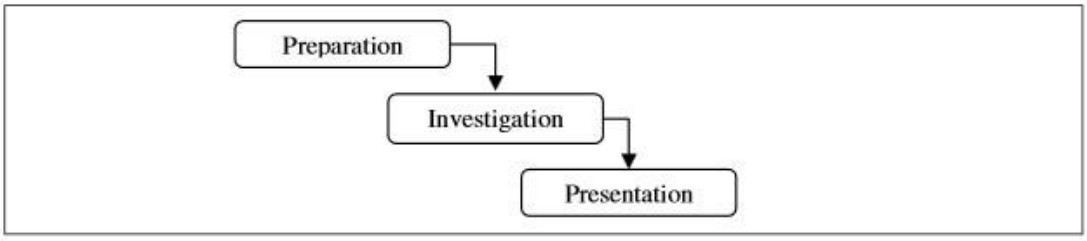
BAB III

METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah *Framework for a Digital Forensic Investigation* (FDFI), metode FDFI membantu mendapatkan bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan.



Gambar 3.1: Merupakan alur dalam melakukan penelitian menggunakan metodologi *Framework for a Digital Forensic Investigation* (FDFI)**.** M. Kohn, J. H. P. Eloff, & M. S. Olivier, (2006)

3.1 *Preparation*

Preparation dilakukan untuk melakukan penentuan kebutuhan yang diperlukan pada penyelidikan dan pencarian bukti. Tahapan ini mengidentifikasi dari halaman *cloud mining* yang mencurigakan disebut dengan *scam*(penipuan). Tahap *preparation* ini juga melakukan identifikasi tentang cara kerja *cloud mining*.

Tahap identifikasi dapat dilanjutkan pada tahap pemeliharaan sesuai dengan kerangka kerja pada metodologi FDFI.

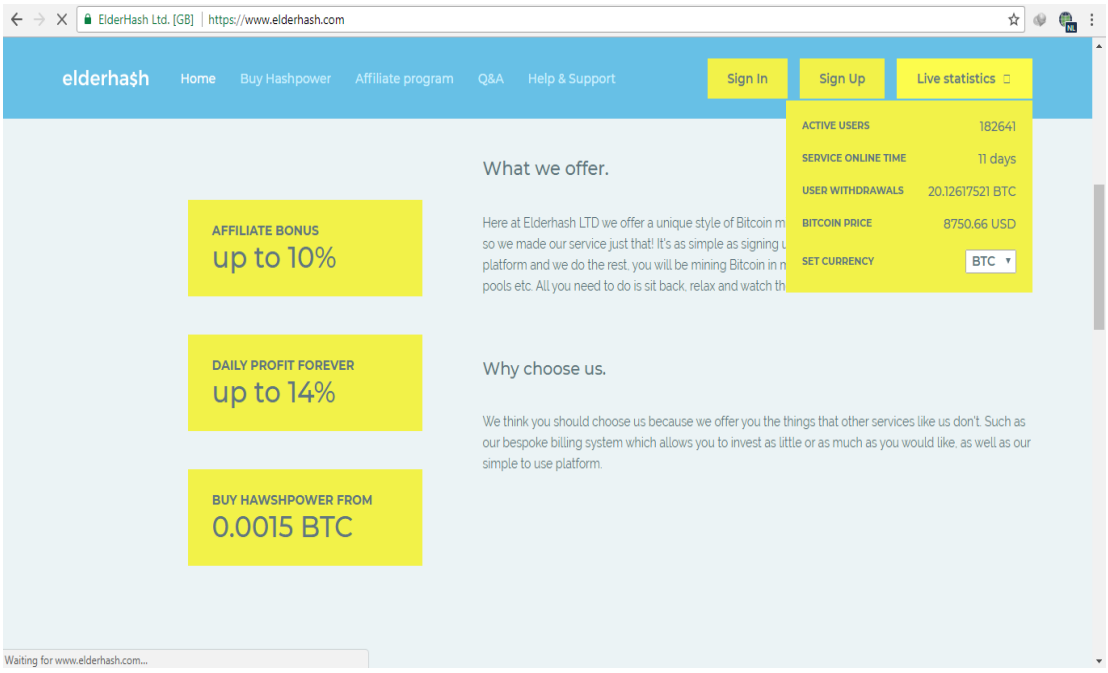
Tahap1: *Preperation* investigasi mencakup hal berikut:

a. Pemberitahuan kepada otoritas yang benar
b. Dokumentasi insiden sebelumnya
c. Perencanaan

Beberapa laporan kasus tentang *cloud mining scammer* pada bebepa situs situs yang dikumpulkan :

a. Well, a few days later, the site was gone! Only the cloudflare proxy at the front remained, and all my LTC were taken“(steemit.com)
b. *Cloud mining* is a scam. If you you had a machine that could literally print money(like a bitcoin ASIC miner)(reddit.com)
c. Reluctantly have to agree that at least at the moment I would have been better off just buying and holding Bitcoin, but **cloud mining** seemed like a good thing at the time. I invested $2500 USD maybe 4 months ago and I doubt I've broken even yet(reddit.com).

Berikut tampilan website cloud mining yang dicurigai sebagai scammer :



Gambar 3.2: Merupakan tampilan halaman awal *cloud mining* yang di curigai *scam*(penipu).

Merujuk dari gambar 3.2 bahwa *website cloud mining* yang di curigai *scammer* biasanya menawarkan penawaran menarik seperti program *referral*, *daily profit* perhari dan *website* baru berjalan beberapa hari.

Cara kerja dari *website cloud mining scammer* biasa nya meminta seseorang untuk deposit berupa bitcoin untuk membeli *speed* atau *hash* dengan harga yang murah dan menjamin dalam beberapa hari modal kembali.

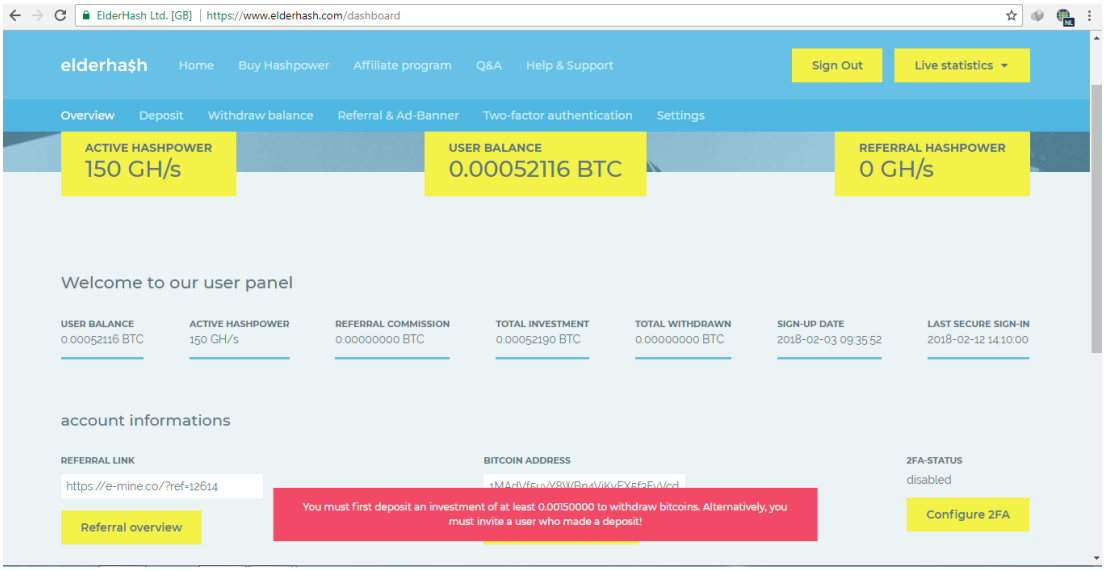
3.2 *Investigation*

Mencari dan menindifikasi bukti dari yang menunjukan *website cloud mining* yang mencurigakan scam (penipuan), membuktikan kebenaran dan kesalahan sebuah fakta yang kemudian menyajikan kesimpulan atas rangkaian temuan dan susunan kejadian.

Tahap2: *Investigation* mencakup sebagai berikut :

a. Mencari dan mengidentifikasi bukti pada komputer .
b. Koleksi bukti dari komputer (*original* diduplikasi).
c. Menyimpan bukti di tempat yang aman .
d. Penyimpanan bukti yang dikumpulkan di tempat kejadian.
e. Pemeriksaan bukti dengan menggunakan alat yang tepat.
f. Analisis (terlihat pada proses pemeriksaan untuk menentukan signifikansi dan nilai dari bukti yang ditemukan) .

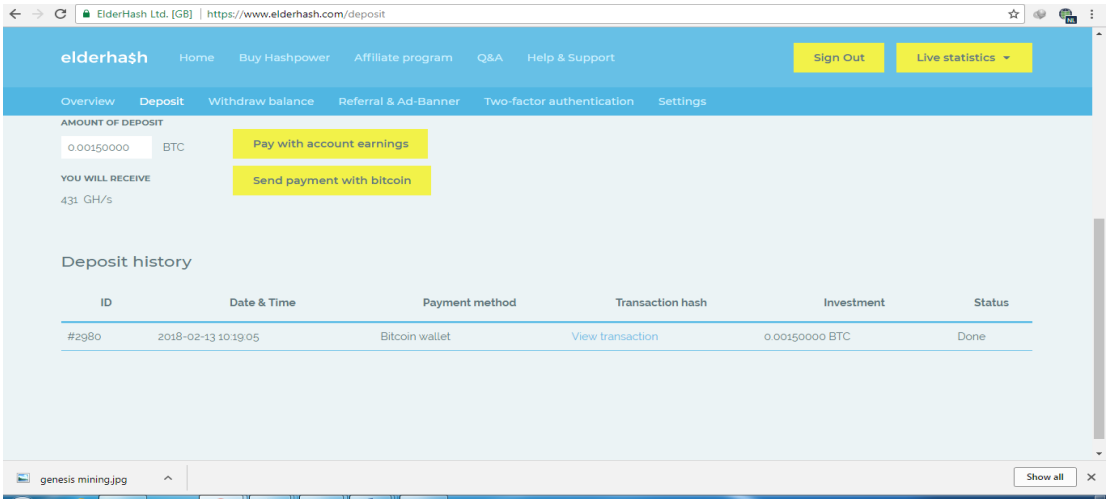
Investigasi dilakakukan dengan mengambil contoh dari penyedia layanan jasa *cloud mining* elderhash.com. Elderhash dicurigai sebagai penyedia layanan jasa *cloud mining scammer*(penipu).



Gambar 3.3: Merupakan tampilan halaman *cloud mining* setelah *log in*.

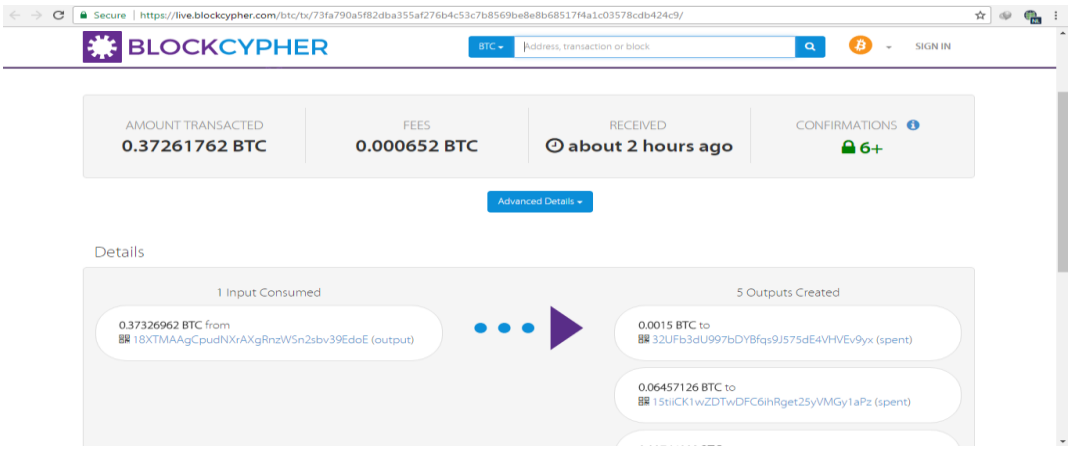
Merujuk dari gambar 3.3 menyatakan untuk deposit sejumlah bitcoin agar bisa *withdraw* bitcoin yang sudah di tambang

Cara kerja pengiriman bitcoin dengan melakukan deposit dari *wallet* bitcoin yang sudah di enkripsi, bitcoin di bagi menjadi beberapa enkripsi, kemudian dari enkripsi tersebut akan menjadi sebuah *block chain* yang belum tersegel, proses penyegelan nya tergantung berapa *block chain* yang menyelesaikan enkripsi tersebut, jika semua *block chain* sudah selasai mengenkrpsi bitcoin tersebut maka *block* yang tadi belum tersegel sudah menjadi tersegel dan penerima akan menerima transkasi tersebut. Transaksi pasti ada *fee* (biaya) yang di butuhkan untuk mengenkripsi bitcoin tersebut.



Gambar 3.4: bukti melakukan deposit di penyedia jasa layanan *cloud mining* elderhash.com

Gambar 3.4 merupakan bukti sudah melakukan deposit dan sudah di *accept* oleh *admin* elderhash tersebut. Kecepatan ghs juga sudah bertambah dari 150ghs menjadi 581ghs.



Gambar 3.5: bukti transaksi bitcoin ke *website cloud mining* elderhash.com

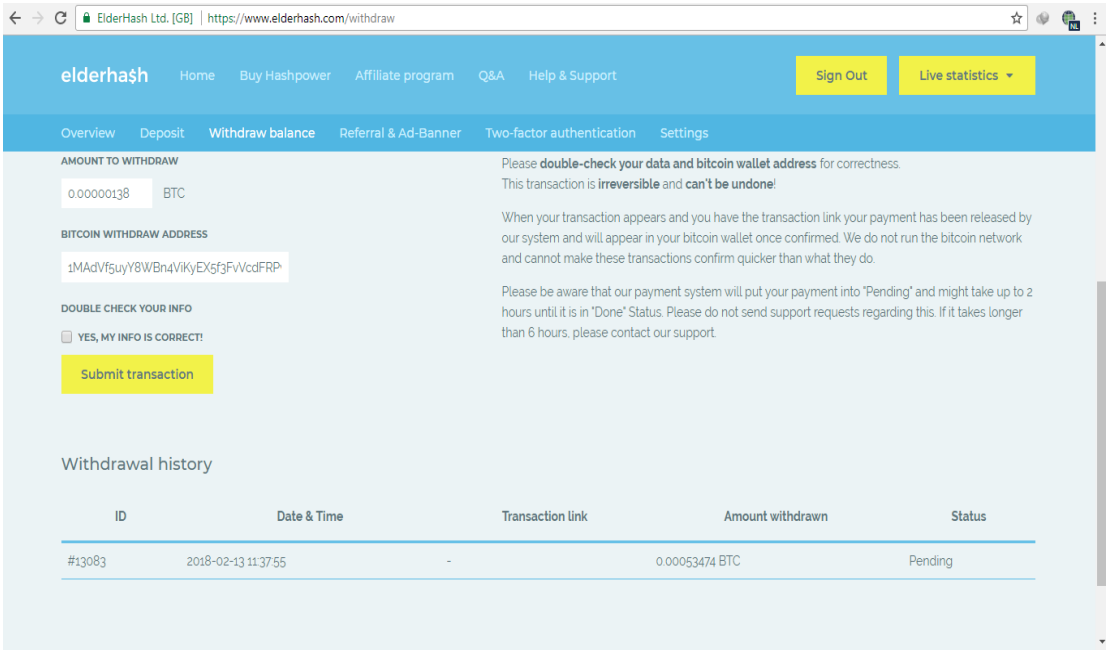
3.3 *Persentation*

Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahapananalisis.

Tahap3: akhir dari penyelidikan forensik mencakup tahap Presentation . Tahap ini penting karena memenuhi persyaratan utama yang ditentukan oleh definisi kata ' forensik ' . Tahap ini akan mencakup langkah-langkah penting berikut :

a. Presentase analisis dan
b. Pembuktian analisis.

pada tahap Presentasi, Investigasi harus membuktikan hipotesis yang dicapai selama penyelidikan .



Gambar 3.6: status *withdraw* bitcoin setelah melakukan deposit

Merujuk dari gambar 3.6 tidak dicantumkan transaksi *link*, seharusnya transaksi *link* tersedia. Berbeda dengan *cloud mining* yang tidak *scam*, di halaman *cloud mining* yang terpercaya disediakan transkasi *link block chain*.

Berikut list dari whois perbedaan antara *cloud mining scammer* dan terpercaya.

Tabel 3.1 : table perbandingan dari whois antara nicehash dan elderhash

Cloud mining scammer (elderhash)	Cloud minng terpercaya (nicehash)
RAW WHOIS DATA Domain name: elderhash.com Registry Domain ID: 2215599157_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 2018-01- 20T15:42:50.00Z Creation Date: 2018-01- 20T15:37:45.00Z	RAW WHOIS DATA Domain Name: NICEHASH.COM Registrar URL: http://www.godaddy.com Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Name Server: EDNA.NS.CLOUDFLARE.COM Name Server: JACK.NS.CLOUDFLARE.COM DNSSEC: signedDelegation

Lanjutan dari tabel 3.1

Registrar Registration Expiration Date: 2019-01-20T15:37:45.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: email@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: Registrant Name: Robert Grant Registrant Organization: ElderHash Ltd.	For complete domain details go to: http://who.godaddy.com/whoischeck.aspx?domain=NICEHASH.COM The data contained in GoDaddy.com, LLC's WhoIs database, while believed by the company to be reliable, is provided "as is" with no guarantee or warranties regarding its accuracy. This information is provided for the sole purpose of assisting you in obtaining information about domain name registration records. Any use of this data for any other purpose is expressly forbidden without the prior written permission of GoDaddy.com, LLC. By submitting an inquiry,

Lanjutan dari tabel 3.1

Registrant Street: 50 Broadway Registrant City: Westminster Registrant State/Province: London Registrant Postal Code: SW1H 0BL Registrant Country: GB Registrant Phone: +44.448927592 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: email@elderhash.com Registry Admin ID: Admin Name: Robert Grant Admin Organization: ElderHash Ltd. Admin Street: 50 Broadway Admin City: Westminster Admin State/Province: London Admin Postal Code: SW1H 0BL Admin Country: GB Admin Phone: +44.448927592	you agree to these terms of usage and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise make possible, dissemination or collection of this data, in part or in its entirety, for any purpose, such as the transmission of unsolicited advertising and and solicitations of any kind, including spam. You further agree not to use this data to enable high volume, automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes. Please note: the registrant of the domain name is specified

Lanjutan dari tabel 3.1

Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: email@elderhash.com Registry Tech ID: Tech Name: Robert Grant Tech Organization: ElderHash Ltd. Tech Street: 50 Broadway Tech City: Westminster Tech State/Province: London Tech Postal Code: SW1H 0BL Tech Country: GB Tech Phone: +44.448927592 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: email@elderhash.com Name Server: andy.ns.cloudflare.com Name Server: ruth.ns.cloudflare.com	in the "registrant" section. In most cases, GoDaddy.com, LLC is not the registrant of domain names listed in this database. Note: WHOIS consumers who are now receiving masked data can find instructions on how to apply for whitelisting here: https://www.godaddy.com/help/masking-contact-information-shared-via-whois-automated-access-points-27421

Lanjutan dari tabel 3.1

DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2018-02-11T22:27:17.53Z <<< For more information on Whois status codes, please visit https://icann.org/epp	

Merujuk tabel 3.1 mempelihatkan hasil yang didapat dari halaman *website* whois dari mulai alamat kedua halaman penyedia layanan jasa *cloud mining* tersebut. Perbedaan yang di dapat nicehash lebih jelas dan terperinci, sedangkan dari elderhash kebalikannya.