Criminal Investigations and Network Analysis (CINA): A DHS Center of Excellence

Cryptocurrency Wallet Seizure Guide

Prepared For: Prepared By: CINA Hexordia



Table of Contents

Table of Contents	2
Description	
iOS Cryptocurrency Wallets	
Phantom	
Uniswap	
SafePal	7
Exodus	
MetaMask	
Bither	
Coinbase	
Coincola	
eToro	
Guarda	
MoonPay	
Rainbow	
Android Cryptocurrency Wallets	
Unstoppable	
Coinbase	
Zengo	
eToro	
Guarda	
Phantom	
MoonPay	
Rainbow	
MetaMask	
OKX	64
Gemini	
Exodus	

Acknowledgment: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 17STCIN00001-08-00.

Disclaimer: The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Description

This report provides a guide on seizing cryptocurrency wallets from select mobile devices, using a step-by-step approach illustrated with screenshots. The focus is on documenting the procedures required to send and secure wallet information on iOS and Android devices, ensuring maximum seizure of cryptocurrency assets.

Definition of Seizing Cryptocurrency: Seizing cryptocurrency, in the context of this report, refers to the act of withdrawing all or the maximum possible funds from a suspect's wallet to a law enforcement agency (LEA))-owned wallet. This process is carried out to ensure that the digital assets are securely transferred and preserved as evidence.

By following this guide, investigators will be equipped with the practical knowledge and visual reference needed to successfully seize cryptocurrency wallets, making this a valuable resource for digital forensic professionals handling cryptocurrency-related cases.

Important Note: This report assumes that the LEA involved has an agency-controlled wallet already set up to receive the funds. This could be either a hardware or software wallet that is ready to receive the funds upon seizure of the wallets. It's important to have multiple cryptocurrency addresses set up (ie BitCoin, Ethereum, etc) as it is often unknown what type of cryptocurrency is being used.

iOS	Android
Phantom	Unstoppable
Uniswap	Coinbase
SafePal	Zengo
Exodus	eToro
MetaMask	Guarda
Bither/Bitpie	Phantom
Coinbase	MoonPay
Coin Cola	Rainbow
eToro	MetaMask
Guarda	OKX
MoonPay	Exodus
Rainbow	Gemini

Assumption: This guide assumes that the mobile phone has been seized and the suspect is logged into their cryptocurrency wallet app.

iOS Cryptocurrency Wallets

Phantom

To perform a seizure of the wallet the suspect must be signed in to their wallet.

1. Select the "Send" button which is the middle left button with the paper airplane icon.



2. After selecting "Send" you will be prompted to select a token in our case we select "Ethereum". Insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press "Next". The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press "MAX". The next screen will display the amount being sent including fees. Finally press "Send", now the transaction is pushed to the blockchain for confirmation.



Uniswap

1. On the home screen select the middle left button with the paper airplane icon, this is the send button.

1:26	808 🗢 🔳)
ж	٢
Wallet 1 0x5AE35C19 (5	
\$4 .72	
 \$0.00 (0.01%) 	
= 7 0	0
Claim your uni.eth usemame	
Claim now Maybe later	
Tokens NFTs Activity	
C Ethereum	\$4.72
0.002 ETH	• 0.01%
Hiden blans () (
Q, Search	Swap

- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to enter a wallet address. The next screen you can select the currency you'd like to use and press the "Max" button to use all funds on this wallet. On the bottom of the screen select "Review Transfer"



SafePal

Download the SafePal wallet from the app store and open the app, follow the steps below.

1. On the home screen select the "Send" button with the up arrow icon.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to select the wallet you are sending from. The next page you will enter the wallet address and press the "MAX" button, then hit the "Next" button on the bottom of the screen. It will then ask you to review it as well the fees associated with it, press the "Send" button and it will begin the transfer.

1:36	525 🗢 🔳)	1:36		\$05 😌 🔳	1:36	525 🌩 🔳)
< Send		<	Send		<	
Q. Search		🙆 dita-11/2	Da	47. 6001	O che-XUZ	
ETH (ERC20)	0.00006228	• • • •				
astronos form	#0.1017	Enc20		>	ETH ERC20	
		То	6) – 8	То	
		Please order address.		Paste		Send X
		 Passe assure to supports the BR 	hat the receiving addres KC20 network	•	• ETH ERC20	
		Amount		_		
		0.00	M	AX ETH	From	0+47376501
		0.00		USD	10	0047270021
		Asailable balance: 0.00			Network Fee Low \$1,52 29,880wei 44,820	600098122 ETH(ERC28) k High \$3.76 73.61Gwei
			Next		Cancel	Send
	_				_	

Exodus

Download the Exodus wallet from the app store and open the app, follow the steps below.

1. On the home screen slide the wallet you want to the right, select "Send".



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press "Continue". A pop up will occur telling you that all transactions are permanent select "Ok". The next screen will allow you to choose the amount of cryptocurrency to send for simplicity, press "All" and then "Preview". The next screen will display the amount being sent including fees. Finally slide the arrow icon at the bottom to the left,



now the transaction is pushed to the blockchain for confirmation.



MetaMask

Download the Metamask wallet from the app store and open the app, follow the steps below.

1. On the home page click the middle button at the bottom of Metamask which will open a window with a few options. Choose "Send".



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. After doing so press "Continue". The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press "USE MAX". The next screen will display the amount being sent including fees. Finally press "Send", now the transaction is pushed to the blockchain for confirmation.



Bither

Download the Bither wallet from the app store and open the app, follow the steps below.

1. On the home screen click on the wallet you want to seize. On the next page click the "Send" button.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" the next page will contain all the next steps. First type in the wallet address you are sending the funds too. Next using the balance given enter that into the "Amount" box as there is no max option. Finally enter the password for the application and press "Send".

6:05	SOS 🗢 🗖	6:05		\$0\$ 🗢 💶
X Balance: B 0.00	••••	× Balance:	s 0.00	
Pay to Bitcoin address		Pay to Bitcoin address		
Amount B 0.00	\$ 0.00	Amount B 0.00		\$ 0.00
Password Password		Password Password		
Miner fee [©]	Dynamic Miner Fee >	Miner fee		Dynamic Miner Fee 5
	Send		S	end

I

I.	The	l'm	I The I'm
q w e	ertyu	i o p	qwertyuiop
a s	d f g h j	k I	asdfghjkl
∲ Z	xcvbn	m 🛛	☆ z x c v b n m ⊗
123	space	next	123 space next
		Ŷ	<u>ب</u>

6:05		505 🗢 🗊
× Baland	ce: p 0.00	
Pay to Bitcoin add	ress	
Amount B 0.00	\$ 0.00	
Password Password		
Miner fee $^{\odot}$	Dynam	ic Miner Fee 🗦
	Send	
I.	The	l'm
q w e	ertyu	i o p
a s	d f g h j	k I
ΰZ	x c v b n	m 🗷
123	space	next
		Ŷ

Coinbase

Download the CoinBase wallet from the app store and open the app, follow the steps below.

1. On the home page select the wallet icon on the bottom left of the page. Then press on the funds you'd like to use. Finally select the "Send" button on the lower right side of the page, you may need to scroll down to see it.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you can enter the amount of funds you want to send, we will select the "Max" button. Next enter the wallet address you are sending to. It may ask to you to verify the wallet address, if it is correct select the "Yes, looks good" button. Finally you can review all the information and select "Confirm" to complete the

transaction.





Coincola

Download the Coin Cola wallet from the app store and open the app, follow the steps below.

1. In the wallet screen of Coin Cola first hit "Deposit". On the deposit screen either take note of the wallet address or save the QR code.

12:06		505 🗢 🔳	12:13		SOS 🗢 🔳
0.00	Total assets		<	OTC LTC	
0.00	= 1.30 USD		Total 0.01988467 L	TC =1.29 USD	
отс	Exchange	Margin	tuallable secure		-
OTC Assets			0.01988467 LTC	0.0000000	00 LTC
0.00002084	BTC = 1.30 USD				_
() Deposit	() Withdraw	Transfer	LTC	Deposit Address	
втс					
Available	On hold			L.2247.9	
0.00000000 BTC	0.0000	0000 BTC	LUqPWEG31Yn	nb8VcuoVGij9qEkd2	yzHfZrY
ETH			l	Copy address	
Available	On hold		Tine		
0.000000 ETH	0.0000	00 ETH	Minimum deposit	amount: 0.01 LTC.	
USDT			Deposit requires	6 confirmations.	
Available	On hold		Please don't depr cept LTC to the ab	osit any other digital a ove address.	issets ex-
0.00000000 USD	T 0.0000	0000 USDT			
EOS					
Available	On hold	•			
0.0000 EOS	0.0000	EOS			
O Exchang	e OTC	Account			

- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. Now on another device that is signed in to the wallet collecting the seizures go to the wallet screen and select the "Withdraw" button. The next page will be selecting the currency, because we have funds in LTC we will select that option. Finally on the last page we will enter the address we noted in the first step and select "All". At the bottom of the page you will select "Withdraw"



eToro

Download the eToro wallet from the app store and open the app, follow the steps below.

1. On the home screen select the funds you want to send, in our case we selected LTC. On the next page select the "Send" button.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" the next page will contain all the final steps. Enter the amount to send, there is no max button but the available funds are below the line. Next enter the wallet address you want to send the funds to. Finally press the "Send" button.

6:44		SOS 🗢 🔳
<	SEND LTC	
AMOUNT (LT	5)	₽USD
Fee%: 0		Available: 0.01883
ADDRESS		
		Ó
 Maximum amou transaction: \$2,9 Fees are compris LTC estimated bi 	nt allowed to be so 99 approximately: ed of 0% eToro fe ockchain fee.	ent per single 47.332702 units. es and 0.000005
Wallet service	e provided by eTor	o USA LLC 🔨

Guarda

Download the Guarda wallet from the app store and open the app, follow the steps below.

1. On the home screen select the wallet you want to send from. In our case we will select BTC. On the next screen select the "Send" button on the bottom of the page.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to enter in the wallet address. There is no max option on Guarda so enter in the total amount available, make to enter in the 0 before the decimal point, then press "Continue". On the last page you can review all the

2:19 50 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$					2:23	\$0\$ 🗢 🔳
 Send 	2:19	\$05 🌩 🔳	2:22	\$05 🗢 🔳)	Confirmation	
Bitcoin 0.001 Sct.27 To address To address To my wallet BTC address Paste 32 Amount BTC USD Advanced options Advanced options Continue Continue<	Send		Send		You're going to send	
To address To my wallet BTC address Paste % Amount BTC - USD Asdation: 0.00075335 BTC + 46.46 USD Advanced options > Advanced options > Continue Continue Continue Continue	Bitcoin	0.001 > 545.47	B Bitcoin	0.001 >	0.00065335 BTC 40.3 USD	В
BTC address Peete % Amount BTC - USD Available: 0.00075335 BTC + 46.46 USD Asslable: 0.00075335 BTC + 46.46 USD Advanced options Advanced options Advanced options Advanced options Advanced options Advanced options Continue Continue Continue Continue	To address	To my wallet	To address	To my wallet	Network fee (excluded)	
Amount BTC - USD Available: 0.00075335 BTC + 46.46 USD Available: 0.00075335 BTC + 46.46 USD Advanced options Advanced options Advanced options Advanced options Continue Continue	BTC address	Paste (3)	bc%qy4mcmduqtf2syfqhts	Bpjx39fvPeste 30	0.00002938 BTC 1.81 USD	
- USD Axakabin: 0.00075335 BTC + 48.46 USD Network fre: - Advanced options > Advanced options > Continue Continue	Amount	втс	0.00075335	втс	Arrival amount	
Advanced options Advanced options Advanced options Advanced options Continue Continue Continue Continue Send		USD	46.46	USD	0.00065335 BTC	
Advanced options	Available: 0.00075335 8 Network fee: -	TC = 46.46 USD	Analable: 0.00075335 8 Network fee: 0.00002912 61	TC = 45.46 USD TC = 1.8 USD	Destination address	
Continue Continue Send	Advanced options	>	Advanced options	>	bc1qy4mcmduqtf2syfqhts8 u6s720pe	pjx39fvy6w6
Continue Continue Send					Satoshi per byte	
Continue Send					13	
Continue Send						
		ue	Continu	*	Send	

information and select "Send" to begin the transfer.

MoonPay

Download the MoonPay wallet from the app store and open the app, follow the steps below.

1. On the home screen select the "MoonPay account" you'd like to send from in this case we will select "Ethereum". Select the three dots at the top right, and then the "Send" button.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" select the "Max" button and then click "Continue". It will then ask to confirm that you want to send the max amount, select the "Confirm and continue with max send" button. On the next page you will enter the wallet address you want to send the funds to. Finally on the last page you can review the transaction and swipe the button at the end to send it.

2:03		SOS 🗢 🔳	2:03
	Send	×	
	0.0055 % \$13.53	ETH	
10%	50% 75%	Max	
Sence Sence	ereum 0.006	Balance > 4 ETH >	< Max send ×
	Continue		
1	2 ^BC	3 DEF	Sending ETH
4 сні	5	6 MNO	To send ETH you need to pay network fees that are also paid in ETH.
7 PORS	8 TUV	9 wxyz	We will deduct the estimated network fee from the amount to make sure we can
	0	$\langle \times \rangle$	broadcast your transaction.
			Confirm and continue with max send
		•	



Rainbow

To perform a seizure of the wallet the suspect must be signed in to their wallet. Download the Rainbow wallet from the app store and open the app, follow the steps below.

1. Select the "Send" button which is the third button underneath the wallet balance.



- 2. To seize the funds it requires a wallet preferably a brand new wallet that was created by your organization for the purpose of receiving the cryptocurrency to be seized.
- 3. After selecting "Send" you will be prompted to insert the address to send the funds to. This field needs to be filled with a wallet owned by your organization. Next if there are multiple wallets on the phone it will ask which wallet to use. The next screen will allow you to choose the amount of cryptocurrency to send for simplicity press "MAX".

12:52 535 🗢 🖬	12:53 App Store	505 P 🗈	12:53 App Store		505 🕈 🗈
Send	Sen	d		Send	
To: Name, ENS, or address	To: 0x23F422	🔊 Save	To: 0x23F4	22	Save
My wallets	Ethereum	\$0.0257	Ethere	eum 7 available	Ø
0x23E0F422 \$0.0299			-		
0x90cEDCAc			0		ETH
-			0	Max	USD
			_		
			Ent	ter an Amou	nt
			0 \$0.22 ~24 f Estimated fee ()	sec (Ô Nor	mal 🕥 🗮
qwertyuio	p		1	2	3
asdfghjkl			4 GHI	5	6 N N N O
☆ z x c v b n m <	×		7 Pars	8 TUV	9 ₩XYZ
123 space return				0	$\langle \times \rangle$
<u>ب</u>					

Android Cryptocurrency Wallets

Unstoppable

1. Press Send to begin the seizure



2. Select the currency to seize



3. Specify the amount to seize and the destination address.



4. Review seizure and press Send to finish.



Coinbase

1. Hit the twin arrows button in the bottom-center.



2. Specify the amount. The app will default to the currency with available funds. Hit the Send button.



3. Specify the destination address and hit the Confirm button.



4. Review and hit the Confirm button.



Zengo

1. Press the twin arrow button at the bottom to begin the seizure.


2. Select the Send option



3. Select the currency to seize



4. Specify the amount to send. There is a 'Use Max' button to seize everything.



5. Specify the destination address.



6. Review seizure and press 'Send' to finish.



eToro

1. Select the currency to seize

LTC Litecoin

10:33 🛔 M 🖬 🐮	•	۵
=		
	Crypto Balance \$1.84	
Wallets		
BITC		0.00001

0.019834 \$1.25



2. Press the send button



3. Enter the amount and the destination address. Press send.



Maximum amount allowed to be sent per single transaction: \$2,999 approximately: 47.243226 units.
Frees are comprised of 0% eToro fees and 0.000005 LTC estimated blockchain fee.

Wallet service provided by eToro USA LLC

4. You will need a 2-step verification code. It is sent to the linked phone number over SMS.



5. Crypto will be sent without further confirmation.



We have received your request to send 0.001 LTC. Check your transactions screen for the transaction status. Wallet service provided by eToro USA LLC

Guarda

1. Select a wallet with funds to seize



2. Click the Send button at the bottom



3. Specify the destination address and amount and then press Continue

9:57 🛔 🎮 🌥 🖼 🔸	۵		
< Send			
Ethereum 1	0.006 > \$15.25		
To address To my wallet			
aB56F2c6cE15e26e99485a85CA9A52	cb Paste 🔛		
0.00001	ETH		
0.02	USD		
Available: 0.0064 ETH ≈ 15.25 USD Network fee: 0.000336 ETH ≈ 0.8 USD			
Advanced options	>		
Continue			

4. Review transaction and then press Send to finish

9:57 🛔 🕅 📥 🖬 🔹 💎 🗋
< Confirmation
You're going to send 0.00001 ETH 0.02 USD
Network fee (excluded) 0.000336 ETH 0.8 USD
Arrival amount 0.00001 ETH 0.02 USD
Destination address 0x20516B44aB56F2c6cE15e26e99485a85CA 9A52cb
Send

Phantom

1. Press Send button to start Seizure



2. Select the currency to seize



3. Specify the destination address and press Next



4. Specify the amount and press Next. There is a 'Max' button to send everything



5. Review the seizure and press Send.



MoonPay

1. Click the three dots on the tile with the desired currency.



2. Hit the Send button



3. Specify the amount and hit Continue. There is a 'MAX' button to seize everything.



4. Specify the destination address



5. Confirm send with swipe



Rainbow

1. Press Send to start seizure



2. Specify the destination address and the currency to use.



3. Specify the amount to seize. There is a 'Max' button to seize everything.



4. Review seizure and press 'Tap to Send' to finish



MetaMask

1. Press the twin arrow button at the bottom to pop out the menu



2. Select the Send option



3. Enter the destination address into the second box



4. Enter the amount to seize. There is a USE MAX button to seize everything.



5. Review the transaction and hit Send to confirm.



OKX

1. Press the send button to begin the seizure



2. Select the currency to Seize



3. Specify the destination address and press Confirm



4. Specify the amount and press Next. There is a 'Max' button to seize everything.



5. Review seizure and press Confirm to finish



Gemini

1. Hit the send button



2. It will prompt for the user's PIN. Enter it here to continue



3. Select the currency to seize



4. Specify the amount and press Continue. There is a 'Send max' button to seize everything.



5. Specify the destination address and press Review withdrawal



6. If you are prompted with a warning message click "Yes, I want to proceed"



7. Confirm by using the Swipe at the bottom


Exodus

1. Hit the send button



2. Enter in the address of the receiving wallet and press continue.



3. Press OK for the warning



4. Select "All" to transfer out all remaining funds



5. Continue with "Slide to Send"

