Yeti Level 3 PDF

This is a PDF to walk you through the Yeti Level 3 Wallet setup. Why have a PDF?

Yeticold.com is hosted outside of Yeti's control. While a website allows for a nice user experience, easier maintenance, and faster onboarding, it ultimately isn't secure. Even with TLS, 2FA, registry locks, etc, a number of attack vectors exist (the host owns you, other people have physical access to the server, BGP hijacking…)

A PGP signed PDF enables you to **distrust all of this infrastructure**. You no longer have to trust the DNS services, website, server, etc.

But what can a PGP signature prove?

I believe this is a common misunderstanding. Seeing a PGP signature verify does not mean you are "in the clear".

When a file's signature passes verification, that means that the file's **integrity** has been cryptographically proven. A failure of integrity would indicate that the file has been tampered with en route. However, who has signed the file? In order to properly verify the **authenticity** (did the signature actually come from the person who is claiming to own that signing key?) you must check the fingerprint of the key from *multiple, independent sources* in *several different ways*.

For example, any attacker can sign a malicious copy of this PDF, with a PGP key labeled "Yeti", and post it on a website Yet1.com. If you were to merely verify the signature, the signature would verify properly, and the attack would be successful. To mitigate this, you should properly authenticate the key used to sign the malicious PDF. You would see that the malicious key had a fingerprint (for example) of XXXX XXXX XXXX 1234, while the valid key had a fingerprint (this is real) of BF0D 3C08 A439 5AC6 11C1 5395 B70B 4A77 F850 548F. You can check this on our Slack, on Podcasts I have been on where I have read it outloud, my public Twitter and email, as well as other forum posts. You should also check this via Tor to avoid network based attacks.

This is the same key that I will use to sign this PDF.

Yeti Level 3 is a 3 of 7 HD Multisig setup where private keys are never on an Internet connected device

There will be 2 laptops used during this guide; the Primary Laptop, and the Secondary Laptop.

Step 1: Gather and Label Required Equipment

- 2 laptops that can run Ubuntu and Bitcoin Core. Almost any laptop made for Windows will work, but if your laptops have an SSD type hard drive some steps will take a few hours instead of a few days. Laptops without SSD type drives cost about $150 USD and laptops with SSD drives cost about $200 USD. Label one laptop "Primary" and the other "Secondary."
- An optical drive to write to the CDs. Most laptops come with one built in, but you can also buy an external optical drive for about $15 on Amazon.
- 14 blank CD-R disks. Label 7 of the blank disks "Descriptor" and the other 7 "Seed 1" "Seed 2" "Seed 3" through "Seed 7."
- A printer and printer paper.
- 2 USB thumb drives. These will cost about $3 each and will be used to install Ubuntu and to transfer transactions between your laptops. Label one "Ubuntu" and the other "Transfer."

Step 2: Install Ubuntu and Label Laptops

Install Ubuntu on both laptops following these rules.

- Use the Long Term Support (LTS) Version of Ubuntu. This is currently 20.04 and is at the top of the download page. Yeti has not been well tested with any other Ubuntu version or Linux distribution.
- If needed, use only trustworthy guides such as the one on the official Ubuntu website
- Make sure to verify the Ubuntu iso download. Another PDF will be released for this. The key fingerprint 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092 should be the key that has signed the Ubuntu download. If not, contact our Slack.
- Use the USB drive you labeled "Ubuntu" to create a Bootable Ubuntu drive. A PDF will also be created for how to do this on Windows and Mac.
- Select **Try Ubuntu**, and then use the **Disk Utility** to delete and erase all existing partitions.
- Create a new partition consisting of the entire device, and then install Ubuntu on that new partition.
- After you see the desktop click on the **9 Dots** in the bottom left corner of your Ubuntu desktop and then click **Software Updater** and then **Install Now** to install the latest security updates.

After the above has been completed on both the Primary Laptop and the Secondary Laptop:

Step 3: On your Primary Laptop:

Step 4: Download Yeti

- On your Primary laptop click on the **9 Dots** in the bottom left corner of your Ubuntu desktop and then click **Terminal**.
- **Copy** the text on the below bullet point
- sudo apt-get update; yes | sudo apt-get install git; git clone https://github.com/jwweatherman/yeticold.git ~/yeticold; python3 ~/yeticold/initialize.py YetiLevelThreePrimary
- In the terminal window right click and select **Paste** and then click **Enter**. (Do not type control+v).
- Yeti will automatically open a Firefox tab that displays step 5.

You are not visiting an external website, but rather using Firefox to display the GUI of Yeti. This is safe. Click **Create Wallet**. You will be presented with Step 5 and Bitcoin Core.

Step 5: Finish Downloading the Blockchain

Step 5 is going to direct you to wait for the blockchain to download on your Primary Laptop. While you wait, Step 5 will tell you to go to your Secondary Laptop, and to visit a URL to begin setup of that device. DO NOT DO THIS. This would introduce trust of the infrastructure. Instead, continue this guide below, which directs you in the same manner the website would.

Step 6: Set up Yeti on your Secondary Laptop

- On your Secondary laptop click on the **9 Dots** in the bottom left corner of your Ubuntu desktop and then click **Terminal**.
- **Copy** the text on the below bullet point
- sudo apt-get update; yes | sudo apt-get install git; git clone https://github.com/jwweatherman/yeticold.git ~/yeticold; python3 ~/yeticold/initialize.py YetiLevelThreeSecondaryCreate
- In the terminal window right click and select Paste and then click Enter. (Do not type control+v).
- Yeti will automatically open a Firefox tab that displays step 7.

Again, you are not visiting an external website, but rather using Firefox to display the GUI of Yeti. This is safe. You will be presented with Step 7 and Bitcoin Core.

Step 7: Finish Downloading the Blockchain

- Because this device is only used to sign transactions it does not need to download the blockchain so you will be able to click **Next** within about 10 minutes.
- Yeti has opened Bitcoin Core. When Bitcoin Core is ready the button will be enabled and you should click **Next** to continue.

Continue to follow all Steps on the Secondary Laptop:

Disconnect your network cable if you have one, further randomize your bitcoin seeds if you wish, copy your seeds to your CDs, and copy the descriptor to CDs.

Be sure to follow the detailed instructions given on all Steps.

The final action (Copy Descriptor to CDs) is Step 11.

Afterwards, move back to your Primary Laptop

Your Primary Laptop was left at Step 5: Finish Downloading the Blockchain, and should be finished by now. If not, wait until it is done syncing, and then click **Next** to continue to Step 12 (still on your Primary Laptop).

Step 12: Import Descriptor

- Insert any of your CDs labeled “Descriptor”
- Click the **Browse** button and select the **Descriptor.txt** from the CD drive
- Click the **Next** button

Continue to follow all steps on the Primary Laptop:

Print the instructions recovery page.

Be sure to follow the detailed instructions given on all Steps.

Step 14: Switch to your Secondary Laptop.

- Switch to your Secondary Laptop, which is currently showing Step 11 (Copy Descriptor to CDs). On Your Secondary Laptop click **Next** to show Step 15.

Step 15: Write Down Private Key 1 of 7

- Your private key is displayed using the NATO phonetic alphabet, with a checksum
- Write down the words on the packet you printed out earlier.
- Click **Next**

Continue to follow all detailed steps on the Secondary Laptop:

Write down Private Keys #2 through #7, and Check Seeds #1 through #7.

Step 29: Switch To Your Primary Laptop

Switch to your Primary Laptop currently showing Step 14 and on your Primary Laptop click **Next** to show Step 30

Step 30: Copy Erase file to USB

- Insert the USB drive labeled “Transfer”
- Open the **Files** application and click on **Documents.**
- Copy the folder named “erase.txt” to the USB drive.
- Eject the USB drive then click **Next**

Be careful that you don’t delete this file when you use the USB to send and receive transactions.

Your Yeti Wallet is now ready to test by sending and receiving small amounts.
The end of Step 30 instructs you to visit a URL in order to view Step 31 and continue this testing. DO NOT DO THIS. This would introduce trust of the infrastructure. Instead, continue this guide below, which directs you in the same manner the website would.

Step 31: Send and Receive using Bitcoin Core

Follow the substeps below to send and receive a small amount to confirm your wallet is working correctly.

Receive

Step 1: Open the Receive Tab

- In the Bitcoin Core application on your Primary Laptop click the **Receive** button in the menu bar.

Step 2: Create a New Address

- Click **Create new receiving address**.

Step 3: Send Bitcoin

- Confirm that your wallet shows "yetiwalletpub". You should now send a small amount of test money to the wallet using the QR code or the address displayed below it.

Send

Step 1: Open Options

- In the Bitcoin core application on your Primary Laptop click **settings** and then **Options**.

Step 2: Open the Wallet tab

- Click on **Wallet.**

Step 3: Enable Coin Control

- Check the **Enable Coin Control features** box and the click **OK**.

Step 4: Open the Send Tab

- Click **Send**.

Step 5: Open the Inputs page

- Click **Inputs**.

Step 6: Select UTXOs

- Select the UTXO you wish to spend and then click **OK**.
- Because of how Core currently handles descriptors, you must spend UTXOs in full

Step 7: Enter the Address and Amount

- Paste the recipient’s address in the **Pay To** text box, then click **Create Unsigned**.

Step 8: Create the PSBT

- Review your transaction then click **Create Unsigned**.

Step 9: Select Save

- Click the **Save** button.

Step 10: Save the PSBT

- Select the **Documents** Folder and then click **Open**.

Step 11: Rename the PSBT

- Rename the file to "unsigned.psbt" then click **Save**.

Step 12: Unsigned PSBT to USB

- Insert the USB drive labeled "Transfer" to your Primary Laptop.
- Copy the file labeled "unsigned.psbt" to the inserted USB drive. The file is located in your "Documents" folder.
- Eject the USB drive.

Step 13: Unsigned PSBT to Secondary Laptop

- Insert the USB drive labeled "Transfer" to your Secondary Laptop.
- Copy the file labeled "unsigned.psbt" to the "Documents" Folder.
- Eject the USB drive.

Step 14: Load the PSBT

- In Bitcoin Core click **file** and then **Load PSBT from file...**

Step 15: Select the PSBT

- Select the "unsigned.psbt" file and then click **Open.**

Step 16: Sign the PSBT

- Click **Sign Tx.**

Step 17: Save the PSBT

- Click **Save** to save the newly signed PSBT.

Step 18: Save to Documents

- Select the "Documents" Folder, change the name to "signed.psbt" and then click **Save**.

Step 19: Signed PSBT to USB

- Insert the USB drive labeled "Transfer" to your Secondary Laptop.
- Copy the "signed.psbt" file from the "Documents" folder to the USB drive.
- Eject the USB drive.

Step 20: Signed PSBT to Primary Laptop

- Insert the USB drive labeled "Transfer" to your Primary Laptop.
- Copy the file labeled "signed.psbt" to the "Documents" Folder. The file is located in your USB drive.
- Eject the USB drive.

Step 21: Load Signed PSBT

- In Bitcoin Core click **file** and then **Load PSBT from file...**

Step 22: Select Signed PSBT

- Select the "signed.psbt" file in your "Documents" folder and then click **Open.**

Step 23: Broadcast the Transaction

- Click **Broadcast Tx.**

Step 24: Confirm Broadcast

- Review the page and then click **Close**.
- If this was successful, this confirms that your wallet is setup correctly

This completes the substeps of Step 31 (Send and Receive using Bitcoin Core) at the bottom of Page 5.

END

Continue to the next page (Page 9) to continue to the next step - Step 32: Restore Your Wallet.

Step 32: Restore Your Wallet

- Set aside the three seed CDs labeled "Seed 1," "Seed 2," and "Seed 3."
- Restart Yeti on your Primary Laptop by clicking on the nine dots in the bottom left corner and click the Level Three icon.

Continue with the following substeps:

When asked to Create or Recover Wallet, Click **Recover Wallet**.

Select **Skip Secondary Install**

Core will open, and you will be redirected back to Step 5: Finish Downloading the Blockchain
This will take some time to have Core resync. While you wait, you can continue below:

On your Secondary Laptop click on the **nine dots** in the bottom left corner and then open **L3Recover.**

This will redirect you to Step 6: Skip Secondary Setup
Click **Next.**

Step 7: Finish Downloading the Blockchain
This opens up Bitcoin Core. Because this device is only used to sign transactions it does not need to download the blockchain, so you will be able to click **Next** within about 10 minutes

Continue to follow all detailed steps on the Secondary Laptop:

Disconnect your network cable if you have one, import your descriptor, and import the three different Seeds that you set aside earlier.

You should now be on the substep Step 13: Switch to your Primary Laptop

- Switch to your Primary Laptop currently showing Step 5 (Finish Downloading the Blockchain) and click Next to show step 14

If your Primary Laptop has finished downloading the Blockchain, click **Next.**

Continue to follow all detailed steps on the Primary Laptop:

Import Descriptor, Rescan Blockchain, and Copy Erase file to USB

Yeti will then tell you to visit a URL to test receiving and sending with the recovered wallet. DO NOT DO THIS. Instead, repeat the test process you have already done from pages 6-8 (you will have to either delete or overwrite the old ‘unsigned.psbt’ and ‘signed.psbt’ files that are on the Transfer USB). Return to the next page - Page 10 (instead of Page 9) afterwards.

Now, Repeat all of Page 9 with Seed 4, Seed 5, and Seed 6.

To summarize, on your Primary Laptop, you must:

- Restart Yeti
- Recover Wallet
- Skip Secondary Install
- Download the Blockchain

Then on the Secondary Laptop, you must:

- Restart Yeti
- Skip Secondary Install
- Open Bitcoin Core
- Disconnect Network
- Import Descriptor
- Import 3 Different Seeds (This time, 4-6)

Back on the Primary Laptop:

- Import Descriptor
- Rescan Blockchain
- Copy Erase File to USB

Then finally, you must test the receiving and sending of the recovered wallet once again. Do not visit the URL to do this. The instructions to do this are on pages 6-8. Instead of returning to Page 9 or 10, return to the next page - Page 11 afterwards.

You have now completed Step 32: Restore Your Wallet. Your wallet functionality and all your backup seeds have been fully tested.

Step 33: Store Seed Packets and Deposit Funds

Store your seed packets in safe locations and then deposit the funds you wish to store in your Yeti Wallet.

- Label 7 envelopes something like "Do Not Open. Last Will and Testament of Steve Jones. Deliver to next of kin." If anyone discovers the envelopes they should know it is important, but inappropriate and uninteresting to open them. Do not give any indication these envelopes are related to bitcoin.
- In each envelope place a seed CD, your paper recovery instructions that contain the equivalent hand written seed words, and a descriptor CD.
- Store the envelopes in places such as home and office safes, lawyers offices, accountant offices, safety deposit boxes, and trusted friends or family members.
- Lawyers and Accountants regularly store important documents for customers without charging a fee. Even if you need to pay for an unnecessary review of your books or your existing will to create a new relationship with a lawyer or accountant, the annual cost to have these documents safely stored and handed over to your loved ones if you die is very cheap.
- Ensure that you distribute your seed packets geographically so that you will be able to recover at least 3 after a major natural disaster.
- Consider distributing your seed packets so that an airline flight is required to spend your bitcoin. This makes physical attacks and extortion attempts less profitable for attackers.
- Do not tell anyone storing these envelopes that they are bitcoin related. Anyone storing these documents should believe they are important, but do not offer a thief financial rewards.
- Consider that someone needs to have 3 seed packets to spend your bitcoin, but only one packet to be able to view your balance and transaction history.
- **After** you have secured your seed packets offsite deposit the funds you wish to secure in your Yeti Wallet and then continue to the next step

Step 34: Erase your Laptops

Erase your Laptops to ensure your Bitcoin can only be spent using your seed packets.

- Power off your Secondary Laptop.
- Insert the usb drive you used to install Ubuntu.
- Boot off of the USB and click **Try Ubuntu**.
- Insert the usb drive labeled "Transfer" usb and copy the "erase.txt" file to the "Documents" folder.
- Click on the **nine dots** in the bottom left corner and open **Terminal**.
- Open the "erase.txt" file stored in the "Documents" folder and copy the first command.
- Right click and Paste the text in the terminal and hit **Enter**.
- Confirm that the hard drive is "not frozen". If it's "frozen" contact support at "yeticold.slack.com".
- Open the "erase.txt" file stored in the "Documents" folder and copy the second command.
- Right click and Paste the text in the terminal and hit **Enter**. You should see the following output:

```
Issuing SECURITY_SET_PASS command, password=”many_numbers_here”
```

- Open the "erase.txt" file stored in the "Documents" folder and copy the third command.
- Right click and Paste the text in the terminal and hit **Enter**. After a few minutes you should see the following output:

```
Issuing SECURITY_ERASE command, password=”many_numbers_here”
```

Your laptop has now been erased. If you don't want to keep your Primary Laptop as a watch-only device repeat Step 34/Page12 using your Primary Laptop.

Your Yeti Level 3 Wallet is complete!