Shadow Doxing and Anonymity Guide

Written by a real investigator

Shadow Dox Guide
Written by a real investigator.
HackForums Release
UID: 3143060 , 3122298

CHAPTER 1: INTRODUCTION

Thank you for purchasing the shadow doxing guide. This guide will show you how investigators like myself find information on YOU. Some information in this guide will show you never before seen techniques to the doxing community. Before we begin however, I must go over the terms of service with this guide.

1. You may NOT leak/distribute this guide.
2. Payments are final.
3. This is strictly for your own education. I am NOT responsible for your actions with the information you learn from this guide. Please be responsible and only use this information for ethical and legal purposes.

SECTION 1: WHAT IS DOXING? AND WHY DO PEOPLE DOX?

"Doxing" is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organization. -Wikipedia

People dox for many reasons like to display power, revenge, harassment, extortion, or even background checks. One great real world example of this would-be companies doing background checks and looking at your social media to see if you would fit well with the organization. Many organizations do this because they do not want an immature person to work with them. The term "Be careful what you post online" or "Once you post something online, there is no deleting it" sort of thing is somewhat true. Something you post 3-4 years in the past could really put you at risk for doxing attacks. One of the most fundamental rules for doxing is to always take a peek at the past.

SECTION 2: PREPAIRING TO DOX

Before you can get started with a dox, you must first complete some tasks to organize and simplify your experience. The first thing I do when starting an investigation is simply, create a folder for the particular person. Any images, videos, or files that you may need to save about this individual you can save here for local storage. If you plan on going the cloud route, you can use Google Drive, but I would not recommend this (Encryption of the documents will be discussed later). So, you have your folder and possibly sub-folders for better organization, but now we need to build a template for our individual. Templates can be simple or complex depending on how much information you are looking for. If you would like to view my template click here. You can also find alternative templates online by simply Google searching. Something I also like doing before investigating an individual and that is completely up to you is to create a clean working environment. Close unnecessary applications, disconnect from social media, and move any trash away from your working environment. Keeping your desk tidy and clean has a direct correlation to your productivity.

CHAPTER 2: BASIC METHODS

SECTION 1: SOCIAL MEDIA INVESTIGATION

Social media, everyone has it, everyone uses it. Social media can be the downfall of an individual who is attempting to stay anonymous. Exploiting social media is one of the easiest and gives you the most information on an individual. For example, Facebook is the largest social media platform on the internet with over 1.59 BILLION users and the wealth of information one can gather is ridiculous. Facebook stores information about a particular person like their work and education, places they lived, contact and basic info, family and relationships, and life events like a marriage date. Another key piece of information that Facebook keeps is pictures. Chances are that the person you are investigating has a selfie of themselves on their Timeline which you could add to your folder. If your individual has a private account, you can use social engineering to get on their friends list (You can impersonate one of his/her friends and say that you made a new account and wish to be on their friends list. I have used this method a couple of times and it has worked without flaw). Now you may be asking yourself, what if my individual doesn't have any social media like Facebook? To that I answer, their mom, dad, brother, or sister will. From my experience, you will find more information on the mothers account than the actual targets. Parents are typically naïve and don't think about what they post before they do it. Some things I found on a targets parents where baby pictures, updated pictures, and even places they have been that may or may not be close to home. It is worth taking a peek.

SECTION 2: DRIZZY DOX TOOL

Now, let's say you don't know your targets name so you can search Facebook. Well there are a number of free dox tools on the internet but one that I used to use when I started doxing is called the Drizzy Dox Tool. This tool is VERY easy to use and can find a deaccent amount of information on your target. You simply type in a username or email into a textbox and click the "Search" button. This searches the web for any pages related to that username/email. However, not all the information will be correct. Please do more investigating when using this tool, this tool is only used to get a base on your target. **Also, the more generic the username is, the higher the chances of false positives.**

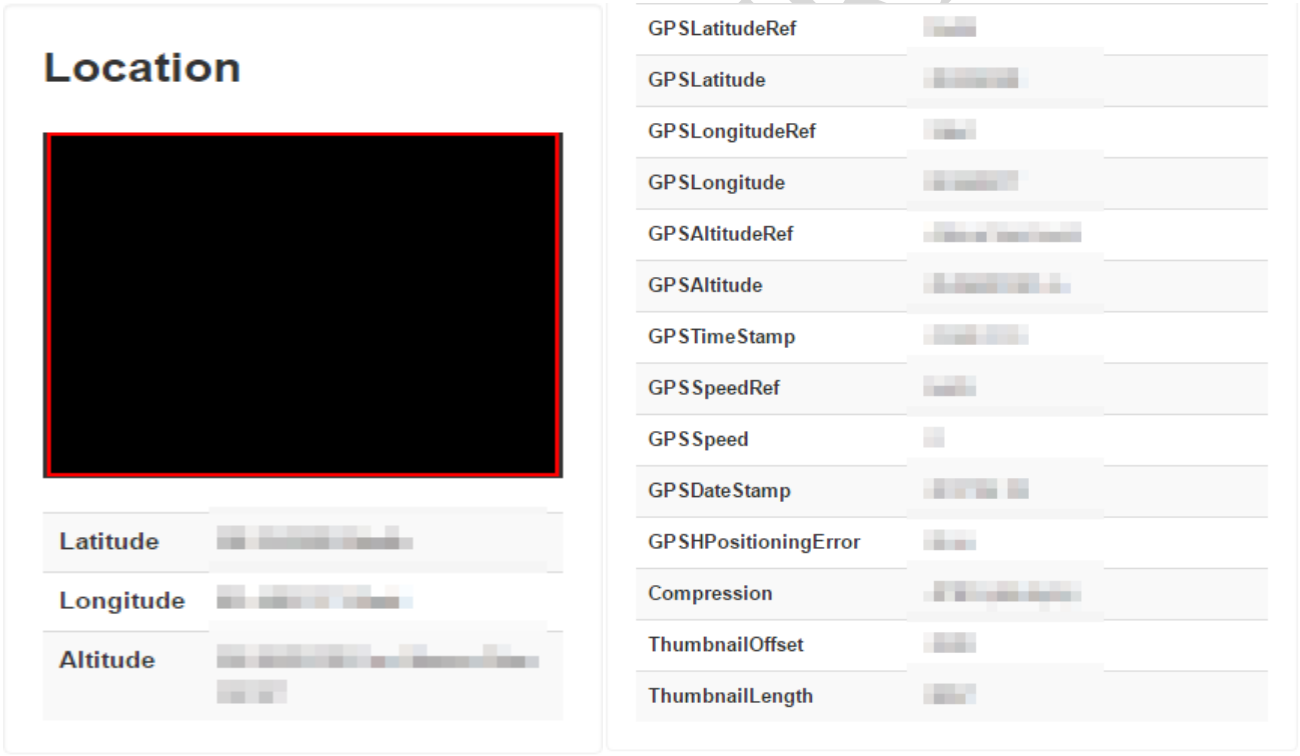
SECTION 3: REVERSE IMAGE SEARCHING

So, you found an interesting image like a selfie or custom profile picture. Here is a simple yet VERY effective way to see where else this image lies on the internet. All you need to do is head on over to TinEye.com. Once on TinEye.com, you can either copy/paste, upload, or place the URL of the image in the search box. This will search through the internet of that image and trace back copies of it. From here you can visit the links found for possible usernames/emails.

CHAPTER 3: ADVANCED METHODS

SECTION 1: EXIF DATA

"Exchangeable image file format is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. The specification uses the following existing file formats with the addition of specific metadata tags: JPEG discrete cosine transform (DCT) for compressed image files, TIFF Rev. 6.0 (RGB or YCbCr) for uncompressed image files, and RIFF WAV for audio files (Linear PCM or ITU-T G.711 μ-Law PCM for uncompressed audio data, and IMA-ADPCM for compressed audio data). It is not used in JPEG 2000, PNG, or GIF." -Wikipedia. For example, exif data can be exploited if you have location services enabled your phone and you take a picture. The scary part is that not a lot of people seem to know about this feature in modern smartphones and this data hidden in images can be highly alarming. Below is just the location aspect of exif data, on the full report it showed many more important pieces of data down to if the flash went off or not. The site I used to extract the data was metapicz.com.



SECTION 2: FACEBOOK EMAIL GRABBING

Surprisingly there is a way to get Facebook emails, it's very simple as well. You will need a Yahoo account for this so go ahead and make one. Doing this requires you to be on your targets friends list so make sure you get there somehow either by sending them a random request or impersonating one of their friends with a new account.

1. First, get on to your targets friends list.
2. Next locate the "Import Contacts" button in Yahoo Mail.
3. Then Select Facebook then press **CRL + F** and search for your targets name.

SECTION 3: IP DOXING

Getting the IP address of your target can get you the location, internet service provider, and more. Using tools like Wireshark in a Skype call can easily grab someone's IP without them knowing. There are other methods of getting someone's IP address like sending them a link that logs their information. One site I love to use for this is grabify.link. Simply clicking on a Grabify link will get your IP logged as seen below.

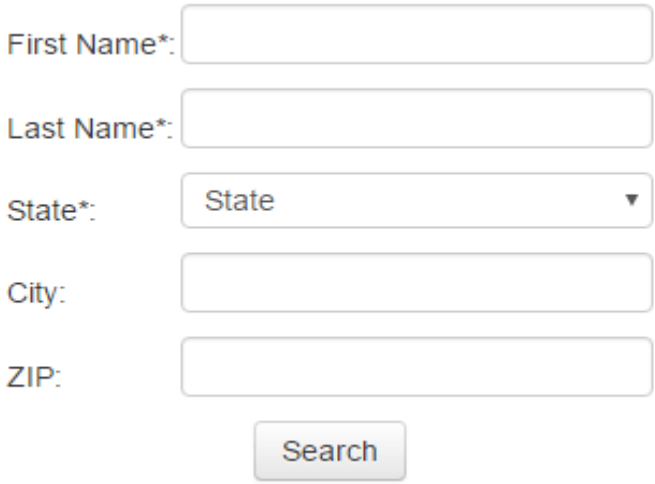
Date/Time	IP Address	Country	User Agent (Hover or tap for more information)	Referring URL	Host Name	ISP
[redacted]	[redacted]	[redacted]	[redacted]	*no referrer*	[redacted]	[redacted]

If you know your target hosts a website it is very easy to get possible addresses, phone numbers, work locations, and even their full name and emails! Many investigators know about this method and it is used by network admins and tech enthusiasts around the world. The website I will be showing you today is whois.domaintools.com. To get information about who is running the website simple type into the search bar the website**.** Example Below: YouTube

```
Registrant Name: DNS Admin
Registrant Organization: Google Inc.
Registrant Street: 1600 Amphitheatre Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
```

SECTION 4: SOCIAL SECURITY NUMBERS

Alright, so social security numbers can be a little tricky to get but, there is one site that I know of that can easily get them. That site is called ssndob.so. SSN are rather cheap on this site ranging from $1.50 to $5.00. However, for this method you will need some pocket change to pay for it. This site only accepts bitcoin so you might as well create a blockchain account. Searching is easy however obtaining the SSN of your target will most likely be one of the last things you do as you will need their relative location (If you know their name you can send them a Grabify link for their location!).



#	Names	DOB Year	Address	SSN	DOB	Action
1	[redacted]		[redacted]	[redacted]	[redacted]	Buy $1.8

SECTION 5: PAYPAL DOXING

Most people today use PayPal for online transactions. Unfortunately, PayPal is vulnerable to doxing. This PayPal method can be exploited to obtain a targets name, date of birth, address, email, phone, and more. All you will need to do is to send $0.01 to their account and you should get a notification with their name.

SECTION 6: OBTAINING HOME INFORMATION

Once you have found your targets address, it is almost essential to take a screenshot and place it in your folder. You can also view information about a house on websites like Zillow.com. Here is an example of a random house and what information you can gain from it.

INTERIOR FEATURES

Bedrooms
Beds: 4

Heating and Cooling
Heating: Other
Heating: Gas
Cooling: Central

Basement
Finished basement

Appliances
Appliances included: Dishwasher, Microwave

Flooring
Floor size: 1,536 sqft
Flooring: Carpet, Hardwood, Laminate, Linoleum / Vinyl

Other Interior Features
Fireplace
Ceiling Fan
Room count: 7

CONSTRUCTION

Type and Style
Structure type: Other
Single Family

Materials
Roof type: Other
Exterior material: Brick, Wood

Dates
Last remodel year: 2008
Built in 1969

Other Construction Features
Stories: 0

EXTERIOR FEATURES

Patio
Deck

Yard
Fenced Yard

Lot
Lot: 0.4 acres

Other Exterior Features
Parcel #: 4000072008014000

COMMUNITY AND NEIGHBORHOOD

Schools
Elementary school: GREEN VALLEY
Middle school: SIMMONS, IRA F
High school: HOOVER

PARKING
Garage spaces: 4
Parking: Garage - Attached
Covered parking spaces: 4

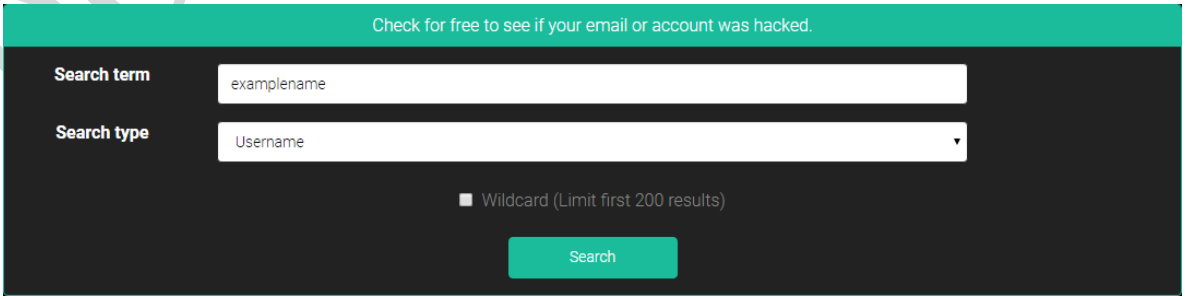
UTILITIES
Sprinkler System

SOURCES
MLS #: 780858

OTHER
Last sold: Jun 2008 for $204,900
Price/sqft: $130
PropertySubType: Single Family Detached, PropertyType: Residential

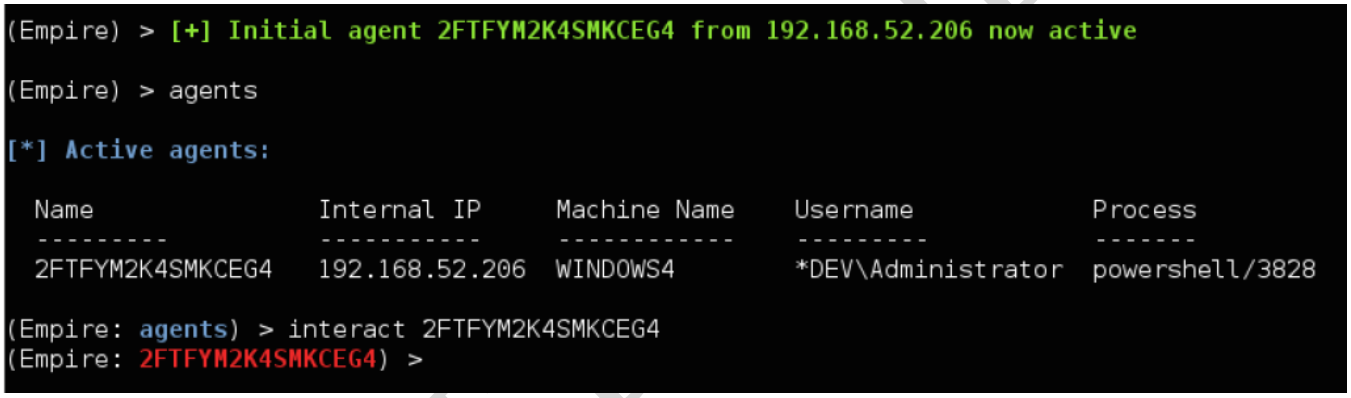
SECTION 7: PASSWORD AND DATABASE SEARCHING

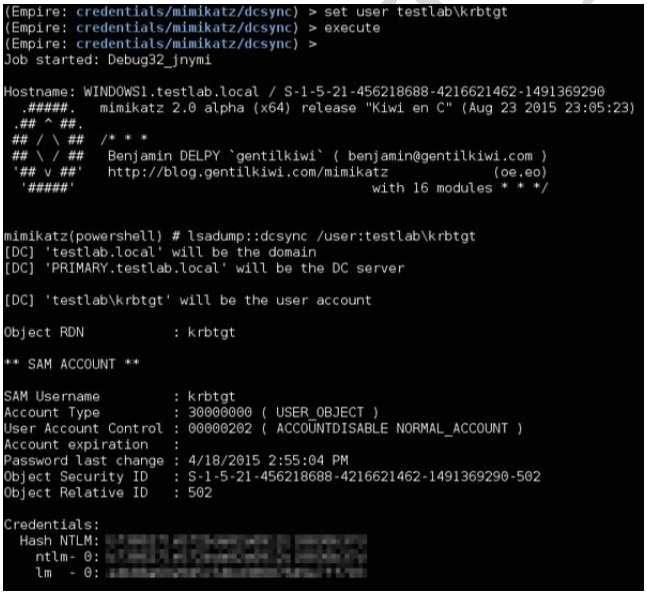
Searching databases can be the easiest way to dox your target. LeakedSoruce used to be a very popular database search site. Unfortunately, LeakedSoruce was raided by the feds. Leaked source allowed you to search for any email, username, IP address, and phone number. Then it would display account passwords associated with that data. LeakedSoruce has over 3 billion accounts in its database. Fortunately, there is a clone of LeakedSoruce that can be found here , however I do not know the accountability of this site. Please be careful when making purchases. Another site for database searching is leakbase.pw. This site offers a 1 day trial with a low cost of $1.00.

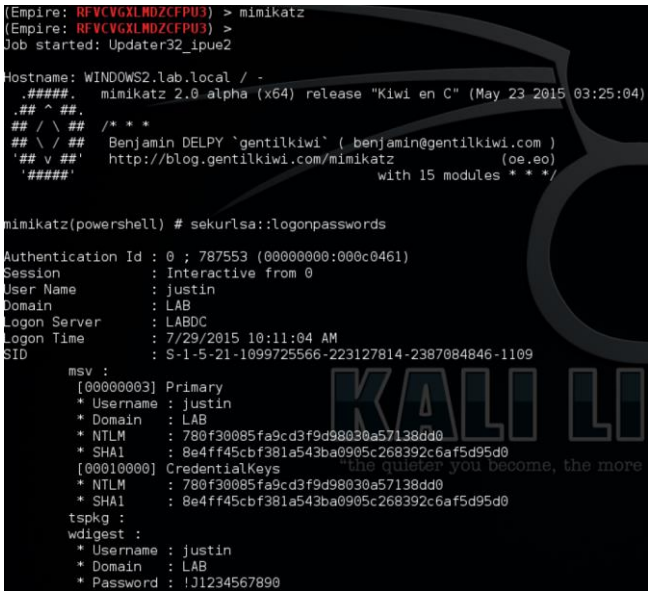


SECTION 7: REMOTE ACCESS

Before I get into this topic, I just want to say that this method is highly illegal and I do not recommend it. This is the most advanced you may ever get at doxing. Using this method requires you to have either physical access or be willing to get your target to download and execute a .bat payload. What this method includes is getting remote access into your targets computer to extract files, cookies, passwords, and even spy on your target. *"Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework."* -PowershellEmpire. Powershell Empire (from what I have used) is FUD and will not raise any detections with anti-virus. Using this tool requires Kali Linux to operate as it has compatibility packages pre-installed on the operating system. You will also need a VPN that is port forwardable and a DNS. There are many tutorials on the internet on how to use this fantastic tool so you can dip your toes into the world of RATing.

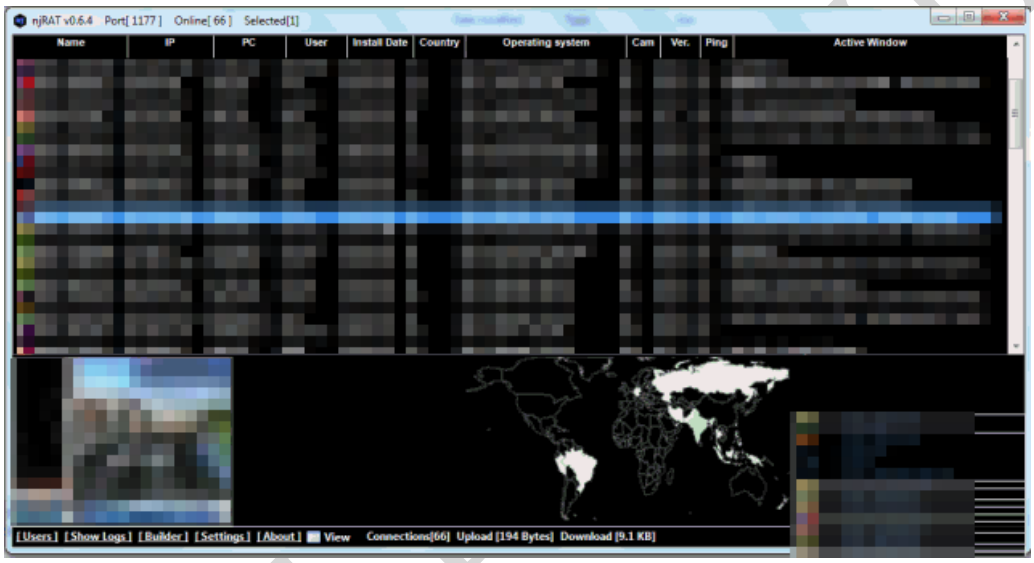


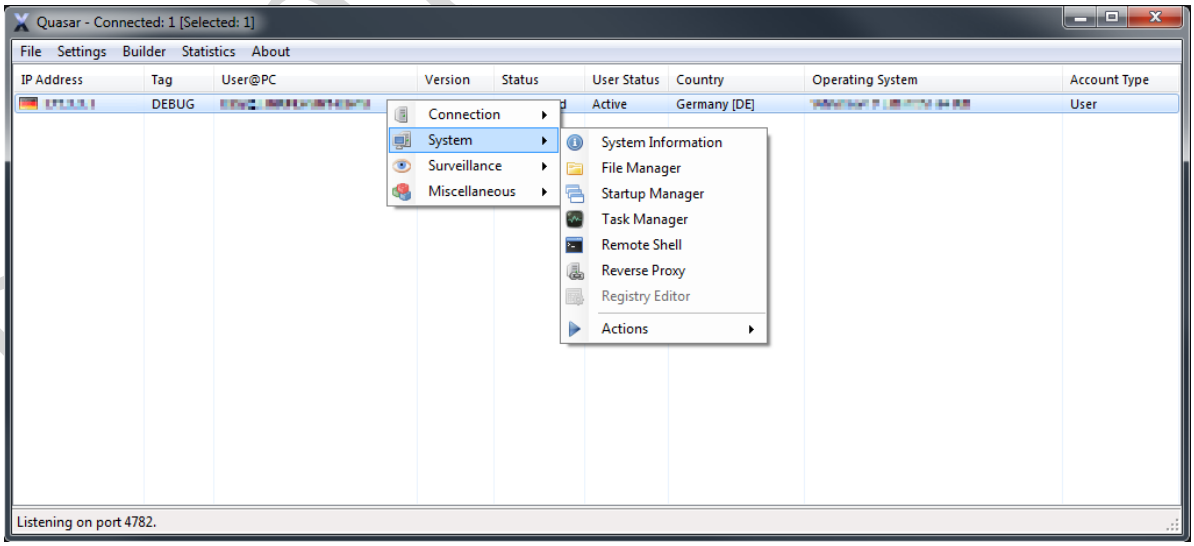




SECTION 7: REMOTE ACCESS

There are also other free and paid “RATs” on the market however you should note, that if you purchase a remote administration tool you may break their terms of service if you use it without your targets permission. For this reason, I recommend using a free RAT like Quasar or njRAT as seen below. You may also need a FUD crypter as your stub will cause detections. Crypters can range in price from $25-$200 or more. (Images taken from online source)





CHAPTER 4: ENCRYPTION & HIDING YOUR FILES

SECTION 1: TEXT FILE ENCRYPTION

Encrypting your doxes can be very simple and only take one to two minutes at most. This method can NOT encrypt anything other than text documents however, so this will only be valid with the actual dox, not the images or downloaded files in your dox folder.

1. Head on over to aesencryption.net.
2. Copy the dox and paste it into the main box on the site.
3. Next set the encryption key to a secure passphrase, you will need to type this in to decrypt the dox later.
4. Set the encryption key to 256 Bit for it to be the most secure.
5. On the bottom right click the "Encrypt" button.

Once you are done encrypting simply copy and replace the scrambled text into your .txt file and click "Save." You have now successfully encrypted your targets dox.

SECTION 2: WINRAR ENCRYPTION

If you wish to encrypt your folder with your targets information inside, I would recommend encrypting it with an application called WinRAR. WinRAR is free and simple to use so things won't get complicated. WinRAR uses AES-256 encryption for RAR5 archives so we will be storing it with this.

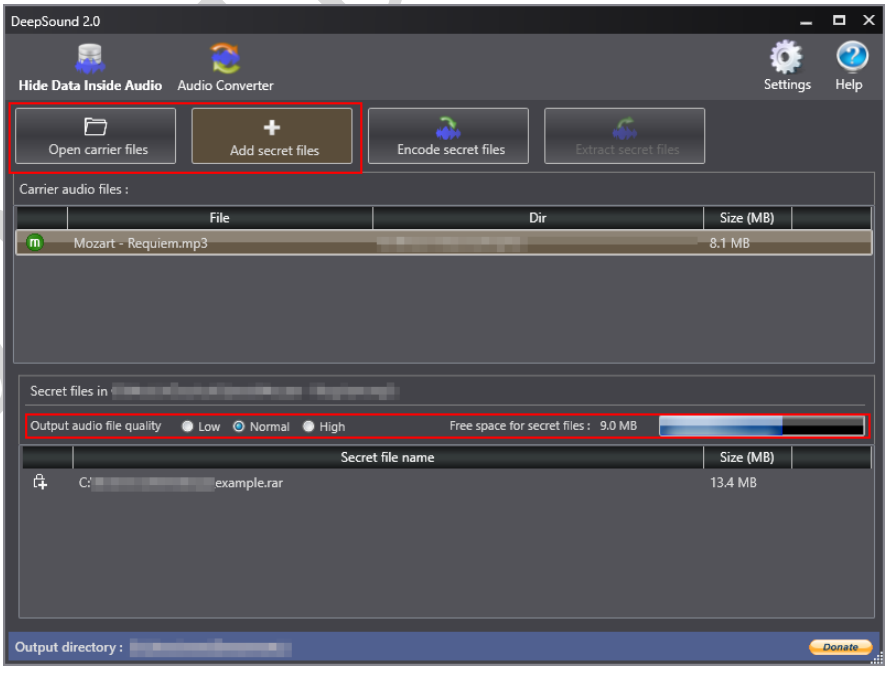
1. Download and install WinRAR from this website here.
2. Once installed, right-click your folder and select "Add to archive…"
3. Under archive format chose "RAR5."
4. Under archive options select "Lock archive" and click the "Set password…" button.
5. Enter your desired password and make sure to include capital letters, numbers, and symbols. This makes your archive much harder to brute force if someone was to get their hands on it; then click the "OK" button.
6. Done! You have encrypted your file.

SECTION 3: STEGANOGRAPHY

"Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video." -Wikipedia. When I am done encrypting my doxes I use steganography to hide them I'm ordinary music files on my computer. One great thing about storing doxes inside of music files is that nobody is going to want to steal music from your computer or if your computer is being investigated by the government, there is a low chance they will ever check your music files. Also, fun fact, your music does not get corrupted and still plays completely fine. Alright, so the tool I will be using today is called "Deep Sound." Like most of the tools in this guide it's easy to use.

1. Download and install Deep Sound here.
2. Click the big button on the left that says "Open carrier files" this will be the audio file that the dox will be stored in.
3. At the bottom select the file quality, higher quality equals less space to store your files.
4. Next click the second large button that says "Add secret files" and add your .rar file.
5. Once you are done click the third button that says "Encode secret files," select the file output and check "Encrypt secret files (AES 256). Like the WinRAR password, make sure you use capital letters, numbers, and symbols.
6. Finally, click the "Encode secret files" button and you should be good to go.

I like to hide my music in a playlist, if you choose to do so for even more fool proof storing, write the music files to CDs and keep them in a CD player.



CHAPTER 5: STAYING ANONYMOUS ONLINE

SECTION 1: SOCIAL MEDIA

In the beginning of this guide I said *"Social media can be the downfall of an individual who is attempting to stay anonymous. Exploiting social media is one of the easiest and gives you the most information on an individual."* I believe this is completely true because almost every single person I investigated had either a selfie or compromising image on their social media account, not to mention it contain their name and location. So, I strongly urge you today to go onto old social media accounts and delete old, compromising posts or either make your account private. But beware, investigators will try to social engineer you to add them on to your friends list. Also, be smart on what you post online. Before I post online I always ask myself *"Is there any compromising information in this picture?"* Think real hard about this one because one slip-up like a random cars license plate in the background could lead to your location.

SECTION 2: USERNAMES, PASSWORDS, AND EMAILS

One of the biggest issues I see today is people using the same username and password for everything. Let me explain why this is bad but it should be pretty self-explanatory.

1. Your username will be the same therefore making it easier to dox and trace you years down the line.
2. If you use the same password for everything then it doesn't take much for all of your accounts to be compromised, let's say you use the password **ABC123** for every online account you have, if I where to find that password in a database like LeakedSource or LeakedBase, then your whole online life would be compromised.

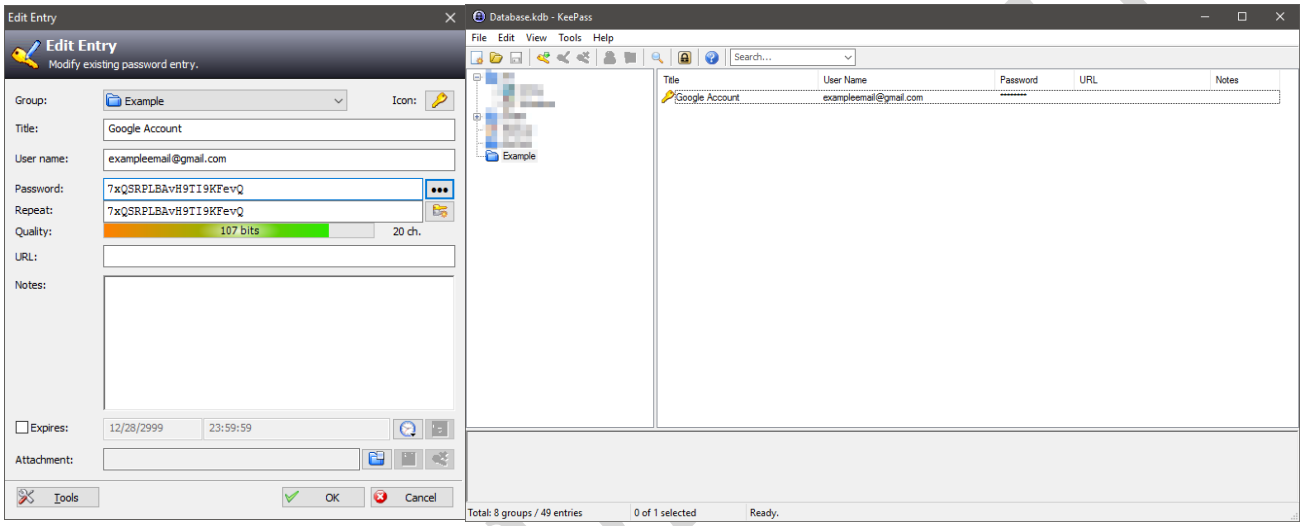
Another issue I see is people using little to absolutely no complexity to their passwords. Most people's passwords are either a family member, a single word, or a word with their birth year at the end. Another issue that people don't realize is that common passwords are typically easier to crack or the hashes are already online. You can see how secure your passwords are by visiting these websites here and here. KeePass is an application I use to safely store my usernames and passwords locally on my computer. KeePass is easy to setup and use and here is how to do it.

1. Download and install KeePass here.
2. Go to file then new and set a secure master password.
3. Now right-click in the large blank white space and click "Add Entry…"
4. Set the title, username, and let KeePass auto set the password.
5. As you can see the account has been added to the database. You can now add other accounts and update passwords this way.

Please note that if you lose the database file (.kdb) all of your logins will be lost. What I like to do is only make your email have a login that you know by heart but still complex in case you lose access to your logins and need to recover your accounts.

SECTION 2: USERAMES, PASSWORDS, AND EMAILS

Also, I recommend updating your database file in a cloud storage server so you can safely back it up. Below are some images of KeePass.

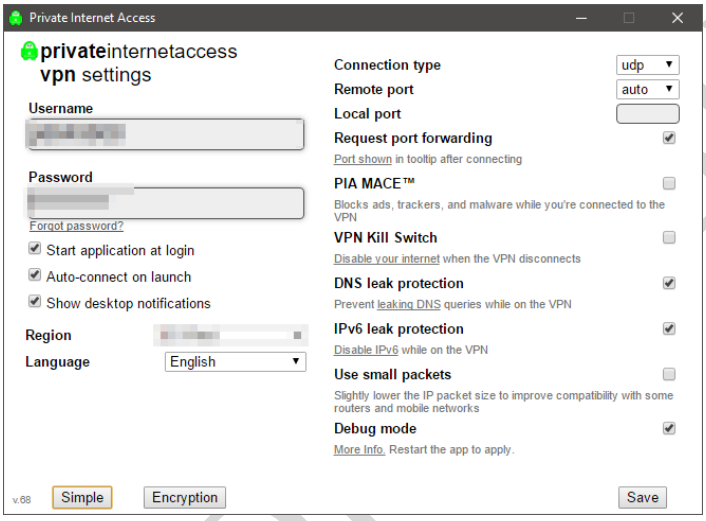


If you plan on creating a new identity online, make sure you use either a common name or a name of a famous person. Doing this could minimize the chances of being doxed because investigators will need to sift through a LOT more search results to find your accounts. Emails are also something you should keep private, one email service that I use is ProtonMail.com because its free and offers encryption for your inbox.

SECTION 3: VPNS PROXIES AND TOR

One of the things that can get you compromised is your IP address. If an investigator find your IP address they can obtain information on your Internet Service Provider (ISP), location, and they can search databases where your IP address has been used to create accounts. Investigators are also known to call ISPs and impersonate employees to try and obtain information like your address. This is why it is absolutely vital to use some sort of VPN or proxy when browsing the internet. Also, your ISP can log your traffic, so they can see whatever you search online. With an encrypted VPN they can no longer see that information. One VPN that I recommend is Private Internet Access. PIA has many servers to choose from around the world. You can also choose your encryption method while using the VPN. PIA also claims to not store logs.

PIA also works for Windows, Mac, and Linux. I personally use PIA for my online browsing and I can vouch for them. Below are some screenshots of the interface.



Data Encryption

- AES-256
- AES-128
- None

Data Authentication

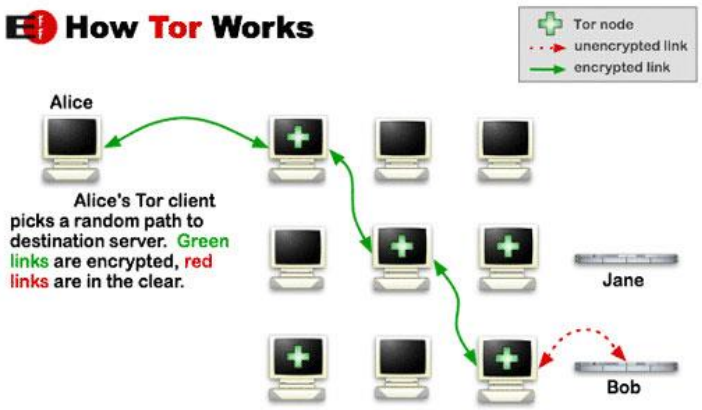
- SHA-256
- SHA-1
- None

Handshake

- RSA-2048
- RSA-3072
- RSA-4096
- ECC-256k 1
- ECC-256r 1
- ECC-521

SECTION 3: VPNS PROXIES AND TOR

Proxies are also a great thing to use if you want anonymity. The difference between a proxy and VPN is that a proxy only secures on particular service like HTTP or HTTPS. VPNs encrypt your whole network using a "tunnel." TOR is also a VERY great option for anonymity as it randomizes and encrypts your connection to websites. TOR is also complex so I will not be spending that much time on explaining it but you can read all about it here and here. Down below is an example of a TOR network.



SECTION 4: CREATING A NEW IDENTITY

If you plan on creating a new identity online it is always great to start with the username. Create a username based off of a popular person or online celebrity. Many people on online forums use other people's names as a display name. For example, if you are signing up for a forum and wish to stay anonymous use a name like Tom Cruise or PewDiePie. This is because if someone is doxing you, it will take ages for them to sift through forums, accounts, and possible passwords to find you. Use a new email too, don't use an old email address as this could still be traced, and finally, the hardest part of all, drop all connections with people you know online. If someone where to find out your old identity you could possibly be doxed.

CHAPTER 4: CONCLUSION AND USEFUL LINKS

Well, that's really all there is too doxing and staying anonymous online. Of course, you can go online and search for other topics like OSINT (Open-Source Intelligence) that may aid you in a dox, but this was a big chunk of information you would need to know to successfully complete a dox. I am now going to list some useful sites that are self-explanatory to use. Please feel free to contact me via PM if you need any information regarding doxing. Anyways, thank you for purchasing my guide and good luck on your doxing adventures!

PEOPLE SEARCHING

- https://pipl.com/
- http://www.whitepages.com/
- https://www.yellowpages.com/
- http://thatsthem.com/
- http://www.peekyou.com/united_kingdom
- http://webmii.com/
-

ADDRESS SEARCHING

- https://www.zillow.com/
- http://www.whitepages.com/

PHONE NUMBER SEARCHING

- http://www.reversemobile.com/index.php
- http://www.whitepages.com/
- https://pipl.com/
- http://thatsthem.com/

IP ADDRESS SEARCHING

- http://whois.domaintools.com/
- http://www.ip-tracker.org/