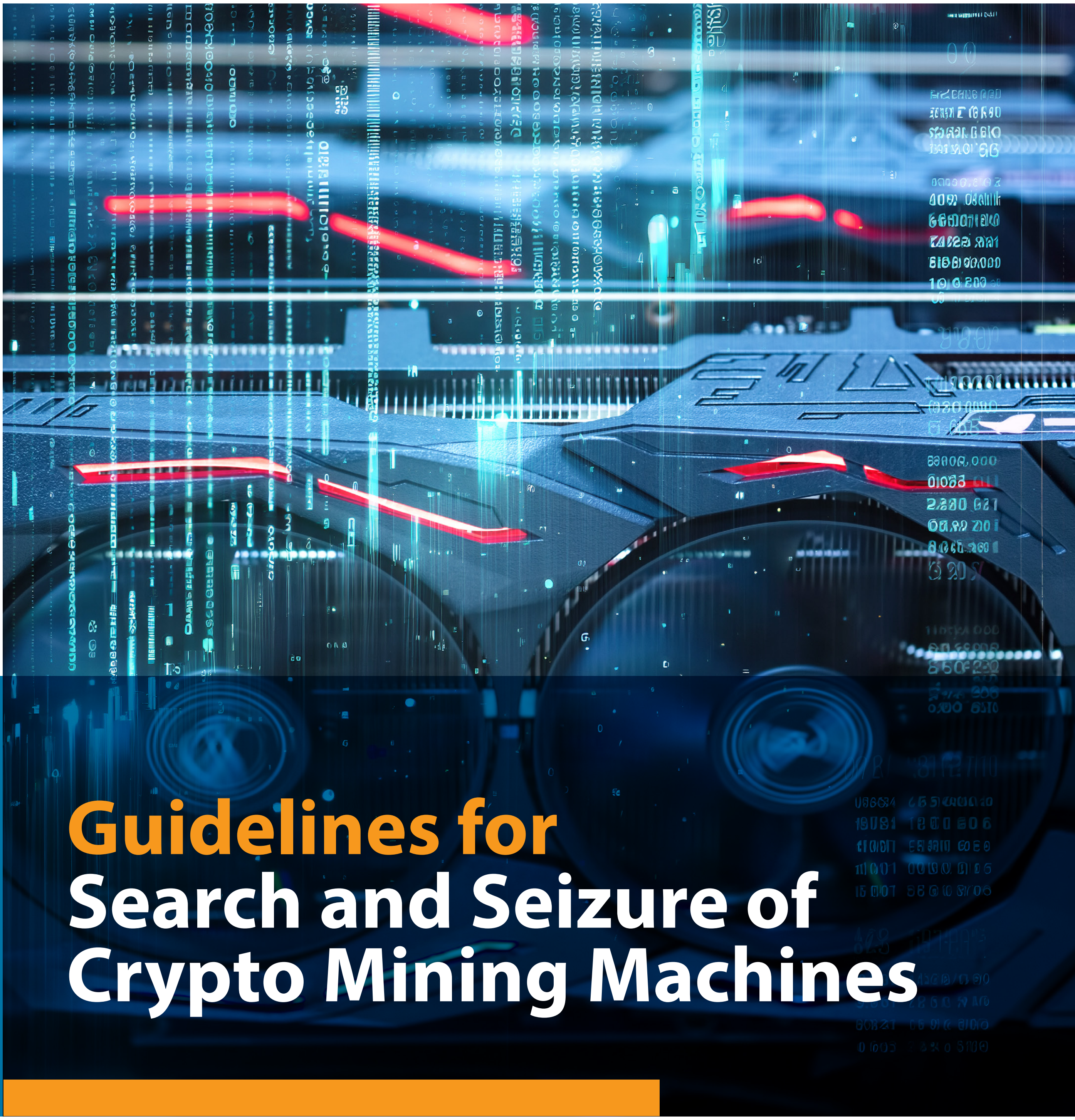
MINISTRY OF DIGITAL

CyberSecurity MALAYSIA



Guidelines for Search and Seizure of Crypto Mining Machines

June, 2025

DISCLAIMER

The purpose of this document is to provide generic guidance and suggested processes on the search and seizure crypto mining machines. It was developed based on input from the relevant agencies, compilation of best available information, knowledge and field experience to provide guidance to law enforcement officers so that activities are performed in a consistent and standardized manner.

This document should be used as a reference. However, differences may exist between the procedures referenced in this document and what is appropriate under field-specific conditions. For the avoidance of doubt, the use of this document shall not in any way create, or be relied upon to give rise to, any right in the Crypto miners which may be enforceable at law in any matter whether civil or criminal.

Any products, manufacturers or organisations referenced in this document are presented for informational purposes only and do not in any way constitute approval or endorsement by CyberSecurity Malaysia.

COPYRIGHT AND CONFIDENTIALITY STATEMENT

ACKNOWLEDGEMENT

This document was jointly developed by CyberSecurity Malaysia (CSM) and **United Nations Office on Drugs and Crime (UNODC)**, with inputs from the **Commercial Crime Investigation Department of Polis DiRaja Malaysia (PDRM), Malaysia Energy Commission and Attorney General Chambers (AGC)** to address challenges in conducting forensic investigation on crypto mining machines. We would like to extend our sincere appreciation to all contributing agencies for their invaluable insights, expertise, and commitment to strengthening forensic capabilities in this evolving domain.

FOREWORD CYBERSECURITY MALAYSIA

The rapid advancement of technology and the growing adoption of cryptocurrencies have introduced both new opportunities and challenges for the digital economy and law enforcement agencies alike. One pressing concern is the illicit use of crypto mining machines, which has been associated with criminal activities such as electricity theft, money laundering, and other financial offences. As crypto mining operations become increasingly sophisticated, the development of comprehensive guidelines to tackle these issues has become essential.

Recognising the critical importance of this issue, Dr. Sarah Khadijah Taylor and her team, in collaboration with the **United Nations Office on Drugs and Crime (UNODC)**, have developed the Guidelines for the Search and Seizure of Crypto Mining Machines. These guidelines are designed to equip Malaysian law enforcement agencies (LEAs) and other relevant authorities with the essential knowledge, procedures, and best practices needed to effectively conduct search and seizure operations targeting illegal crypto mining activities.

The successful development of these guidelines would not have been possible without the steadfast support and contributions of key stakeholders, including the **Commercial Crime Investigation Department of Polis Diraja Malaysia (PDRM)**, the **Malaysia Energy Commission,** and the **Attorney General's Chambers (AGC)**. Furthermore, valuable insights and best practices were gained through collaboration with international counterparts and experts from the UNODC, enriching the guidelines and ensuring their alignment with global standards.

This initiative stands as a testament to our shared commitment to protecting Malaysia's digital landscape and tackling the challenges brought by emerging technologies. Through ongoing collaboration and strategic partnerships, we can strengthen the resilience of our digital economy while safeguarding the safety and security of our nation.

I firmly believe that the implementation of these guidelines will empower our enforcement agencies to combat illegal activity more effectively, thereby fostering a secure and sustainable digital ecosystem in Malaysia.

DATO' Ts. DR HAJI AMIRUDIN ABDUL WAHAB FASc
Chief Executive Officer(CEO)
CyberSecurity Malaysia

DOCUMENT OVERVIEW

The increasing integration of digital technologies into daily life has led to a surge in criminal cases involving digital evidence. These guidelines have been developed to address the challenges of collecting, preserving and managing such evidence in a manner that ensures its integrity and admissibility in court. Traditional investigative approaches are no longer sufficient given the volatile and often complex nature of digital data, ranging from mobile devices and cloud storage to encrypted communications. This document provides a standardized, practical framework for law enforcement officers, digital forensic analysts and relevant stakeholders to conduct digital evidence collection effectively, thereby enhancing the credibility of investigations and supporting successful legal outcomes.

DOCUMENT PURPOSE

The purpose of this document is to provide guidance to the Law Enforcement Agency (LEA) in handling digital evidence for investigation. This document is applicable to LEA operating under different operational frameworks. The statements in this document are made in general so that it can be adopted by various LEA. As each agency may have its own process, the agency may need to elaborate further on each statement.

DOCUMENT SCOPE

This document focuses on the proper handling and collection of digital evidence in investigations. It explains key methods for collecting data such as imaging, cloning and memory dumps. The document also highlights potential risks such as contamination of evidence, legal issues and data loss. It provides practical guidance to ensure digital evidence is handled correctly and securely during investigations. This document serves as a practical guide for professionals involved in digital forensics and investigations.

TABLE OF CONTENT

ABBREVIATIONS AND ACRONYM

OS	Operating System
SSID	Service Set Identifier
CPU	Central Processing Unit
GPU	Graphical Processing Unit
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Authority
FPGA	Field-Programmable Gate Array
USB	Universal Serial Bus
SSD	Solid-state Drive
CCTV	Closed Circuit Television

LIST OF TERMINOLOGIES

Controlled Cryptowallet	A wallet that is under the control of the law enforcement agency whose role is to handle seized criminal proceeds.
Controlled Address	An official and secured address, controlled only by the seizing agency. It is where the corresponding private key is stored offline. Controlled Addresses are generated from a Controlled Cryptowallet.
Cryptocurrencies	Also known as "virtual currencies" and a subset of "virtual assets". It is a digital or virtual currency that uses cryptography for security and operates independently of a central bank. It is decentralized, meaning that transactions are recorded on a distributed ledger technology such as blockchain. Cryptocurrencies use encryption techniques to generate new units and to verify the transfer of funds.
Crypto mining	Process of solving complex mathematical puzzles or algorithms, by using computing power, with the purpose of validating and securing transactions on a blockchain network.
Crypto miner	An individual or entity that uses computer power to validate transactions and create new units of cryptocurrency, typically by solving complex mathematical problems within a blockchain network for rewards.
Cryptowallet	A device or program that is used to send and receive cryptocurrencies.
Hosted wallet	A crypto wallet hosted by a third-party financial institution, known as the cryptocurrencies exchanger, or third-party custodian services company. The term unhosted wallet could also interchange with non-custodial wallet.
OSINT	Open Source Intelligence Tool
Unhosted Wallet	A type of cryptowallet where the owner has sole access to the private keys. The term unhosted wallet could also interchange with non-custodial wallet.
Public IP address	An IP address that is accessible directly over the internet and is assigned to a network router by the Internet Service Provider.
Private IP address	An IP address that is assigned to a device by a network router. Each device within the same network is allocated a unique private IP address.
MAC address	Also known as a physical address or hardware address. It is a unique identifier assigned to network interface controllers by the manufacturer. It is a 48-bit address expressed in hexadecimal format and is typically represented as six sets of two-digit hexadecimal numbers separated by colons or hyphens.
PoW	Proof-of-work (PoW) is a consensus mechanism in blockchain networks that forms the consensus model of Bitcoin.
SSID	A service set identifier (SSID) is a sequence of characters that uniquely identifies a WiFi network.

1. UNDERSTANDING CRYPTO MINING

1.1 Overview of Crypto Mining

Crypto mining is the process of solving complex mathematical puzzles, by using computing power, with the purpose of validating and securing transactions on a blockchain network. Crypto mining is conducted by the crypto miners. A crypto miner is an individual who uses computing power to solve complex mathematical problems and at the end, earns cryptocurrency.

When a user makes a cryptocurrency transaction, this transaction will be validated and secured, and will be included in a new block. This new block then is added into the chain of existing blocks, known as blockchain. Crypto miners validate transactions by competing with each other to solve mathematical puzzles. Successful crypto miners are rewarded with a newly minted cryptocurrency and transaction fees.

The process of solving mathematical puzzles to validate transactions is the core of Proof of Work (PoW). Nevertheless, there are several other methods to validate transactions other than PoW, such as Proof of Stake(PoS) and Proof of Authority(PoA). PoW is the most common consensus mechanism used by popular cryptocurrencies such as Litecoin and Bitcoin. The PoW is known as crypto mining and the participating nodes in the process are known as crypto miners. Figure 1 illustrates how crypto mining works.

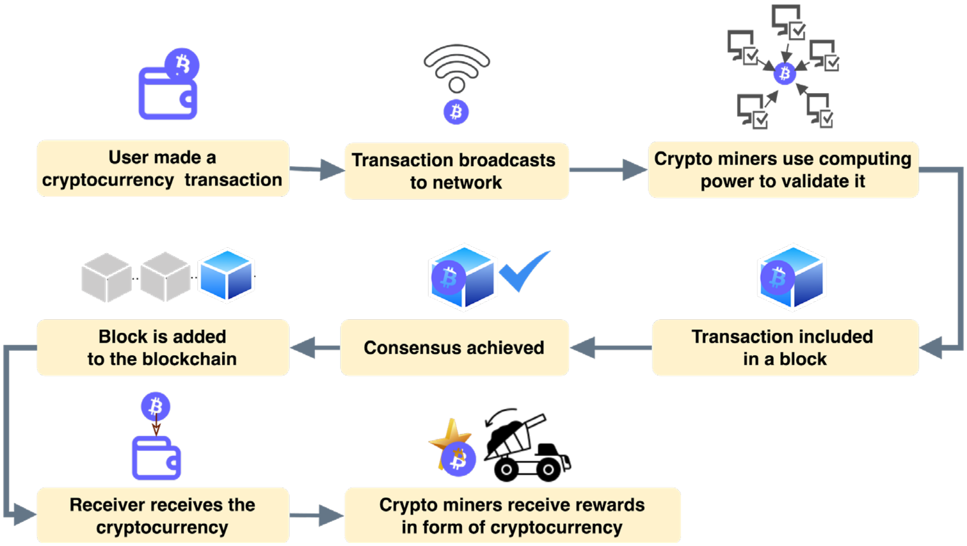

User made a cryptocurrency transaction
Transaction broadcasts to network
Crypto miners use computing power to validate it
Transaction included in a block
Consensus achieved
Block is added to the blockchain
Receiver receives the cryptocurrency
Crypto miners receive rewards in form of cryptocurrency

Figure 1. Illustration of how crypto mining works

Crypto mining serves two primary purposes:

- **Transaction validation:** Crypto miners validate transactions by solving complex mathematical problems. This process ensures the integrity and security of the transactions on the blockchain.
- **Issuance of new cryptocurrency tokens:** In addition to verifying transactions, Crypto miners are also responsible for creating new units of the cryptocurrency as rewards for their work. This process is often referred to as "block rewards."

Crypto mining requires significant computational power and energy consumption, as Crypto miners use powerful computers or specialized hardware (such as ASICs and GPU machines) to solve these mathematical problems. As a result, crypto mining can be resource-intensive and costly, particularly for popular cryptocurrencies like Bitcoin.

In order to maximize profit, some crypto miners resorted to stealing electricity. These crypto miners tamper the electrical wiring systems by making illegal connections to the mining machines. This activity causes huge financial loss to a country and imposes safety risks to the general public. Hence the criminal stealing the electricity for own benefit needs to be investigated and prosecuted so that justice can be rightfully served.

1.2 Component of Crypto Mining

Generally, crypto mining involves three main components; crypto mining machine, mining pool (pool client and pool server) and cryptowallet. Figure 1 shows the overall component of crypto mining. The details of the crypto mining components are explained in the following subsections.

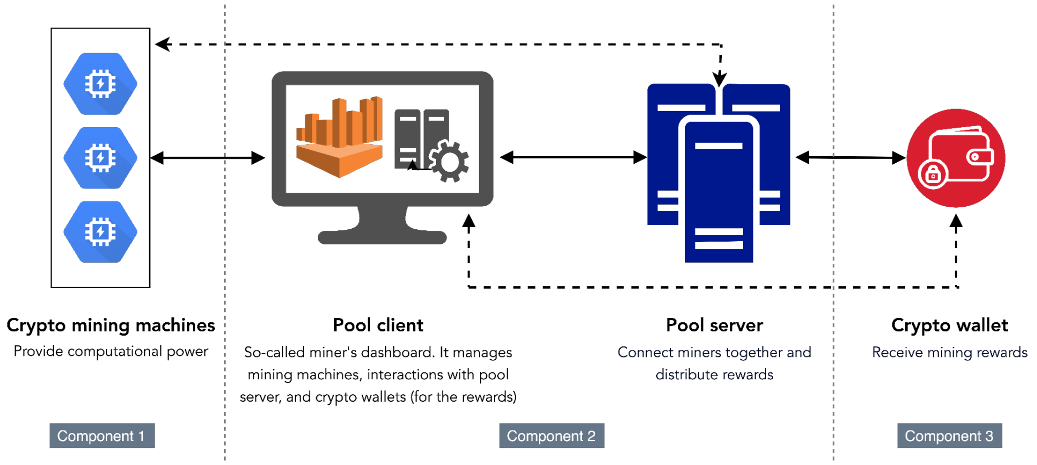

Crypto mining machines
Provide computational power
Pool client
So-called miner's dashboard. It manages mining machines, interactions with pool server, and crypto wallets (for the rewards)
Pool server
Connect miners together and distribute rewards
Crypto wallet
Receive mining rewards
Component 1
Component 2
Component 3

Figure 2. Crypto mining components

1.2.1 Component 1: Crypto Mining Machines

A crypto mining machine, also known as a mining rig or mining hardware, is a computer system designed specifically for the purpose of mining cryptocurrencies. These machines are optimized for performing the complex mathematical calculations required for cryptocurrency mining efficiently.

There are several types of crypto mining machines; CPU, GPU, FPGA and ASIC. There is also a crypto mining process that utilizes cloud technology. In this case, the machine that runs the mining activity can be a mobile phone, a computer or a server. ASIC, FPGA and CPU machines use internal storage drives while GPU machines use external storage drives to store data. The external storage drives for GPU machines can be USB flash drives or external SSD drives.

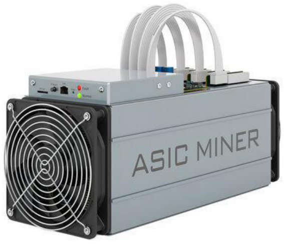


Figure 3. ASIC Miner machine
Source: https://stock.adobe.com/search?k=asic+miner

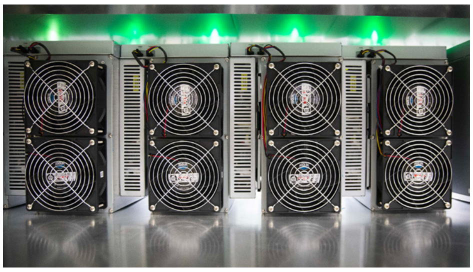


Figure 4. A rig of ASIC machine
Source: https://www.coindesk.com/tag/asic-mining/

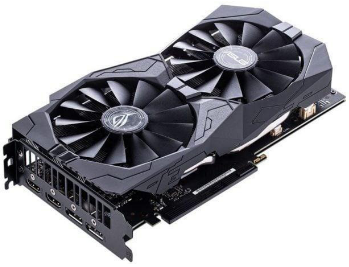


Figure 5. A single GPU machine
Source: https://www.hellotech.com/blog/whats-a-gpu-what-gpu-do-you-have

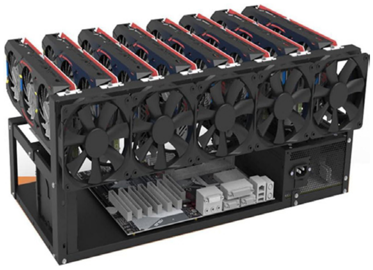


Figure 6. A rig of GPU machine
Source: https://www.amazon.in/Mining-Currency-Bitcoin-Accessories-Included/dp/B08XJWPBQ6

In order for the machine to function, it needs to be installed with a mining OS. Examples of mining OS are such as MiningOS, Hiveon OS and MinerOS. These OS utilize special algorithms such as Ethash, CryptoNight and Scrypt. The OS used in crypto mining machines is generally Linux-based.

For ASIC machines, the OS is typically pre-installed in its internal storage drive. This is generally the same for FPGA machines. When turning on the machine, the OS will prompt the user and ask for the pool server address. Users will then need to enter the pool server address. See section 1.2.2 Mining Pool for the process of getting the address.

For the CPU and GPU machines, the OS needs to be downloaded from the pool server. The downloaded OS then needs to be installed into a storage drive. Some OS require the crypto miners to set up a PIN number, and the common PIN number would be 12345. Crypto miners will also need to enter details into the OS such as email address, SSID name, SSID password, public IP address and name preference for the machine.

Mining OS requires a low-bandwidth but constant Internet connection because it needs to exchange packets with the mining pool server on a regular basis. ASICs machines, as of now, only support ethernet connection (using UTP network cable), while the other types of machines can support ethernet and WiFi connection.

1.2.2 Component 2: Mining Pool

A mining pool is a group of crypto miners who connect their mining machines over a network to boost their chances of earning the reward for opening a new block[1]. Incentives are typically distributed amongst the participants based on their respective shares, or the percentage of each person's labour or processing power across the entire group. Joining a mining pool is the most economical method to raise chances of getting rewards.

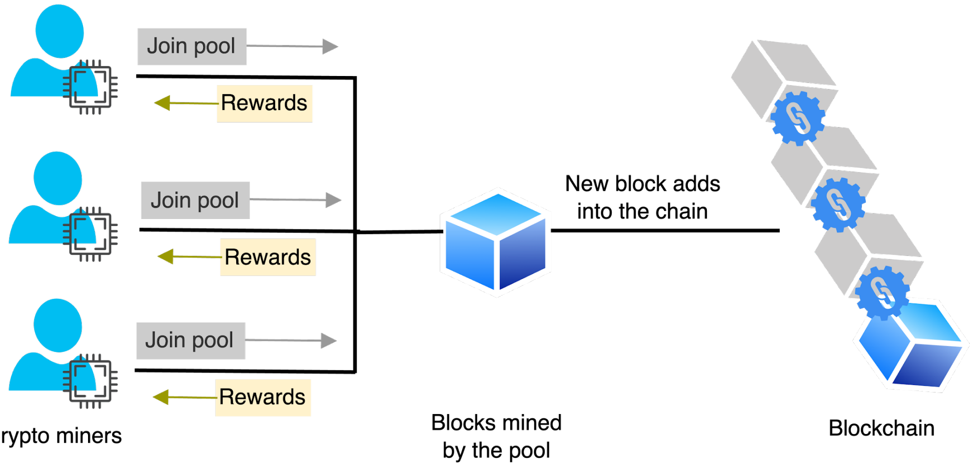


Figure 7. Illustration of how mining pool works

Crypto miners can also perform solo mining. In this case, crypto miners will solely depend on their computational power to get rewards. Crypto miners will connect their mining machines to the pool server and choose to perform solo mining.

To join a mining pool, crypto miners will have to go to the pool server's website and create an account. The account; which referred to as pool client, is a dashboard where crypto miners can manage the mining machines, manage interaction with the pool server and specify the crypto wallet's addresses for the rewards. Once an account has been created, a miner can download the mining OS from the pool server.

Crypto mining pools such as NiceHash, Slush Pool and via BTC offer a cloud-based pool client where crypto miners can login into the pool client from any devices with Internet connection. Since it is cloud-based, crypto miners can monitor the mining machines remotely, including stopping or restarting the machines.

Since the pool client is cloud based, the miner does not have to be at the premise where the mining machine is located, rather they can monitor the machine remotely. Crypto miners can also use the pool client to stop the mining activity remotely.

To use the mining pool service, crypto miners will have to pay some amount of cryptocurrency to the mining pool providers. The transaction records for the fee can be viewed from the pool client. To receive mining rewards, crypto miners need to enter a crypto wallet address to the pool client. Mining reward is transferred to the address depending on the time frame that is set on the pool client. Rewards come in a form of cryptocurrency token such as Bitcoin, Kaspa or Litecoin.

1.2.3 Component 3: Crypto Wallet

In order to receive mining rewards, crypto miners need to have a crypto wallet. There are two (2) kinds of crypto wallet; hosted and unhosted. Hosted wallets are wallets hosted on cloud by third parties. Unhosted wallets, on the other hand, are standalone and self-managed by the users.

Reward from the crypto mining activity, the cryptocurrency, is transferred into the crypto wallet. Crypto miners can monitor the received rewards from the pool client.

1.2 Setting up a Crypto Mining Machine

Generally, a crypto miner will perform the following steps in order to conduct crypto mining process:

i. Determine type of coin to mine

Crypto miners typically will mine new cryptocurrency tokens that have potential to grow. Investigator can refer to this website to get a list of token that can be mined: https://coinmarketcap.com/view/pow/

ii. Choose a pool server

There are lots of options for mining pools. Some of the popular mining pools are Poolin, Antpool, Antminer, F2Pool, viaBTC, SlushPool, BinancePool, Ekapool and many more.

iii. Set up a pool client account

Crypto miners will have to create an account to join the pool servers. The account requires Crypto miners to enter username and password. Some pool servers have multi- factor authentication for security enhancement. The account is typically a cloud-based account, where Crypto miners can login from any device. Once an account is created, a pool server address will be generated for the mining machine.

Example of a pool server address is like this: http://dnx.us.ekapool.com:19666/. This address indicates that the pool server is Ekapool.com, the mined token is Dynex (DNX) and 19666 is the port number.

iv. Download mining operating system(OS) from the pool server

Mining machines like GPUs require Crypto miners to download the OS from the pool server. Crypto miners can download it from the pool client account that has been set up earlier. Machines like ASICs do not require Crypto miners to download the OS as it is already embedded in the machine.

v. Configure mining operating system on mining machine

Machine is connected to the Internet and the pool server address is entered into the OS for the machine to connect to the pool server. Other information to be entered are such as network SSID and SSID password.

vi. Press START on the pool client

Crypto miners add computers to the pool client after OS configuration. Press the machine's start button to begin mining. Since the pool client works on any device, this may be done remotely. The pool client will let crypto miners control machine temperature, downtime, watt consumption, fan usage, etc.

1.3 Roles involved in the Crypto Mining Operations

As described in Figure 2, crypto mining involved three components. Each of these components is typically maintained by a designated individual. In some cases, an individual can take up two or more roles. The roles involved in the crypto mining operations are described below and illustrated in the following figure.

Component 1 of crypto mining involves the mining machines. These machines are maintained by one or more technicians. Their job is to make sure the mining machines are up and running. Sometimes, they are also tasked with ensuring the Internet and the CCTV are working well.

Component 2 involves the operator of the mining operation. This individual monitors the operation of the mining by conducting tweaks on the pool client to ensure the mining machines and the profit gained are at optimal level. The pool operator is often in contact with the technician in case that the machines are in error mode.

Component 3 involves the crypto wallet owner. This owner is often the investor for the mining operation. From time to time, the owner will receive updates on the mining operation from the Operator.

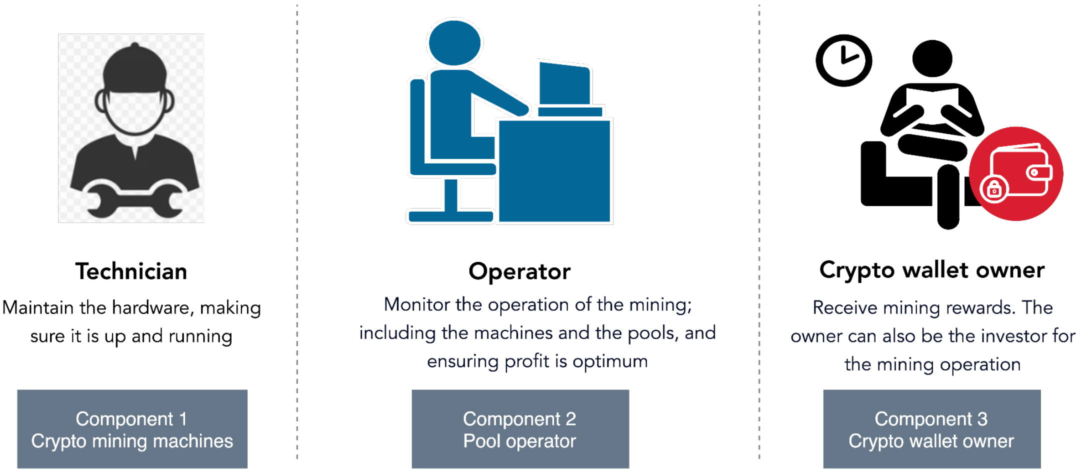

Technician
Maintain the hardware, making sure it is up and running
Component 1
Crypto mining machines
Operator
Monitor the operation of the mining; including the machines and the pools, and ensuring profit is optimum
Component 2
Pool operator
Crypto wallet owner
Receive mining rewards. The owner can also be the investor for the mining operation
Component 3
Crypto wallet owner

Figure 6. Roles involved in the crypto mining operation

1.4 Common Network Topology of Crypto Mining Machines

Crypto mining requires the Internet to perform the mining work. For mining involving several machines, each of the machines will be connected to a switch, before being connected to the router. A switch acts as the intermediary between mining hardware (also known as mining machine) to the router. Figure 6 below shows the network topology.

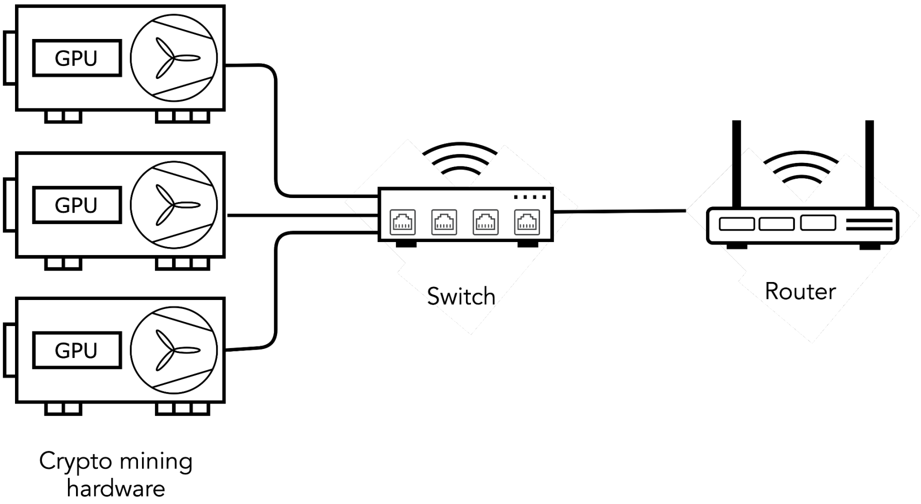


Figure 7. Crypto Mining Network Topology

Each type of hardware for the crypto mining activity stores data important for investigation. Table 1 explains data that could be extracted from each component involved in the crypto mining activity.

Types of device	Potential data to be extracted
Crypto mining hardware	• Serial number • Brand and model • Public IP address • MAC Address • Pool server name
Switch	• Serial number • Brand and model • Public IP address • MAC Address
Router	• Serial number • Brand and model • Public IP address • MAC Address • Internet Service Provider(ISP) • IP address & MAC address devices connected to the router

Table 1. Types of device and potential data that can be extracted

2. PREPARING FOR SEARCH AND SEIZURE

The investigation of an offence involving cryptocurrencies shall be conducted under the law of the relevant agency. Officers shall ensure that the requirements of the law are being met before conducting the search and seizure.

The typical locations where crypto mining is conducted through electricity theft include shop lots, factories, and domestic housing areas, mostly in abandoned areas, which are usually installed without the presence of a security guard. The following subsections detailed out the preparation process prior to the seizure activity.

2.1 Conduct Onsite Survey

The premise hosting the crypto mining activities are usually installed with high security features. Therefore onsite surveys need to be conducted in order to understand the security level as well as to strategies the entry into the premise during the onsite investigation.

The following are the information recommended to be collected during the onsite surveys:

- Premise address and its environment (shop lots, factories, and domestic housing areas)
- Billing information (Electricity, water, internet, etc)
- Condition and location of electrical power supply wiring and cabling
- Presence of CCTV and its location
- Door security feature (Strong door, biometric access, physical lock, etc)
- Number of security guards and their schedule
- Type of internet connection and possible location of router
- Other supporting documents such as the following:
  - Grant of the shopslots
  - Tenancy agreement
  - Company registration
  - Sale and purchase agreement.
- Take photographs of the following:
  - the exact location of the building
  - the surrounding of the building
  - show the specific floor where necessary
  - the serial numbers of electric poles

Table 2. Checklist for onsite survey activities

2.2 Form an Onsite Investigation Team

Investigating crypto mining cases require expertise in several domains. To ensure a successful investigation, a team consisting of the following expertise is recommended to be formed:

● Law Enforcement Officer	Officer who are in charge of conducting crime scene investigation
● Electrical energy expert/ Licensee / installation owner	Experts on electrical cabling and tampering who can confirm the presence of electricity theft
● Digital forensic expert	Experts on digital forensic who can preserve and collect digital evidence
● Anti-money laundering expert	Experts on money trail analysis and methods to obscure fundings as some cases may invoke the provision of Anti-Money Laundering.
● Tax evasion expert	Experts on money trail analysis and tax evasion strategies as some cases may invoke the provision of Income Tax Act.

Table 3. Suggestion of team members for crypto mining onsite investigation

2.3 Form Onsite Investigation Strategy

Typical operation of crypto mining involves several layers of operators. This is explained and shown in Figure 1 in section Overview of Crypto Mining Machine. Crypto mining machines, the CCTV and the Internet connection can be operated and maintained by technicians. While the mining pool client can be operated and maintained by a pool operator. The crypto wallets can be owned and maintained by the owner or the investors of the crypto mining operation.

All the individuals operating and maintaining components of crypto mining are not necessarily the same person. They can also be at different locations. Therefore conducting an onsite investigation for such a case requires proper strategy. Recommendations for the successful onsite investigation of crypto mining machines:

- It it best that investigators to enter all premises at the same time
- Do not turn off the mining machines until data has been completely preserved
- Be cautious on presence of CCTV, if suspects discover suspicious activity, they can turn off machine remotely
- The ultimate goal is to find a wallet owner. This person is possible to be the investor or funder or the mastermind for the crypto mining activity. Hence strive to look for wallet addresses from the mining machine or pool client, or by interviewing the mining operators or the system administrators.

Table 4. Recommendations for the successful crypto mining machines search and seizure

2.4 Prepare Equipment

To guarantee seamless onsite investigation at the premise, equipment needs to be prepared beforehands. The following are the documentations and equipment recommended to be prepared for the onsite investigation:

- Forensic acquisition tool (hardware and software)
- Forensic triage tool or pre-analysis tool
- Forensic computer (a laptop equipped with forensic software)
- Plyers, cutters and scissor
- Ethernet cables
- Controlled Wallet

Table 5. Checklist for onsite investigation equipment

Controlled Wallet is a cryptocurrency wallet owned by the Law Enforcement Agency. This wallet is used for the purpose of securely storing the seized cryptocurrency. There are specific procedures that need to be followed when generating a Government Controlled Wallet. To generate one, please refer to the **Malaysia Policy and Procedure for Seizing Cryptocurrency**[9] or the **INTERPOL Guidelines for Seizing Virtual Assets**[8].

3. CONDUCTING SEARCH AND SEIZURE

The general procedure for conducting crypto mining search and seizure happens at the crime scene. The process is described in the following subsections.

3.1 Processing and Seizing Crypto Mining Machines

The suggested procedure to process crypto mining machines involves several steps. The steps are summarized in Figure 8 and explained in the following subsections.

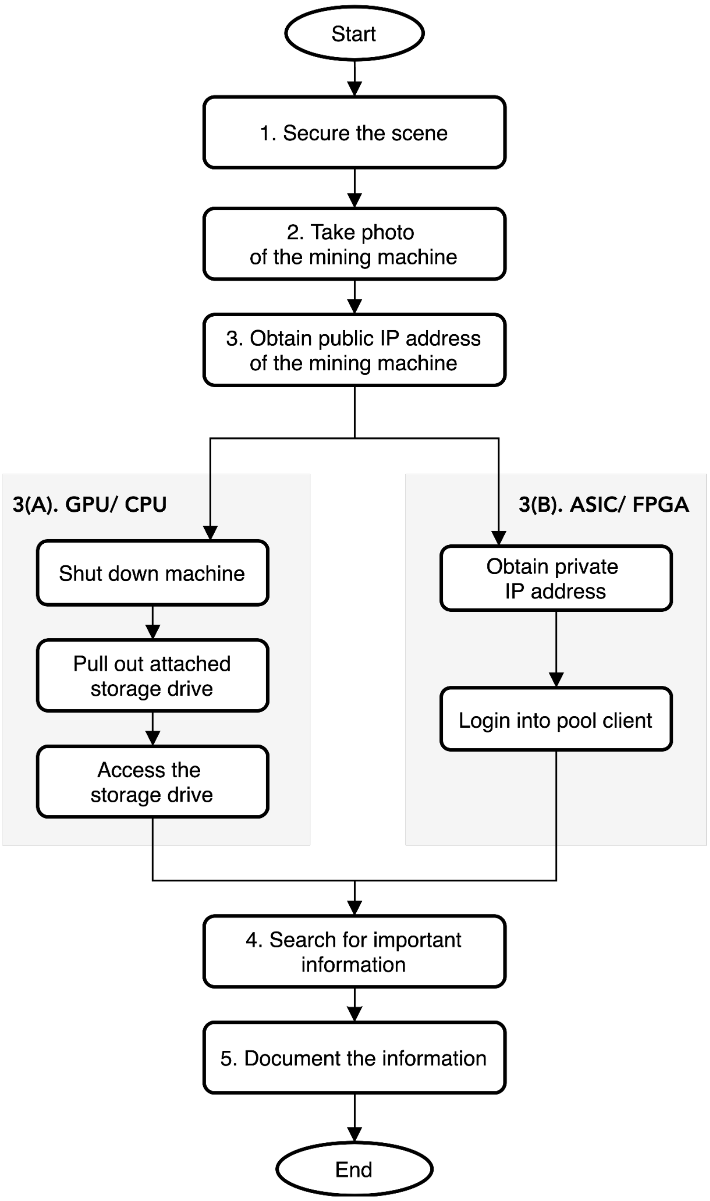

Start
1. Secure the scene
2. Take photo of the mining machine
3. Obtain public IP address of the mining machine
3(A). GPU/ CPU
Shut down machine
Pull out attached storage drive
Access the storage drive
3(B). ASIC/ FPGA
Obtain private IP address
Login into pool client
4. Search for important information
5. Document the information
End

Figure 8. Steps involved in processing crypto mining machines at crime scene

1. Secure the scene

Upon arrival at the onsite, follow the agency's procedures to secure the scene. Then scout the area for the existence of crypto mining machines.

2. Take photos of the mining machines

Next take photos of the mining machines, close up and overall view. Ensure important information such as machine unique identifier (serial number, MAC address, etc), brand and model is captured in the photos. Example of overall and close up views are as following:

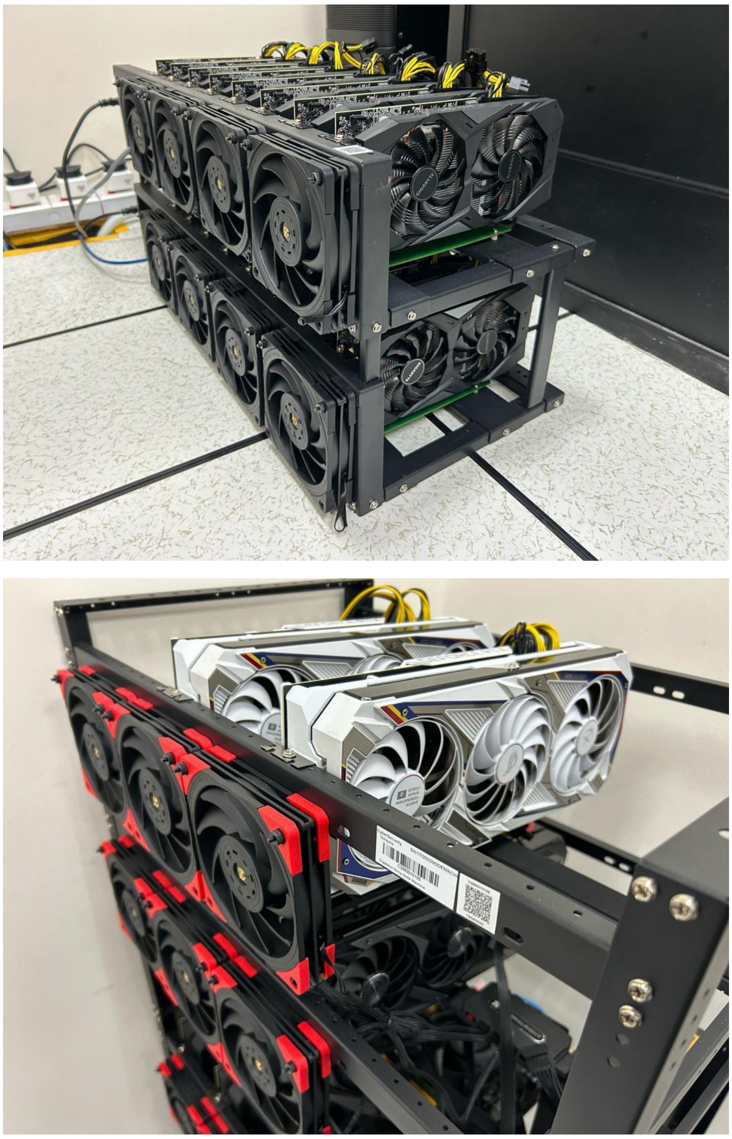
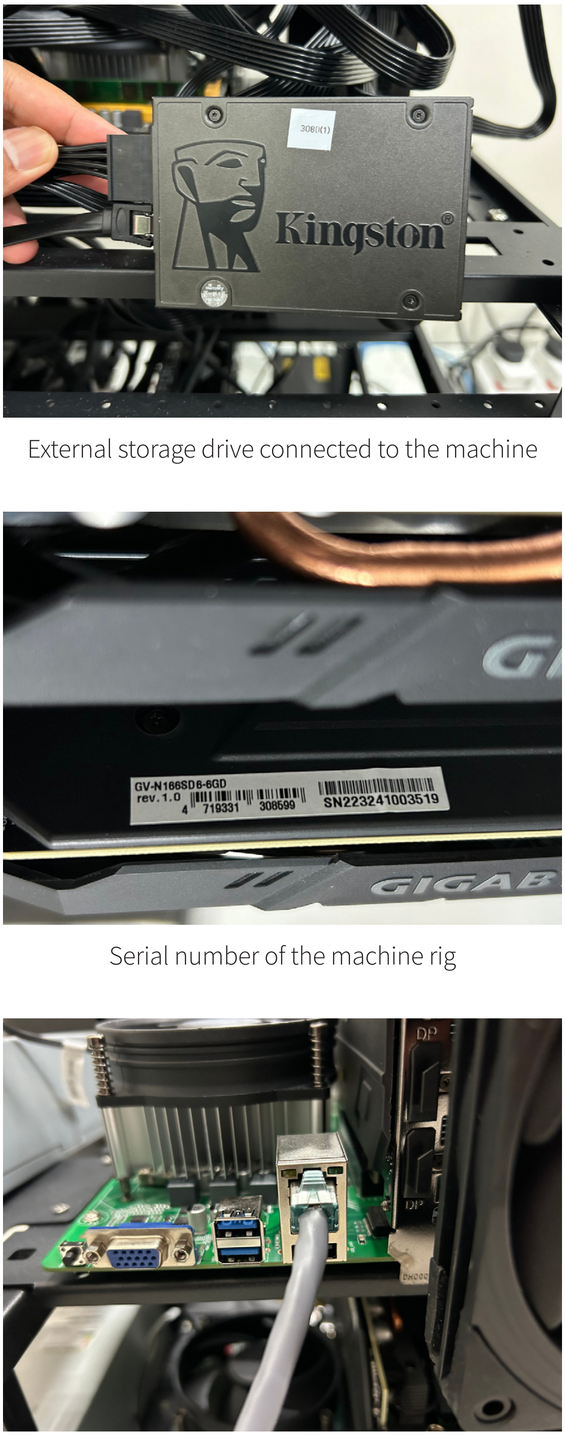


Figure 9. Overall view of GPU mining machines



External storage drive connected to the machine

Serial number of the machine rig

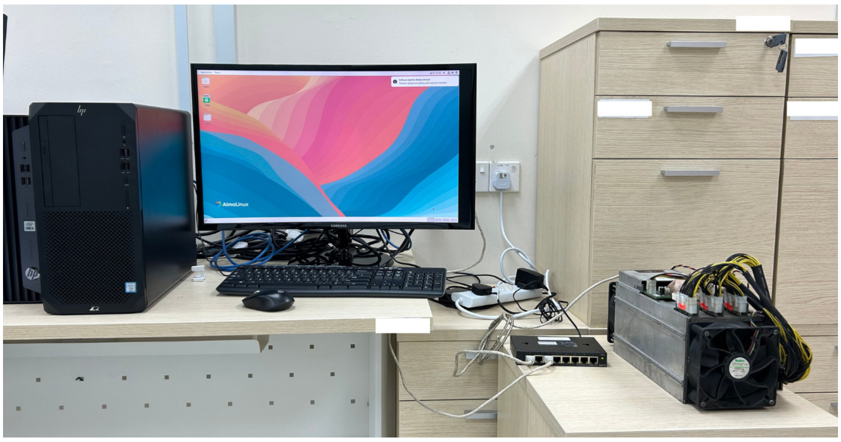
Ethernet cable connected to the machine

Figure 10. Close up view of GPU mining machines

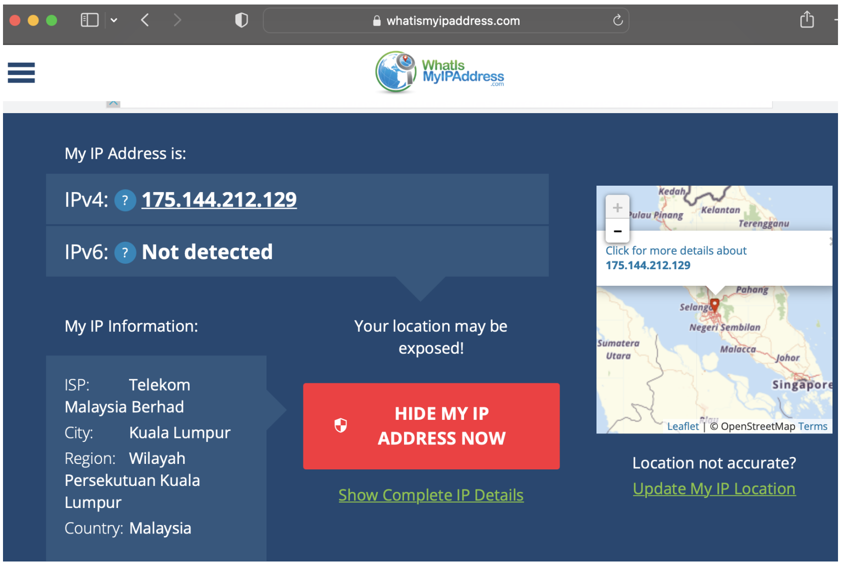
3. Obtain public IP address

Next, obtain the public IP address of the mining machines. The public IP address can be used to obtain the Internet subscriber's information from the telecommunication provider. To get the public IP address, investigator can follow these steps:

i. Connect the mining machine to the forensic workstation using Ethernet cable



ii. From the forensic workstation, open OSINT tool such as www.whatismyipaddress.com to obtain the public IP address



My IP Address is:

IPv4: ? 175.144.212.129

IPv6: ? Not detected

My IP Information:

ISP: Telekom Malaysia Berhad

City: Kuala Lumpur

Region: Wilayah Persekutuan Kuala Lumpur

Country: Malaysia

Your location may be exposed!

Click for more details about 175.144.212.129

Location not accurate?

iii. Screenshot or save the page into the case folder.

Then determine if the machine is a GPU/CPU or an ASIC/FPGA machine. The next step will depend on the type of machine.

3 (A). GPU / CPU machines

If GPU or CPU machines are discovered, then shut the machines down by turning off the power supply. Then pull out the attached storage drive, usually a USB flash drive or USB SSD disc.

Connect the storage drive to the forensic workstation. Before connecting, ensure that the USB port on the workstation is configured to write-block. This can be achieved by using write block hardware or by configuring the setting on the forensic workstation.

If you choose to configure the setting on Windows machine, you may refer to this URL: https://www.minitool.com/news/enable-write-protection-on-usb.html

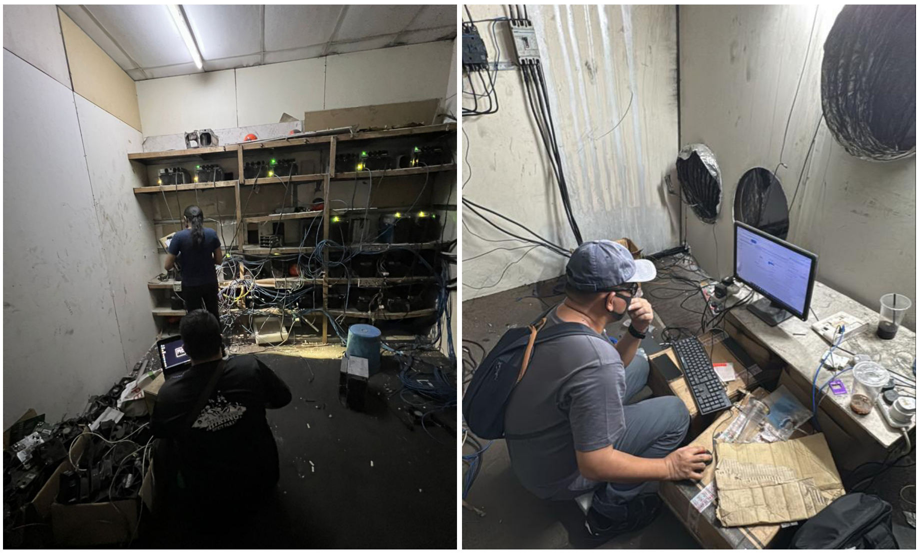
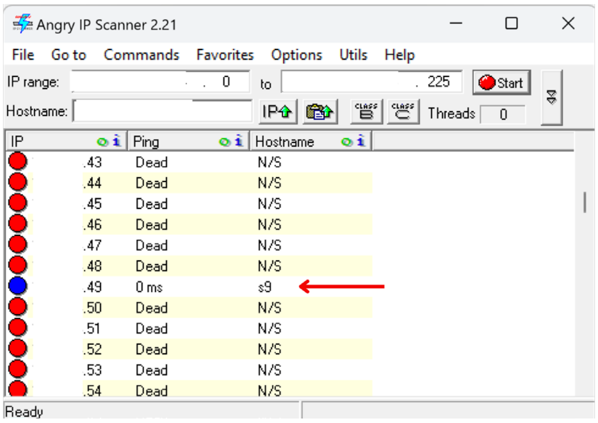


Figure 11. Processing mining machines at crime scene

3 (B). ASIC / FPGA machines

Processing ASIC or FPGA machines are a bit tricky because the investigator needs to get the private IP address to access the pool client. Investigators can use default private IP addresses such as 192.168.1.0 or 192.168.1.1. If this is unsuccessful, then investigators can interview mining operators or use IP scanner tools to scan the addresses. Example of a free IP scanner tool is Angry IP Scanner, which can be downloaded here: https://angryip.org/ .



IP range: . 0 to . 225

Threads 0

IP	Ping	Hostname
🔴 .43	Dead	N/S
🔴 .44	Dead	N/S
🔴 .45	Dead	N/S
🔴 .46	Dead	N/S
🔴 .47	Dead	N/S
🔴 .48	Dead	N/S
🔵 .49	0 ms	s9
🔴 .50	Dead	N/S
🔴 .51	Dead	N/S
🔴 .52	Dead	N/S
🔴 .53	Dead	N/S
🔴 .54	Dead	N/S

Ready

Figure 12. Screenshot of IP scanning tool. The blue button indicates the machine is currently active and is connected to the pool server.

Connect the mining machines to a forensic workstation using ethernet cable. If the machines are connected to a switch, then use the switch to connect to the forensic workstation by using Ethernet cable.

Open the web browser from the workstation and enter the private IP address. Now the pool client will be displayed on screen. If it has a login page, request for username and password from the mining machine operator. Upon successful login, investigators will be able to see the dashboard used by the mining pool operator to manage all the mining machines.

4. Search for important information

Search for important information from the storage drive (for GPU and CPU) and pool client (for ASIC and FPGA) that can discover the ownership of the machines. Searching can be done by using a forensic tool or by manually accessing the drive and triage for important information.
These are some of the information that can be found from the machines, as follows :

- Crypto wallet addresses. This information is important to trace the owner of the mining profit
- Pool server name, machine unique account ID, cryptocurrency type. This information can be used by investigators to get owner information by contacting the pool server
- IP address (public and private), MAC address, network SSID name, network SSID password. This information can be used by investigators to get information of the Internet ownership by contacting telecommunication provider

5. Document information

All the information extracted from the mining machines need to be properly documented in a form or in the investigator’s case work note. Photographs can also be used as a method to document this information.

At the end of this process, seize all the mining machines. Register them in the evidence seizure list, uniquely label them, package and seal them properly. Finally submit the evidence to the digital forensic laboratory for further analysis.

3.2 Processing and Collecting Data from Mining Pool

Cryptominers typically join a mining pool by creating an account and login into this account. This account is a cloud-based account, where users can login from any device. Mining pool dashboard provides a wealth of information, such as wallet address, user profile, phone number and email address.

Investigators will need to interview suspects to obtain information about the mining pool provider that mining machines are connecting to. Request suspect cooperation to access the pool account. Next, obtain the following information from the pool account:

- Crypto wallet addresses - to trace the owner of the mining profit
- Pool server name, machine unique account ID, farm address, cryptocurrency type - to get owner information by contacting the pool server
- IP address(public and private), MAC address, network SSID name, network SSID password - to get information of the Internet ownership by contacting telecommunication provider
- User profile (emails, phone numbers, name, home address) - to get owner information
- Pool client billing information (wallet address, transaction history) - to get owner details by conducting tracing on the wallet address and transaction history

The information obtained can be used to reveal the owner and the counterparty of the mining operation. Refer to best practices on collecting data displayed on screen.

At the end of this process, seize suspect devices that are used to access the pool, as it may contain more information of the mining operation, such as instant messaging communication and online transactions. This can be a computer or a mobile phone. Register them in the evidence seizure list, uniquely label them, package and seal them properly. Finally submit the evidence to the digital forensic laboratory for further analysis.

3.3 Processing and Seizing Crypto Wallets

Discovered crypto wallets at the scene need to be processed accordingly. If a suspect is using a hosted wallet, investigators can request for cooperation from the exchanger to suspend the account. If the exchanger does not cooperate or the location of the exchanger is unknown, then the investigator needs to preserve the proceeds of crime (the cryptocurrency) by transferring it into the Government Controlled Wallet. If suspect is using a unhosted wallet, proceed with transferring the cryptocurrency into the Government Controlled Wallet.

As this process requires very attentive steps, investigators are advised to make this process clear before proceeding to seizing the cryptocurrency. Please refer to the ***Malaysia Policy and Procedure for Seizing Cryptocurrency*** or the ***INTERPOL Guidelines for Seizing Virtual Assets*** for the steps in seizing the tainted cryptocurrency.

At the end of this process, seize all devices that contain crypto wallets application. Register them in the evidence seizure list, uniquely label them, package and seal them properly. Finally submit the evidence to the digital forensic laboratory for further analysis.

3.4 Processing and Seizing Other Types of Evidence

Digital devices discovered onsite need to be processed as well. Examples are computers, mobile phones, CCTV, hardware wallets, USB drives and tablets, among others. These may contain information that can support the investigation. An email address discovered in a mobile phone may be the same email address that is used to register for mining pool account. This may lead to the discovery of the owner for the mining machines. Therefore these digital devices need to be processed as well.

To do so, please refer to current best practices for seizing digital evidence, such as the UNODC Digital Evidence Best Practice Guides. At the end of the process, ensure that each evidence is properly documented on the evidence seizure list. Finally submit the evidence to the digital forensic laboratory for further analysis. Ensure that the chain of custody is documented properly.

3.5 Summary

In an ideal situation, investigators would be able to get evidence from three (3) components of the crypto mining; (1) mining machine, (2) mining pool and (3) crypto wallets. However it is worth highlighting that this is not always the case, as criminals may use anti-forensic technology to obscure their trails, such as encryption and remote wiping.

The following table shows data that can be extracted on each component of crypto mining that may assist investigation and prosecution of stealing of electricity.

Mining machine	Mining pool	Crypto wallet
• Pool server address • Public IP address • Private IP address • Network SSID • Network SSID password • Coin type • MAC address	• Wallet address • Machine details • Machine usage details • User profile • Multi-factor authentication details (mobile phone number, authenticator, email) • Machine private IP address • Billing wallet address	• User profile • Types of coin • Total coin • Transaction details

Table 5. List of data to be documented related to the crypto mining activity

In some cases, cryptominers take their operations very seriously and implement strict physical security measures to protect their setup. These may include reinforced doors, surveillance systems such as CCTV, and even hiring security guards to monitor the premises around the clock. Such measures are often intended to prevent theft of expensive mining equipment, avoid detection, and deter law enforcement or unauthorized entry. Investigators should be prepared to encounter well-secured locations and coordinate with relevant authorities to ensure proper procedures are followed during entry, evidence collection, and equipment seizure.

4. REPORTING THE SEARCH AND SEIZURE

At the end of the digital evidence seizure, the investigator will need to create a brief report of the activities conducted onsite. Now that digital evidence has been collected at the crime scene, investigators need to put the summary of the detailed activities in the form of a report. The goal of the reporting process is to present a clear, accurate, and comprehensive account of the investigation, ensuring that the results are understandable and usable by the prosecutors of the case or the higher management.

Report is written by the investigator that handles the digital evidence. Table 6 shows the recommended list of details to be documented in the report for the crypto mining onsite investigation.

- Mining machine information (as seen on the physical machine)
- Brand, model, manufacturer, serial number, whether it is connected to power supply and Internet
- Internet connection
- Types of connection (WIFI, Ethernet cable, mobile hotspot, etc), public IP address, MAC address, telecommunication provider, network SSID name
- Crypto wallet addresses
- Address where the rewards go into, as well as address for the pool server billing fee
- Mining Pool information
- Pool server name, the mined cryptocurrency type, MAC address, user profile (Email address, phone number, username, social media username, etc)
- Network device information (Switch and router)
- Public IP address, MAC address, Internet Service Provider, IP address and MAC address devices connected to the router, serial number, brand and model
- Other digital device information (Computer, mobile phone, CCTV) *discovered at crime scene

Table 6. Checklist of details to be documented related to the crypto mining search and seizure

The chain of custody of the seized evidence must also be documented. Investigators may use the current agency's chain of custody form to document the list of all the officers in charge of the evidence.

Now that the digital evidence has been collected, it needs to be analyzed in order to extract deleted data, recover any hidden data and reconstruct all the data into meaningful facts. Following the Reporting process, investigators then submit the digital evidence to the digital forensics laboratory for the purpose of analysis.

5. SUBMISSION OF EVIDENCE TO FORENSIC LABORATORY

Digital evidence that needs forensic analysis can be submitted to a digital forensic laboratory. The purpose of sending the digital evidence to the forensic laboratory is for data recovery, data reconstruction, analysis and correlation.

The following items need to be supplied to the laboratory when requesting for digital evidence analysis:

a. Case objective - clear scoping for the analysis
b. Triage information - data that has been collected at the crime scene
c. The digital evidence - mining machines, cables and power supply

When submitting the digital evidence to the forensic lab, clear case objectives need to be supplied to the forensic laboratory. Examples of case objectives are as following:

- To verify that the submitted devices can be used for crypto mining activities
- To verify that the submitted devices have been used for crypto mining activities
- To extract information from the machine such as cryptocurrency address, MAC address, public and private IP address, network SSID and other important information.
- To conduct cryptotracing on these addresses to get insights of suspect's operation
- To confirm that these addresses are linked to cryptomining activities

At the end of the analysis process, the laboratory will produce a forensic report. This report can be submitted to the prosecutor for case review. It can also be tendered into the court to support the case investigation.

6. RISK CONSIDERATION AND MITIGATION

When conducting a seizure on crypto mining machines, it is crucial that the machines are still running when investigators enter the premises. A lot of data that can unravel the ownership of the mining machines can be extracted when the machines are running. However this is very challenging since the machines can be turned off remotely. Hence on-site investigation strategies need to be brainstormed and properly planned with the investigation team.

In modern cryptomining operations, especially those conducted covertly or illegally, it is increasingly common for operators to employ advanced surveillance systems, such as CCTV cameras that can be accessed and controlled remotely via the internet. These systems allow the operators—or their accomplices—to monitor the premises in real time from any location.

One significant risk arises when CCTV operators detect the presence of law enforcement or investigation teams approaching the site. Upon noticing suspicious activity or uniformed officers, they can immediately respond by shutting down mining machines remotely, wiping digital logs, or disconnecting systems to prevent evidence collection. In some cases, they may even alert individuals inside or nearby to hide or flee, further complicating the investigation. This risk can be potentially mitigated by employing a thorough and discreet on-site investigation strategy such as covert surveillance before entry.

Human factors pose significant risks in any investigation. Errors can occur due to oversight, lack of training, fatigue, or misunderstanding of procedures. More seriously, misconduct—such as intentional tampering with evidence, unauthorized access, or leaking information—can compromise the integrity of the investigation. Bias, whether conscious or unconscious, may also influence how evidence is collected, interpreted, or reported, leading to inaccurate conclusions or unfair targeting of suspects.

These issues not only weaken the credibility of the investigation but can also affect legal proceedings, potentially causing key evidence to be challenged or dismissed in court. Implement a buddy system by assigning a second investigator or officer to observe, verify, and co-sign critical actions during the evidence handling process. This adds a layer of accountability and helps catch mistakes early, reducing the risk of accidental or deliberate misconduct.

7. GETTING EXTERNAL ASSISTANCE

In terms of investigation channels, various agencies may be involved depending on the scope and nature of the cryptomining case. This typically includes the police or cybercrime investigation units, as well as technical regulatory bodies such as the Energy Commission for cases involving illegal electricity tapping or infrastructure tampering. Collaboration with these agencies is essential for conducting joint operations, executing search warrants, and verifying technical findings. In cross-border cases where illicit mining operations span multiple jurisdictions or involve foreign actors, assistance from INTERPOL may be sought to facilitate coordination and communication with international law enforcement agencies. INTERPOL can provide support in intelligence sharing, locating suspects, and coordinating simultaneous enforcement actions across borders.

For prosecution channels, formal legal cooperation mechanisms may be activated. This includes using the Mutual Legal Assistance (MLA) framework and, for regional matters, the ASEAN Mutual Legal Assistance Treaty (ASEAN MLA). These channels are essential for obtaining foreign evidence, witness statements, or suspect extradition in a legally admissible manner. Engagement with transnational and international crime units within the Attorney General's Chambers (AGC) and the Department of Justice (DOJ) can further support complex prosecutions involving multiple jurisdictions. These units specialize in handling cross-border legal issues, ensuring that investigative and prosecutorial efforts align with international law and due process.

When engaging commercial service providers—such as digital forensic firms, cloud service providers, or blockchain analytics companies—careful consideration must be given to their trustworthiness, credentials, and potential conflicts of interest. Due diligence should be conducted to ensure that their involvement does not compromise the investigation or violate data privacy laws. Confidentiality agreements should be established where necessary, and access to case-sensitive information should be limited strictly to relevant personnel. Maintaining the confidentiality, integrity, and chain of custody of the evidence is paramount throughout the engagement with any third-party providers.

8. SUMMARY

The increasing prevalence of cryptocurrency mining activities has led to a corresponding rise in criminal cases involving illicit mining operations. Recognizing the limitations of traditional forensic methods in handling the volatile and complex nature of cryptocurrencies, these guidelines have been developed to provide a standardized and effective framework for investigators and digital forensic analysts. The document addresses key challenges in preserving digital evidence specific to cryptomining environments, including live data capture, remote shutdown risks, and identification of ownership. By following these guidelines, investigators can enhance the reliability of their findings, support successful prosecutions, and contribute to the growing body of knowledge in the field of cryptocurrency-related forensics.

REFERENCE

1. ‘What is a Mining Pool?’. Investopia.com. Viewed on 26th Mar 2024,https://www.investopedia.com/terms/m/mining-pool.asp
2. Digital Evidence Guides. UNODC. 2023.
3. M.Rometi et al. ‘A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares’. https://arxiv.org/abs/1905.05999. Viewed 26th Mar 2024.
4. Nate Drake and Jonas P. DeMuro. ‘Best crypto mining pools’. https://www.techradar.com/best/mining-pools. Viewed 26th Mar 2024.
5. Li Yan Kang et al. ‘Research on monitoring technology of power stealing behavior in bitcoin mining based on analyzing electric energy data. Energy Reports. Elsevier. 2022.
6. Sarah Taylor et. al. ‘A comprehensive forensic preservation methodology for crypto wallets’.
7. Forensic Science International: Digital Investigation. Volumes 42–43, 2022. ISSN 2666-2817. https://doi.org/10.1016/j.fsidi.2022.301477 .
8. INTERPOL Guidelines for Seizing Virtual Assets. 2023
9. Malaysia Policy and Procedure for Seizing Cryptocurrencies. 2022. https://www.cybersecurity.my/en/knowledge_banks/principles_guidelines/main/detail/2339/index.html

CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999
Fax: +603 8008 7000
Email: enquiry@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
www.cybersecurity.my

@cybersecuritymy
CyberSecurityMalaysia
cybersecurity_malaysia
CyberSecurityMy

MINISTRY OF DIGITAL