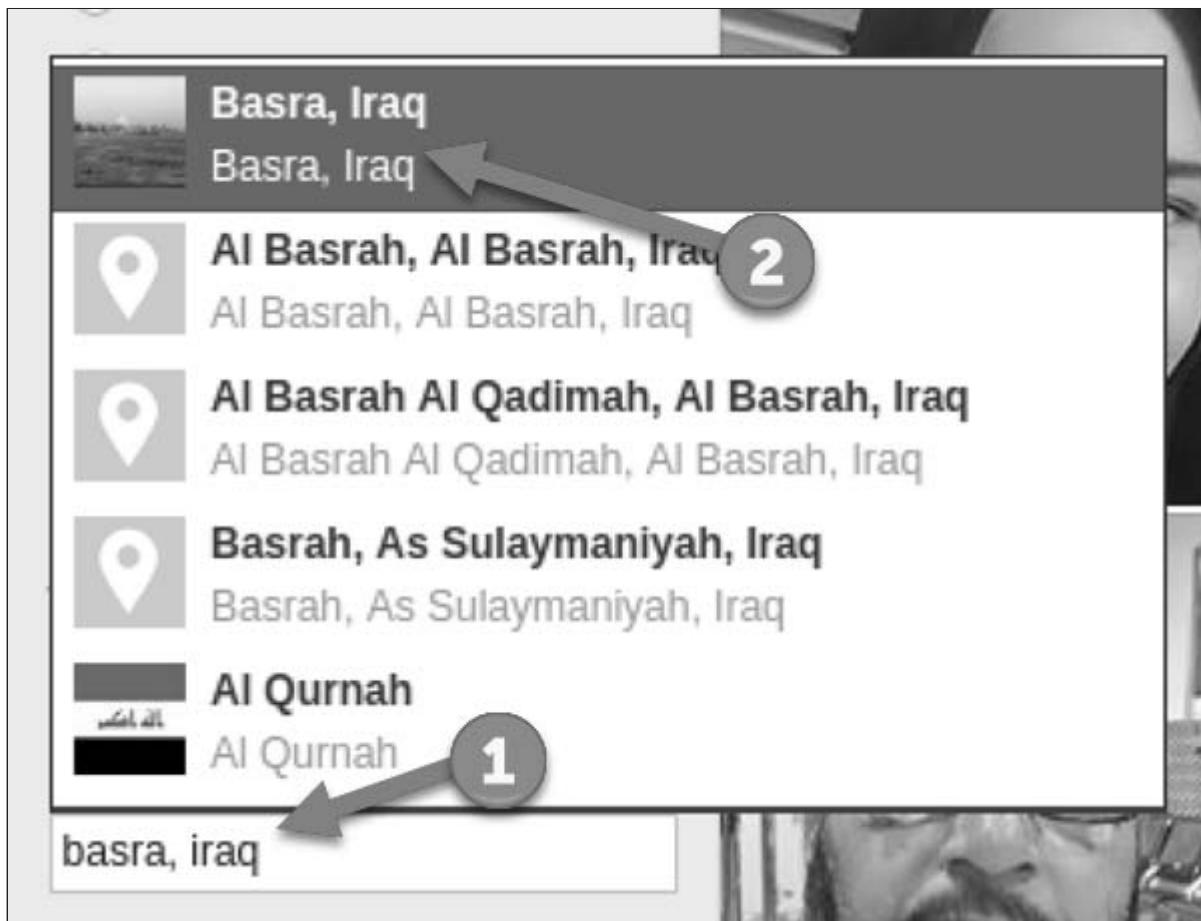
Our first goal is to find any image from a certain location and date. To accomplish this, let's go ahead and just use the search bar. Type `photo` in the search bar (as shown at arrow 1 below) and press Enter.

A screenshot of a Facebook search results page. At the top, there is a search bar containing the word 'photo'. An arrow labeled '1' points to this search bar. Below the search bar is a navigation bar with tabs: All, Posts, People, Photos, and Videos. The 'Photos' tab is highlighted. Another arrow labeled '2' points to the 'Photos' tab. The main content area is titled 'Filter Results' and contains sections for 'POSTS FROM' and 'POST TYPE'. Under 'POSTS FROM', 'Anyone' is selected. Under 'POST TYPE', 'All Posts' is selected. To the right of the filter section is a large, blurred thumbnail of a photo, likely representing the result of the search query.

4. Now we change the search category to photos by clicking on the "Photos" heading (arrow 2 above).
5. We select the date by clicking on the "Choose a Location..." link (arrow 2 below).



6. Enter Basra, Iraq into the location search field (arrow 1 below) and then select the "Basra, Iraq" entry (arrow 2 below) from the list that Facebook shows you.



You should now have photos tagged to Basra, Iraq on your screen. We want to localize the date to 23 February 2008. Facebook's filters only allow us to filter to the nearest month (February). To get more specific and have them return results from a single day, we will use a helper site <https://intelx.io/tools?tab=facebook>.

7. Visit <https://intelx.io/tools?tab=facebook> in another tab or browser window.

We will use this page to find how to format the Facebook filter to look for photos on a date within a certain range.

8. Scroll to the bottom of the page and click on the dropdown form field (arrow 1 below). Select the "Photos" option (arrow 2).

Alternative Facebook Graph Search

This tool is based on the sowdust code. Disclaimer: It is your responsibility to use this tool responsibly and ethically. It is not a service.

For some searches, you may need to enter a key word or location first. If you get no results, you can try a different search term. For example, if you're looking for posts from people in London, just use "london" as the search term.

Search

What do you want to search: -- select a search type -- ▾

-- select a search type --

- Posts
- People
- Photos
- Pages
- Places
- Videos
- Top
- Events

9. Now we need to enter our date range from 22 February 2008 to 23 February 2008. As shown below, the form fields move from year to month to day. Using the drop downs, make your screen look like the below image and click the Add date filter button (arrow 2).

What do you want to search: Photos ▾

Search Photos

Posted by	Entity id	add filter
Tagged with location	Entity id	add filter
Photos you have seen		add filter
Filter by date		
Start date:	2008 ▾ 2 ▾ 22 ▾	
End date:	2008 ▾ 2 ▾ 23 ▾	Add date filter

At the bottom of the window, you should see the following text:

```
rp_creation_time
```

```
{"start_year": "2008", "start_month": "2008-2", "end_year": "2008", "end_month": "2008-2", "s
```

- Now we find what the Facebook entity ID is for Basra, Iraq by decoding the filter string from our original Facebook query. Go back to the Facebook page and copy everything after the "filters=". The string should look like:

```
eyJycF9sb2NhdkGI vbi I 6I ntcI m5hbWVcI j pcI mxvY2F0aW9uXCI sXCJhcmdzXCI 6XCI xMTAzMDA2Nj g50Tk2M
```

- In another browser tab, open the CyberChef web page <https://gchq.github.io/CyberChef/>.
- Drag the From Base64 from the Operations column to the Recipe column and drop it.

Download CyberChef [Download](#)

Last build: 2 days ago - v9 supports multiple inputs and outputs

Operations

- Search...
- Favourites
- To Base64
- From Base64** (1)
- To Hex

Recipe (2)

From Base64

Alphabet: A-Za-zA-Z0-9+/=

Remove non-alphabet chars

13. Paste the filter string

(eyJycF9sb2NhdG1vbiI6IntcIm5hbWVcijpcImxvY2F0aw9uXCI sXCJhcmdzXCI 6XCI xMTAzMDA2Nj g50Tk2 into the Input column (1 below) and look for the args number in the Output column (arrow 2).

Input

length: 100
lines: 1

(eyJycF9sb2NhdG1vbiI6IntcIm5hbWVcijpcImxvY2F0aw9uXCI sXCJhcmdzXCI 6XCI xMTAzMDA2Nj g50Tk2

Output

time: 1ms
length: 73
lines: 1

{"rp_location": "", "name": "location", "args": "110300668999603"} (2)

14. Copy that number (110300668999603) and paste it into the IntelX "Tagged with location" entity ID field (arrow 1 below). Then click the add filter button (arrow 2).

Search

What do you want to search: Photos ▾

Search Photos

Posted by

Entity id

add filter

Tagged with location

110300668999603

add filter

Photos you have seen

add filter

1

2

15. Scroll down to the bottom of the page and view the filters for date and location (shown below).

Show URL Open URL in a new window **View Filters** **1**

- **rp_creation_time** {"start_year":"2008","start_month":"2008-2","end_year":"2008","end_month":"2008-2","start_day":"2008-2-22","end_day":"2008-2-23"}
- **rp_location** { location : 110300668999603}

16. Click the Open URL in a new window button (arrow 1 above) to open the URL in another browser window or click here <https://www.facebook.com/search/photos/?q=photos&epa=FILTERS&filters=eyJycF9jcmVhdGlvbl90aW1ljoie1wibmFtZVwiOlwiY3JIYXRpb25fc>
If it worked, you should see a results page with a single image (shown below).

Public Photos



 Log into Facebook

You need to be logged into Facebook as a valid user for this to retrieve the correct results.

17. Click on the photo to get the details (shown below with the names blurred out). We can see the date (1) and location (2) of the photo. In the live version of the content, you can also view the person's name that posted it and the four other people in the image.



Find Facebook account from email

For the next task, we have an email address (johndoe@example.com) and want to find the Facebook account name and entity ID of the user associated with it. For this technique, you will create a Facebook page.

1. Create a new Facebook page by clicking the Create link (1) and then selecting Page (2).

The image shows a screenshot of the Facebook 'Create' menu. At the top, there are three main options: 'Home', 'Find Friends', and 'Create'. The 'Create' option is highlighted with a dark grey background. Below it, two items are listed: 'Page' and 'Ad'. Each item has a small icon to its left: a flag for 'Page' and a megaphone for 'Ad'. To the right of each item is a large, semi-transparent circular overlay containing the number '2'. The 'Page' section also includes the text 'Connect and share with customers or fans'. The 'Ad' section includes the text 'Advertise your business, brand or organization'.

2. Select the Get Started button under the Community or Public Figure option.
3. Create a name for your page and fill it in the field (1). Then fill in the category field (2). The name and category do not matter for this technique. We need to fill them out to get Facebook to make the page we need. Click the Continue button when you have completed entering your info.

Community or Public Figure

Connect with people in your community and share important to you with a free Facebook Page.

Page Name

1

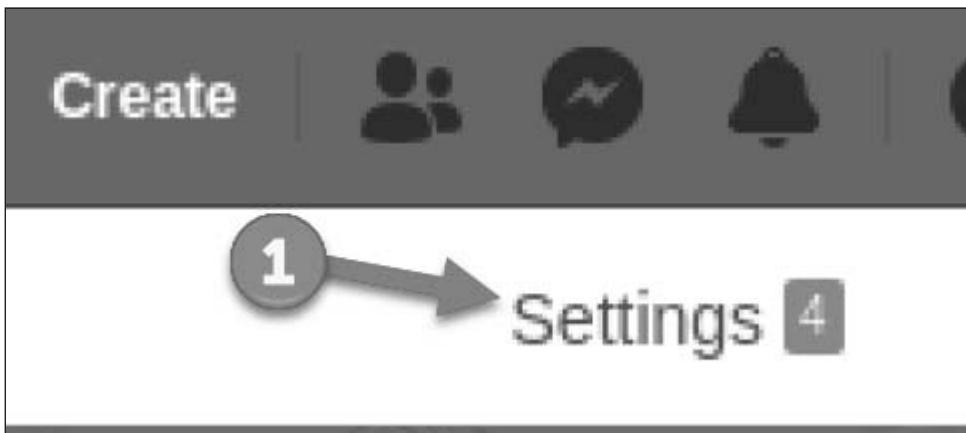
Name your Page

Category

2

Add a category to describe your Page

- Skip the next two pages of adding a page photo and cover image.
- Click the Settings button in the upper right (arrow 1).



- Click the Page Roles (arrow 1) option on the left side of the screen.

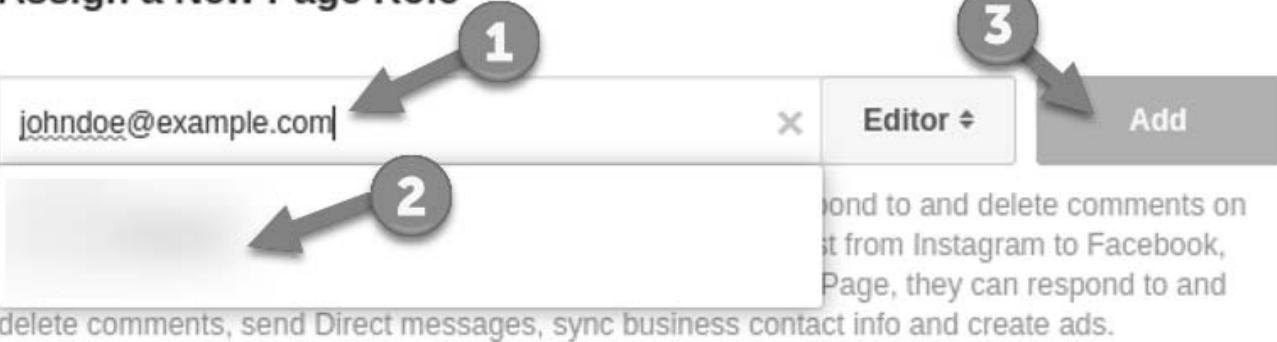


- In the Assign a New Page Role field on the right, type in the `johndoe@example.com` email address (arrow 1 below). When you enter the final m, Facebook should display the name of the account that is tied to that address (blurred out at arrow 2 below).

Warning

DO NOT CLICK THE "Add" BUTTON (arrow 3) as this will alert the user.

Assign a New Page Role



8. The lab is complete. Feel free to try other searches or log out of Facebook.



Click Here to See Our Findings



Names of people in Iraq photo Direct link to image: Click here to view image Facebook user posting photo: Dan Jarman
Four people tagged in the image: Richard Fitzpatrick, Chris August, Barrie Peach and Kathleen Reid

Facebook info for email address johndoe@example.com Facebook user name: Hira Ali Facebook entity ID:
100008037220634

This page intentionally left blank.

Tweet Analysis

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Use Twitter's advanced search
 - Analyze the account's tweets
 - Examine any hashtags used
 - Examine any geolocation

Objectives

- Become comfortable with using the Twitter advanced search feature to find users
- Use common web sites to analyze Twitter tweets
- Examine tweets with geolocation and hashtags

Goals

Someone mentioned to your customer that there is a Twitter account tweeting strange content. Your customer reports that the profile name of the account is "Dread Pirate Roberts" (this is different from the Twitter account name) and the profile states the account is from "County Clare, Ireland". Find the Twitter account name for your customer.

Analyze the tweets from the above account for languages, geolocation, sentiment, and other related information. Investigate and record what cities and countries the user tweets from.

Your customer also mentioned that this account may be involved in a travel-related, tweeting challenge. Find out what other Twitter accounts are using the same hashtag as this account and where they are reportedly tweeting from.

1. Use Twitter's advanced search form to find the account.
2. Use the <https://socialbearing.com> site to analyze the account's tweets.
3. Find others associated with the hashtag that this account used, the account name(s) and locations.

 Do Not Authenticate to Twitter

You must not be logged in to Twitter to be able to see the Near This Place search option.

Preparation

No VPN

Step-by-step instructions

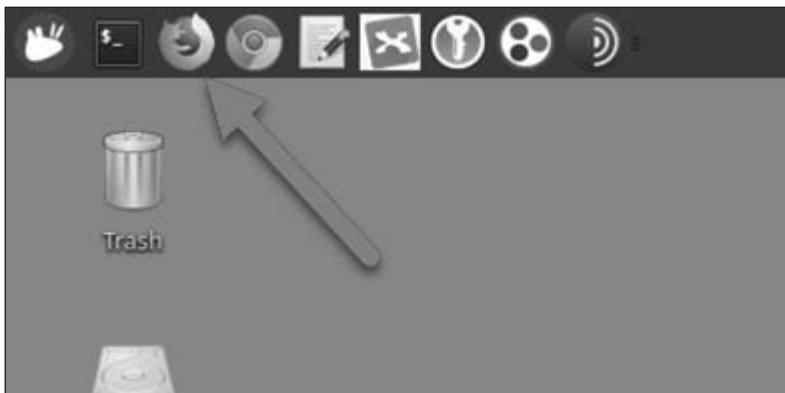
Use Twitter's advanced search

For some social media assessments, you need to have an account on the web site that you can log into and use for your searches. Since most of the Twitter content is public, you will not need a sock puppet Twitter account for this lab work.

Document with a MindMap or Hunchly

Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

1. Our first step is to launch a Firefox browser window by clicking the Firefox icon in the menu bar.



2. In the browser, visit the <https://twitter.com/search-advanced> site.

A screenshot of the Twitter Advanced search interface. At the top, there are navigation links for "Home" and "Moments", and a search bar labeled "Search Twitter". The main title is "Advanced search". Below the title, there are several input fields and dropdown menus:

- "Words":
 - All of these words
 - This exact phrase
 - Any of these words
 - None of these words
 - These hashtags
- "Written in": A dropdown menu set to "All languages".

We know from your client that the user's name (not the account name) is "Dread Pirate Roberts".

3. This is required content and should be typed into the All of these words field.
4. Next, the customer also mentioned a location. Type: County Clare, Ireland into the Near this place form field (shown below).

Words	
All of these words	Dread Pirate Roberts
This exact phrase	
Any of these words	
None of these words	
These hashtags	
Written in	All languages ▾
People	
From these accounts	
To these accounts	
Mentioning these accounts	
Places	
Near this place	County Clare, Ireland

These fields make it easier for you to get your query data formatted correctly even if you do not know all the Twitter search operators.

5. Click the Search button at the bottom of the window when you are ready to search.
Your results may be disappointing. You might see the No results for... message on the screen (below).
6. We are looking for a user account and not a tweet mentioning that data so click on the People header tab.

Dread Pirate Roberts near:"County Clare, Ireland" within:15mi

Top Latest People Photos Videos News Broadcasts

Search filters · Show

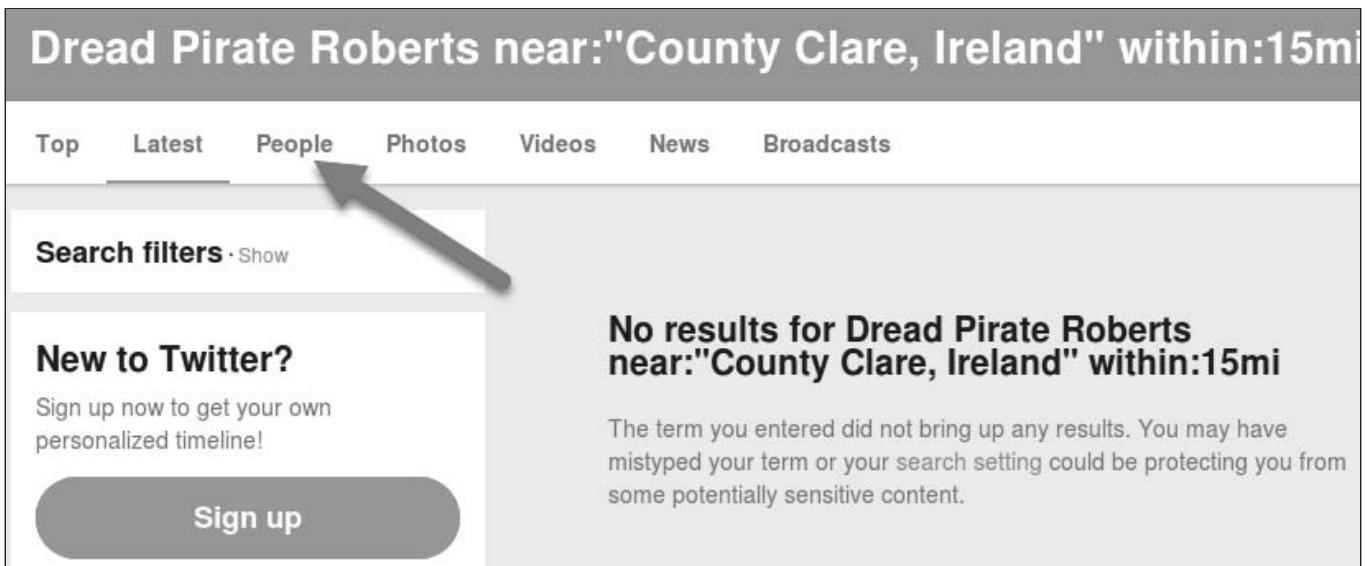
New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

No results for Dread Pirate Roberts near:"County Clare, Ireland" within:15mi

The term you entered did not bring up any results. You may have mistyped your term or your search setting could be protecting you from some potentially sensitive content.



Now we should see a Twitter account (below) that has the words Dread Pirate Roberts in the profile.

7. Note the name of the account (it is the content after the @).
8. Let's confirm the location by clicking the account's name (shown below).

Dread Pirate Roberts near:"County Clare, Ireland" within:15mi

Top Latest People Photos Videos News Broadcasts

Search filters · Show

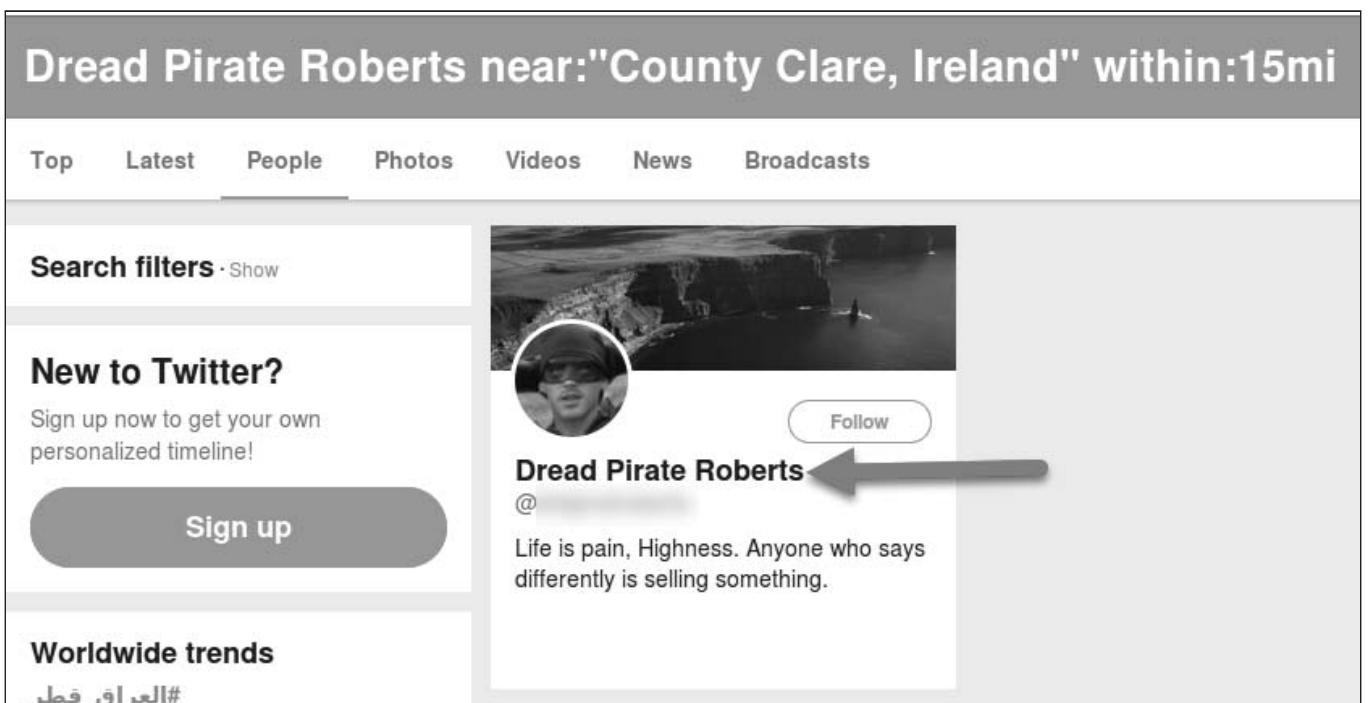
New to Twitter?

Sign up now to get your own personalized timeline!

Sign up

Worldwide trends

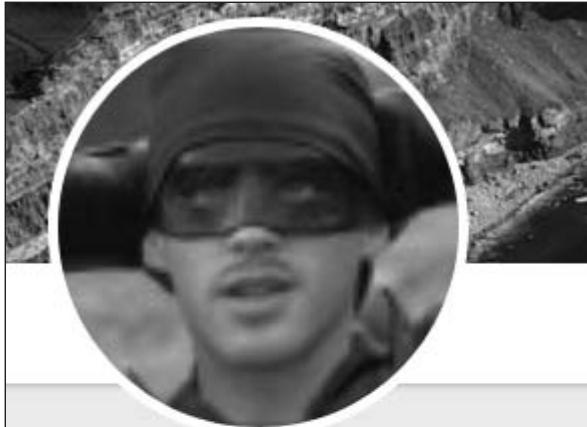
#العراق_فطر



The account is found at the <https://twitter.com/drdpiratroborts> URL and, sure enough, has the location set to County Clare, Ireland (see below).

Document Everything

At this point in a live assessment, you would document all the information about this account, account name, profile photo, when the account was created, etc. You may be able to pivot on any number of those pieces of data. You don't need to do that for this lab.



Dread Pirate Roberts

@drdpiratroberts

Life is pain, Highness. Anyone who says differently is selling something.

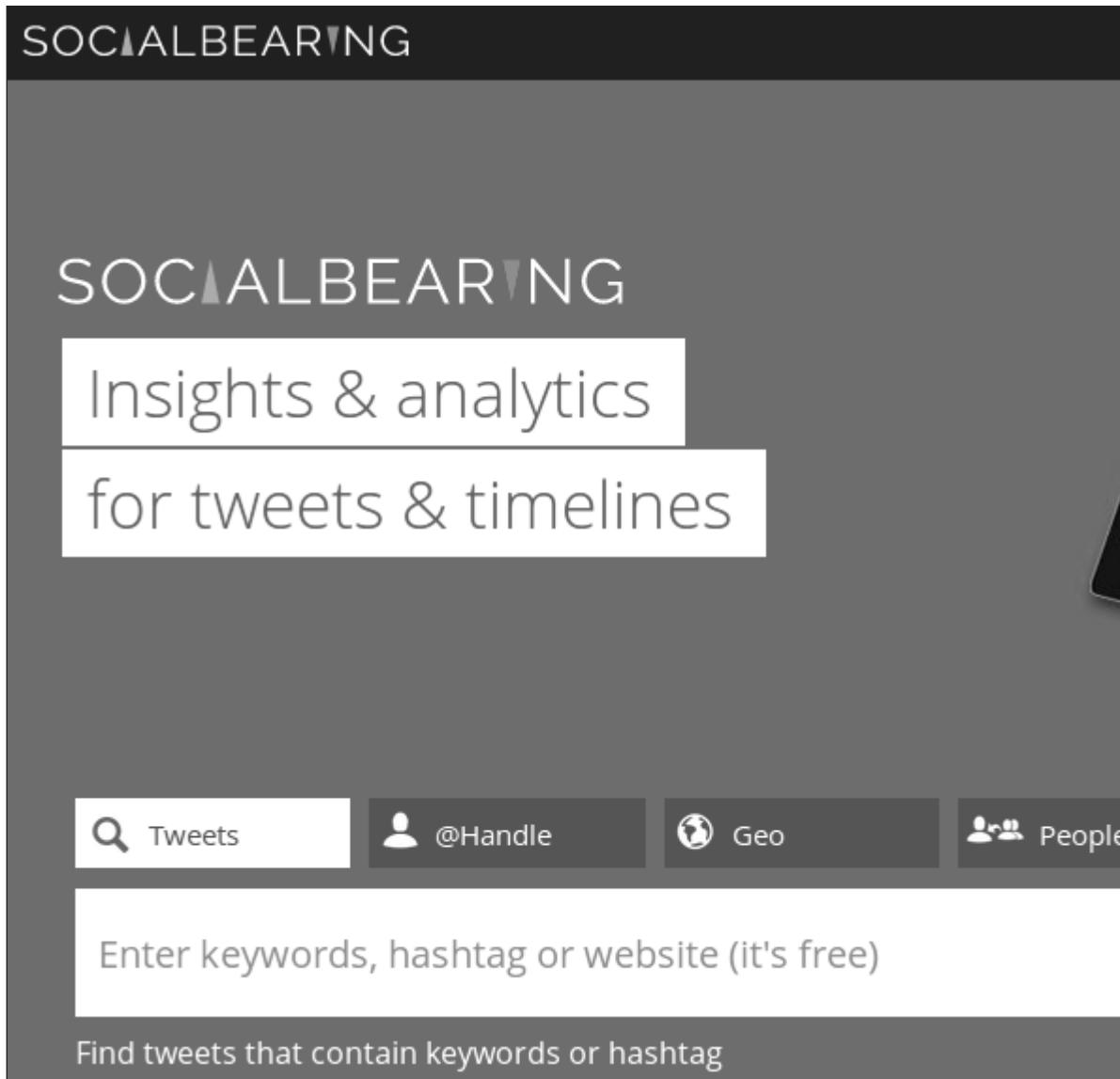
⌚ County Clare, Ireland



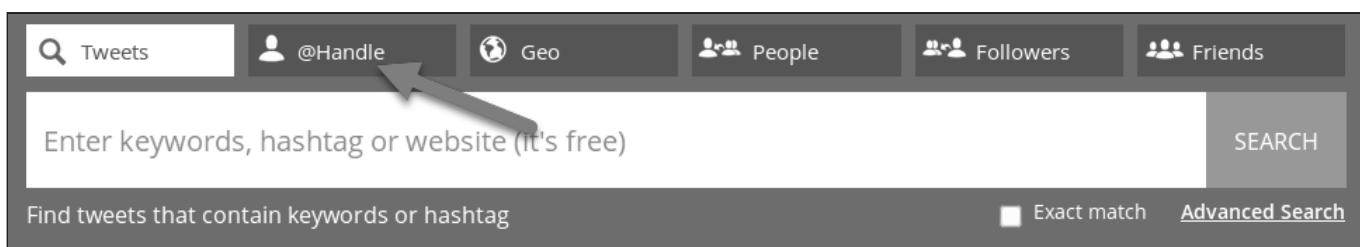
Joined July 2016

Analyze the account's tweets

1. Visit the <https://socialbearing.com> web site in the browser.



- When the site shows in your browser, click on the @Handle tab in the middle of the page (see below) to perform a search of a Twitter user's profile.



- Search for the Twitter account by typing `drdpi ratroberts` into the form field and clicking the Search button.

The screenshot shows a search interface for Twitter users. At the top, there are three input fields: 'Tweets' with a magnifying glass icon, '@Handle' with a user icon, and 'Geo' with a globe icon. Below these, the handle '@drdpiratroberts' is entered. A large button at the bottom reads 'Timeline analytics for any public Twitter account'.

SocialBearing.com will load that user's most recent 200 tweets and analyze them. The direct link to the SocialBearing site for this Twitter user is <https://socialbearing.com/search/user/drdpiratroberts> (<https://sec487.info/c4>) and looks like the image below. (Note that the time frames and other data may show different values).

The screenshot displays a summary of the user's activity. At the top, it says 'User search & analytics for '@drdpiratroberts''. Below that, it states 'Showing the user timeline for @drdpiratroberts. Twitter limits number of tweets returned to 3,200'. There are sharing options for Twitter, Facebook, LinkedIn, and CSV. The main data table includes:

TWEETS	TIMEFRAME	REACH	IMPRESSIONS	TOTAL RT'S	TOTAL FAVES
9	384 days	9	81	0	2
LOAD MORE				@0	@2
		REPLIES	HIDDEN		
		0	0		

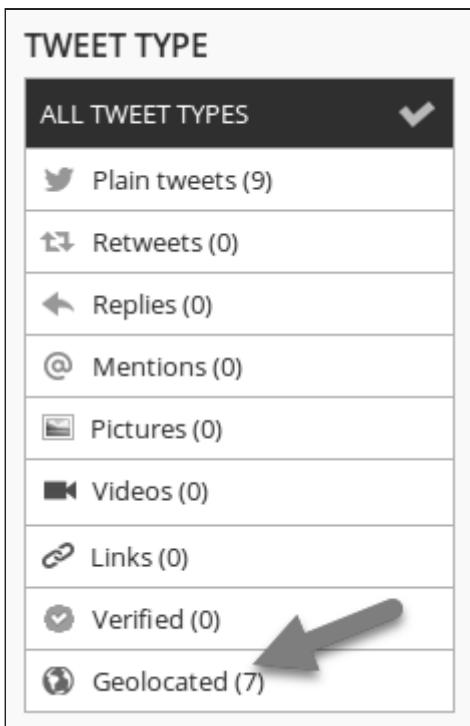
- While this information is interesting, the real power in the site, can be found by scrolling down the window and looking on the left.

There are filters that reduce the data in the main portion of the window to reveal what you are looking for.

If you don't see the filters on the left, then your window might be too narrow to display them. There is a pop-out menu that you can click to reveal them (shown below).

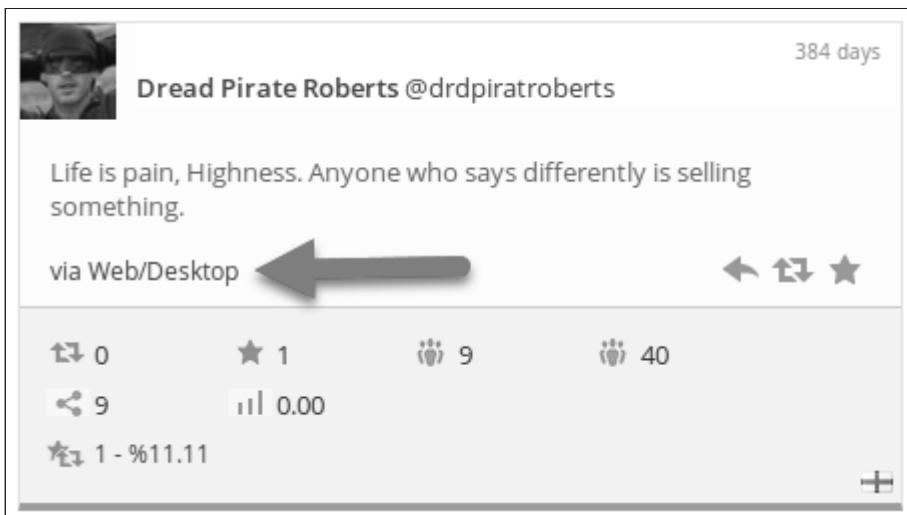


Looking at the filter section marked Tweet Type we can see that this user has tweeted 9 times and geolocated 7 of those.



5. Take some time to browse around the page and examine the other filters and data presented.

Something interesting is that this page will show what the client software was that was used to send the tweets. This is shown in each tweet after the via tag (shown below).



Now we know more data about this user and can see that they have geolocated tweets. Let's see where they are tweeting from.

Examine any hashtags used

1. Scrolling down on the left side filters, we see the user tweeted with the #sec487AroundTheWorld hashtag (shown below).

TOP HASHTAGS

Top hashtags found in tweets

ALL HASHTAGS

#sec487aroundtheworld (7)

2. SocialBearing's web site allows users to pull tweets using their hashtags from 7 days prior. These tweets were made long ago so we will need to use a different web site to retrieve the data. Let's revisit the Twitter Advanced Search form and enter the hashtag to see if others are using it. In the browser, visit the <https://twitter.com/search-advanced> site.
3. Enter the hashtag sec487AroundTheWorld into the These hashtags field and click the Search button.

Advanced search

Words

All of these words

This exact phrase

Any of these words

None of these words

These hashtags



Direct URL

You can go directly to the hashtag search by visiting <https://twitter.com/search?q=%23sec487AroundTheWorld&src=typd>.

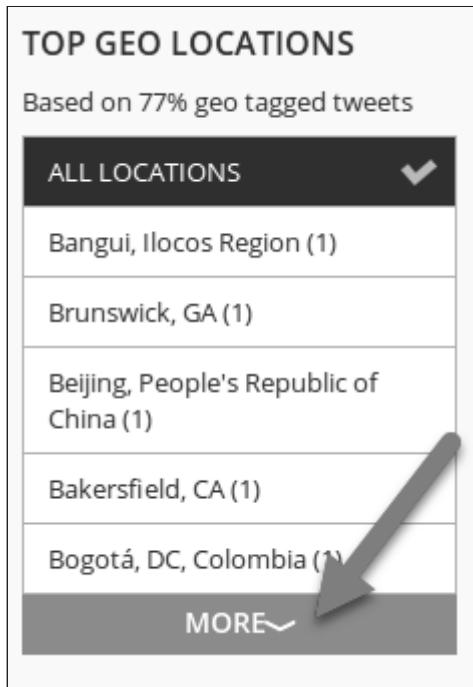
4. The default view only shows the Top Tweets instead of all of them. Click the Latest option to change the view and show the rest of the tweets (below).



5. In your notes, write down some of the other user accounts that have tweeted using the hashtag and where they have tweeted from.

Examine any geolocation

1. On the left side of the SocialBearing web site filter section, you can scroll down to the TOP GEO LOCATIONS to see the places where this user geolocated their tweets.



2. Since they tweeted such a few number of times, expanding this section (by clicking on the MORE button) will show all the places they tweeted.
3. Write down in your notes the locations where this user tweeted.

Odd Tweet Dates

Did you notice the dates when these tweets were sent? All 10 tweets from "around the world" were sent on November 25, 2017. Impossible, yes? But not if you know how to fake your GPS location.

4. This lab is completed. When finished, close the web browser.

Click Here to See Our Findings

1. The Twitter account name is: drdpiratroborts
2. The locations where @drdpiratroborts tweeted from:
 - a. Bahrain
 - b. Bakersfield
 - c. Bangui
 - d. Barcelona
 - e. Beijing

- f. Bermuda
 - g. Bogota
 - h. Brunswick
3. Twitter Account Name: OsintNinja (and others) tweeted using the #sec487AroundTheWorld hashtag.
 4. OsintNinja's Tweet Location: Bethesda

This page intentionally left blank.

Twitter Bot Analysis

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - censusAmericans
 - moorehn
 - spainandcatalan
 - trashcanlife
 - warrior101abn

Objectives

- Analyze the Twitter activity of several accounts to determine if they are "bot" accounts.

Goals

- Examine the Twitter activity from the following Twitter accounts. Determine if the accounts are automated, bot accounts. Discover and record evidence to support your findings.
 - censusAmericans
 - moorehn
 - spainandcatalan
 - trashcanlife
 - warrior101abn

Preparation

VPN if problems

Step-by-step instructions

1. Visit the <https://makeadverbsgreatagain.org/allegedly/> site.
2. Enter each username and click the Submit button.
3. Analyze the results.



Click Here to See Our Findings



censusAmericans

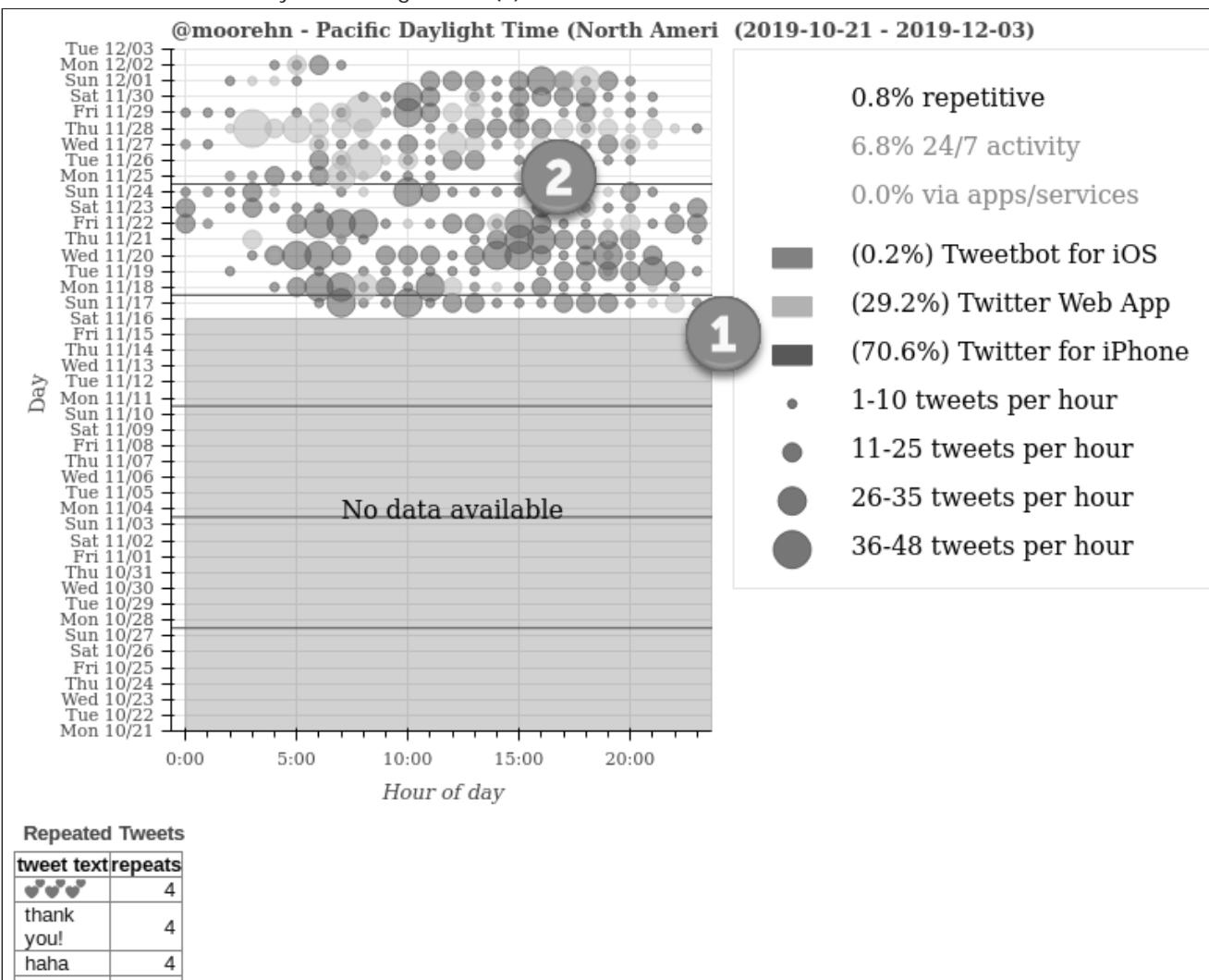
- Most likely a BOT due to 24/7 tweeting (1) and source of tweets being an app (2).



moorehn

- Most likely not a BOT due to source of tweets (1).

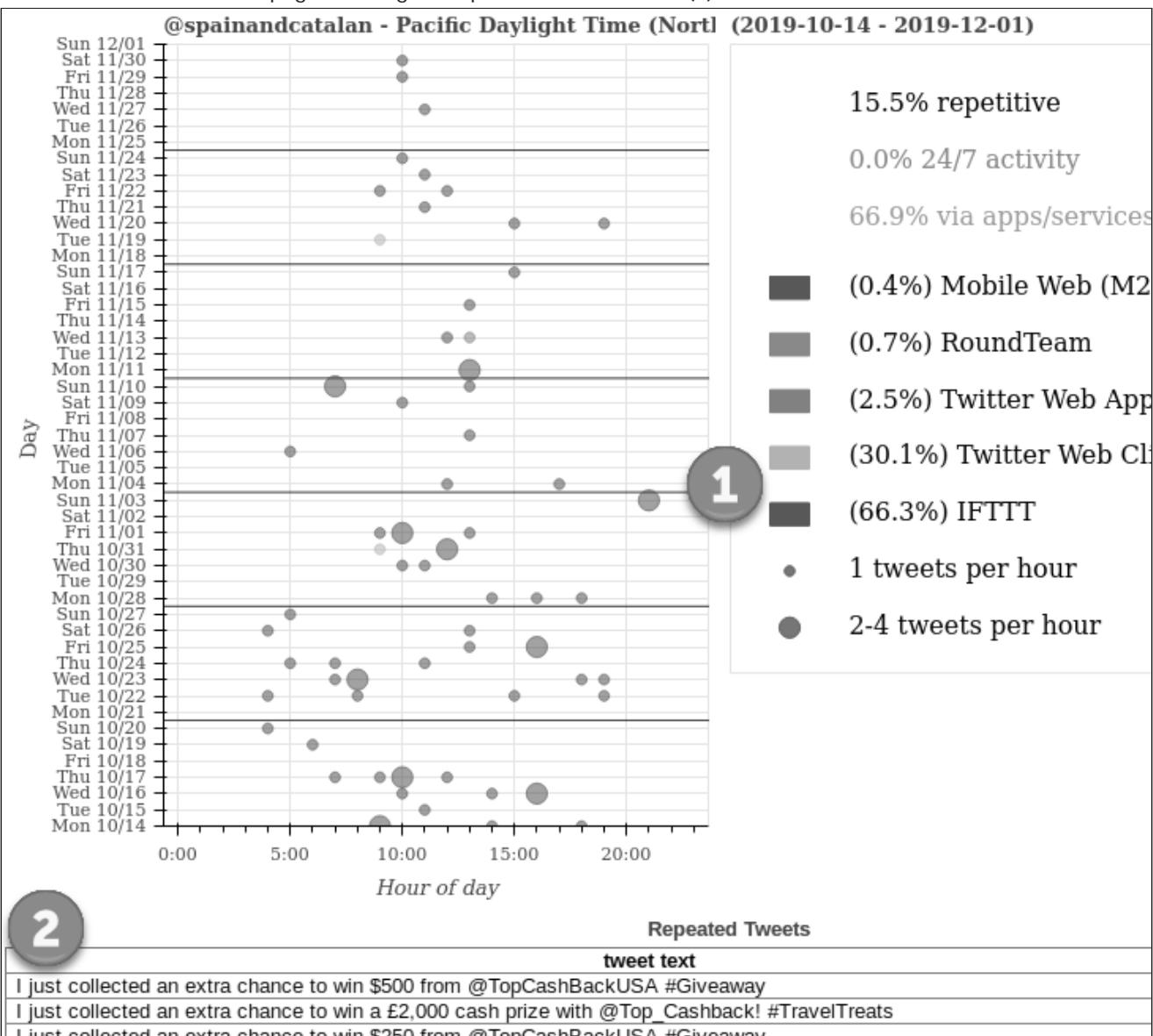
- However, user is most likely scheduling tweets (2).



spainandcatalan

- Probably not a BOT due to the IFTTT source of tweets along with the Twitter Web Client (1).

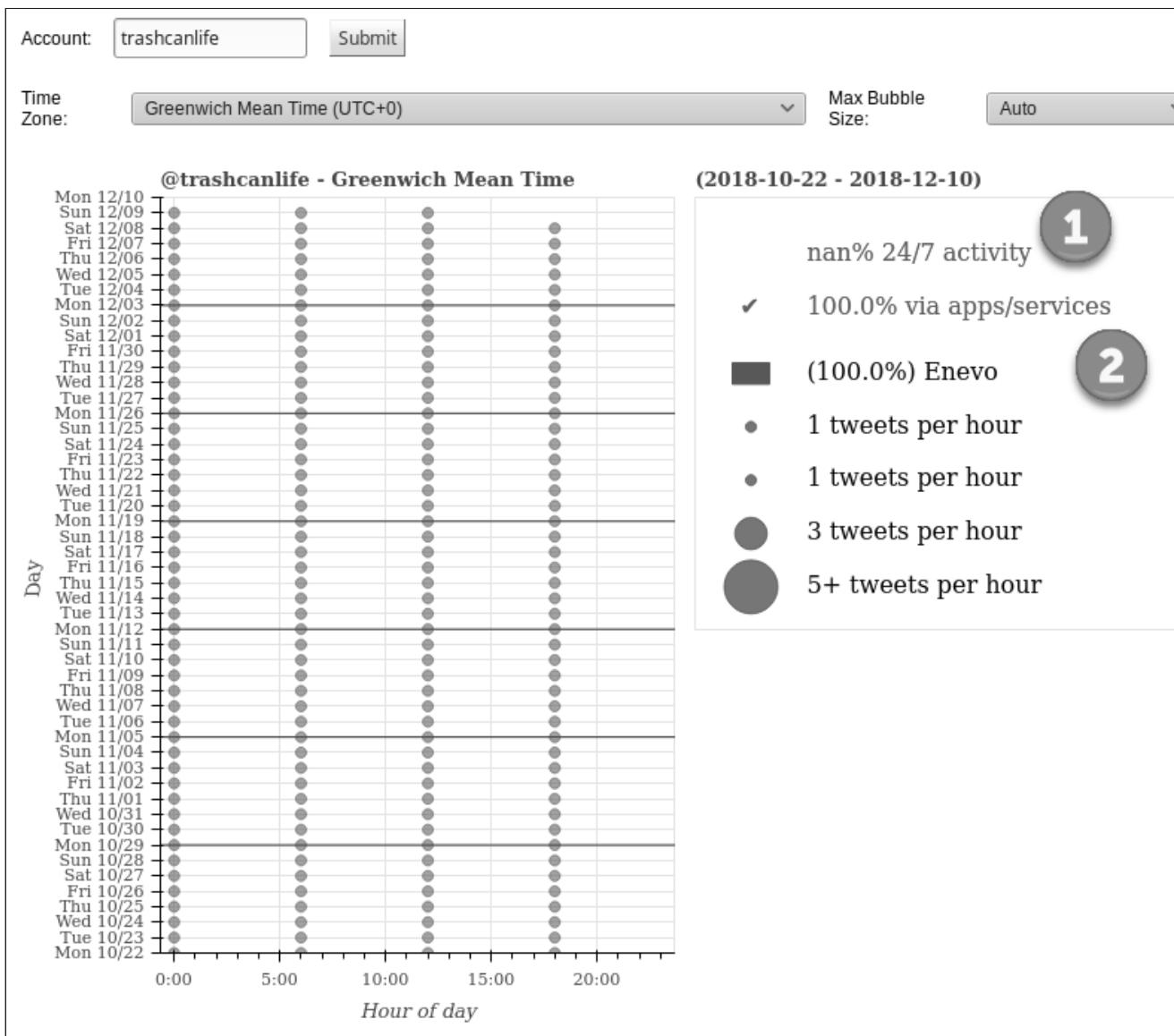
- Examine the bottom of the page showing the repeated tweet content (2).



trashcanlife

- Definitely a BOT due to tweeting so regularly (1) and source of tweets being an app (2).

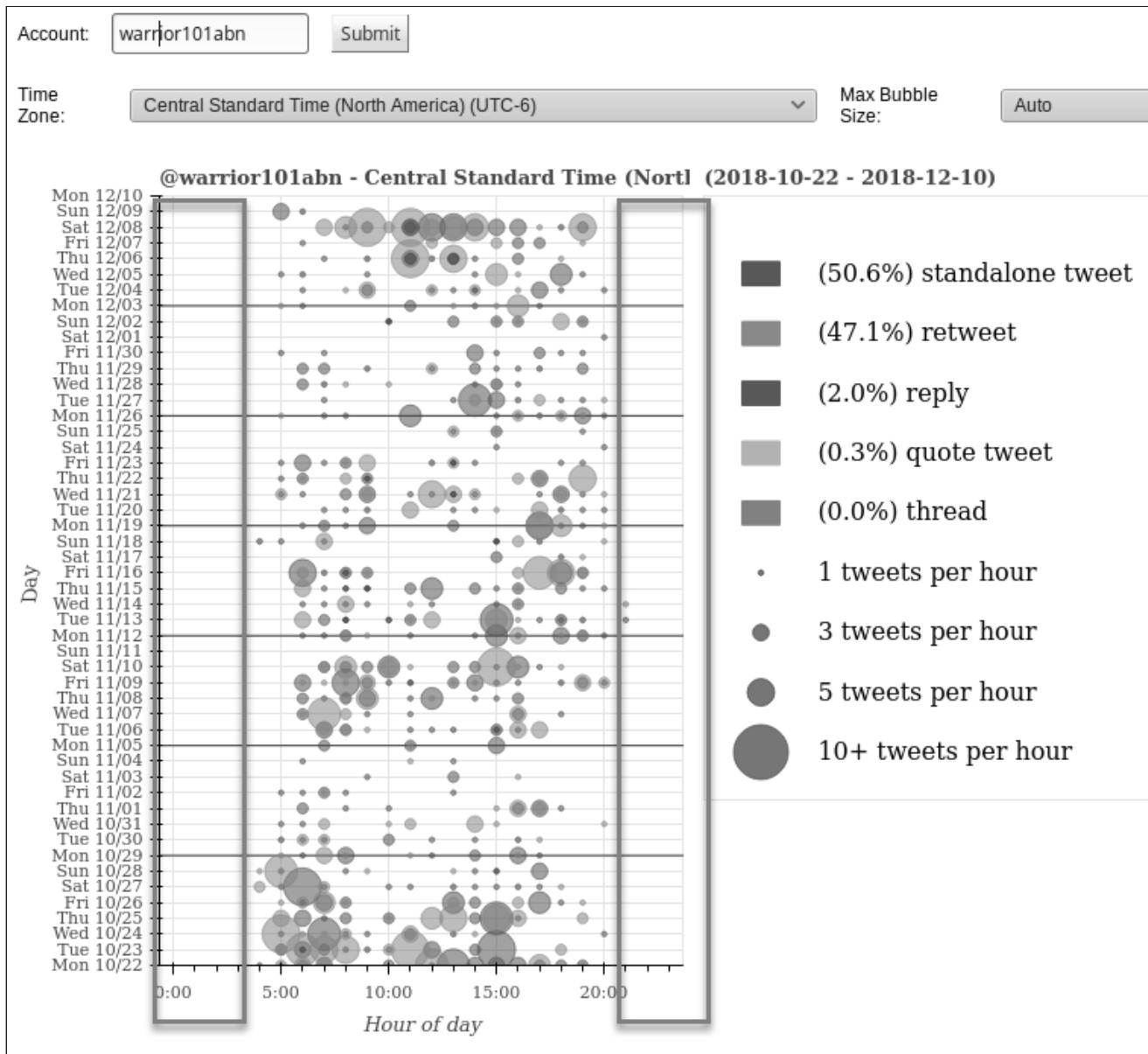
- Also, Twitter bio states that this *IS* a bot.



warrior101abn

- Most likely not a BOT due to tweet times, variety of activity (retweets, original tweets, etc.).

- Shifting the time zone to account for the location the account reportedly is in, this account tweets from roughly 0500 - 2000hrs.



This page intentionally left blank.

Aerial Adventure

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Find an image of your jacket
 - Map the distance traveled on your walk
 - Find the photo sphere
 - [CHALLENGE] Find the vehicle's details
 - [CHALLENGE] Portuguese Navy Ships
- Answers
 - Green, VW Bug
 - Vehicle south west of the GPS coordinates on Y-460 road
 - Portuguese Navy Ships

Objectives

- Gain experience using an online mapping application
- Become familiar with measuring distance on an online mapping application
- Use Street View and user-uploaded photo-spheres to perform reconnaissance of areas

Goals

The scenario for the first portion of the lab is that you were on vacation and hiking the Valley of the Waters Track towards The Conservation Hut, Fletcher St, Wentworth Falls NSW 2782, Australia.

Around the intersection of the Shortcut Track you remembered taking off your favorite blue jacket but not necessarily putting it in your pack. When you got to the hut, you found your jacket was missing. What happened to the jacket? Where is it?

1. Using Google Maps' Street View, **find** an image of the jacket somewhere on the trail.

After going back and getting your jacket, you and your partner decide to walk back to your hotel, the POET'S COTTAGE Blue Mountains Tranquility. From the Conservation Hut, you walked on Fletcher street and made a left on Fitzgerald street. You took another left onto the Valley road. That took you north to the Poet's cottage. You told your spouse that it was about $\frac{1}{2}$ km walk but your spouse insisted it was more. Who was right?

2. Using Google Maps, map the distance traveled on your walk and **find** out who was right.

A customer said they attended a game at the Meadowlands Sports Complex. They parked their vehicle in lot L and were walking towards the stadium when a person in a green VW Bug car approached them. It was an old friend from their childhood! They enjoyed talking with the old friend and, in the excitement, forgot to get their contact information. They remembered seeing someone take one of those Google Photo Sphere photos in the lot near them just before the encounter. Your customer would like you to gather identifying information from the car that could be used to find the person.

3. Using Google Maps, **find** the photo sphere in lot L of the Meadowlands stadium and gather information from the car that could help your customer **find** their friend.

Challenge!

4. South west of the GPS coordinates -52.4271917,-71.416559 on the Y-460 road, there is a photo sphere. Find the manufacturer name and license plate number of the truck you see in it.
5. Visit <https://www.google.com/maps/search/portugal+naval+base/@38.6690383,-9.1467065,223m/data=!3m1!1e3> and, based upon the lengths of the largest 3 ships in the center of the image, identify the "classes" of the Portuguese Navy ships.

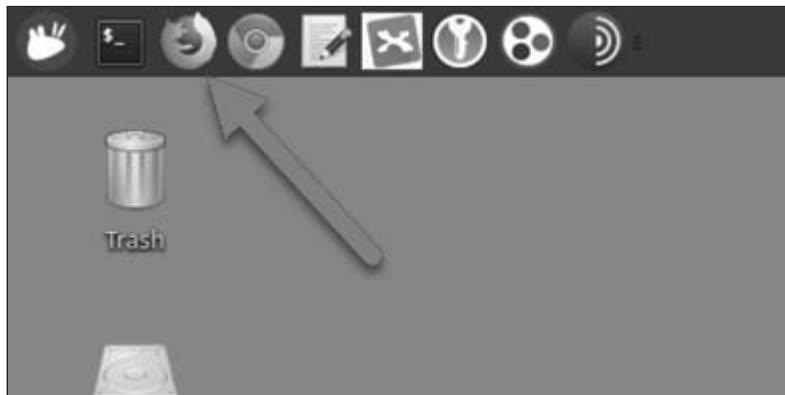
Preparation

No VPN

Step-by-step instructions

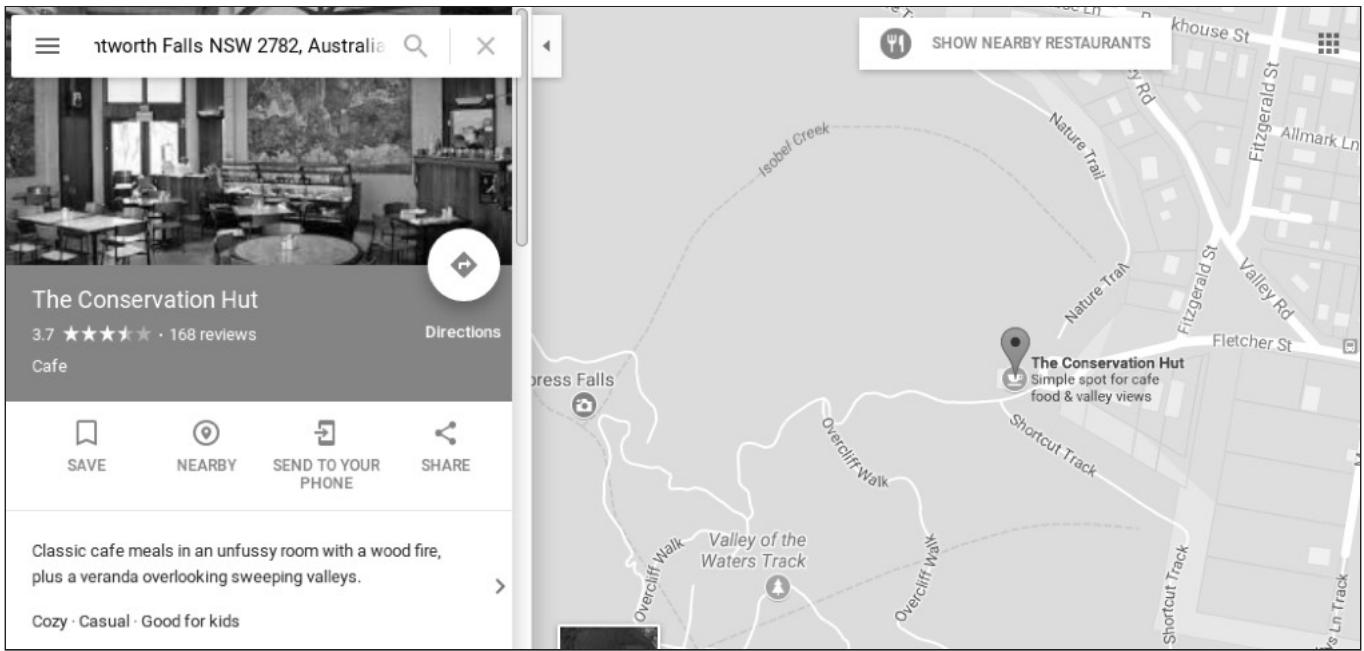
Find an image of your jacket

1. Our first step is to launch a Firefox browser window by clicking the icon in the menu bar.



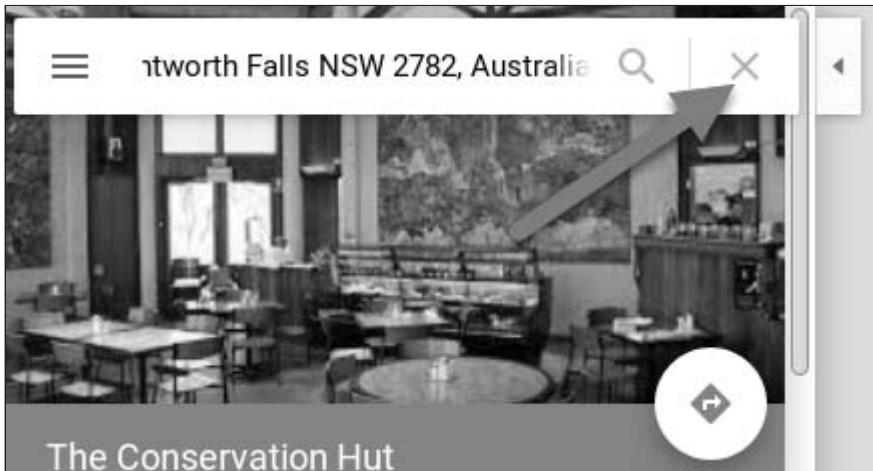
2. Visit the <https://www.google.com/maps> web page.
3. In the Search Google Maps field, paste the location of the first scenario: The Conservation Hut, Fletcher St, Wentworth Falls NSW 2782, Australia and press Enter.

The map should look like below.



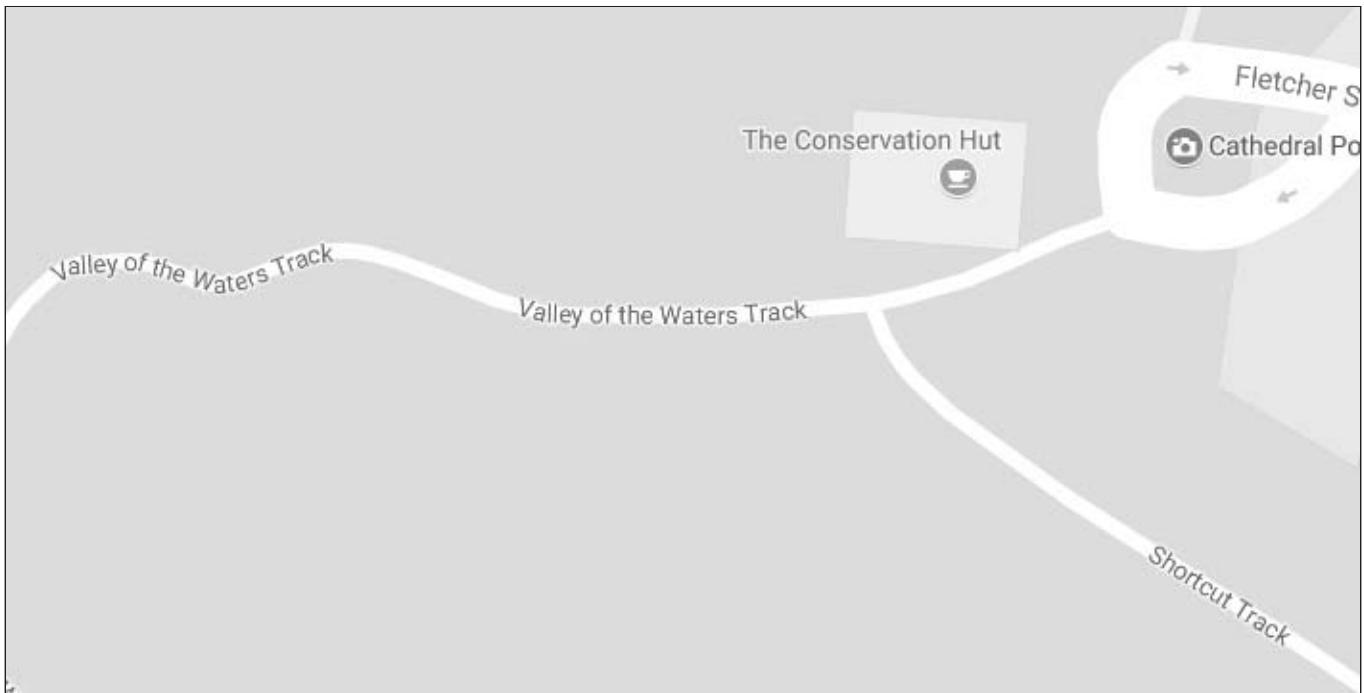
We have found the place and can see that there are walking tracks or hiking trails nearby.

- Let's give ourselves some room and close the side panel by clicking the X next to the search field.



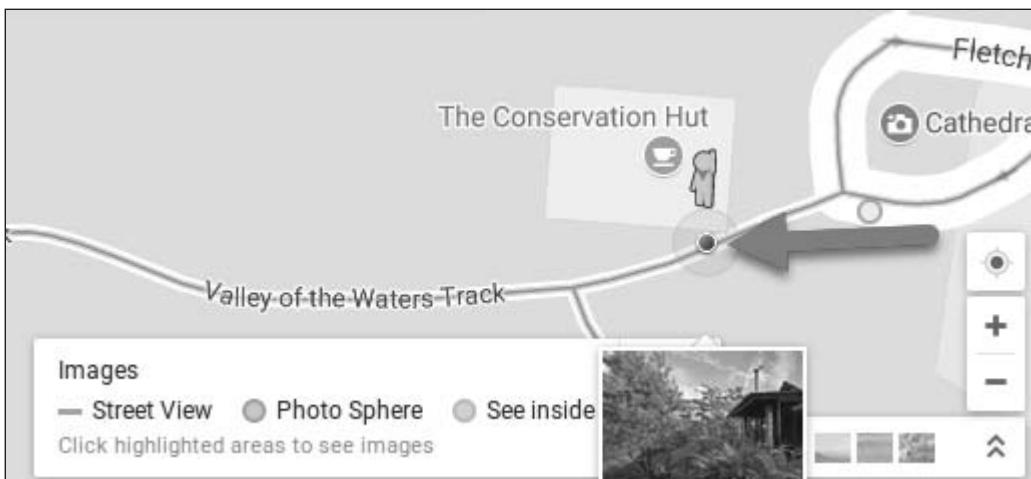
- Now let's zoom into The Conservation Hut by using the mouse wheel, double clicking near it, or using the + on the right side of the window.

The scenario mentioned the intersection of the Valley of the Waters Track and the Shortcut Track. Zoom in on that intersection as we did below.



To find your jacket we will use the Street View on Google Maps. Street View not only shows streets but has tracks that are on trails and even inside buildings! Here, someone has walked the trails/tracks and then uploaded that content to Google.

6. To use this feature, click and drag the small, yellow person in the lower-right of the window over to the trail just below The Conservation Hut and release it.



The map view shifts to the Street View images as seen below. Your initial view may be different from what is shown below depending upon which direction the view is facing. Since we want to start at The Hut and work westward, your view needs to rotate around until your view matches what is shown below.

- To do this, click on the images and drag one direction until your view approximately matches what is shown on the screen below.

You need to be looking westward (arrows 2 and 3) and at a track that goes down a hill (arrow 1).



What we want to do is "walk" forward on the track until the yellow person-icon is at the Shortcut Track junction.

- To do this, click on the part of the trail in front of you (down the hill).

Your view should shift forward a bit. Arrow 1 points to what looks like a sign. Click the map "in front of you" to move forward repeatedly until you come to the intersection.



- When your view approaches the intersection, click and drag on the image to visually look left (down the Shortcut Track).

You will see a blue jacket hanging on a sign (shown below). Hey! There's your jacket!

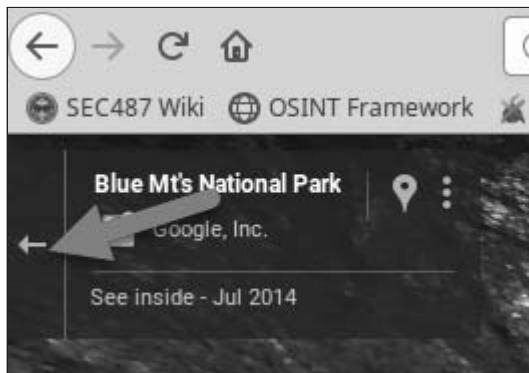
10. To view it closer, use the scroll-wheel or + sign on right of the window to zoom in or click on this link <https://sec487.info/z5>.



You found your coat!

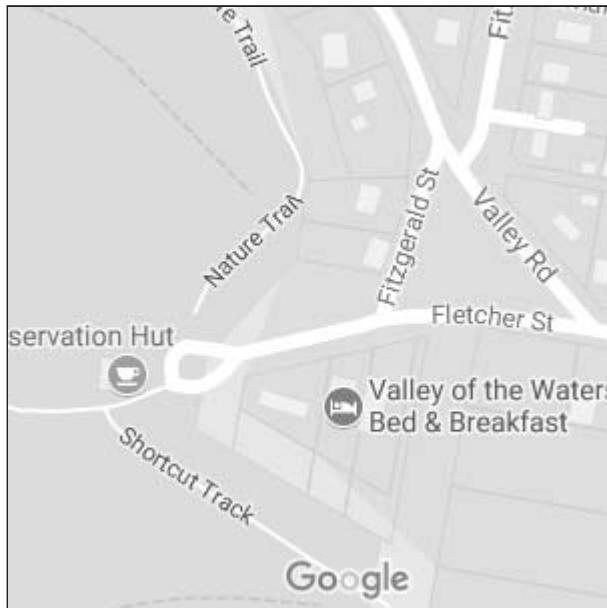
Map the distance traveled on your walk

1. For the next item, we need to leave the Street View images by clicking once on the left-facing arrow in the upper left of the window (shown below).

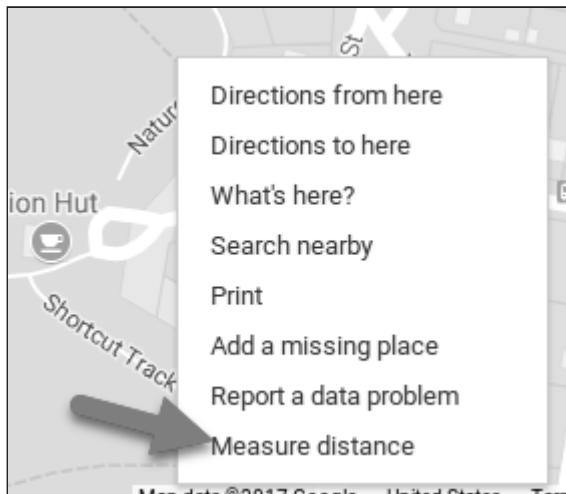


2. Click and drag the map until the Cathedral Point in the center of the Fletcher St circle, is near the bottom of the screen.

You may also need to zoom out a little bit to see more of the screen (shown below).

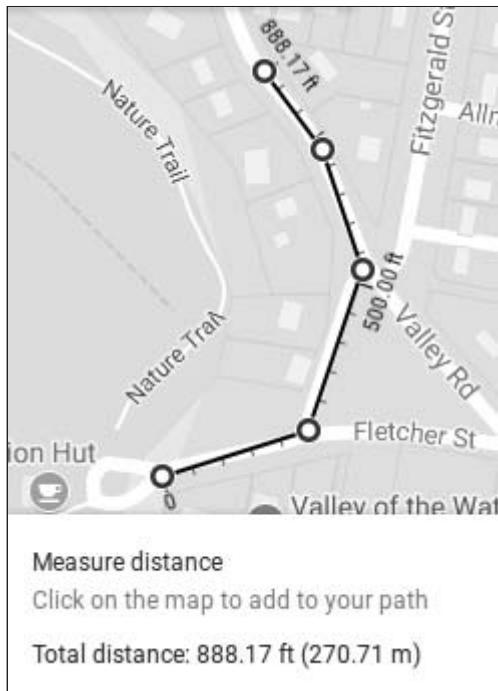


- To map the route you took to the POET'S COTTAGE Blue Mountains Tranquility on Valley Rd, right click at the Fletcher St circle and select the Measure Distance option from the menu.



- The next place you click on the map will be the second point. Click just to the right of the circle to begin.

After that, click one time on each segment of the track you took up to the Poet's Cottage. Each time you click on the screen, Google will place a marker and calculate the distance. We have done some of the work below. If you accidentally add a point, just click it to remove it or drag it to where you'd like it to be.

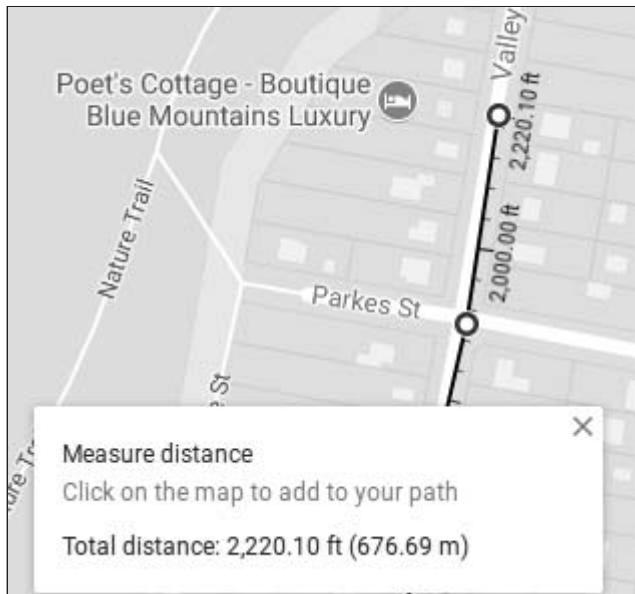


You will get to a point, as we did above, where you cannot go further north but need to.

- When this happens, click and drag the map down to reposition it.

This step might be challenging using a touch pad on a computer. If you have a mouse, try using that for this part.

You can then keep on measuring your distances. When you reach Poet's Cottage (you may need to zoom in to see it), you should have the total, rough distance you and your spouse walked. Who won the bet? We show that the walk would have been over 500 meters (roughly 676m).



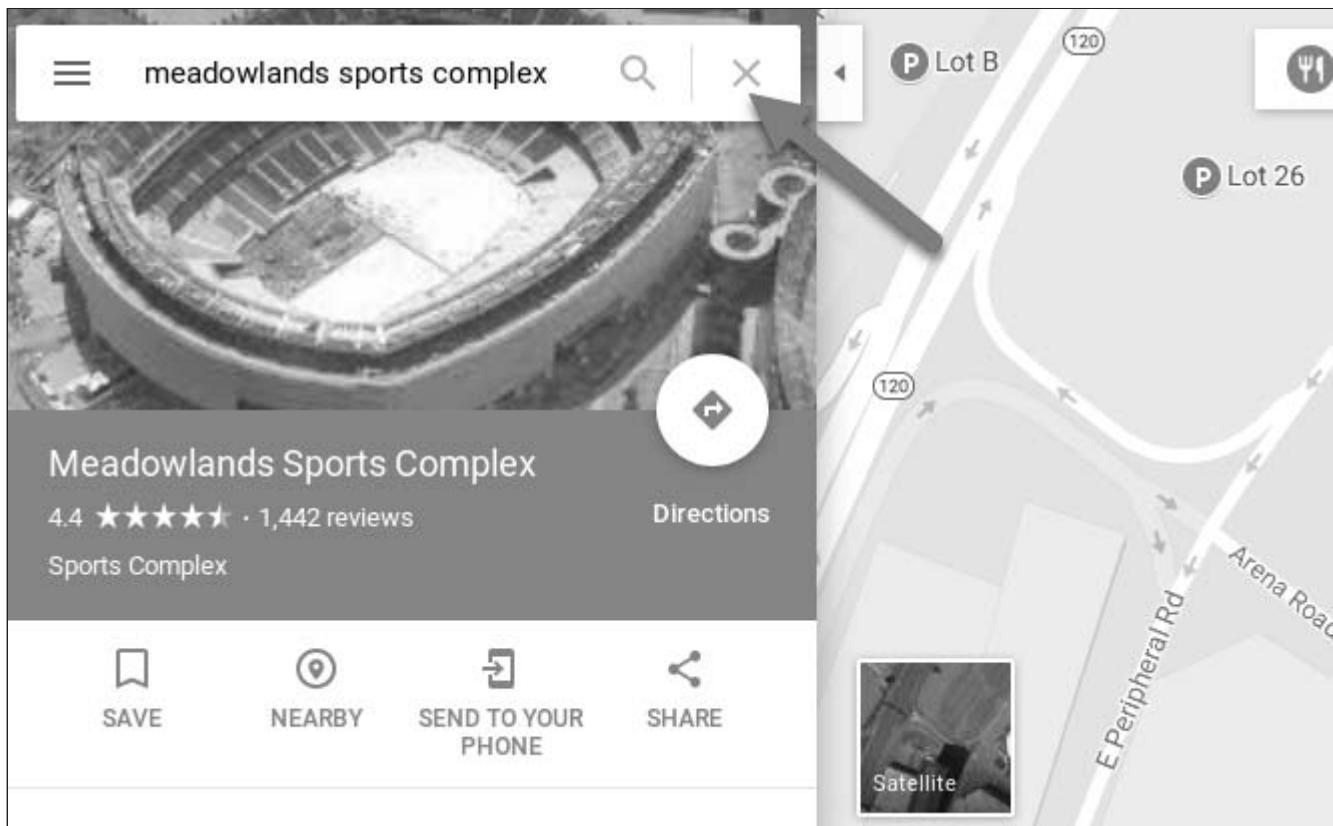
Looks like your partner was correct in that it was over a 500m walk.

- When finished measuring distance, click once on the X in the Measure Distance box to close it.

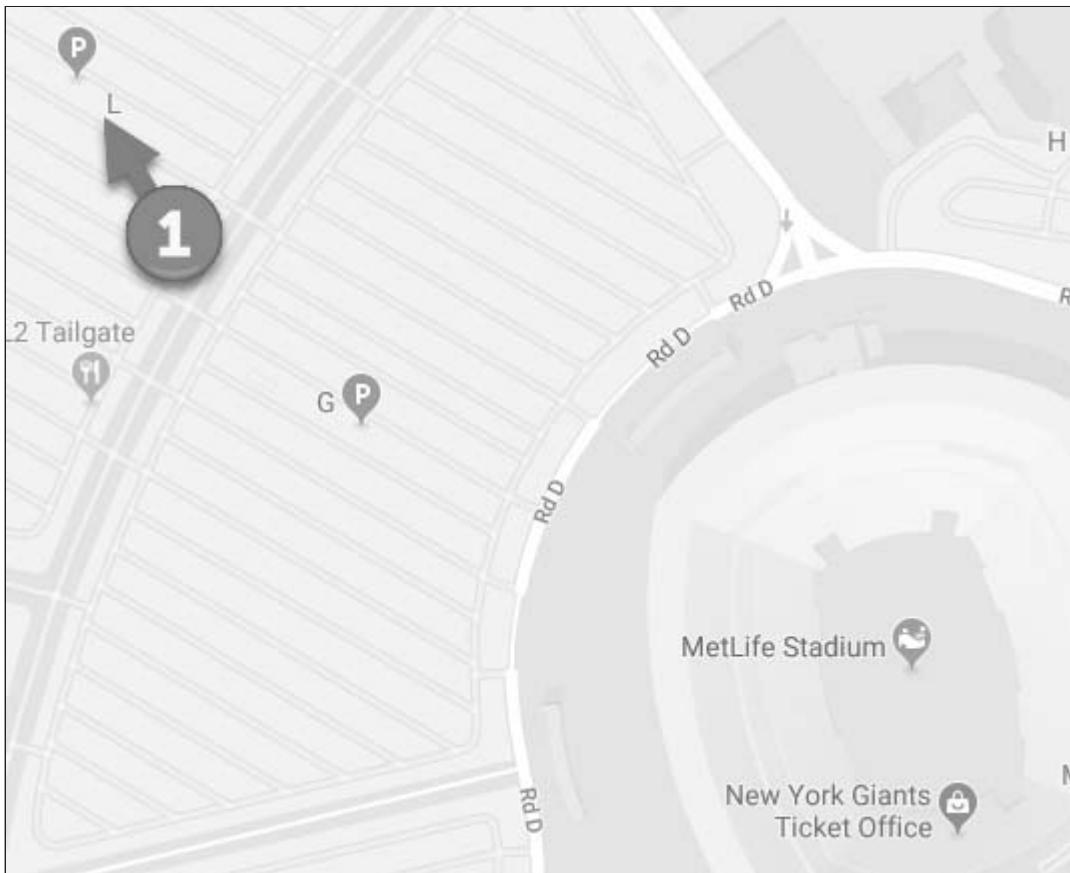
Find the photo sphere

We know that we need to move the view to the Meadowlands Sports Complex and look in parking lot L.

- In the Search Google Maps field, type: Meadowlands Sports Complex and press Enter.
- Once again, close the left pane by clicking the X (shown below) to give yourself more room.



3. Next, zoom out a little bit and locate Lot L (it should be a little bit to the north-west or left and above of the MetLife Stadium).



4. Your client mentioned a photo sphere, so we need to bring out the little person again and drag them over to lot L.

This should show a single photo sphere near the L2 Tailgate.

5. Drop the yellow figure onto that photo sphere.



6. Click and drag the image around to turn your view until you see the green VW Bug car.
7. This is the target. Zoom in and write down the plate number in your notes.



That should help locating the friend. When you have recorded the information, click the arrow to close the Street View content.

[CHALLENGE] Find the vehicle's details

Your target is 6.08 km (direct, not on roads) south west of the GPS coordinates -52.426963,-71.4156355 where there is a photo sphere. What is the manufacturer name and license plate number of the truck you see in it?

You know how to measure distances and to use photo spheres. Use these skills to get that truck license plate number.

[CHALLENGE] Portuguese Navy Ships

- Measure the 3 ships in the center of <https://www.google.com/maps/search/portugal+naval+base/@38.6690383,-9.1467065,223m/data=!3m1!1e3>
- If you want to use Chrome, you can use Google's 3D view to get better look <https://earth.google.com/web/@38.6690991,-9.14644627,2.27092704a,154.48604703d,35y,41.93770626h,49.14000346t,0r>.

Answers



Click Here to See Our Findings



Green, VW Bug

- License Plate: AH-84264
- State: Connecticut

Challenge!

Vehicle south west of the GPS coordinates on Y-460 road

Short URL to the location: <https://sec487.info/gd>

- Manufacturer: Rexton
- Plate number: FH-CP-79 (Chile)



Portuguese Navy Ships

- Visit the Wikipedia page for Portuguese Navy Ships [https://en.wikipedia.org/wiki/
List_of_active_Portuguese_Navy_ships](https://en.wikipedia.org/wiki/List_of_active_Portuguese_Navy_ships)
- Top ship is a Bartolomeu Dias-class frigates (based upon its length of ~123m long and its deck configuration)
- Bottom 2 ships are Vasco da Gama-class frigates (based upon their lengths ~116m long and deck configurations with dual stacks)

This page intentionally left blank.

Location Challenge

Table of Contents



- Objectives
- Goals
 - Targets
 - Flags
- Preparation
- Instructions

Objectives

- Find as many flags as you can about a location

Goals

1. Choose one of the targets below
2. Using passive/non-interactive techniques, find as many of the flags as you can about the target
3. Score your results

Targets

Choose one to research. You are permitted to use a web browser to gather your data.

1. Wunstorf Air Force Base (52.455364,9.4293561)
2. Aerodrom Kubinka (55.6110862,36.6436147)
3. Langebaanweg Airforce Base (-32.9719977,18.1546452)

4. PAF Base, Nur Khan (33.6126228,73.0959173)

Flags

1. What is the length of the longest runway that you can see from Google Maps?
2. How many aircraft can you count in the aerial imagery of that location on <https://bing.com/maps>?
3. How many aircraft can you count in the aerial imagery of that location on [https://www.google.com/maps/?](https://www.google.com/maps/)
4. Identify the number of each of the above aircraft and give their model name (for example: 11 Airbus A321 planes).
5. What are the runway numbers (found on each end of each runway)? You get 1 point for each runway combination (08-26)

Preparation

VPN if problems

Instructions

1. Select your target from the above list.
2. Using free and public internet sources, find the above "flags" about your target.
3. Record your activities in your favorite documentation application. If you do not have a favorite one, there is a spreadsheet in the VM's student home directory in the labs -> location-challenge directory.
4. This file can be opened using LibreOffice Calc application (similar to Microsoft Excel) from the menu system (arrows 1 and 2 below).



5. When finished, score your work. Give yourself 1 point for every validated flag (if you find multiples of a flag, each one gets an additional point so if you find 1 email address you get 1 point but find 3 of them and you get 3 points).

This page intentionally left blank.

Domains and IPs

Table of Contents

- Objectives
- Goals
- Preparation
- Answers

Objectives

- Retrieve DNS information using web pages and command line tools

Goals

Using the tools and techniques discussed in the courseware, answer the following questions:

1. What are the host/domain names of the DNS Name Servers for repubblica.it?
2. How many hostnames using the elgenero.com domain name start with server? (Example: server-mail.elgenero.com)
3. What company does the souq.com domain use for their email?
4. According to the <https://dnsdumpster.com/> site, how many souq.com hosts resolve to internal IP addresses? (Look for IP addresses starting with 10.)
5. How many IP addresses does the m.visir.is host resolve to?
6. What hosts are approved to send mail as the laprensa.com.ni domain (look for SPF records)?
7. What IP address did the crhoy.com domain resolve to in 2014-10-01 (October 1, 2014)?

Preparation

VPN if problems

Answers



Click Here to See Our Results



There are many methods to solve the challenges. Below are the results we obtained. Keep in mind that the results you see on your screen may be in a different order from what you see below.

1. dig -t ns repubbl i ca. i t

```
; ANSWER SECTION:  
repubbl i ca. i t.      21599  IN  NS  ns-1477.awsdns-56.org.  
repubbl i ca. i t.      21599  IN  NS  ns-1541.awsdns-00.co.uk.  
repubbl i ca. i t.      21599  IN  NS  ns-353.awsdns-44.com.  
repubbl i ca. i t.      21599  IN  NS  ns-723.awsdns-26.net.
```

2. cd /opt/tools/dnsrecon; ./dnsrecon.py -d el genero. com -t brt -D subdomains-top1million-5000.txt (We removed the other hosts found from the output below to make it more readable)

```
[*] A server. el genero. com 50.23.113.243  
[*] A server1. el genero. com 185.152.66.199  
[*] A server2. el genero. com 185.152.66.199  
[*] A server3. el genero. com 198.23.103.73  
[*] A server4. el genero. com 198.23.103.73  
[*] A server5. el genero. com 198.23.103.73
```

3. dig +noall +answer -t mx souq. com

```
souq. com.      21576  IN  MX  1 aspmx.l.google.com.  
souq. com.      21576  IN  MX  2 alt1.aspmx.l.google.com.  
souq. com.      21576  IN  MX  3 alt2.aspmx.l.google.com.  
souq. com.      21576  IN  MX  4 aspmx2.googlemail.com.  
souq. com.      21576  IN  MX  5 aspmx3.googlemail.com.
```

Google!

4. Our results are below.

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

checkout-service.prod.souq.com	172.29.214.150
api1.post.staging.souq.com	10.10.65.143
stg3.post.staging.souq.com	10.10.65.143
api3.post.staging.souq.com	10.10.65.143
stg4.post.staging.souq.com	10.10.215.7
voc.post.staging.souq.com	10.10.65.143
cs.post.staging.souq.com	10.10.65.143



5. dig m.visir.is

```
; ANSWER SECTION:
m.visir.is.      1527    IN  A   96.45.82.142
m.visir.is.      1527    IN  A   96.45.82.18
m.visir.is.      1527    IN  A   96.45.83.249
m.visir.is.      1527    IN  A   96.45.83.23
```

6. dig -t txt laprensa.com.ni

```
; ANSWER SECTION:
laprensa.com.ni. 299 IN  TXT "v=spf1 ip4:190.212.136.182/32
include:_spf.google.com
include:mail.zendesk.com
include:servers.mcsv.net
include:spf.mandrillapp.com ~all"
```

Or, using <https://centralops.net/co/>:

laprensa.com.ni	IN	TXT	v=spf1 ip4:190.212.136.182/32 include:_spf.google.com include:mail.zendesk.com include:servers.mcsv.net include:spf.mandrillapp.com ~all
laprensa.com.ni	IN	SPF	v=spf1 ip4:190.212.136.182/32 include:_spf.google.com include:mail.zendesk.com include:servers.mcsv.net include:spf.mandrillapp.com ~all

7. According to the <https://securitytrails.com/domain/Crhoy.com/history> a site, for that date (number 1 in the image), the IP addresses were (number 2 below):

<p>198.41.191.133 ↗ 198.41.190.133 ↗ 198.41.189.133 ↗ 198.41.188.133 ↗ 198.41.187.133 ↗</p>	2	2014-09-30 (5 years ago)	2014-10-29 (5 years ago)	29 days
	1			

Domain Challenge

Table of Contents

- Objectives
- Goals
 - Targets
 - Flags
- Preparation
- Instructions

Objectives

- Find as many flags as you can about a domain name on the Internet

Goals

1. Choose one of the targets below
2. Using passive/non-interactive techniques, find as many of the flags as you can about the target and document where you found each flag (URL)
3. Score your results

Targets

Choose one to research. DO NOT SCAN OR RUN ANY TESTING TOOL AGAINST THE TARGET. You are permitted to use a web browser to gather your data.

1. giac.org
2. eccouncil.org

3. isc2.org
4. crest-approved.org

Flags

1. Current IPv4 address(es)
2. Current IPv6 address(es)
3. Past IP addresses
4. The DNS Name Server(s) that handles the domain (IP and domain name)
5. What is the country the domain hosted in?
6. Record 5 sub domains of the domain (you get 1 point for every 5 subdomains you find)
7. Is the domain or IP black listed on SPAM lists? If so, which?
8. Has the domain ever hosted or been associated with malware?
9. What is the registrar for the domain in Whois?
10. What web server is running on the domain?
11. What are the prior web server software that this domain has used?
12. Are they using a CDN (Content Delivery Network) for the web site?
13. Is there a Google Analytics code in the web site? If so, what other sites use it?

Preparation

VPN if problems

Instructions

1. Select your target from the above list.

2. Using free and public Internet sources, find the above "flags" about your target.
3. Record your activities in your favorite documentation application. If you do not have a favorite one, there is a spreadsheet in the VM's student home directory in the labs -> domain-challenge directory.
4. This file can be opened using LibreOffice Calc application (similar to Microsoft Excel) from the menu system (arrows 1 and 2 below).



5. Remember to record the location or URL where you found the information.
6. When finished, score your work. Give yourself 1 point for every validated flag (if you find multiples of a flag, each one gets an additional point so if you find 1 email address you get 1 point but find 3 of them and you get 3 points).

This page intentionally left blank.

Wireless OSINT

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Map the addresses of wireless networks
 - Determine the time frames
 - Come up with final recommendations

Objectives

- Use the Wigle.net web site to research wireless networks
- Use online mapping sites to geolocate points

Goals

Your company was hired by a law firm to piece together information from the phone of a client (the "subject") in Pittsburgh, Pennsylvania. They would like you to use OSINT to validate the alibi of the client. The firm's client reported that they had no minutes left on their monthly cell phone plan, so they only used wireless networks on the day in question.

The story the client told the law firm was that, around 11:30p on a Friday night, they drove from a friend's home at The Cork Factory Lofts building home, using the fastest path. The subject rents a room with "Mr. and Mrs. Bell" (no address provided) and he said Mr. Bell remembered hearing the subject open the door to his house at 1:00a and then go to his room.

The law firm managed to get a forensics dump of the data on the subject's cell phone. In that content, they found two wireless networks (SSIDs) that the subject's phone connected to during these time periods. They are below.

1. Apple Network 5c4ebf
2. 07B407579076

Your goals:

1. Map the street addresses of these wireless networks and what buildings are at each location.
2. Determine if the time frames of the story are plausible by mapping directions to each of the locations.
3. Come up with final recommendations for the law firm.

Preparation



Step-by-step instructions

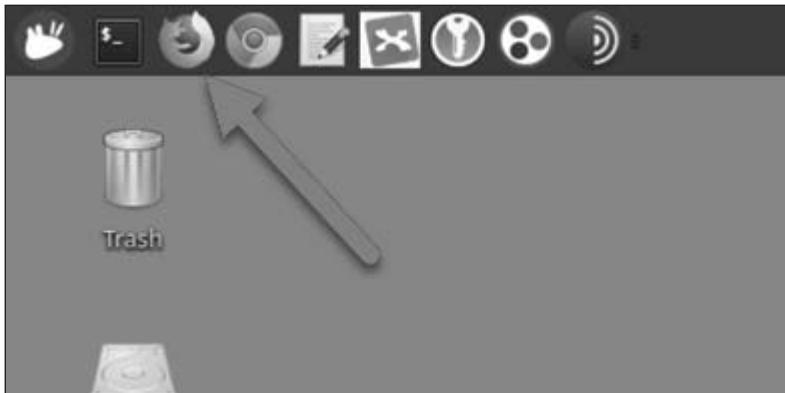
Map the addresses of wireless networks

For this work, you will need to register for a WiGLE.net account so you can search for the specific networks in their system. You can then perform the searches, discover the latitude and longitude coordinates, map those on a mapping application and determine what buildings are at those locations.

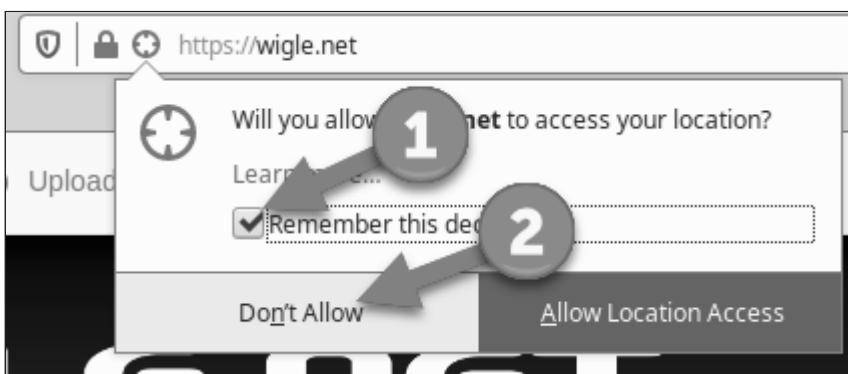
Documentation Tools

Consider using a MindMap and/or a new Hunchly case to track your work in this lab. If you choose to use Hunchly, use the Chrome browser for the lab instead of Firefox.

1. Your first step is to launch a Firefox window by clicking the Firefox icon in the menu bar.



2. Visit the <https://wigle.net> page in the browser.
3. When you do, the browser will most likely ask if WiGLE.net can access your location. You do not want this so click the Remember this decision box and then click Don't Allow.

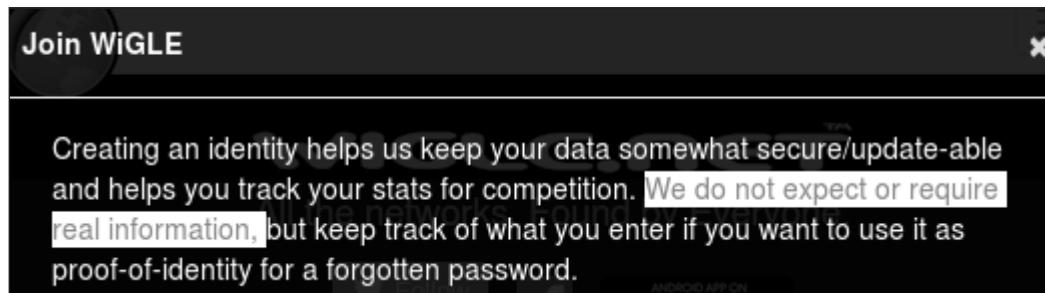


Now you need to create an account on their system. On the right side of the browser window is the Login link.

4. Mouse over the Login link and a drop-down menu appears.
5. At the bottom of the menu is the Register option. Click the Register link.



The WiGLE site owners understand many of us might try to use a fake identity to make the WiGLE.net user account. See the highlighted data from the registration page below.

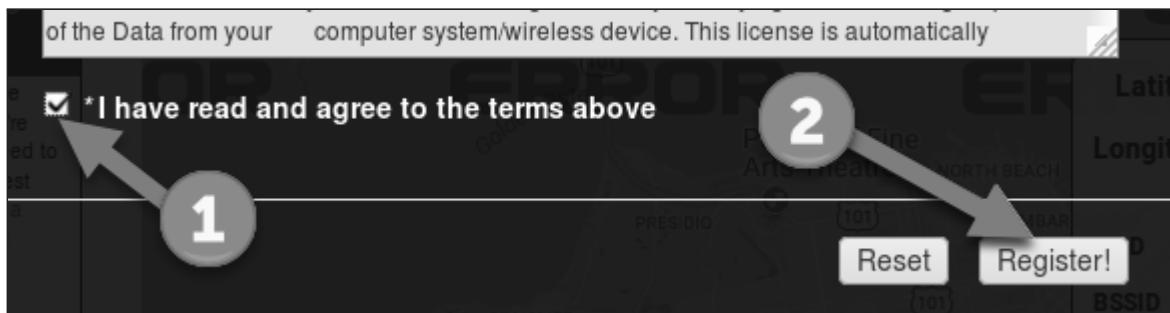


So, you do not need to use a real email address, or names? You are free to do so if you would like but we recommend using something more anonymous. The example.com domain is one that no one can use as a real domain for web services or email. Consider using that for the email address domain (e.g., whateveryouwant@example.com).

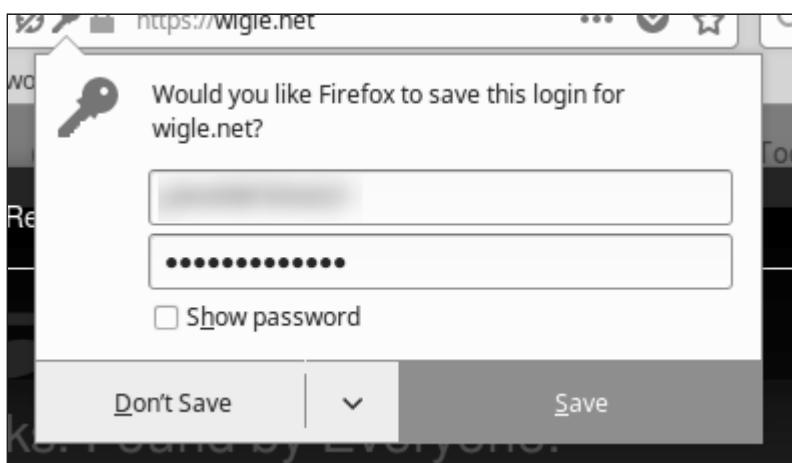
6. On the registration page, enter an email, user name, and password.
7. You will then need to complete the CAPTCHA (I'm not a robot box) before they will allow you to save the account.

Each CAPTCHA is different. Follow the directions on the screen to click on the cars or signs or whatever it asks you to click on.

- Once the CAPTCHA is completed, scroll down the page and check the I have read and agree to the terms above box then press the Register! button.



The browser may ask if you want it to remember your user name and password. Choose whether you do or do not and select the appropriate button.



Now you should be logged into WiGLE.net. Congrats! You are now prepared to perform detailed searches on the site. All the search forms are in the View menu button at the top of the screen.

- Mouse over the View button and then click on the Advanced Search option.



Since the law firm (in the scenario) provided us the names of the wireless networks, we can perform an "SSID/Network Name (exact match)" search. The first network was `Apple Network 5c4ebf`. Enter this content in that field and press Enter.

The screenshot shows a search interface with the following fields:

- Minimum data quality:** 0
- Encryption status:** (dropdown menu)
- BSSID/MAC:** 0A:2C:EF:3D:25:1B or 1st 3 Octets: 0A
- SSID / Network Name (exact match):** Apple Network 5c4ebf (highlighted with a red arrow)
- SSID / Network Name (wildcards¹: % and _):** foobar%
- Must Be a FreeNet** (checkbox)
- Must Be a Commercial Pay** (checkbox)

10. To view the results, scroll down in the window.

You should see a result (shown below). The details of this network are:

- Network ID (or BSSID): 00:11:24:5C:4E:BF
- SSID: `Apple Network 5c4ebf`
- The first and last seen dates are shown.
- It is not using encryption.
- Latitude, Longitude: 40.45509338, -79.98260498

The screenshot shows a table with the following data:

<< showing records 1 to 1 >>								
Map	Net ID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long
map	00:11:24:5C:4E:BF	Apple Network 5c4ebf	infra	2005-12-28T10:00:00.000Z	2011-05-03T22:00:00.000Z		40.45509338	-79.98260498

11. Click the Net ID link to view details (shown below).

Computed Network Properties

Network ID	
Type	
QoS	0
Cell Attributes	
SSID	Apple Network 5c4ebf
Est. Latitude	40.45509338
Est. Longitude	-79.98260498
First Seen	2005-12-28T18:13:31.000Z
Most Recently Seen	2011-05-04T05:26:57.000Z
comment	

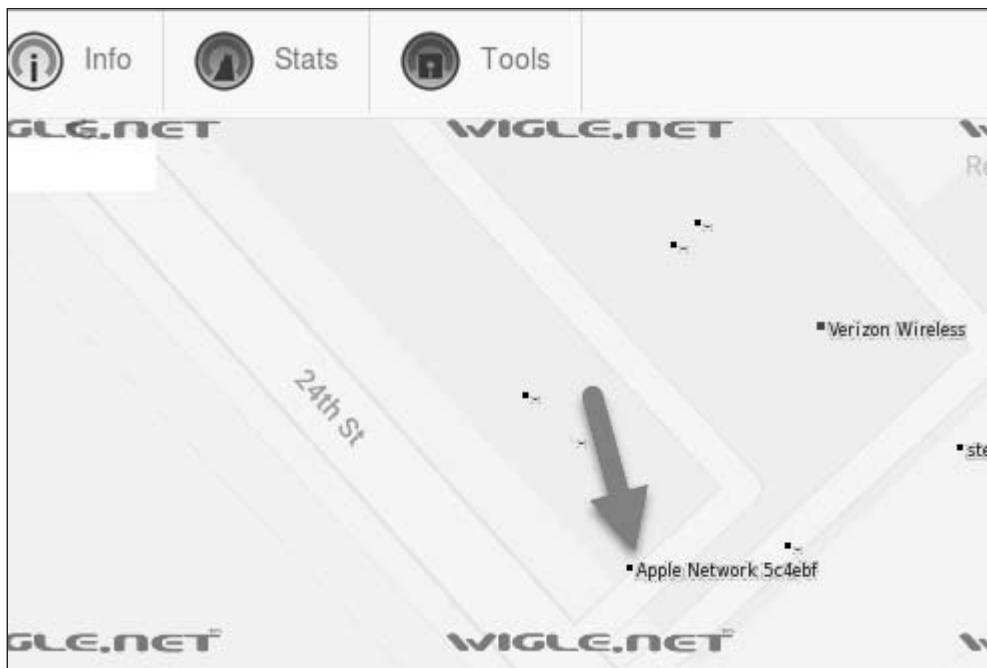
Map data ©2017 Google

Different Views

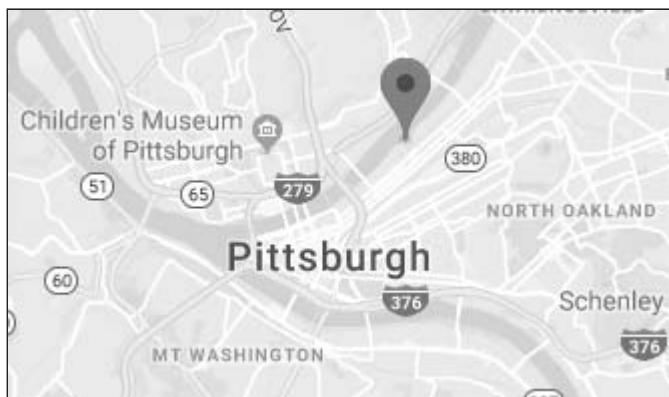
Your web page may look like the one below (not automatically showing to Google map). If it does, click the "Loading..." link and it will take you to the Google Map (shown in the picture below).

Network ID	Loading...
Type	
QoS	0
Cell Attributes	
SSID	Apple Network 5c4ebf

This is what the page will look like once you click the Loading... link or the map.



Zoom in and out until you see a bigger portion of the map and you will see the GPS location is around The Cork Factory Lofts; the location given by the subject for the place he met his friend. If you want, take the latitude and longitude and paste it into the Google Maps tab to confirm that this location is in Pittsburgh, PA. The image below confirms that it is in Pittsburgh.



Since that location corroborates with the building given by the subject, we can move on to the second network.

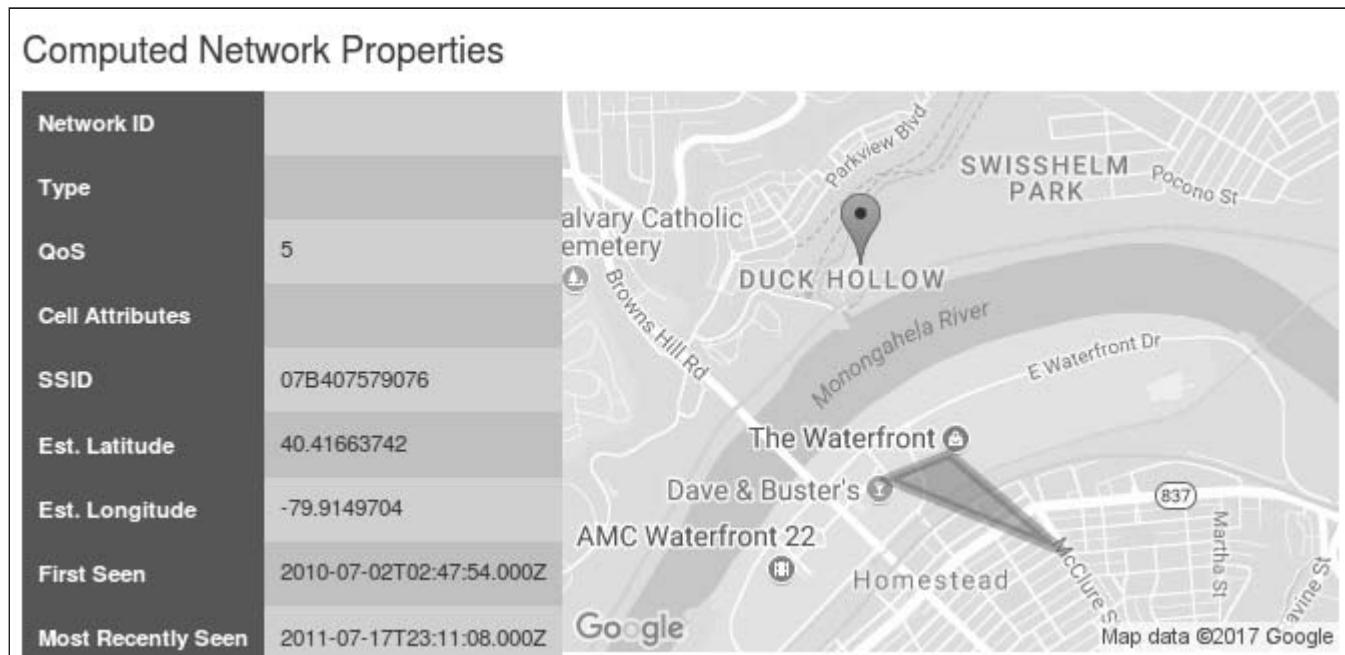
12. Switch back to the WiGLE.net tab, mouse-over the View icon and selecting the Advanced Search, and then type the 07B407579076 into the correct search field and press Enter.
13. To view the results, scroll down in the window.

You may see the result shown below. The details of this network are:

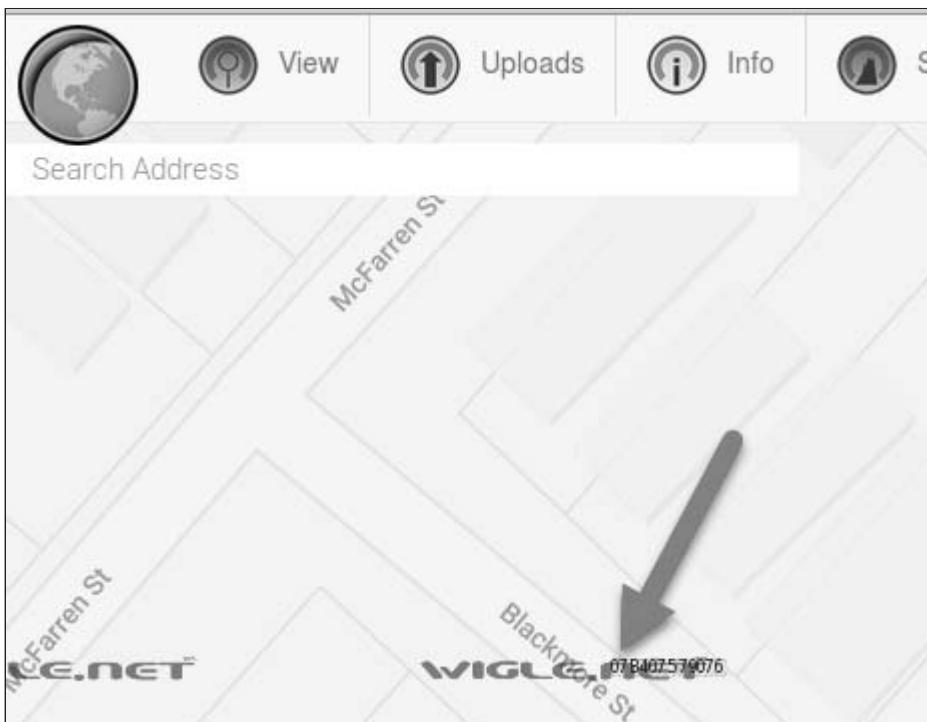
- Network ID (or BSSID): 00:12:0E:83:F4:C9
- SSID: 07B407579076
- The first and last seen dates are shown.
- It was using WEP encryption.
- Latitude, Longitude: 40.41663742, -79.9149704

WiGLE Network Search Results									
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long
map	00:12:0E:83:F4:C9	07B407579076		infra	2010-07-01T19:00:00.000Z	2011-07-17T16:00:00.000Z		40.41663742	-79.9149704
more results									

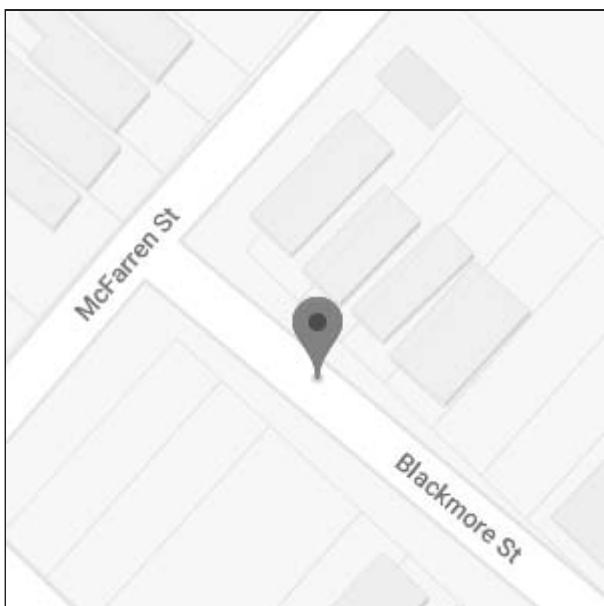
If your web page has loaded the Google map view, then you may see a gray triangle instead of a single point. This is because the signal from this network was discovered in several places. WiGLE does its best to geolocation the source using these data points.



If your web page just shows the "Loading..." page (as shown above), click that link to see the Google map of the network.



14. Take the latitude and longitude and paste them into the Google Maps tab in your browser to check the address. You will need to zoom in to see the street names (below).



The subject said he rents a room from Mr. Bell (no address provided). Let's see if any of these houses might be owned by a Mr. Bell. Don't worry if the house that Mr. Bell owns is not right in front of the latitude and longitude plot point. Remember that geolocation of wireless network signals is, in general, not precise when performed from war-driving.

15. In the Google Maps page, left click once on the house at the corner of McFarren St and Blackmore St (shown below).



16. Open a new browser tab and visit <https://www.google.com>

We will take the last name of the possible home owner "Bell" and combine it with the approximate address of the wireless network.

17. In the search field, type: `bell 134 blackmore st Pittsburgh PA 15217` and press enter.

Out of the results, the one from the www.city-data.com site (shown as the second result below) is what we are looking for as it contains the address and the word "Bell". In your results, you may need to scroll down the page to find it. If you do not see it, visit the <https://sec487.info/cm> URL in your browser as that is a direct link to the data.

bell 134 blackmore st Pittsburgh PA 15217

All Shopping Maps Images News More Settings To

About 108,000 results (0.73 seconds)

Blackmore St, Pittsburgh PA - Rehold Address Directory
<https://rehold.com> › Pennsylvania › Pittsburgh, PA › Blackmore Street ▾
On 6-200 Blackmore St, Pittsburgh PA we have 25 property listings for the 76 residents and businesses.
The average home sale price on Blackmore St has been \$34k. 6. Blackmore St, Pittsburgh, PA 15217.
Lot/Land. 3 beds1 bathLot: 2,342 sqftBuilt in 1900. Residents, Crime, Phone, More Information. Paul R
Harakal, (412) ...

Property valuation of Blackmore Street, Pittsburgh, PA: 111 (LEONA ...
www.city-data.com › ... › Allegheny County, PA property tax assessment data ▾
134 Blackmore Street Pittsburgh, PA 15217. Find on map >> Show street view. Owner: GEORGE D
BELL & EILEEN R BELL Owner description: Regular-Etux Or Et Vir Fair market land value: \$25,700. Fair
market total value: \$41,400. County assessed value for land: \$23,400. County assessed value total:
\$23,400

18. Click on the link to visit the city-data.com site.
19. When you get to the site's page, scroll down the page to the "134" house number (shown below).

It looks like the house is owned by George D. Bell and Eileen R. Bell.

134 Blackmore Street
Pittsburgh, PA 15217
📍 Find on map >>
📸 Show street view
Owner: **GEORGE D BELL & EILEEN R BELL**
Owner description: Regular-Etux Or Et Vir
Fair market land value: \$25,700

With this data, we can say that the subject's phone seems to have visited both locations that he mentioned in his story.

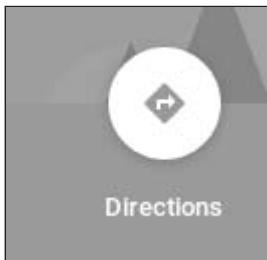
Determine the time frames

For this next section, we can use the Google Maps application again to map the routes between the locations to see estimated times for travel between them. We can use street addresses or latitudes and longitudes. Remember that the only time frame for travel we had from the story was that it took the subject 1.5 hours to get from The Cork Factory to Mr. Bell's home.

1. Switch back to the Google Maps tab in the browser, it should still be on Mr. Bell's home (40. 41663742, -79. 9149704).

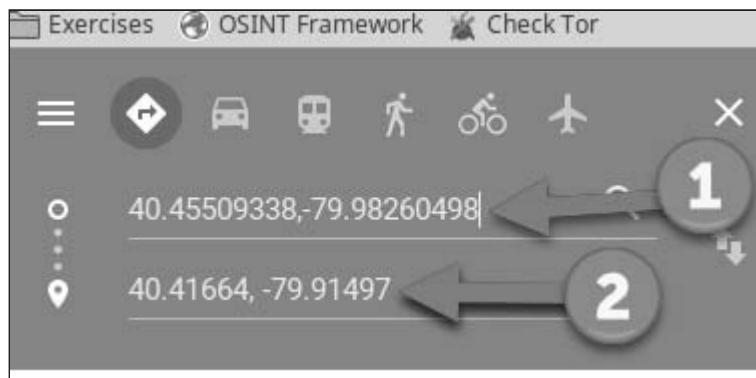
If you closed the tab or used it for other searches, perform a Google Maps search for this location.

2. Press the Directions button to start a route.



We will be working backwards. The last place the subject went was Mr. Bell's home from The Cork Factory (at 40. 45509338, -79. 98260498).

3. Paste the latitude and longitude of The Cork Factory into the Choose starting point... field and press enter.



The map should show the it takes about 15-20 minutes to drive from one to the other. If we wanted, we could change the "Leave now" option on the mapping site to "Depart at" 11:30p on a

Friday night to see if traffic is different at that time. What you will find is that it still takes 16-26 minutes to get to the destination using the fastest route. It took the subject 1.5 hours to travel this.

Come up with final recommendations

Wireless network geolocation from war-driving is not precise but we were able to confirm the locations the subject visited on the night in question. What was not confirmed was the amount of time that it took the subject to travel from The Cork Factory to Mr. Bell's home. There is a little over 1 hour of time that is unaccounted for. It could be that there was an accident or something delayed him. The law firm will want to question him about this.

1. This lab is completed. When finished, close the web browser.

Spiderfoot

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Use the Spiderfoot application
 - Analyze the Spiderfoot data

Objectives

- Gain experience in using the Spiderfoot recon framework tool
- Gather OSINT data about a domain

Goals

Your customer wants you to perform a custom, passive reconnaissance gathering effort on open source information about the possibly malicious IP address 120.50.8.2. They are looking for any online reports where this IP address was noted as being involved with sending spam, malicious traffic, and other cyber issues.

1. Using the Spiderfoot tool, run a custom, passive scan on the IP address 120.50.8.2.
2. Use 3 modules for this work:
 - Fortiguard.com
 - Internet Storm Center
 - Watchguard

3. Analyze the results and gather meaningful data to answer your customer's requests.

⚠ Scan Completion Time

Using the *Passive Use Case*, with all of its modules enabled, will take a while to run. Below, we chose to only enable a few modules to make the lab run faster. If you complete the lab quickly, try re-running the scan with the *Passive Use Case*.

Preparation

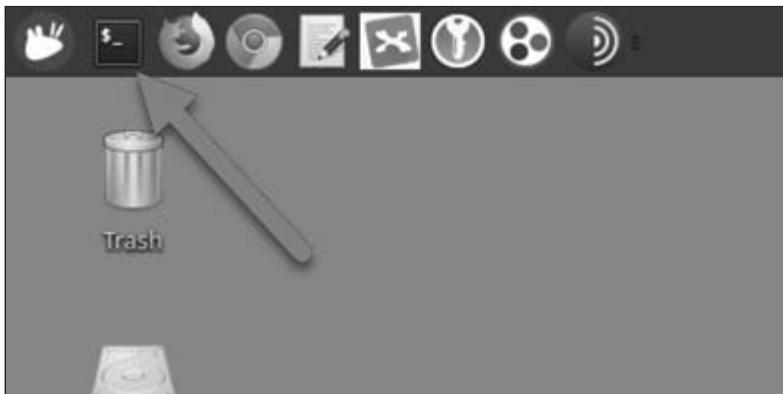
VPN if problems

Step-by-step instructions

Use the Spiderfoot application

Spiderfoot can find and collect huge amounts of data. You need to figure out what is useful and turn that data into intelligence.

1. Our first step is to launch a terminal window by clicking the icon in the menu bar.



2. In the terminal, change directories to the location where Spiderfoot is installed by typing: `cd /opt/tools/spiderfoot`

3. Then press Enter.

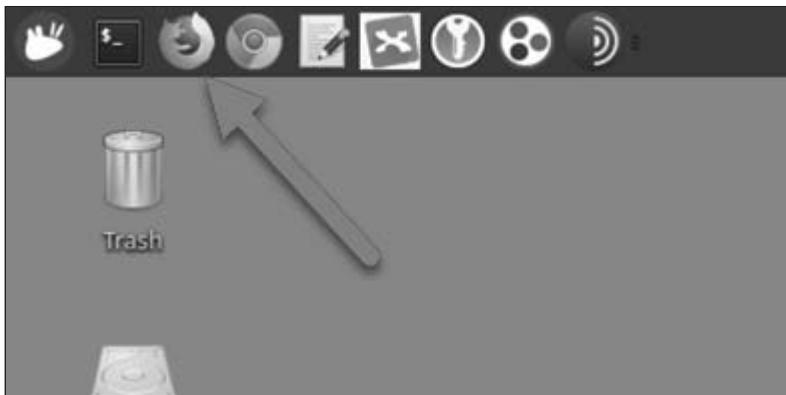
```
student@sec487 (21:06:08) : ~$ cd /opt/tools/spiderfoot/  
student@sec487 (21:06:22) : /opt/tools/spiderfoot$ █
```

4. To run the Spiderfoot server, type: ./sf.py and press Enter.

Your window will show the output of a variety of python commands (shown below) and that a web server was launched and is listening on http://127.0.0.1:5001 (arrow 1). The Spiderfoot user interface is at that web address.

```
student@sec487 (13:15:21) :/opt/tools/spiderfoot$ ./sf.py  
Attempting to verify database and update if necessary...  
Starting web server at http://127.0.0.1:5001 ...  
*****  
1  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://127.0.0.1:5001  
*****  
  
[02/Dec/2019:13:15:29] ENGINE Listening for SIGHUP.  
[02/Dec/2019:13:15:29] ENGINE Listening for SIGTERM.  
[02/Dec/2019:13:15:29] ENGINE Listening for SIGUSR1.  
[02/Dec/2019:13:15:29] ENGINE Bus STARTING  
[02/Dec/2019:13:15:29] ENGINE Serving on http://127.0.0.1:5001  
[02/Dec/2019:13:15:29] ENGINE Bus STARTED
```

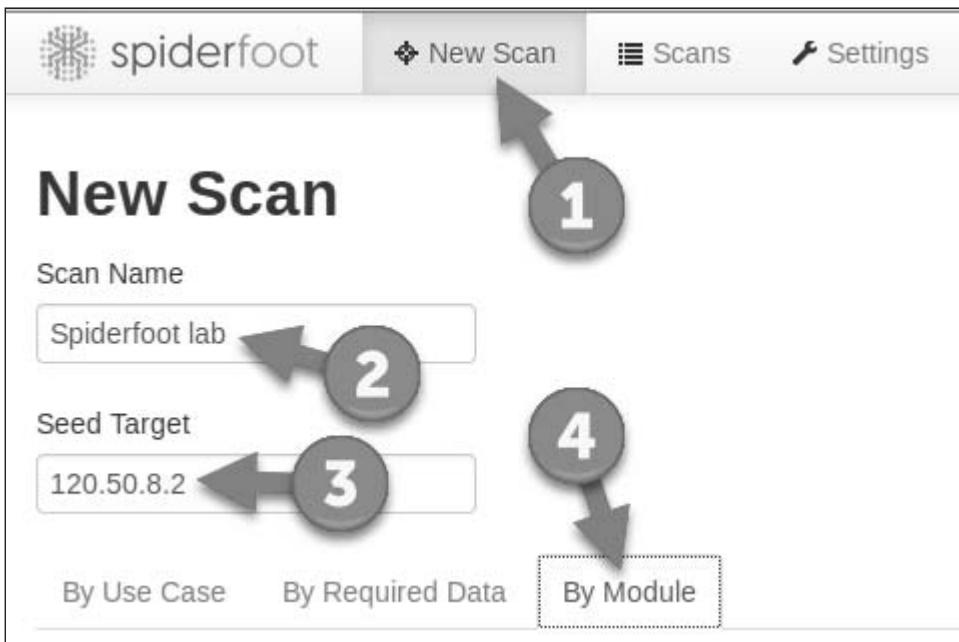
5. Launch a Firefox window by clicking the icon in the menu bar.



6. In the URL bar, type `http://127.0.0.1:5001` and press Enter to visit the Spiderfoot web interface.

There are many settings for you to browse through in the Settings tab. If you'd like to take a moment and look through it, you can.

7. To start a scan, click the New Scan button at the top of the window (arrow 1 below).



8. Enter a name for the scan (we chose to use "Spiderfoot lab") in the Scan Name field (arrow 2 above).

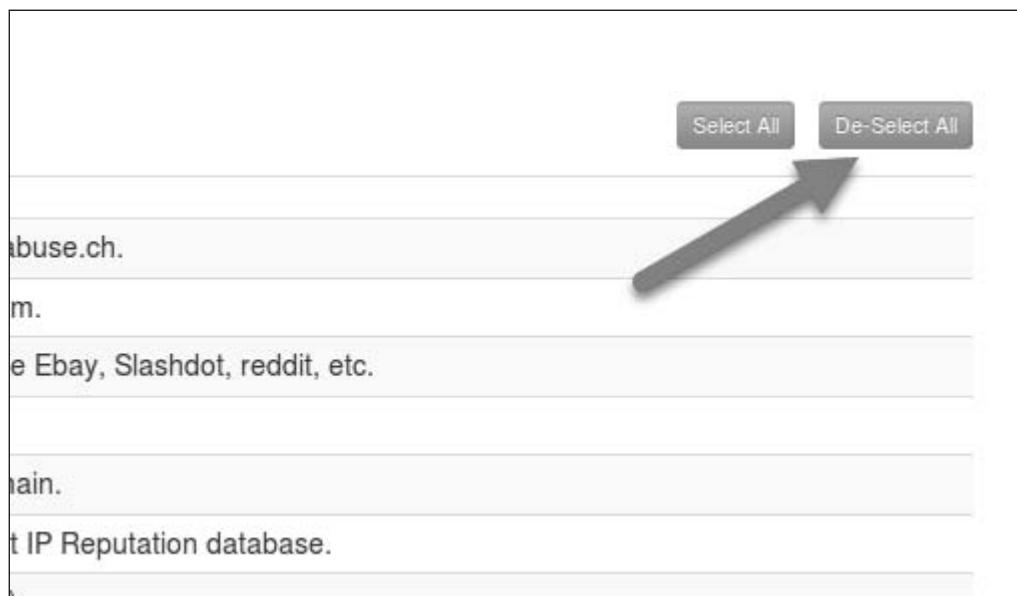
9. Next, enter the domain, IP or email address in the Seed Target field (arrow 3 above). Type:

120.50.8.2

We now need to select which modules to have Spiderfoot run against our target. The customer requested that this be a passive scan where you do not interact with the target domain's

systems. Spiderfoot happens to have a "Passive" use case that will run its modules that do not interact with the target domain or IP addresses. While you *CAN* use that, it will take longer to run than us enabling just a few strategic modules. We will take the faster approach for the lab and if you'd like to run the "Passive Use Case" understand it will take a lot longer to finish and you will have much more data to sort through.

10. Scroll down the screen and press the By Module hyperlink (arrow 4 above).
11. First thing you need to do is press the De-Select All button on the right of the section to uncheck all the module options (see below).



12. We will enable just a few modules for this lab to ensure it runs fast. Enable the following modules by clicking your mouse in the check box next to them (as shown below). Enable the following modules:

- Fortiguard.com
- Internet Storm Center
- Watchguard

spiderfoot	New Scan	Scans	Settings
<input type="checkbox"/> Errors	Identify common error messages in content like SQL errors, etc.		
<input type="checkbox"/> Ethereum Finder	Identify ethereum addresses in scraped webpages.		
<input type="checkbox"/> File Metadata	Extracts meta data from documents and images.		
<input type="checkbox"/> Flickr	Look up e-mail addresses on Flickr.		
<input checked="" type="checkbox"/> Fortiguard.com	Check if an IP is malicious according to Fortiguard.com.		
<input type="checkbox"/> Fraudguard 	Obtain threat information from Fraudguard.io		
<input type="checkbox"/> FullContact 	Gather domain and e-mail information from fullcontact.com.		

13. At this point, you are ready to start the scan by pressing the Run Scan button.

<input type="checkbox"/> Wigle.net 
<input type="checkbox"/> Wikileaks
<input type="checkbox"/> Wikipedia Edits
<input type="checkbox"/> XForce Exchange 
<input type="checkbox"/> Yahoo
<input type="checkbox"/> Yandex
<input type="checkbox"/> Zone-H Defacement Check
Run Scan

Note: Scan will be started immediately.

The web page then shifts to the "Status" page where you can see what the scan is doing and what data it has found.

The top portion contains overall graphs of the retrieved content and the status of the scan. In a longer scan, you can move between this graph and the findings. Your scan may have found more or less results than the one in this lab documentation depending upon what new sources sprung up and which older ones disappeared.



- To view the data Spiderfoot collected, let's scroll up to the top of the page and click on the orange segment above Malicious IP Address.

This will take your browser to the area of Spiderfoot where you can browse the data it collected. You can see in the picture below that the several modules found issues. Each has a URL that you can use to get more information.

Spiderfoot lab

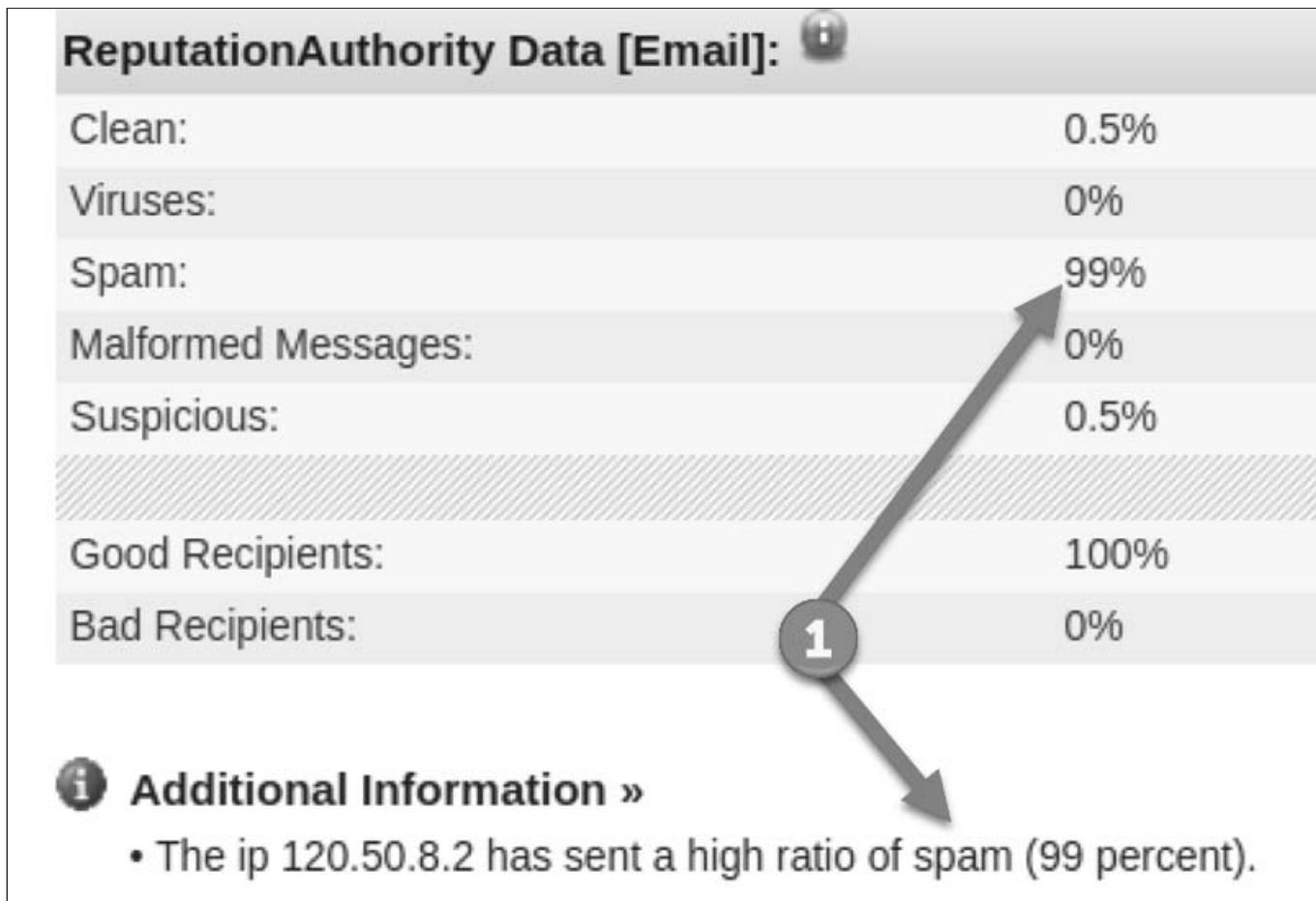
The screenshot shows the Spiderfoot lab interface with a table of data elements. The table has columns for Data Element, Source Data Element, and Source Module. Two rows are shown, each with a checkbox and a link. Arrows point to the links in both rows.

	Data Element	Source Data Element	Source Module
<input type="checkbox"/>	Internet Storm Center [120.50.8.2] https://isc.sans.edu/api/ip/120.50.8.2	120.50.8.2	sfp_isc
<input type="checkbox"/>	Watchguard Reputation Authority Lookup [120.50.8.2] http://reputationauthority.org/lookup?ip=120.50.8.2	120.50.8.2	sfp_watchguard

But all this Spiderfoot content is just data until you analyze it and ensure that it is relevant to our customer's query.

Analyze the Spiderfoot data

1. Open up each of the URLs that were in the results (the arrows in the image above) and look for anything that looks malicious that your customer may need to know about.
2. In our scan, we found the WatchGuard results ([http://reputationauthority.org/lookup?
ip=120.50.8.2](http://reputationauthority.org/lookup?ip=120.50.8.2)) contained evidence of several attacks coming from this IP address. What else can you find on that site? When did these attacks occur?



3. To quit the Spiderfoot program in the terminal window, press `CONTROL c`.
4. Then type: `exit` and press Enter.

Government Trivia

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Mississippi Lowe Brothers LLC
 - Matthew Johnson Frank
 - Aircraft Information
 - Lowe Brothers LLC.
 - Matthew Johnson Frank
 - Aircraft Information

Objectives

- Become comfortable using government sites to achieve OSINT goals

Goals

We have questions for you to find the answers to below. Using government web sites, discover and record your answers to the questions. For each trivia question, there may be more than one way to discover the answer (as happens in the real-world of OSINT assessments where you can gather data through many different sources).

1. In Mississippi, USA, two brothers created the Lowe Brothers LLC company.
 - What were their names?
 - When was the effective date when they registered for their company name?

- When was the paperwork for their company name filed?
2. There is a convicted sex offender named Matthew Johnson Frank in Alaska, USA.
- What is his date of birth?
 - What is the name of the last known city he lived in?
 - What crime was he convicted of on 3/9/2004?
3. For the aircraft identifier ("tail number") ZK-RKB :
- What type of aircraft is it (for example: a helicopter, plane, or something else)?
 - What is the model type and number of the aircraft?
 - What is the serial number of the aircraft?

Preparation

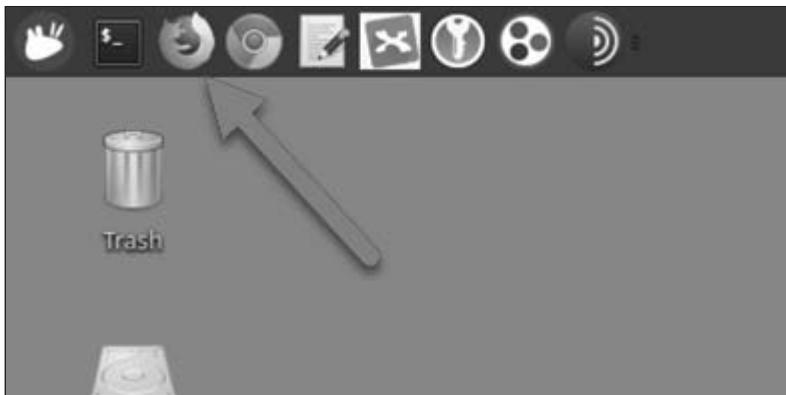
No VPN

Step-by-step instructions

For this lab, you only need our web browser and some way to keep track of notes.

Mississippi Lowe Brothers LLC

1. Our first step is to launch a Firefox browser window by clicking the Firefox icon in the menu bar.



Our challenge is to find business data for a company in Mississippi, United States. Companies can register to get a business license or send corporate filings to the state agency. So, let's use the DuckDuckGo.com web site to find the correct office.

2. Visit <https://duckduckgo.com> in the browser and type: mississippi business registration in the search field.



The results show the corp.sos.ms.gov domain that looks promising.

3. Click the link to the corp.sos.ms.gov result in DuckDuckGo (shown below). If you do not see this result, click on this link to be taken there <https://sec487.info/gg>.

The screenshot shows a search results page from a web browser. The search term 'mississippi business registration' is entered in the search bar. Below the search bar, there are filters for 'Web', 'Images', 'Videos', 'News', 'Maps', and 'Settings'. Underneath these, there are dropdown menus for 'All Regions', 'Safe Search: Moderate', and 'Any Time'. The main search results are displayed below, with the first result being 'Mississippi Secretary of State' with a link to <https://corp.sos.ms.gov/corp/portal/c/page/corpbusinessidsearch/portal.aspx>. There is also a long list of other links related to the Mississippi Secretary of State's website.

The resulting page shows a search field.

- Enter Lowe brothers LLC into the search field and click the Search button.

The screenshot shows the 'Business Search' interface. At the top, there are four search fields: 'Business Name', 'Business ID', 'Officer Name', and 'Registered Agent'. Below these is a section titled 'Search Criteria' with four radio button options: 'Starting with' (selected), 'All Words', 'Any Word', and 'Sounds Like'. A large search input field contains the text 'Lowe brothers LLC'. To the right of the input field is a 'Search' button. Two numbered arrows point to the search input field: arrow 1 points to the 'Starting with' radio button, and arrow 2 points to the 'Search' button.

The results that are produced should have an entry with a Business ID of 734832 (shown below). Get more details about that record by clicking the "Details" button on the far right.

The screenshot shows a table titled 'Business Name Search Results'. The columns are 'Business Name', 'Business ID', 'Type', 'Status', 'Create Date', and two 'Details' buttons. There are two entries in the table:

Business Name	Business ID	Type	Status	Create Date	
LOWE BROTHERS LLC	734832	Limited Liability Company (LLC)	Dissolved	06/10/2003	<button>Details</button>
Lowe Brothers Trucking LLC	1029996	Limited Liability Company (LLC)	Dissolved	10/22/2013	<button>Details</button>

The details screen brings up a window with many of the details you need to answer the questions above. Write this in your notes.

View Filed Documents	Opt-in or Opt-out of Email updates	Print Business Details
Name History		
Name LOWE BROTHERS LLC	Name Type Legal	
Business Information		
Business Type:	Limited Liability Company	
Business ID:	734832	
Status:	Dissolved	
Effective Date:	06/13/2003	
State of Incorporation:	Mississippi	
Principal Office Address:	NO PRINCIPAL OFFICE ADDRESS FOUND	
Registered Agent		
Name		
117 HOLLOWDEN LANE MADISON, MS 39110		
Officers & Directors		
Name	Title	
117 HOLLOWDEN LANE MADISON, MS 39110	Other	
129 MIDDLEFIELD DRIVE CANTON, MS 39046	Other	

As for when their business was created and filed, this page doesn't show. However, it looks like there may be additional information you can gather. Up at the top of the window, there is a View Filed Documents link that looks interesting.

5. Click the View Filed Documents link to view other documents.

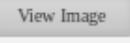
When you click the link, a box will drop down and reveal the Name Reservation Form that was submitted to the government in 2003.

LOWE BROTHERS LLC

User Actions

[View Filed Documents](#) [Opt-in or Opt-out of Email updates](#) [Print Business Details](#)

Filed Documents X

Type	Filed Date	Document
Failure to File AR	12/05/2011 11:59 PM	
Name Reservation Form	06/10/2003 12:00 AM	

Name History

You can find a variety of information about businesses, who owned them, when they were active, and where from these search areas in state government sites.

Matthew Johnson Frank

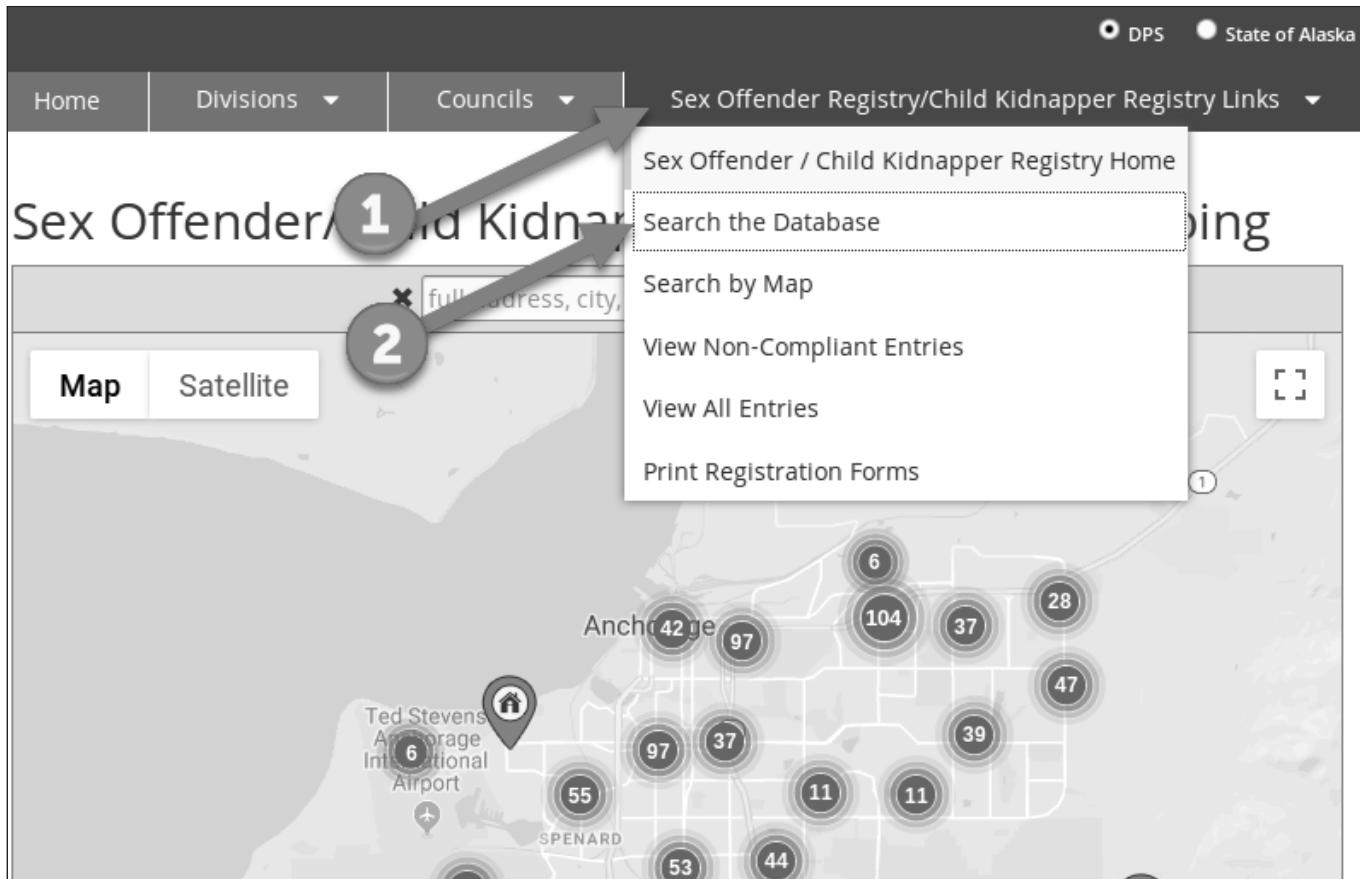
You know that Matthew John Frank is a sex offender in Alaska. Let's use the Bing search engine to find the Alaska sex offender registry.

1. In the URL field of your browser, visit <https://www.bing.com>.
2. In the search field type: al aska sex offender and click the search magnifying glass or press Enter.

You should see results such as the one displayed below. You see the Sex Offender Registry for dps.alaska.gov.



3. Click on the Sex Offender/Child Kidnapper Registry result. If you do not see this result, visit this link <https://sec487.info/gh>.
4. On the next screen, you will need to click on the Sex Offender Registry/Child Kidnapper Registry Links link on the top right of the page (arrow 1 below).



Choose the Search the Database from the drop down menu (arrow 2 above).

5. Enter `matthew` into the First Name field and `frank` into the Last Name and then click the Submit Query button.

The screenshot shows the search interface for the Sex Offender Registry/Child Kidnap Registry. The search parameters are set to "First Name: matthew" and "Last Name: frank". Other fields like Address Type, Zip Code, and City are set to "All Types", "All Cities", and "All Cities" respectively. There are "Reset" and "Submit Query" buttons at the bottom.

There should be a single result that is returned (below).

Name	Zip Code	Compliant (Y/N)
FRANK, MATTHEW JOHNSON	99680	Y

Showing 1 to 1 of 1 entries

Previous 1 Next

6. To get details on the entry, click the FRANK, MATTHEW JOHNSON link.

The questions you need to answer are below. You should be able to find the answers on the page. Record this data in your notes.

Race: INDIAN (AMERICAN OR ALASKAN NATIVE)	Sex: MALE																		
Hair: BLACK	Eyes: BLACK	Height: 5' 11"	Weight: 220 Lbs.																
Date of Birth:	Employer: TCSA ELECTRIC CO																		
02/09/1966																			
Address Info: <div style="text-align: center; margin-bottom: 10px;"> 1 </div> <table> <tr> <td>Employer Address:</td> <td>POWER PLANT</td> <td>Last Updated:</td> <td>03/15/2017</td> </tr> <tr> <td>City: TUNTUTULIAK</td> <td>State: AK</td> <td>Zip:</td> <td>99680</td> </tr> <tr> <td>Residential Address:</td> <td>2ND HOUSE - UPPER VILLAGE</td> <td>Last Updated:</td> <td>03/20/2018</td> </tr> <tr> <td>City: TUNTUTULIAK</td> <td>State: AK</td> <td>Zip:</td> <td>99680</td> </tr> </table> <div style="text-align: center; margin-top: 10px;"> 2 </div>				Employer Address:	POWER PLANT	Last Updated:	03/15/2017	City: TUNTUTULIAK	State: AK	Zip:	99680	Residential Address:	2ND HOUSE - UPPER VILLAGE	Last Updated:	03/20/2018	City: TUNTUTULIAK	State: AK	Zip:	99680
Employer Address:	POWER PLANT	Last Updated:	03/15/2017																
City: TUNTUTULIAK	State: AK	Zip:	99680																
Residential Address:	2ND HOUSE - UPPER VILLAGE	Last Updated:	03/20/2018																
City: TUNTUTULIAK	State: AK	Zip:	99680																
Alaska Convictions <div style="text-align: right; margin-top: 10px;"> 3 </div> <table> <tr> <td>Court Docket Number: 4BE-03-431</td> <td>Court: DISTRICT COURT BETHEL</td> </tr> <tr> <td>Conviction Date: 03/09/2004</td> <td>Offense Date: 08/10/2002</td> </tr> <tr> <td>Statute: AS11.41.425(A)(1)(C)</td> <td>Description: Attempted Sexual Assault 3</td> </tr> </table>				Court Docket Number: 4BE-03-431	Court: DISTRICT COURT BETHEL	Conviction Date: 03/09/2004	Offense Date: 08/10/2002	Statute: AS11.41.425(A)(1)(C)	Description: Attempted Sexual Assault 3										
Court Docket Number: 4BE-03-431	Court: DISTRICT COURT BETHEL																		
Conviction Date: 03/09/2004	Offense Date: 08/10/2002																		
Statute: AS11.41.425(A)(1)(C)	Description: Attempted Sexual Assault 3																		

- What is his date of birth?
- What is the name of the last known city he lived in?
- What crime was he convicted of on 3/9/2004?

Aircraft Information

You have the aircraft registration code for an aircraft and you need to figure out some details about it. There are many paths to figuring this out. You will walk through one below. Let's start by figuring out what country the "ZK" registration is for.

- In a browser tab, visit <https://www.google.com>
- When that page comes up, type: `aircraft registration zk` and then click the Google Search button.

Google search results for "aircraft registration zk":

- List of aircraft registration prefixes - Wikipedia**
https://en.wikipedia.org/wiki/List_of_aircraft_registration_prefixes ▾
This is a list of aircraft registration prefixes used by civil aircraft: Contents. 1 Current (post-1928) ZK-RB*, ZK-RC*, ZK-RD* gyrocopters; ZK-Q** marks are prohibited by ICAO; Remainder for fixed-wing aircraft From 1921 until 1929, G-NZ.
Current (post-1928 ... · Pre-1928 allocations
- Aircraft registration - Wikipedia**
https://en.wikipedia.org/wiki/Aircraft_registration ▾
An aircraft registration is a code unique to a single aircraft, required by international convention to VH-Uxx, then immediately expanded to all VH-xxx marks. New Zealand: G-NZxx to ZK-Zxx, then immediately expanded to all ZK-xxx marks.
Choice of aircraft registry · Country-specific usage · Decolonisation and
- Aircraft Registration Country Codes / Prefixes**
aircraft-registration-country-codes.blogspot.com/ ▾
International aircraft registration numbers in terms of country prefixes: list both prefixes and ... Z - Zimbabwe; Z3 - Macedonia; ZA - Albania; ZK - New Zealand ...

Your results may look similar or different as Google's results change over time. You could visit these pages OR just look at the information that they share with Google to see that the registration code ZK belongs to New Zealand (arrow 1 in image above).

With this information, you can head to the New Zealand government web site and look up the additional details you need.

3. In your web browser, visit <https://wwwcaa.govt.nz/> which is the Civil Aviation Authority for New Zealand.
4. Enter the RKB string into the field with the ZK- already populated (as shown below).

Licensing reminder for the hols

If you want your licence issued or amended before the Christmas/New Year holidays, please get your applications in early.

[Read more ➔](#)

Email notification service

You can now subscribe to receive email alerts for 'Education and events'.

[Read more ➔](#)

 [Submit a 005 online](#)



 [ZK-RKB](#)



Your answers should be on the results page and also found from clicking the RKB link.

5. The lab is finished. Close the web browser.

 [Click Here to See Our Findings](#) 

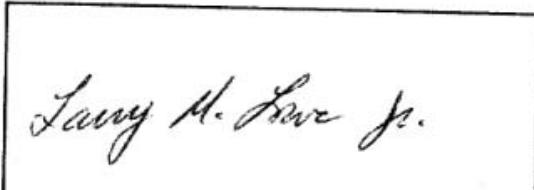
Lowe Brothers LLC.

The brothers' names were:

- Larry M. Lowe Jr.
- William J. Lowe

Image at: <https://sec487.info/ge>

2 of 3 Automatic Zoom

By: Signature  (Please keep writing within blocks)

Printed Name **LARRY M. LOWE JR.** Title **CFO**

Street and Mailing Address

Physical Address **117 Hollenden Lane**

P.O. Box

City, State, ZIP5, ZIP4 **Madison** MS **39110 -**

By: Signature  (Please keep writing within blocks)

Printed Name **William J. Lowe** Title **C.E.O.**

Street and Mailing Address

- Effective date: 06/13/2003
- Filed date: 06/10/2003

Matthew Johnson Frank

<https://dps.alaska.gov/SORWeb/registry/Detail?SexOffenderId=934436378980907847> (<https://sec487.info/gf>)

- What is his date of birth? 2/9/1966
- What is the name of the last known city he lived in? TUNTUTULIAK
- What crime was he convicted of on 3/9/2004? Attempted Sexual Assault 3

Aircraft Information

- What type of aircraft is it (helicopter? plane? something else?)? balloon
- What is the model type and number of the aircraft? Cameron N-65
- What is the serial number of the aircraft? 2072

Reg Mark	1 Man. Model	Serial No	MCTOW (Kg)	Mode S Code Country/Aircraft	Name and Address
RKB	Cameron N-65	2072	589	110010000 00011100010011 HEX C80F13	M E Ragg 54 Totara Place RD 3 Cromwell 9383

Business OSINT

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Collect host names
 - Use DNSRecon to collect host names

Objectives

- Increase comfort with performing business OSINT
- Gain experience using web and python-based tools for host and domain-based OSINT

Goals

1. Collect and analyze the host names and data found on Censys.io for information about what IT and development systems the Panera Bread corporation uses.
2. Use the DNSRecon python script to retrieve host data from the DNS servers of Panera Bread.

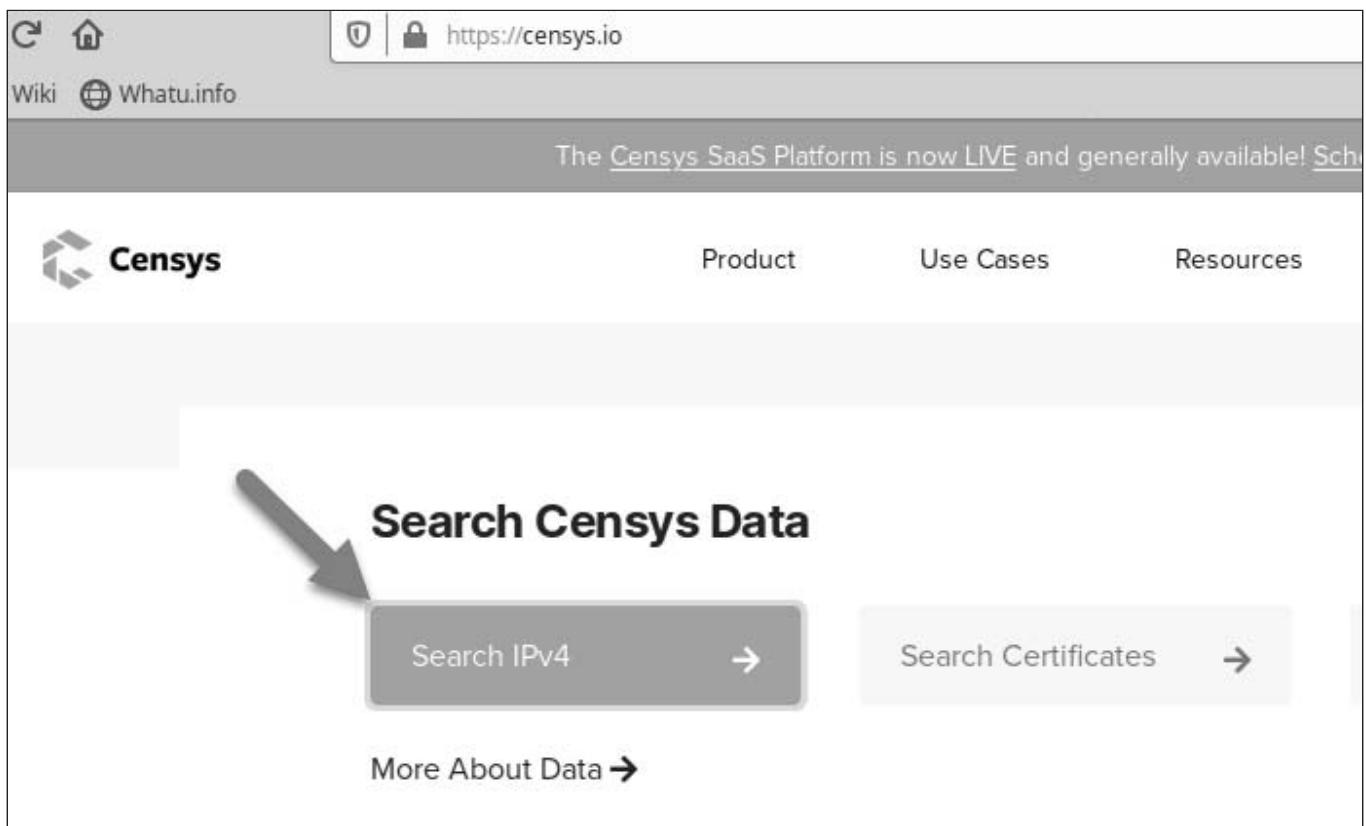
Preparation

Yes VPN

Step-by-step instructions

Collect host names

1. Let's check out the Censys.io site and see what host names it has recorded by typing: <https://censys.io> in the URL bar and pressing Enter.
2. Scroll down the Censys web page until you see the Search IPv4 button (shown below). Click that button.



3. In the search field of the <https://censys.io> site, type: panera and press Enter (shown below).

The screenshot shows the Censys search interface. In the top navigation bar, there is a logo for Censys, a search bar labeled "IPv4 Hosts" with a dropdown arrow, and a search input field containing the query "panera". A large gray arrow points from the text "The results (shown below) that you retrieve may be different from the images below depending on how many Panera servers were added or removed in recent days/weeks. Regardless, you can now see the host names of systems." down to the search results.

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:

- 342 AKAMAI-AS - Akamai Technologies, Inc.
- 81 AMAZON-AES - Amazon.com, Inc.
- 65 AMAZON-02 - Amazon.com, Inc.
- 58 AKAMAI-ASN1
- 37 DIGITALOCEAN-ASN - DigitalOcean, LLC

More

Protocol:

IPv4 Hosts
Page: 1/39 Results: 973 Time: 88ms

204.52.196.130
PANERA - PANERA BREAD COMPANY (40360) United States
Cisco Network 443/https
autonomous_system.name: PANERA - PANERA BREAD COMPANY
EMBEDDED NETWORK

204.52.196.173 (origin-pnra.panerabread.com)
PANERA - PANERA BREAD COMPANY (40360) United States
443/https, 80/http
Panera Bread SSO pnra.panerabread.com
443.https.get.body:<html> <head> <title>Panera

The results (shown below) that you retrieve may be different from the images below depending on how many Panera servers were added or removed in recent days/weeks. Regardless, you can now see the host names of systems.

<p>Quick Filters For all fields, see Data Definitions</p> <p>Autonomous System:</p> <ul style="list-style-type: none"> 342 AKAMAI-AS - Akamai Technologies, Inc. 81 AMAZON-AES - Amazon.com, Inc. 65 AMAZON-02 - Amazon.com, Inc. 58 AKAMAI-ASN1 37 DIGITALOCEAN-ASN - DigitalOcean, LLC <p><input checked="" type="checkbox"/> More</p> <p>Protocol:</p> <ul style="list-style-type: none"> 940 80/http 908 443/https 167 22/ssh 137 21/ftp 92 110/pop3 <p><input checked="" type="checkbox"/> More</p>	<p>IPv4 Hosts Page: 1/39 Results: 973 Time: 88ms</p> <p>204.52.196.130</p> <ul style="list-style-type: none"> PANERA - PANERA BREAD COMPANY (40360) United States Cisco Network 443/https autonomous_system.name: PANERA - PANERA BREAD COMPANY <p>EMBEDDED NETWORK</p> <p>204.52.196.173 (origin-pnra.panerabread.com)</p> <ul style="list-style-type: none"> PANERA - PANERA BREAD COMPANY (40360) United States 443/https, 80/http Panera Bread SSO pnra.panerabread.com 443.https.get.body: <html> <head > <title> Panera <p>204.52.196.89 (order.panerabread.com)</p> <ul style="list-style-type: none"> PANERA - PANERA BREAD COMPANY (40360) United States 443/https, 80/http *.panerabread.com, panerabread.com 443.https.get.body: Panera
---	--

You can scroll down the page and visit the next page and continue doing this until you have collected all the data. Looking down the page, you can already see some host names that would be of interest to our customers. Some samples are:

- hi pchat. panerabread. com looks to be a secure instant messaging platform (<https://www.atlassian.com/software/hipchat>, <https://sec487.info/g4>)
- pnra-preprodhf. panerabread. com seems to indicate that this is a "preproduction" ('preprod') site that may show content before it goes live on the main web site.
- ori gi n-mobapi -uat. panerabread. com shows the letters "UAT" in the name which could stand for "user acceptance testing" which is a stage of the software development lifecycle again, possibly showing content before it hits the main web site.
- anyconnect. panerabread. com might be the VPN (Virtual Private Network) server that they use to remote into the Panera systems as AnyConnect is Cisco's software (<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html>, <https://sec487.info/g5>) to manage a VPN.

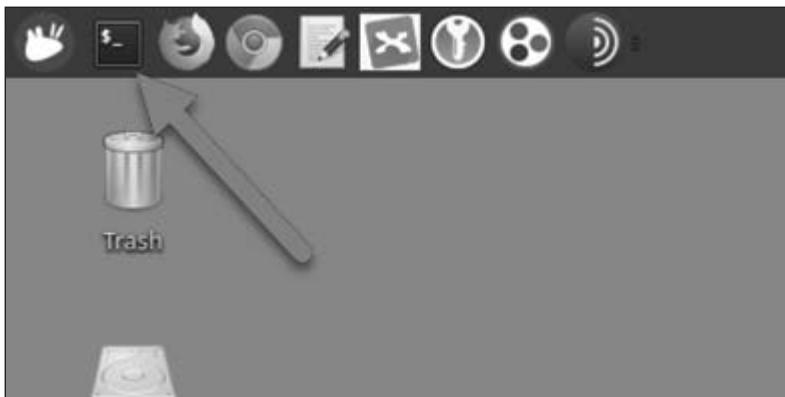
4. See if you can pick out 3 more systems that may be of interest and write them in your notes.

Use DNSRecon to collect host names

Carlos Perez's DNSRecon Python script (<https://github.com/darkoperator/dnsrecon>) is an extremely-capable tool for rapid DNS interrogation. Since our customer required that you not interact with web servers but allowed DNS servers, let's ask the DNS servers for the panerabread.com domain to tell us about all the hosts it knows about.

To do this, DNSRecon is going to make many requests to DNS servers asking for host names using a variety of methods.

1. You need to launch a Terminal window to use the tool. Click the Terminal icon in the menu bar.



2. Now you need to change directory to the /opt/tools/dnsrecon directory by typing: `cd /opt/tools/dnsrecon` then press Enter.
3. Let's see what options exist for this tool by typing: `./dnsrecon.py -h` then press Enter.

```

Terminal
File Edit View Terminal Tabs Help
-D DICTIONARY, --dictionary DICTIONARY
    Dictionary file of subdomain and hostnames to use for
    brute force. Filter out of brute force domain lookup,
    records that resolve to the wildcard defined IP
    address when saving records.
-f
    Filter out of brute force domain lookup, records that
    resolve to the wildcard defined IP address when saving
    records.
-t TYPE, --type TYPE Type of enumeration to perform.
-a
    Perform AXFR with standard enumeration.
-s
    Perform a reverse lookup of IPv4 ranges in the SPF
    record with standard enumeration.
-g
    Perform Google enumeration with standard enumeration.
-b
    Perform Bing enumeration with standard enumeration.
-w
    Perform deep whois record analysis and reverse lookup
    of IP ranges found through Whois when doing a standard
    enumeration.
-z
--threads THREADS
    Performs a DNSSEC zone walk with standard enumeration.
    Number of threads to use in reverse lookups, forward
    lookups, brute force and SRV record enumeration.
--lifetime LIFETIME
    Time to wait for a server to response to a query.
--db DB
    SQLite 3 file to save found records.
-x XML, --xml XML
    XML file to save found records.
-c CSV, --csv CSV
    Comma separated value file.
-j JSON, --json JSON
    JSON file.
--iw
    Continue brute forcing a domain even if a wildcard
    records are discovered.
-v
    Enable verbose

student@sec487 (08:39:00) : /opt/tools/dnsrecon$ █

```

4. Scroll up in the terminal window to see all the flags you could send to DNSRecon.

You are going to have DNSRecon perform a standard (-t std) type of enumeration and then, perform a more-detailed examination of one of the subnets that is registered to the target company. For each IP address in the network, it will ask the DNS server if there is a host name associated with it. This is commonly called a Reverse or PTR (pointer) query because it uses the PTR DNS records to perform reverse DNS queries of IP addresses to host names.

5. Start the DNSRecon tool by typing: `./dnsrecon.py -d panerabread.com -t std -w` (remember to keep the `./` on the beginning of this statement!) then press Enter.



Wait for the Pause

There will be a lot of data in the window (which you should probably copy and paste into your notes). The script will pause at a certain point and ask for your input. Keep following the lab and you will see instructions on what to tell the script to do.

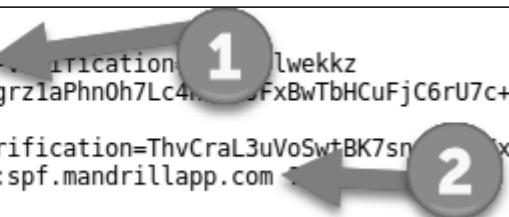
Let's look at some of the more-important content below.

```
student@sec487 (14: 00: 19) : /opt/tools/dnsrecon$ ./dnsrecon.py -d panerabread.com -t std -w
[*] Performing General Enumeration of Domain: panerabread.com
[-] DNSSEC is not configured for panerabread.com
[*]      SOA ns1.customer.level3.net 209.244.4.20
[*]      NS ns8.customer.level3.net 209.244.4.117
[*]      MX mx2.panerabread.ipphmx.com 68.232.146.122
[*]      MX mx2.panerabread.ipphmx.com 68.232.148.194
[*]      MX mx2.panerabread.ipphmx.com 68.232.148.190
[*]      MX mx2.panerabread.ipphmx.com 68.232.130.142
[*]      A panerabread.com 204.52.196.176
```

The first section shows what the DNS servers for panerabread.com are (ns#.customer.level3.net) and that Panera is using the Level3 company for DNS services.

Moving down the results, there are TXT records (shown below) that have the words "dropbox-domain-verification" in them that may indicate that Panera might be using the cloud servers of Dropbox. There is also mention of "mandrillapp.com" which was bought by MailChimp and is a vendor that is used with email systems.

```
[*]      TXT panerabread.com MS=ms13557607
[*]      TXT panerabread.com dropbox-domain-verification=lwekkz
[*]      TXT panerabread.com BAMnNE+tDpWiiwgrz1aPhnOh7Lc4...FxBwTbHCuFjC6rU7c+E+3Nw==
[*]      TXT panerabread.com google-site-verification=ThvCraL3uVoSwtBK7sn...
[*]      TXT panerabread.com v=spf1 include:spf.mandrillapp.com
[*] Enumerating SRV Records
```



Scrolling down to the bottom of the output, you should see a prompt like the one below. It is telling you that it has looked up the computer IP address networks of Panera and has found several. DNSRecon needs you to choose which one to do the PTR (reverse IP address) requests upon.

6. You should type the number next to the line showing 204.52.196.0-204.52.196.255 PANERA BREAD COMPANY and then press Enter.

In the image below, that is entry 3. Your output may be different than below.

```
[+] 27 Records Found
[*] Performing Whois lookup against records found.
[*] The following IP Ranges where found:
[*]   0) 209.244.0.0-209.247.255.255 Level 3 Communications, Inc.
[*]   1) 170.147.0.0-170.147.255.255 Intelcom Group
[*]   2) 68.232.128.0-68.232.159.255 Cisco Systems Ironport Division
[*]   3) 204.52.196.0-204.52.196.255 PANERA BREAD COMPANY
[*]   4) 12.234.67.0-12.234.67.15 PANERA BREAD
[*]   5) 52.96.0.0-52.115.255.255 Microsoft Corporation
[*] What Range do you wish to do a Revers Lookup for?
[*] number, comma separated list, a for all or n for none
3
```

Once you press the Enter key, DNSRecon makes DNS requests for each IP address in this network. What you should see is a LENGTHY list of host names for systems at the panerabread.com domain.

In this output (below), it is easy to see the "dev", "test", and "uat" strings in the host names of systems showing that this may be content that is not in production yet (and that your client asked to know about). Note that, just because there is a domain name, it does not mean that there is a web server up and running or that you could access if there was (there may be authentication in front of the data).

```
[*] PANERA BREAD COMPANY
[*] Performing Reverse Lookup of range 204.52.196.0-204.52.196.255
[*] Performing Reverse Lookup from 204.52.196.0 to 204.52.196.255
[*]     PTR origin-peg-qa.paneracloud.com 204.52.196.50
[*]     PTR d1xakaapp01.paneracloud.com 204.52.196.51
[*]     PTR assets-preprod.paneracloud.com 204.52.196.54
[*]     PTR test.login.paneracloud.com 204.52.196.54
[*]     PTR Origin-assets-uat.panerabread.com 204.52.196.55
[*]     PTR origin-assets.panerabread.com 204.52.196.56
[*]     PTR benefitslogin-preprod.panerabread.com 204.52.196.60
[*]     PTR benefitslogin.panerabread.com 204.52.196.61
[*]     PTR airlock.panerabread.com 204.52.196.65
[*]     PTR customer-preprod.panerabread.com 204.52.196.67
[*]     PTR marketing.panerabread.com 204.52.196.69
[*]     PTR origin-www-qa-beta.panerabread.com 204.52.196.74
[*]     PTR origin-account.panerabread.com 204.52.196.76
[*]     PTR origin-www-qa-test.panerabread.com 204.52.196.77
[*]     PTR accounttest.panerabread.com 204.52.196.77
[*]     PTR origin-www-api-qa.paneracloud.com 204.52.196.78
```

You could take each of these host names and look them up on Archive.org or Google cache and try to view the cached content of the page. If you have some time, try it out and see what you find. Remember to document it for your customer and for yourself!

7. This lab is completed. When finished, close the terminal window by typing: `exit` and pressing Enter.

This page intentionally left blank.

Tor

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Use the Tor Browser
 - Examine Tor Browser Circuit
 - Examine Dread Tor Service
 - Research a Site on FreshOnions
 - Have Extra Time?

Objectives

- Gain familiarity with the Tor Browser
- Examine Tor Browser Circuits
- *OPTION 1* - Visit a Tor social media site to learn what users are sharing
- *OPTION 2* - Research a Tor Onion Service

Goals

1. Launch the Tor Browser (/opt/tools/tor-browser or in taskbar) and visit several Tor web sites.
2. Change your Tor Browser circuit on surface web sites to examine the different nodes your traffic flows through.
3. *OPTION 1* - Visit the <http://dreadditelidet.onion/d> OpSec Tor service and read what users are sharing.

4. Take the moderator of the /d/OpSec Dread channel's user name (from the above step) and look for accounts they might have on the surface web. Can you find anything that would tie surface web to dark web accounts?
5. *OPTION 2* - Retrieve a few pieces of data about the <http://pasternjau12k53d.onion/> Tor hidden service (a paste service much like PasteBin). Visit the FreshOnions (<http://vps7nsnlz3n4ckiie5evi5oz2znes7p57gmrvundbmgt22luzd4z2id.onion/>) site and find out:
 - a. When that site was first seen
 - b. When that site was last seen
 - c. What server that site is reportedly running

Preparation

You should not need to enable the VPN for this lab. If you have network issues, you may enable it.

VPN if problems

Disturbing Content

This is a live exercise in the dark web. You might see disturbing content. This lab was designed to minimize your exposure to the illegal, unethical, and disturbing sides of the dark web. If you are concerned about seeing content that could be disturbing or against your belief-system, please do not try to visit other sites outside of what the lab contains and do not look at other student's screens.

Conduct Reminder

Please remain professional during this exercise. The dark web contains sites that sell illegal goods, show pornographic videos, and are best NOT visited during this class. You are welcome to visit a wide variety of the sites to see what they contain and please do not engage in illegal or risky activities while in the classroom.

Slow Server Responses

You can expect that browsing sites on Tor will most likely be slower than your normal web browsing. Please be patient.

Unavailable Sites

While we tried to pick hidden services that were most likely to not disappear or be shut down, there is always the chance that they can and will be. If you find a site is no longer at the address in the lab or is down, please move on to another site. This is why this lab has multiple *OPTIONS*.

Step-by-step instructions

Use the Tor Browser

Tor Browser (<https://www.torproject.org/projects/torbrowser.html.en>, <https://sec487.info/83>) allows people to easily access resources within and through the Tor dark web network. It is a special version of Firefox that has some security add-ons and patches to increase your security and anonymity.

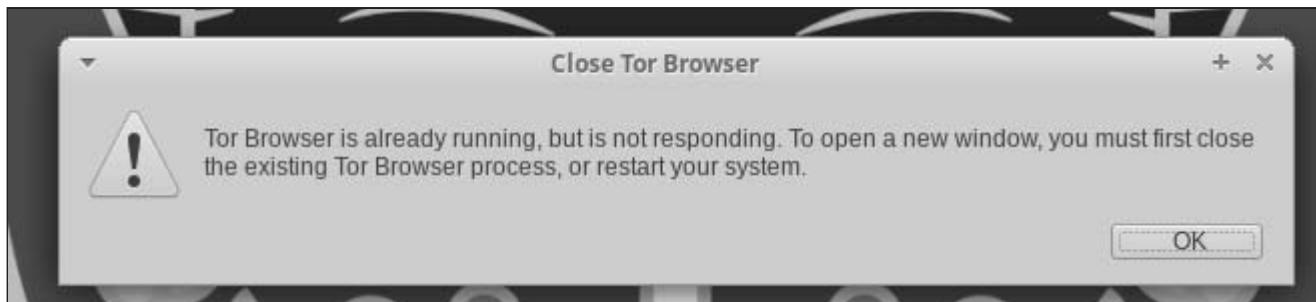
1. Click the Tor Browser icon in the menu bar to launch the browser.



Tor Browser ships with its own copy of Tor so the Tor Browser will establish its own route into Tor. First thing to ensure when you launch the browser, is that it is using the Tor network. To do that, you can visit a web page that checks the IP address you used to reach it against a list of known Tor exit nodes. If our IP matches an exit node's IP, then you are using Tor.

Tor Browser Error

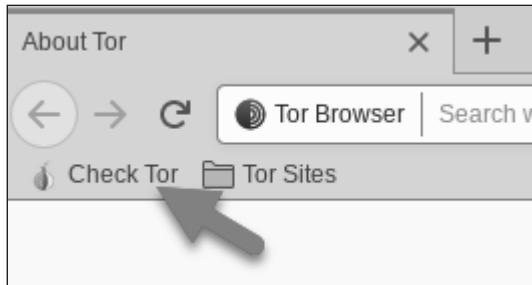
If you click the Tor Browser icon twice, you will see a message like the one below. Click the OK button and wait for the other Tor Browser window to open.



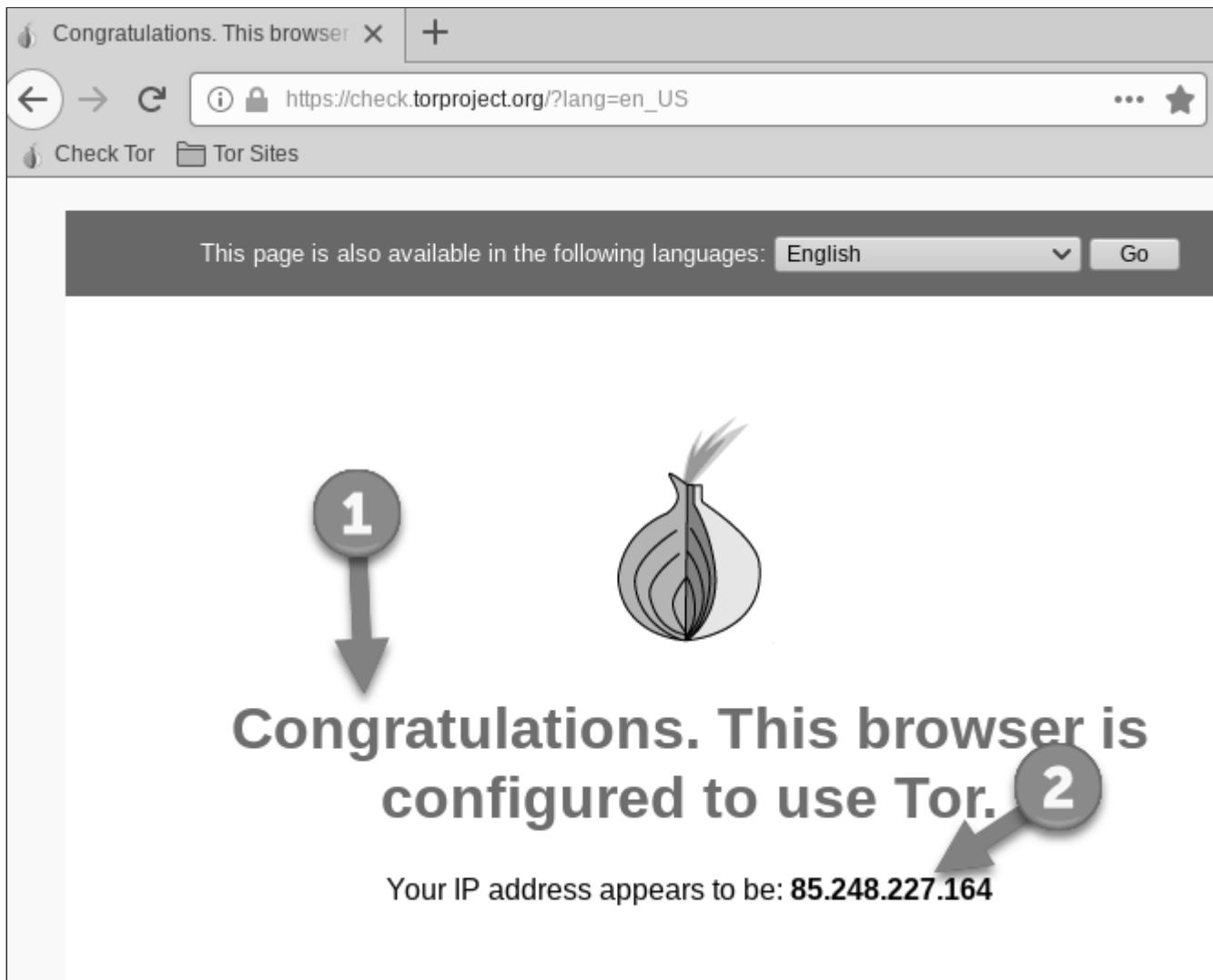
Tor Browser Update

The Tor Browser is regularly updated. If you receive an error that **WARNING: this browser is out of date.**, you can update the browser to the newest version. The lab will work fine without the update as well.

1. To do this checking of your IP, you will use the <https://check.torproject.org> web site (either type it into the URL bar of the browser or click the Check Tor link in the bookmark bar (arrow below)).



2. In the middle of the page it will note if you are or are not using a Tor exit node to visit the site.



Your IP Address

The IP address your computer has will most likely be different from what is shown in the image.

Now that your browser is using Tor, you can visit .onion hidden services and normal, surface web sites. Let's start with the dark web hidden service sites. We have picked a few "safer" bookmarks and added them to the bookmark bar.

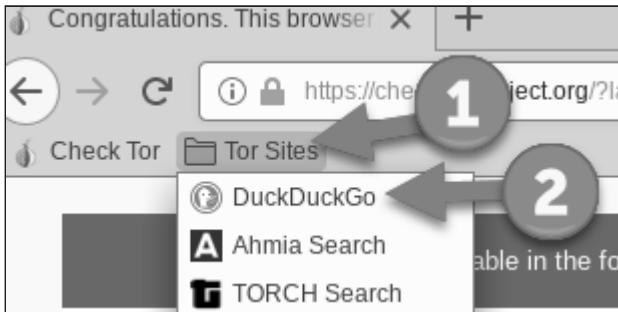
Examine Tor Browser Circuit

Each connection to a Tor or surface web site can have its own circuit. These source-routed paths through Tor can be viewed from the Tor Browser.

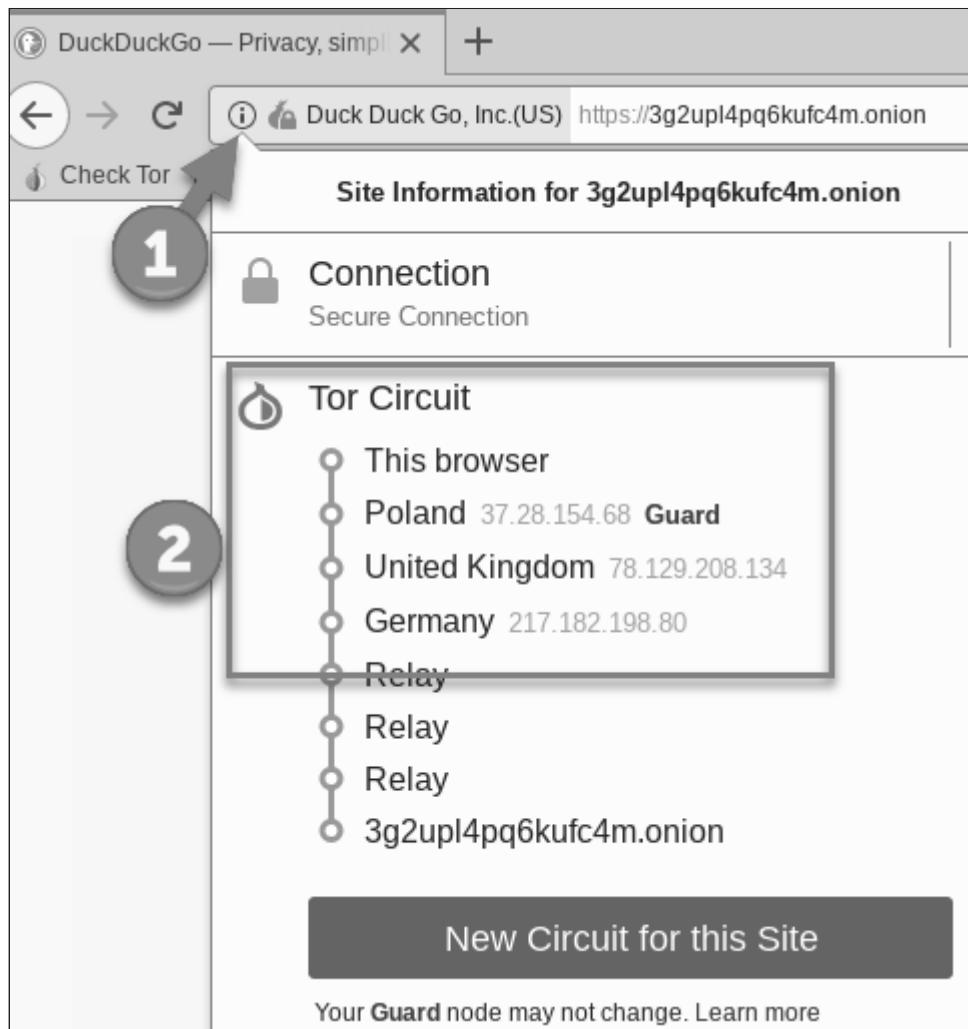
Different Circuit In Your Browser

Your browser's circuit will have different countries and IP addresses than what you see in the images below. This is normal and expected.

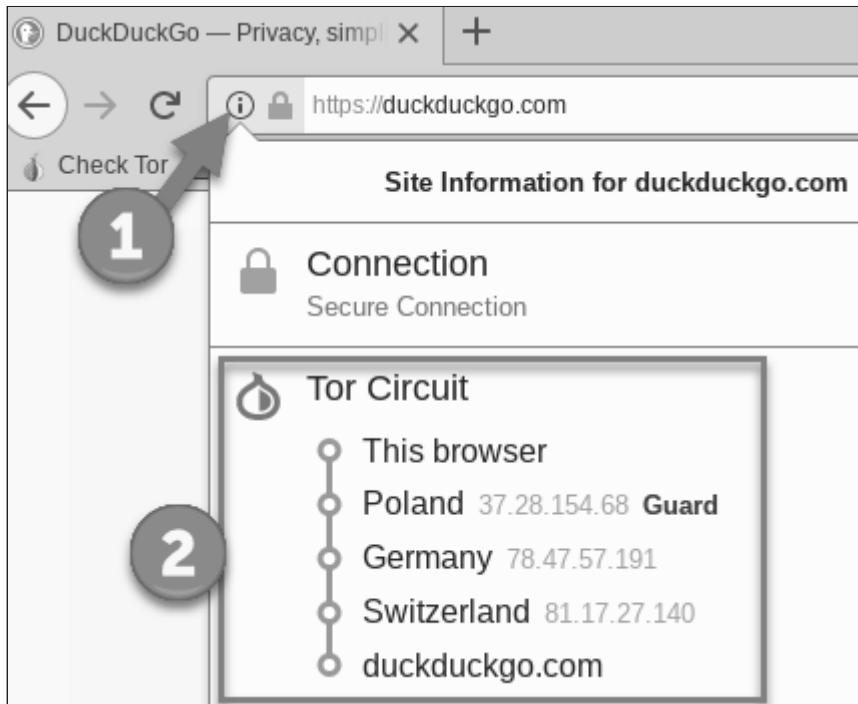
1. You will visit the DuckDuckGo Tor service (arrow 2 below) by using the bookmark in your Tor Browser (arrow 1 below).



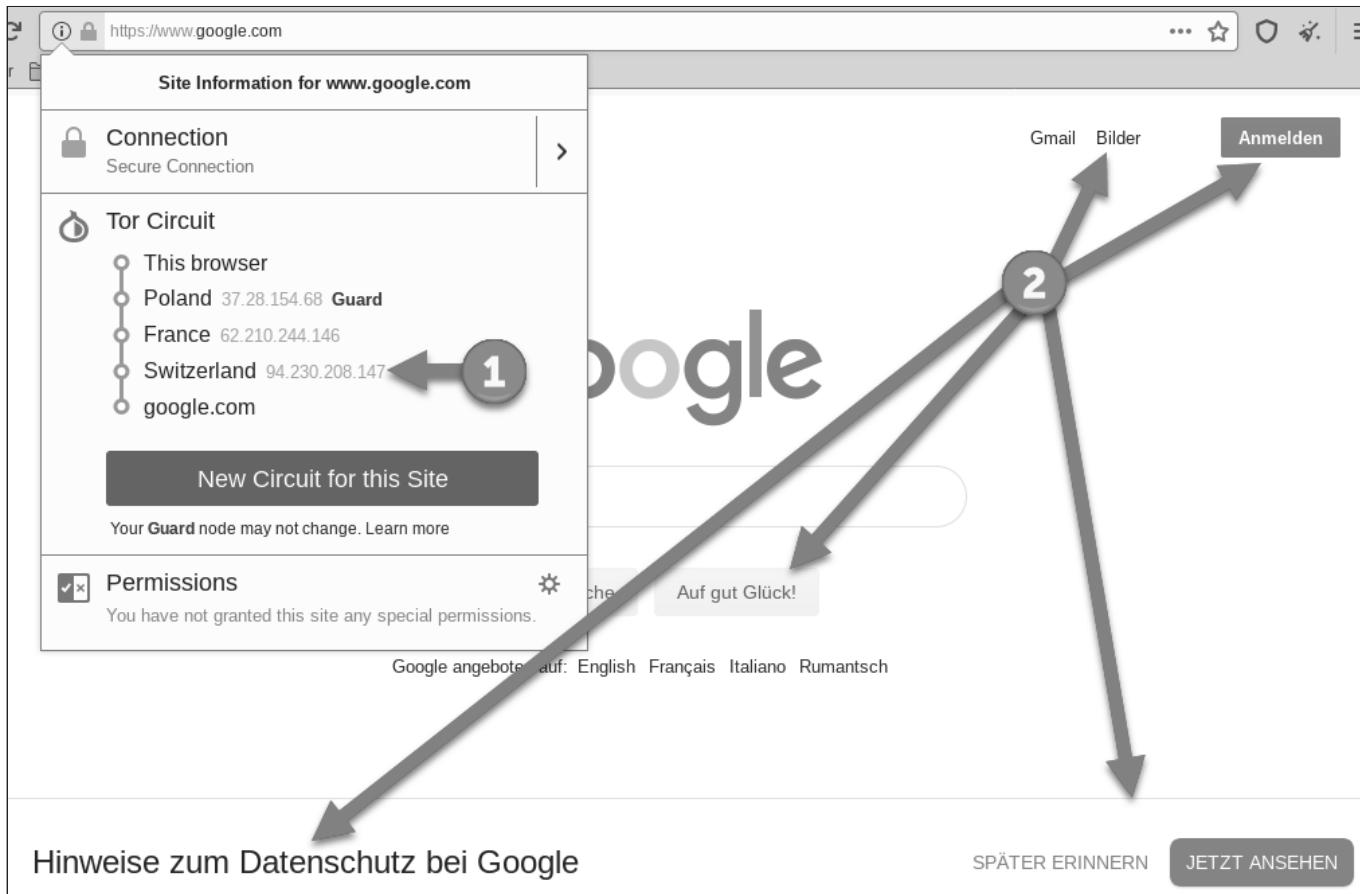
2. Next, click once on the i inside a circle in the URL bar (arrow 1 below). This will show all the Tor nodes that your current circuit to DuckDuckGo uses (number 2 below).



3. Let's visit the <https://duckduckgo.com> web site on the surface web from our Tor Browser and examine our circuit. In the URL bar, type: <https://duckduckgo.com> and press Enter.
4. Go back to view the Tor circuit (arrow 1 below). The nodes your system is using to get to the web site are most likely different from before (number 2 below).



5. If you choose to visit a surface web site (like <https://www.google.com>) that changes your language based upon what country your traffic comes from, you may see the contents of the page written in the language used where your Exit node is located. An example is below. Our Exit node is shown as Switzerland (arrow 1 below) and you can see that the language on the page (arrows coming from 2 below) reflect that.



Examine Dread Tor Service

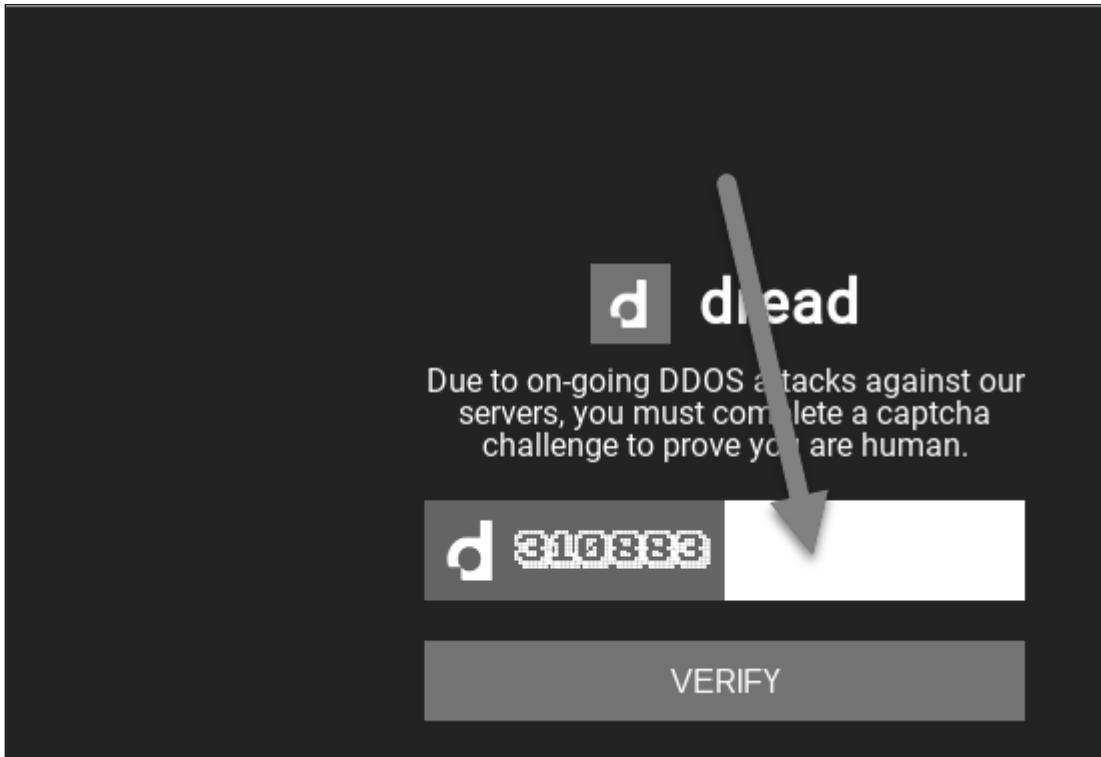
Dread Site May Be Unreachable

There are times when Dread is "down" and not reachable. If that happens, skip this section of the lab.

The <http://dreadditevelidot.onion/d/OpSec> Tor service is similar to the surface web's <https://www.reddit.com/> social media site. While there are places Dread that you won't go in class (due to them hosting profanity and unethical/illegal issues), you can use some of the information posted to better understand what techniques and tips people are sharing to stay "secure" in their dark web.

transactions. The /d/OpSec area of the Tor service is a place for people to share how to increase their Operational Security or OpSec.

1. Visit the <http://dreadditevelidot.onion/d/OpSec> in your Tor Browser. When you do, you may be asked to solve a CAPTCHA (see below). Your CAPTCHA will be different than the one below. Solve it to gain access to the site.



2. Your browser should take you to the forum (shown below). A couple things to point out on this page:

- The Dread posts (arrow 1) have titles at their top. We suggest clicking on the one named [GUIDE] Want Good OPSEC? Assess Your Risks! (arrow 2 below).
- Arrow 2 points to the user that posted the message. In this case /u/MunMunMun (the /u/ specifies this is a user with the name MunMunMun) is the OPSEC Moderator and the poster of this content.

The screenshot shows a Tor-based social media platform called 'dread'. The top navigation bar includes a logo, the word 'dread', and sections for 'Rules', 'Tor Security Guide', and 'PGP Guide'. A sorting option 'Sort posts by Hot' is visible. Two posts from the user '/u/MunMunMun' are listed:

- [NEW WIKI ADDITION] PGP Guide** (by /u/MunMunMun, OPSEC Munderator, 1 month ago) - This post has 3 upvotes and 2 comments. It is circled with a large number '1' and has an arrow pointing to it from callout '1'.
- [GUIDE] Want Good OPSEC? Assess Your Risks!** (by /u/MunMunMun, OPSEC Munderator, 3 months ago) - This post has 9 upvotes and 4 comments. It is circled with a large number '2' and has an arrow pointing to it from callout '2'.

3. Click on the guide mentioned above (arrow 2 above) to read the message. Feel free to click around to other posts in this area if you feel comfortable doing so.

The user name MunMunMun might be used by this poster both on this Tor social media site and on the surface web. Consider using some of the techniques you used earlier in the course to see if you can find any surface web profiles that may be this user's.

Research a Site on FreshOnions

We will use the FreshOnions (<http://vps7nsnlz3n4ckiie5evi5oz2znes7p57gmrundbmagt22luzd4z2id.onion/>) site to research the Paster.ninja hidden service at pasternjaui2k53d.onion.

⚠ FreshOnions Site May Be Unreachable

There are times when FreshOnions is "down" and not reachable. If that happens, skip this section of the lab.

1. In the Tor Browser, visit the <http://vps7nsnlz3n4ckiie5evi5oz2znes7p57gmrundbmgat22luzd4z2id.onion/> site.
2. Copy <http://pasternj au12k53d.onion/>, paste the URL into the Freshonions search field, and click GO>>.



The page that is returned should have all the data you need to record.

Status	Dead
Created At	
Visited At	
Last Seen	
Portscanned	
Language	
Server	
Useful 404 (Gen)	Yes
Useful 404 (PHP)	Yes
Useful 404 (Dir)	Yes

3. This concludes the lab. You can close Tor Browser when you are ready.

Have Extra Time?

Keep in mind that there are MANY more hidden services that are not listed here and that some of these sites may not work anymore or may have inappropriate content. Please be respectful of the other students in the class when visiting other sites. If you have finished the lab early, check out other Tor services like:

- TorLinks <http://torlinkbgs6aabns.onion/>
- The Hidden Wiki http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- Tor66 Search Engine - <http://tor66sezptuu2nta.onion>
- You can also browse web sites on the internet (<https://google.com>, <https://facebook.com>, <https://cnn.com>, etc.) if you'd like by typing in their web addresses. Your traffic will bounce through Tor circuits to get to the web sites. Because of this your browsing experience will be a little bit slower than normal, but you gain pseudo-anonymity.



Click Here to See Our Findings



The FreshOnions analysis of the Paster.ninja Hidden Service (pasternjaui2k53d.onion) looked like this for us:

Status	1 Alive
Created At	2019-02-10 08:28:42
Visited At	2019-04-19 07:54:47
Last Seen	2 2019-04-19 07:54:47
Portscanned	Never
Language	English
Server	3 nginx/1.6.2
Useful 404 (Gen)	Yes
Useful 404 (PHP)	Yes
Useful 404 (Dir)	Yes

HaveIBeenPwned

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Check HIBP Web Page
 - Visit Pastebin Dump Site

Objectives

- Find the password of a user using breach data
- Use multiple sources to achieve your OSINT goals

Goals

1. Find the names of the breach "dumps" where the email address parthpatel1470@gmail.com was found
2. Find a Pastebin.com breach data dump that has the password this email account used on a site

Preparation

Yes VPN

Step-by-step instructions

Check HIBP Web Page

The HaveIBeenPwned (HIBP) <https://haveibeenpwned.com> site is an excellent resource for people to check to see if their email addresses (or domains if you control one) were found in a data dump from a hacked or leaked database. Troy Hunt's site provides single lookups and API access to this data. It is regularly updated and maintained. When sites get hacked and their database contents are disclosed, Troy gathers that data and adds it to his project.

The screenshot shows the homepage of the HaveIBeenPwned website. At the top, there is a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the navigation bar is a large, stylized logo with the text ':--have i been pwned?'. Underneath the logo, there is a subtext: 'Check if you have an account that has been compromised in a data breach'. A large input field is present for entering an email address, with a 'pwned?' button next to it. Below the input field, there is a call-to-action for 1Password: 'Generate secure, unique passwords for every account' with a 'Learn more at 1Password.com' link and a 'Why 1Password?' link. At the bottom of the page, there are four statistics: '416 owned websites', '9,138,980,630 owned accounts', '104,751 pastes', and '123,721,249 paste accounts'.

416 owned websites	9,138,980,630 owned accounts	104,751 pastes	123,721,249 paste accounts
-----------------------	---------------------------------	-------------------	-------------------------------

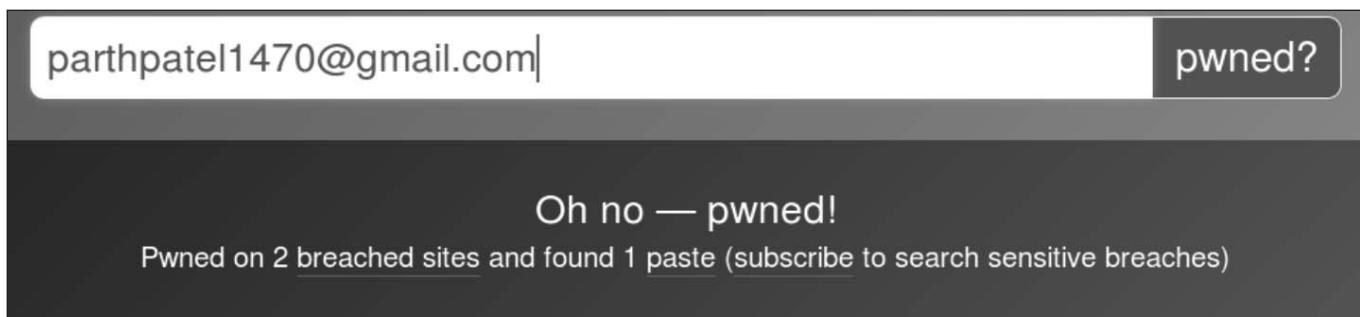
We can enter an email into the form field and click the pwned? button to see if it was found in any breached data. An attacker with this knowledge may download the breached data with the user names and passwords, grab the user's password and then try to use that password on other sites

with that user's user name. This is a password-reuse attack and, since many people use the same email address and password across multiple sites, it works.

1. Launch Firefox (or Chrome) and visit the <https://haveibeenpwned.com/> web page.
2. Let's see if the email `parthpatel 1470@gmail.com` was found in a data breach by typing it into the email address or user name form field and clicking the pwned? button.



The results you receive should show that the email address was found in at least one breach (shown below).



3. Oh no! The email was found in breaches and Pastebin pastes. Scroll down the page and view what the names of the breaches were and what types of information was found in them.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

EyeEm

EyeEm: In February 2018, photography website EyeEm suffered a data breach. The breach was identified among a collection of other large incidents and exposed almost 20M unique email addresses, names, usernames, bios and password hashes. The data was provided to HIBP by a source who asked for it to be attributed to "Kuroi'sh or Gabriel Kimiae-Asadi Bildstein".

Compromised data: Bios, Email addresses, Names, Passwords, Usernames



GameSalad: In February 2019, the education and game creation website Game Salad suffered a data breach. The incident impacted 1.5M accounts and exposed email addresses, usernames, IP addresses and passwords stored as SHA-256 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, IP addresses, Passwords, Usernames

While this might be helpful information, it doesn't give us the password to that email account. Let's shift to look at Pastebin and see if we can find the pastes that may have this data.

Visit Pastebin Dump Site

1. Visit the Pastebin dump collection site <https://psbdmp.ws> in your browser.
2. Enter the target email address (`parthpatel1470@gmail.com`) in the search field and then click the Search button.

The screenshot shows a web page titled "Pastebin dump collection". At the top, there is a navigation bar with links for Home, Dumps, Archive, API, and Donate. Below the title, there is a search bar containing the email address "parthpatel1470@gmail.com". To the right of the search bar is a "Search" button. Two numbered arrows point to these elements: arrow 1 points to the search bar, and arrow 2 points to the search button.

The results (shown below) indicate that there are at least 3 pastes that had this email address in them. Looking at the oldest one (arrow 1), you can see that it contained email addresses and passwords (arrow 2). This is what you want!

Pastebin dump collection

parthpatel1470@gmail.com Search

pA2H8PgJ	email/pass:5673	2018-07-15 23:48
JWQTEAzt	email/pass:5673	2018-01-20 18:42
2U1F0jKy	email/pass:1053	2018-01-21 15:34

3. Right click on the JWQTEAzt link (<https://pastebin.com/JWQTEAzt>) and open it in a new tab. You should see something like the image below indicating that the original paste cannot be found on the live pastebin.com site.

We hope you have learned by this point in the class that you may be able to still retrieve that data. In fact, the <https://psbdmp.ws> site has an archive section where that dump might be.

4. Close that browser tab and, in the psbdmp.ws tab, click on the Archive link (arrow 1 below).

5. The page shows the proper format to retrieve the dump from this site (arrow 1).

The screenshot shows a web page with the title "Search for specific dumps?". Below the title, there is a text block: "If you want to download specific dump and you know only id, you can use our archive with **20260373** dumps!" An arrow labeled "1" points to the placeholder "DUMP_ID" in the URL below. The URL is https://psbdmp.ws/archive/DUMP_ID. Below this, another URL is shown: <https://psbdmp.ws/archive/aY1swD1q>.

There is the format. You need to just add the unique pastebin.com paste to the current URL like so: <https://psbdmp.ws/archive/JWQTEAzt>.

6. Visit the <https://psbdmp.ws/archive/JWQTEAzt> page in your web browser and search for the parthpatel1470@gmail.com email address to find the password.

In the image below, you located the email address (arrow 1) and blurred the password (arrow 2).

The screenshot shows a browser window with the URL <https://psbdmp.ws/archive/JWQTEAzt>. The page displays a list of email addresses and their corresponding hash values. An arrow labeled "1" points to the email address "parthpatel1470@gmail.com". Another arrow labeled "2" points to the password field for this entry, which is blurred. The list includes:

- :106648/100096501
- rohitmalav2349@gmail.com::rawiswar
- vaibhavshan@gmail.com::10209611313813337
- anand.21i@gmail.com::10154455234331323
- shc@gmail.com::123456
- parthpatel1470@gmail.com:: [REDACTED]
- nooracosmetics@gmail.com::442274989493699

7. This lab is completed when you find the password.

Click Here to See Our Findings ▾

The image below shows the password we found.

https://psbdmp.ws/archive/JWQTEAzt

Check Tor OSINT - start.me

::106648/100096501
rohitmalav2349@gmail.com::rawiswar
vaibhavshan@gmail.com::10209611313813337
anand.21i@gmail.com::10154455234331323
abc@gmail.com::123456
parthpatel1470@gmail.com::981789318631061
nooracosmetics@gmail.com::442274989493699

This page intentionally left blank.

International Issues

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions
 - Translations
 - 4th most popular app
 - 8th most popular app
 - 7th most popular web site

Objectives

- Gain experience in translating foreign languages
- Gain confidence in determining the top mobile applications used in a foreign country
- Gain confidence in determining the top web sites used in a foreign country

Goals

1. Use a language translator to translate the phrase You keep using that word. I do not think it means what you think it means. into...
 - Japanese. Then take that output and translate the Japanese into...
 - Welsh. Then take that output and translate the Welsh into...
 - Polish. Then take that output and translate the Polish into...
 - English. Then write down what the phrase.

2. Find the 4th most popular, free, iOS (Apple) application in Canada.
3. Find the 8th most popular, grossing Android application in Japan.
4. Find the 7th most popular web site in Pakistan.

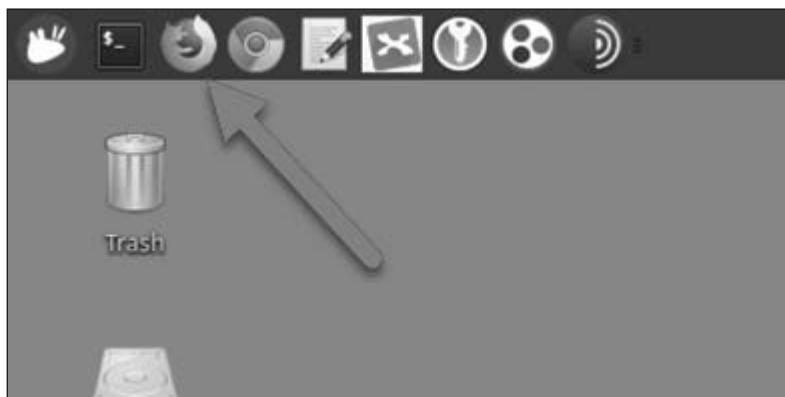
Preparation

VPN if problems

Step-by-step instructions

Translations

1. Our first step is to launch the Firefox web browser by clicking the icon in the menu bar.



2. Visit the <https://translate.google.com> site.
3. In the right pane, select the triangle and click Japanese to tell Google to translate the content into Japanese.

The screenshot shows the Google Translate interface. At the top, there are tabs for 'Text' (selected) and 'Documents'. Below that, a row of language buttons includes 'DETECT LANGUAGE', 'ENGLISH', 'SPANISH', 'FRENCH', a dropdown arrow, 'ENGLISH' (selected), 'SPANISH', and 'ARABIC'. A large grey arrow labeled '1' points upwards from the 'ARABIC' button towards the top right corner. Below this row is a search bar with the placeholder 'Search languages' and a back arrow. The main area displays a grid of language pairs. The first column contains 'Chinese', 'Chinese (Simplified)', 'Chinese (Traditional)', 'Corsican', 'Croatian', 'Czech', 'Danish', 'Dutch', and a checked 'English' button. The second column contains 'Hungarian', 'Icelandic', 'Igbo', 'Indonesian', 'Irish', 'Italian', 'Japanese', 'Javanese', and 'Kannada'. The third column contains 'Mongolian', 'Myanmar (Burmese)', 'Nepali', 'Norwegian', 'Pashto', 'Persian', 'Polish', 'Portuguese', and 'Punjabi'. The fourth column contains 'Telugu', 'Thai', 'Turkish', 'Ukrainian', 'Urdu', 'Uzbek', 'Vietnamese', and 'Welsh'. A large grey arrow labeled '2' points downwards from the 'Japanese' button in the second column towards the bottom center.

4. Type the following phrase into the left pane. You keep using that word. I do not think it means what you think it means.
5. Switch the Japanese content from the right pane to the left by clicking the double arrows (arrow 1 below).

The screenshot shows the Google Translate interface with the text 'You keep using that word. I do not think it means what you think it means.' in the English input field. The output field on the right shows the Japanese translation: 'その言葉を使い続けます。私はそれがあなたがそれが意味すると思うものを意味するとは思わない。' (Sono kotoba o tsukai tsudzukemasu. Watashi wa sore ga anata ga sore ga imi suru to omou mono o imi suru to wa omowanai.). A large grey arrow labeled '1' points downwards from the double arrow icon between the input and output fields. The interface also includes a 'Sign in' button at the top right, and a small note at the bottom left: 'Did you mean: You keep using that word. I don't think it means what you think it means.'

6. Click the triangle in the right pane (arrow 1 below) to change the language.

The screenshot shows the Google Translate interface. On the left, there's a text input field containing Japanese text: "その言葉を使い続けます。私はそれがあなたがそれが意味すると思うものを意味するとは思わない。". Below this is the original Japanese text: "Sono kotoba o tsukai tsudzukemasu. Watashi wa sore ga anata ga sore ga imi suru to omou mono o imi suru to wa omowanai.". To the right, the English translation is displayed: "Continue to use that word. I don't think it means what you think it means." A large gray arrow points from the number '1' in a circle on the Japanese text towards the English sentence.

7. Choose Welsh from the list (arrow 1 below).

The screenshot shows a language selection dropdown menu. At the top, it says "ENGLISH" and "SPANISH" with a downward arrow icon. Below this is a horizontal bar with a progress indicator. The list of languages includes: (Burmese), Telugu, Thai, Turkish, Ukrainian, Urdu, Uzbek, Vietnamese, Welsh, and Xhosa. A large gray arrow points from the number '1' in a circle on the left towards the "Welsh" option.

	ENGLISH	SPANISH
(Burmese)	Telugu	
	Thai	
	Turkish	
	Ukrainian	
	Urdu	
	Uzbek	
	Vietnamese	
	Welsh	
	Xhosa	

8. Switch the Welsh content from the right pane to the left just as you did for the Japanese content above.

The screenshot shows the Google Translate interface. The source text is "Parhewch i ddefnyddio'r gair hwnnw. Nid wyf yn credu ei fod yn golgyu'r hyn rydych chi'n meddwl y mae'n ei olygu." The target language is set to Japanese. The translated text is "その言葉を使い続けます。私はそれがあなたがそれが意味するとと思うものを意味するとは思わない。" Below the Japanese text, there is a detailed explanation: "Sono kotoba o tsukai tsudzukemasu. Watashi wa sore ga anata ga sore ga imi suru to omou mono o imi suru to wa omowanai." There are also audio playback icons and a copy/share button.

9. Click the triangle in the right pane to change the language and then choose Polish from the list.
10. Switch the Polish content from the right pane to the left just as you did for the Welsh content above.
11. Click the triangle in the right pane to change the language and then choose English from the list.
12. Write down the phrase that is shown in the English pane.

The screenshot shows the Google Translate interface. The source text is "Nadal używaj tego słowa. Nie sądzę, żeby to znaczyło, co myślisz." The target language is set to English. The English translation is displayed in a large, highlighted box with a large gray arrow pointing to it. Below the English text, there is a detailed explanation: "You still use that word. I don't think that means what you think it means." There are also audio playback icons and a copy/share button.

Record the English output in your lab book or notes.

Different Results

Your results may be different from what we received or what other students received depending upon how the text is translated. This reinforces our point that translating material is challenging.

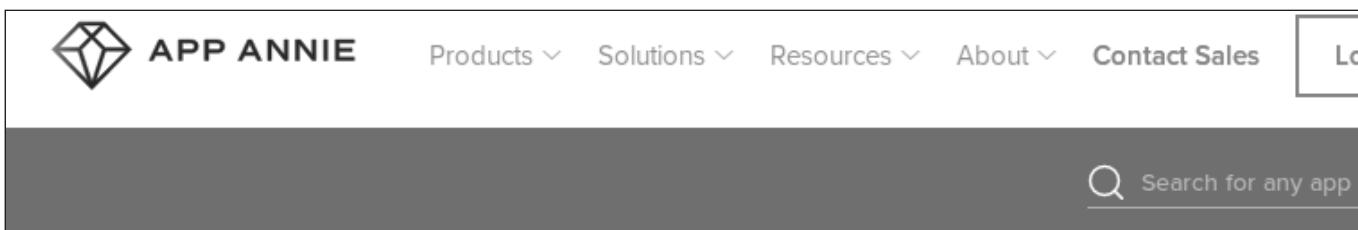
4th most popular app

To find this information, you will use the App Annie web site. If you try to navigate through the site to get to the top apps, the site will ask us to create an account (they are free). Instead, you will visit the URL directly and bypass their login.

Popular Sites Change

The popularity of apps changes every day. The ones you see in these screenshots below will most likely not be the ones you see when you run your searches.

1. Enter <https://sec487.info/do> (or <https://www.appannie.com/en/apps/google-play/top/south-korea/overall>) into the browser URL bar and press Enter.
2. Click on the "Google Play" and change it to "iOS Store".



The screenshot shows the App Annie homepage. At the top, there is a navigation bar with links for Products, Solutions, Resources, About, Contact Sales, and a location dropdown. Below the navigation is a search bar with a magnifying glass icon and the placeholder text "Search for any app". The main content area features a large title "Top Apps on Google Play, South Korea, Overall," followed by a subtitle: "Stay ahead of the market with App Annie Intelligence. Monitor the top apps across countries, categories and platforms." Below the title, there is a dropdown menu for selecting the platform, currently set to "Google Play" with a red arrow pointing to it. Other options in the dropdown are "Country" (set to "South Korea"), "Category" (set to "Overall"), and "All Apps".

3. Change the country to Canada by clicking on the "South Korea" and choosing "Canada".

Top Apps on iOS Store, South Korea

Stay ahead of the market with App Annie Intelligence. Monitor the top apps.

The screenshot shows the App Annie Intelligence interface. A large red circle labeled '1' points to the 'Country' dropdown menu, which is open to show options: Australia, Canada, China, and France. Another red circle labeled '2' points to the 'FREE' button next to the app name '무신사 - MU...'. The interface includes navigation buttons for 'iOS Store', 'Device iPhone', 'Category', and 'South Korea'.

Record what the 4th most popular free, iOS app in Canada is in your notes.

8th most popular app

1. Click on the "iOS Store" and change it to "Google Play".
2. Change the country to Japan by clicking on the "Canada" and choosing "Japan".

Record what the 8th most popular grossing, Android app in Japan is in your notes.

Bonus

For a bonus - If the app name is in Japanese, use the drawing translator in Google Translate to draw these characters and convert them into English or use the Google Translate application on your phone to take a picture and then highlight the area you want translated.

7th most popular web site

1. Visit <https://www.alexa.com/topsites> in your browser.

You may need to close the "What would you like to accomplish with Alexa" pop up box by clicking the X in the upper right. This may or may not appear on your screen.

2. Click on By Country to change the country.

The top 500 sites on the web

Global By Country By Category

Showing 50 of 500 results

Once you do this, many country names will appear on the page.

3. Find the word Pakistan and click it.
4. Scroll down the screen and find the 7th most popular web site.

	Site	Daily Time o...	Daily Pagevi...	% of Traffic F...	Total Sites Li...
1	Google.com	12:13	14.95	0.50%	2,227,065
2	Youtube.com	11:16	6.49	17.00%	1,718,050
3	Facebook.com	18:15	7.94	8.20%	4,066,031
4	Google.com.pk	5:19	6.76	5.80%	3,042
5	Urdupoint.com	4:48	3.74	39.40%	6,901
6	Yahoo.com	4:37	4.45	7.80%	465,935
7	Wikipedia.org	14:30	8.93	24.60%	381
8		3:55	2.94	71.60%	1,302,797

Record the 7th most popular web site in Pakistan is in your notes.

Click Here to See Our Findings ▼

For this lab, we will show you the translation that we received from the first part of the lab but, because the most popular apps and sites change daily, there is little value in showing that content.

The translation from Polish to English that we performed generated the following text: Continue to use this word. I don't think it means what you think.

Solo CTF

Table of Contents

- Objectives
- Exercise: Scenario - Everyone PLEASE READ
- Preparation
- Exercise – Step-by-step instructions
 - Preparations
 - Customer Requirement Gathering
 - Decide on TTPs
 - Note Taking
 - Remaining OSINT Process Steps
 - Visit the First Web Site
 - Visit the Tor hidden service
 - Contact your customer
 - Next steps
 - When are you done?

Objectives

- Work through the process of an OSINT investigation
- Gain confidence in using an OSINT process
- Practice using the skills that you gained during the course to

Exercise: Scenario - Everyone PLEASE READ

"We've been hacked!" Missy Cruz, your customer and internal security chief for a large movie company, says into the phone. "We need your help."

You ask Ms. Cruz, "What happened?", "When did it happen?", "What have you done?" and related questions to try to understand the scope of what happened and what your role will be. Here is what she said.

"Earlier today, someone called our office and said we should visit the <https://sec487.info/grand> web site because there was something there that we should know about. They gave no other details...then they hung up.

As you know, we make movies and were working on The Princess Bride 2 (TPB2) script with some writers. We had to keep it a secret and used a special computer to share the files on the internet. Well, it looks like someone found it and got the script. We haven't done anything more with this than what I told you. That web site has weird content on it though. We knew that you'd know what it is and what to do.

Here is what we need you to do:

1. Go check out the <https://sec487.info/grand> web site, find out what you can.
2. Looks like there was some "onion" site mentioned. I couldn't get there from my browser on the internet but maybe that has some additional details.
3. After you visit the onion site, send me an email (missycruz487@gmail.com) for next steps. You don't need to put anything in the email body. Just send the email to me with the numbers "487" in the subject. I'll send you instructions on what we would like you to do after you visit that site.

"Whatever you do, please keep this work 100% passive with no interaction with the targets. Thanks for your help. I look forward to your email." and with that, she ended the call.



Emailing Your Customer

We included the interactive "please email your customer" to make the assessment feel more like a real one where you might be reaching out to your customer for clarification or further instructions. We are not trying to collect emails from all students taking this class. We delete the emails to this mailbox and will NOT use them or their email addresses for anything other than sending the one reply for this lab to you. You can feel free to use a sock puppet account or other email address to send this message.

If you prefer to not send an email, view the contents of `/home/student/labs/lab5.4/customer_reply` in a web browser or text editor.

Preparation

VPN if problems

The Solo CTF is the culmination of this course. The goal is not to give you new techniques or introduce novel resources but, instead, allow you to practice a full assessment and put into practice many of the labs that you worked during the course.

During this lab, we will point you in the direction of resources or towards previous labs and allow you to use your knowledge and analysis skills to take the next steps in the investigation.

As with most OSINT assessments, there are many ways to complete your objectives. You will head down a path, pivot on data, and repeat the cycle. But you do not need to follow our script for the lab. In the sections you feel comfortable in (or in which you'd like a challenge), try gathering data and analyze it yourself and see where it leads your work.

We expect this lab to take 30 minutes to 2+ hours. Take your time.

Ready to give it a try?

- Go as fast as you want.
- Document along the way (Hunchly and/or notes in MindMap or other system).
- Follow your process.

- If you have questions about possible next steps, ask your instructor.

Exercise – Step-by-step instructions

Preparations

If you are going to treat this as a real (simulated) assessment, you will need to work through our process.

Customer Requirement Gathering

You already completed this step. You had a phone call with your client where they gave you initial details of what they want you to do. You know what you need to do and what the assessment rules are.

Decide on TTPs

You need to visit a web site on the internet then probably move to the dark web. For now, just surf a few web pages and collect the data to figure out what it means and maybe it will determine the next steps.

Your TTPs will change as you move deeper into the assessment and find yourself pivoting on different data points as you will do in this lab. Stay flexible.

Note Taking

Decide how you will take the notes that your customer needs. This lab is a longer one with many changes and twists. There will be many data points to collect, analyze, and possibly pivot upon. You will need to collect images and screenshots too.

Our first suggestion is to create a directory on your computer to store any images and documents you download in your assessment. You can also store your MindMap or another note file in there.

1. Create a local folder to store OSINT documents. To do this, you will need to either use a terminal or use the GUI. The command to make a directory from the terminal is `mkdi r /home/student/`

I abs/[NAME] (where [NAME] is replaced by what you want to call the directory). Below we will use `solo-ctf-notes` for the directory name, but you can choose what you like.



Graphical Method

If you'd like to do this via the GUI, follow the process below, otherwise skip to step 6.

2. Double click on the Home icon on your desktop (arrow 1).

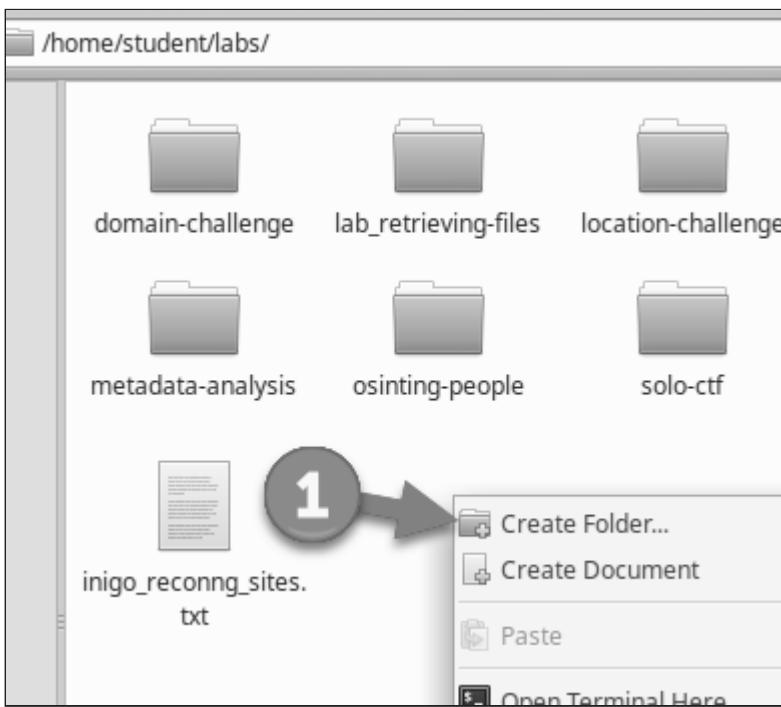


We will put our new directory in the labs directory but you can put it wherever you wish.

3. Double click on the labs folder (arrow 1).

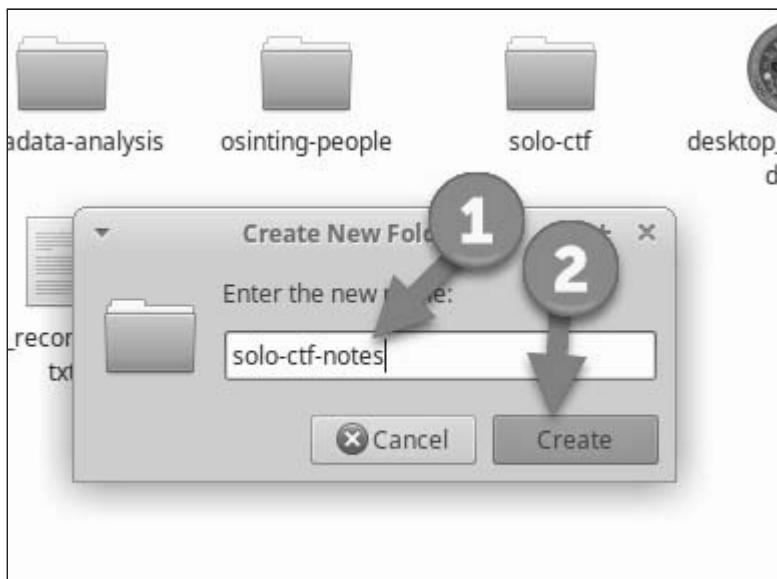


4. Right click in the window and, to create a new folder, select Create Folder... (arrow 1).

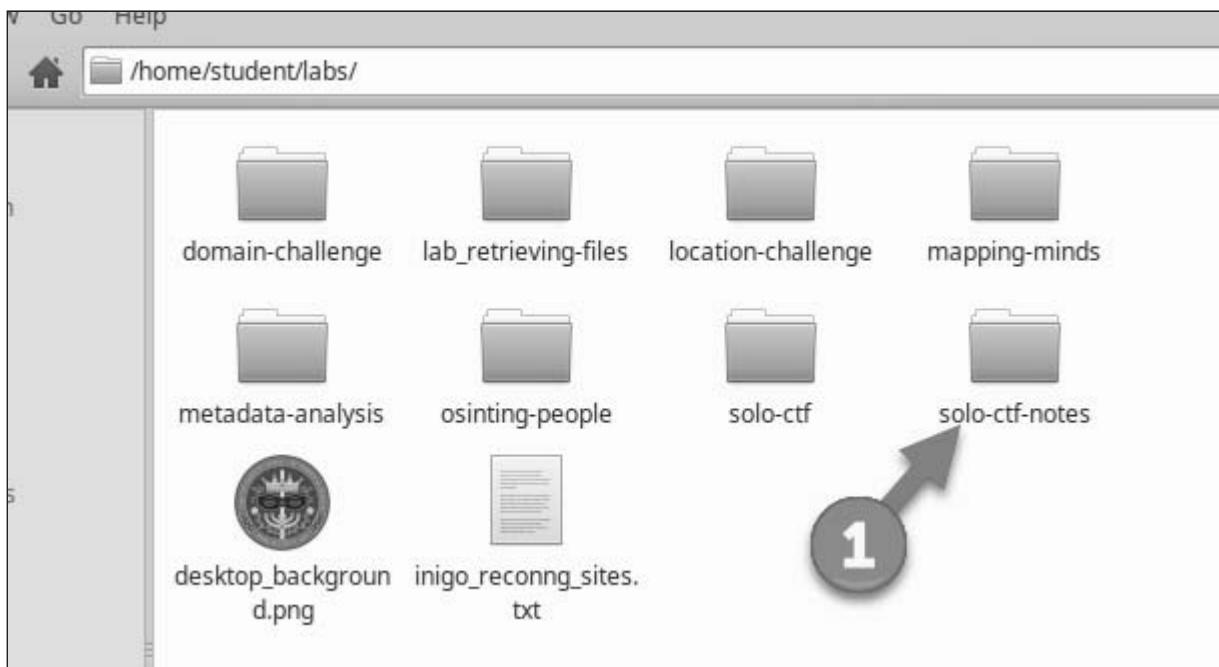


5. Name the folder. For our lab we will name `solo-ctf-notes` (arrow 1) then press the Create button (arrow 2).

In your real cases, you may have code names for cases or specific case-naming guidelines that you need to follow.



Your folder list should look like the one below unless you picked a different name for the directory.



We may need to drag content like pictures or files we download into this window, so we will keep it open.



Rejoin the Lab

Please rejoin the lab here if you skipped the above steps.

6. Choose how you will document your assessment notes and create the document.

At this point you need to choose how you will take your notes. Are you using a MindMap? A text file? A LibreOffice Calc spreadsheet? Using Hunchly plus something else? Google Docs? There are MANY choices to start with. Your assessment can start with one and then move to use others as you see fit.

We leave this step to you to execute as you already know how to use the MindMap document and have edited text files with gedit in previous labs. Remember that you can use your host computer's screen capture tools or the Capture app within the VM in the upper right of the menu bar to capture screenshots.

For this lab, practice taking the time to document:

- Every place where you retrieved data from. Each data point should have a corresponding URL or tool that tells how the information was retrieved.
- Dates and times of when data was discovered can be important in the future. Make sure you document these pieces of data.
- Take your screenshots along the way. You find something interesting, take a picture and save it.

Whatever you use for your documentation, you should probably enter in the following data points into your notes in a summary or introduction type of place.

- Today's date and time
- What you are doing?
- Why are you doing it?
- Who told you to do it and when?
- What system(s) are you using to perform the OSINT?
- How are you connecting to the internet? Using a VPN? Proxy?
- What steps did you take to clean your system?

These, and other starting questions will be important to your customer, the court system (if your work is used in legal proceedings), and to your company. It also helps your memory as, you will probably be doing a variety of other cases after you complete this one. Documenting the above questions help you when you need to come back to a case after a month or a year to understand what you did and how.

If you are using Hunchly in Google Chrome, you may want to launch the browser and create a new case in Hunchly then set that as the current case.

Remaining OSINT Process Steps

From our coursework, you learned that, at this point, you can go ahead and begin your data collection, analysis, pivoting, and repeating the data gathering steps. You will start this in the next section, and keep in mind:

- Consider all the facts and what other factors could be involved.
- Watch for bias/logical fallacies.
- What are the pivot points where you need to collect more data?
- What is of interest to your customer?

For your customer's output/report, there is nothing for you to submit or turn in.

Sample Report

David Mashburn, SEC487 SANS instructor, created a PDF report from his work in this lab. It is in the /home/student/labs/solo-ctf/ directory and is named SoloCTF_ExampleReport1_Mashburn.pdf .

Visit the First Web Site

On Your Own

All week you have been doing some of these tasks. Since this is a lab where you need to work on your own a bit more, we will not be telling you where to click or showing screenshots for every action. This is to encourage you to rely on your course notes and the data in the previous labs.

1. Launch a web browser and visit the <https://sec487.info/grand> web site.

It appears that this is a Pastebin post or, more commonly referred to as a paste.

Document what it shows, when it was posted, and other data.

What are the pivot points you found? We see the following as points for additional research:

- The 7kwhfti56l24m4ckbzcvdrqt74r5y4pgvprccfnsmn7r2sygfzycizyd.onion address. This appears to be a Tor hidden service.
- There is a hacker name in ASCII text at the bottom of the message. You should record Mad4MiracleMax.
- The URL for the actual pastebin page may be something you can pivot on too. Record that.



Document!

Remember to take screenshots of what you see. Is there a date for the paste?

Looks like the next step might be to visit that Tor hidden service. What would you use to visit that site? Yes, the Tor Browser.

Visit the Tor hidden service

1. Launch the Tor Browser and visit the <http://7kwhfti56l24m4ckbzcvdrqt74r5y4pgvprccfnsmn7r2sygfzycizyd.onion> site.
2. Data in the dark web can be transient. Save this page locally to your system by right clicking on the page and selecting Save Page As.



Horizontal Line

This page has content above a horizontal line that is to introduce this document to anyone that happens to find it and is not in the SEC487 course. You can ignore all content above the line and begin your collection after the Manifesto Begins content.



Document

Remember to save this page in your `/home/students/labs/solo-ctf-notes` directory.

There are many pieces of data to collect and potentially pivot upon in this document. We picked out the data below as possible points (which should be recorded). You may have found other data too!

- <https://tpb2.osint.ninja/> is the location where the page reports the script was stolen from.
- The person REALLY likes the character Miracle Max in the original The Princess Bride movie. By extension, they are a big fan of the actor who played Miracle Max, Billy Crystal.
- There are 4 demands, but each appears to be written in their own language. You may need to translate those.
- Looks like there are GPS coordinates in one of these demands.
- Signed with the Mad4MiracleMax moniker.

Your customer asked you to email her right after you found out what was on the Tor site. Ensure you have good notes and have explored all the content you need to on this Tor hidden service than you can close the Tor Browser.

3. You must translate the demands that Mad4MiracleMax made so that you can give those to your customer.

We did the translating foreign languages in a lab on day 5. Refer to those notes for the process if you do not remember.



Hunchly

If you are using Chrome and Hunchly, do the language translations in that browser so it is recorded. If not, record screenshots as you go.

Contact your customer

1. Contact your customer by sending an email from one of your personal, business, or sock puppet accounts to *missycruz487@gmail.com*. Put 487 in the subject line and no content in the body.

!!! tip If you do not wish to send an email to get further customer instructions, look at the contents of /home/student/labs/lab5.4/customer_reply or click below.



Click Here for Missy Cruz's Instructions

Thanks for emailing. I've got an important meeting right now (as you can imagine). We are still trying to keep this quiet (no press).

First, please do NOT connect/friend/etc to the targets, their colleagues, family, and friends.

Here's what I'd like you to do:

- a. We spoke to Billy Crystal's manager and they'd like us to do some OSINT on his online profile to look for security issues. Please research things like his basic data, social media, and other relevant data.
- b. Look at that location you found. Figure out where it is, what is happening there in the coming week, how the attacker could get in and out of the place (roads, waterways, trails, etc.), any photos and images of the place would be good to grab. If we do give the money, we may wish to try to apprehend them as they are leaving.
- c. See if you can find the social media accounts of and the first and last name of the Mad4MiracleMax person.

Thanks for your help! I'll be in touch again soon.

Next steps

According to the email from your customer, your next goals are to:

- 1 - Look at the actor that played Miracle Max's online profile. See what you can find out about the actor Billy Crystal that may be risky to him. Some ideas are below but you can choose what to look for.

- Basic data - Full name, home address(es), phone number(s), email address(es), social media accounts (professional and personal).
- Upcoming events that he will be appearing at
- Other interesting information that may be helpful in reducing his risk profile.

2 - There was a location in the demands.

- Where is that location?
- Where specifically on the property does the attacker want the money dropped? What building or place?
- What are the approach and egress points for that location and overall property? How would the attacker get in to grab the money and how could they escape? Think about waterways, roads, and trails in your research.
- Are there events happening at that location in the coming week that could give the attacker a reason to be there?

3 - Find out more information about someone named Mad4MiracleMax

- Can you find their full name?
- Are they on other social media sites?
- Can you find 2 locations where they have said that they live/are from?

Those are the directions. Go to it!

When are you done?

An excellent question that some students have posed is, "How do I know when I've found enough?" Since this is a learning exercise, the guidelines below should help.

 Click Here to See When to Stop 

1. For the Billy Crystal objective, you are doing a high-level risk assessment of him. Above, we noted most of the information you should collect. Once you have it, you are done with this objective.
2. For the location analysis, again, answer the questions in the section above and anything else you can think of that would help your customer if they do go through with a ransom drop.
3. Investigation the Mad4MiracleMax persona is a challenging one. Find all the social media accounts that you can for his user name, his location, and his first and last name.

You are free to leave the class when you are finished.

This page intentionally left blank.

Cached Content

Table of Contents

- Objectives
- Goals
- Preparation
- Step-by-step instructions

Objectives

- Explore retrieving cached content safely from Google Cache

Goals

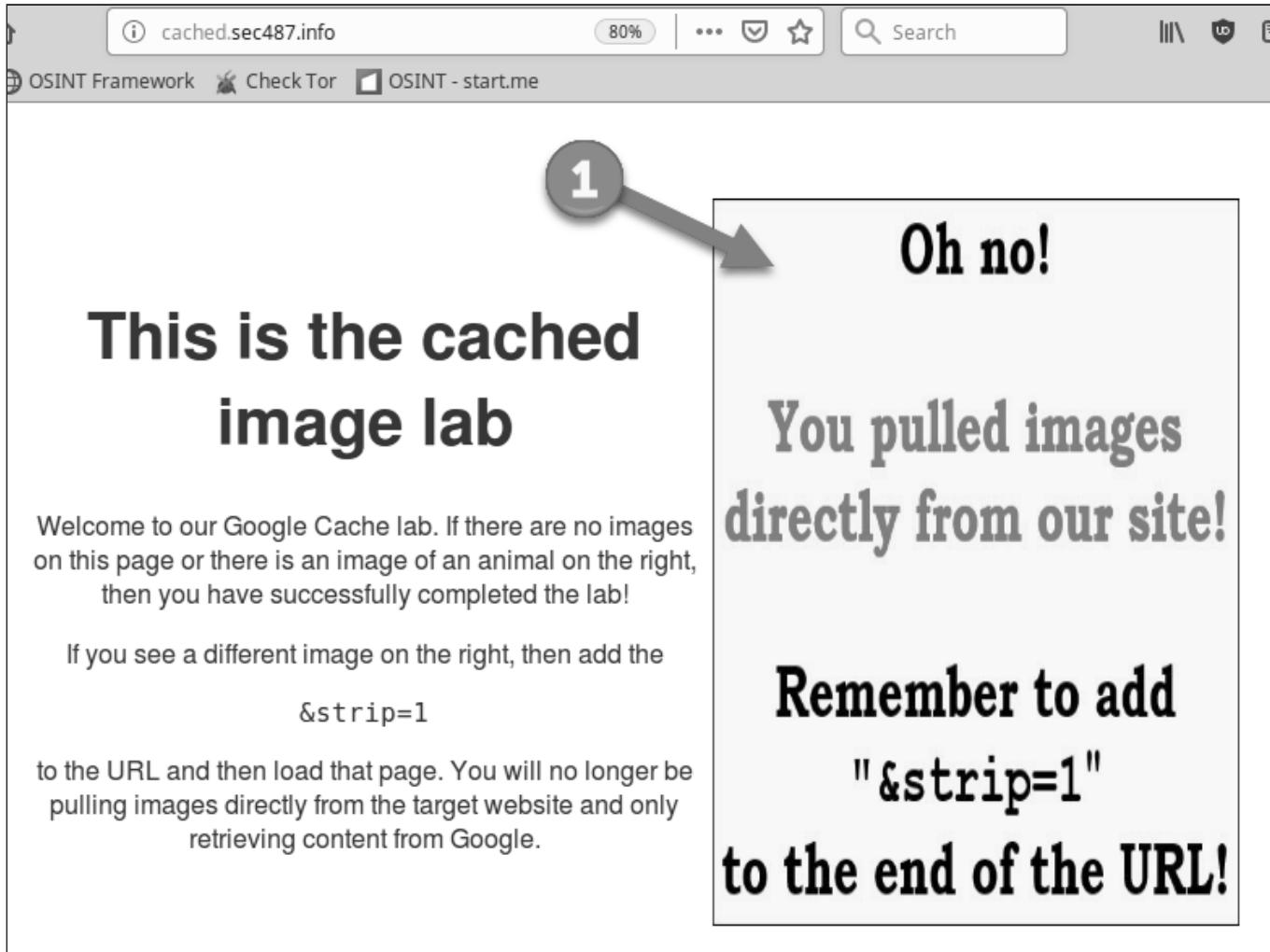
1. Retrieve the original content from <http://cached.sec487.info> without loading images from the site directly (if you see a bright yellow image, you have pulled content from the site instead of cached content)
2. You must use Google Cache but can use other sites as well.

Preparation

VPN if problems

Step-by-step instructions

1. The <http://cached.sec487.info> web site looks like the image below.



2. Search for this domain in Google.
3. View Google's cache for this page. What image do you see? Same one labelled as #1 in the above image or an image of an animal?
4. Use another caching/archiving web site to find the original image that used to be on this site.

 Click Here to See Our Findings

At least 2 other caching or archiving sites have the original content from this site.

1. <http://archive.is>

The screenshot shows a browser window with the URL archive.is/http://cached.sec487.info/ in the address bar. The page title is "archive.today" and the sub-page title is "webpage capture". Below the address bar, there are links for "EC487 Wiki", "OSINT Framework", "Check Tor", and "OSINT - start.me". The main content area displays search examples and a list of URLs ordered from newest to oldest. A thumbnail image of a cartoon character is shown, with the caption "This is a cached image lab". The timestamp "4 Nov 2018 21:04" is visible below the thumbnail.

2. <https://archive.org>

The screenshot shows a browser window with the URL https://web.archive.org/web/*/http://cached.sec487.info/ in the address bar. The page title is "INTERNET ARCHIVE" and the sub-page title is "WayBackMachine". Below the address bar, there are links for "SEC487 Wiki", "OSINT Framework", "Check Tor", and "OSINT - start.me". The main content area displays the text "Explore more than 343 billion web pages saved over time". A thumbnail image of a cartoon character is shown, with the caption "This is a cached image lab". The timestamp "4 Nov 2018 21:04" is visible below the thumbnail. A large grey arrow points to the timestamp "Saved 1 time November 4, 2018." at the bottom of the page. At the bottom of the page, there are links for "Summary of cached.sec487.info" and "Site Map of cached.sec487.info".

This page intentionally left blank.